

IBM SPSS Statistics Server Administratorhandbuch



Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen“ auf Seite 61 gelesen werden.

Produktinformation

Diese Ausgabe bezieht sich auf Version 29, Release 0, Modifikation 1 von IBM® SPSS Statistics Server und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

© **Copyright International Business Machines Corporation .**

Inhaltsverzeichnis

| | |
|--|-----------|
| Kapitel 1. Übersicht..... | 1 |
| Produkte und Betriebssysteme..... | 1 |
| Architektur..... | 1 |
| Softwarekomponenten..... | 3 |
| Verteilten Modus verwenden..... | 4 |
| Server-Software verwalten..... | 4 |
| Verwenden dieses Dokuments..... | 5 |
| Kapitel 2. Installation..... | 7 |
| Server-Software installieren..... | 7 |
| Clientanwendung installieren..... | 7 |
| Kapitel 3. Datenzugriff..... | 9 |
| Ansicht der Daten..... | 9 |
| Datenzugriffstechnologie..... | 9 |
| Connect ODBC..... | 9 |
| Auf Daten zugreifen..... | 10 |
| Referenzdaten..... | 10 |
| Datenzugriff steuern..... | 11 |
| Datenquellen..... | 11 |
| UNIX-Umgebung für Datenzugriff konfigurieren..... | 12 |
| Kapitel 4. Belegung und Wartung konfigurieren, überwachen..... | 15 |
| Endbenutzerkonten und Dateien verwalten..... | 15 |
| Konten..... | 15 |
| Datenzugriff..... | 15 |
| Dateien..... | 15 |
| Profile..... | 16 |
| ODBC -Datenquellen konfigurieren..... | 16 |
| ODBC -Datenquellen und IBM SPSS Data Access Pack..... | 16 |
| Sortierengine eines anderen Anbieters verwenden..... | 16 |
| IBM SPSS Statistics-Serveradministration..... | 17 |
| Xspannungen konfigurieren..... | 17 |
| Konfigurieren der Befehlszeilenschnittstelle des Produktionsmodus zur Übergabe von Jobs..... | 17 |
| Mehrere Instanzen konfigurieren..... | 19 |
| Servicestart steuern..... | 19 |
| Befehlszeilenparameter für Startscript..... | 20 |
| Sonstige Wartung..... | 21 |
| Server-Software starten und stoppen..... | 21 |
| Service oder Dämon starten..... | 21 |
| Service oder Dämon stoppen..... | 21 |
| Konfiguration zur Leistungsverbesserung..... | 22 |
| Kapitel 5. Unterstützende Endbenutzer..... | 23 |
| Authentifizierung (Authentication)..... | 23 |
| Authentifizierung auf Betriebssystemebene konfigurieren..... | 23 |
| Konfigurieren von PAM..... | 24 |
| Interne Authentifizierung konfigurieren..... | 24 |
| unix2 -authentifizierung Konfigurieren..... | 25 |
| Single Sign-on (SSO) konfigurieren..... | 26 |

| | |
|--|-----------|
| Berechtigungen..... | 31 |
| Berechtigungen auf Administratorebene..... | 31 |
| Gruppenberechtigung..... | 31 |
| Profile..... | 32 |
| Client-und Serverversionen..... | 32 |
| Benutzer über eine Firewall verbinden..... | 33 |
| Verbindungen über eine Firewall konfigurieren..... | 33 |
| Benutzer mit PPTP verbinden..... | 35 |
| Verwenden von SSL zur sicheren Datenübertragung..... | 35 |
| Funktionsweise von SSL..... | 36 |
| Aktivieren von SSL mit GSKit..... | 36 |
| Aktivieren von SSL mithilfe von OpenSSL | 40 |
| Ländereinstellung festlegen..... | 43 |
| Verbindung zur Server-Software herstellen..... | 45 |
| Zugriff auf Daten und Dateien..... | 45 |
| Daten und Dateien speichern..... | 45 |
| | |
| Kapitel 6. Leistung analysieren und verbessern..... | 47 |
| Leistungsinformationen abrufen..... | 47 |
| Plattenbelegung verbessern..... | 48 |
| Verbessern der CPU-Belastung..... | 49 |
| Speicherbelegung verbessern..... | 49 |
| Netzauslastung verbessern..... | 49 |
| IBM SPSS Statistics Effizient Verwenden..... | 50 |
| | |
| Anhang A. Fehlerbehebung..... | 51 |
| Server-Software..... | 51 |
| Client-Software..... | 51 |
| | |
| Anhang B. IBM SPSS Statistics Batch Facility..... | 53 |
| Was Sie wissen müssen..... | 53 |
| | |
| Anhang C. Tasks für das Betriebssystem Windows..... | 55 |
| Dateieigenschaften..... | 55 |
| Systemeigenschaften..... | 55 |
| Benutzermanager..... | 56 |
| Systemsteuerung für Services..... | 56 |
| Task-Manager..... | 56 |
| ODBC -Administrator..... | 56 |
| So konfigurieren Sie einen System-DSN..... | 57 |
| So konfigurieren Sie einen Benutzer-DSN..... | 57 |
| | |
| Anhang D. UNIX-Betriebssystemtasks..... | 59 |
| Chmod..... | 59 |
| Umschlag..... | 59 |
| Scripts..... | 59 |
| ps und kill..... | 60 |
| odbc.ini..... | 60 |
| | |
| Bemerkungen..... | 61 |
| Marken..... | 62 |
| | |
| Index..... | 65 |

Kapitel 1. Übersicht

Die IBM SPSS Statistics -Servertechnologie ist eine **verteilte Architektur** und unterstützt zusammen mit Optimierungen für das Schlüsseldatenmanagement skalierbare Analysen. Die Technologie basiert auf Client/Server. Er verteilt Clientanforderungen für ressourcenintensive Operationen an leistungsfähige Server-Software. Wenn Client und Server so zusammenarbeiten, wird dies als **Modus für verteilte Analysen** bezeichnet. Mit der verteilten Analyse können Endbenutzer Analysen durchführen, die ihre Desktop-Computer nicht unterstützen.

Für maximale Flexibilität können Clientanwendungen, die die Servertechnologie verwenden, auch so konfiguriert werden, dass sie ausschließlich auf dem Desktop-Computer des Endbenutzers ausgeführt werden. Dies wird als **lokaler Analysemodus** bezeichnet. Endbenutzer können einfach zwischen den Modi wechseln.

Produkte und Betriebssysteme

Die Servertechnologie unterstützt die IBM SPSS Statistics -Clientanwendung und die Server-Software wird unter verschiedenen Betriebssystemen ausgeführt (Einzelheiten finden Sie in den Installationsanweisungen). Sie können mehrere Versionen der Server-Software an Ihrem Standort, auf demselben Server-Computer oder auf verschiedenen Server-Computern installieren.

Architektur

Die Server-Software verfügt über eine zweischichtige verteilte Architektur. Es verteilt Softwareoperationen zwischen dem Client und den Server-Computern. Speicherintensive Operationen, wie beispielsweise der Zugriff auf eine große Datenbank oder die Analyse einer großen Datendatei, werden auf dem Server-Computer ausgeführt, ohne die Daten auf den Client-Computer herunterzuladen.

Clientschicht

Die **Clientanwendung**. Sie wird auf dem Desktop-Computer des Endbenutzers installiert und ausgeführt. Die Clientanwendung stellt die grafische Benutzerschnittstelle für Datenzugriff und Analyse bereit. Es stellt die Ergebnisse der Analysen des Endbenutzers dar.

Serverschicht

Die **Server**-Software. Sie wird auf einem vernetzten Server-Computer installiert und ausgeführt. Die Server-Software stellt das Framework bereit, das erforderlich ist, um mehrere Clients, die Algorithmen, die in der statistischen Analyse verwendet werden, und den Datenzugriff zu verarbeiten.

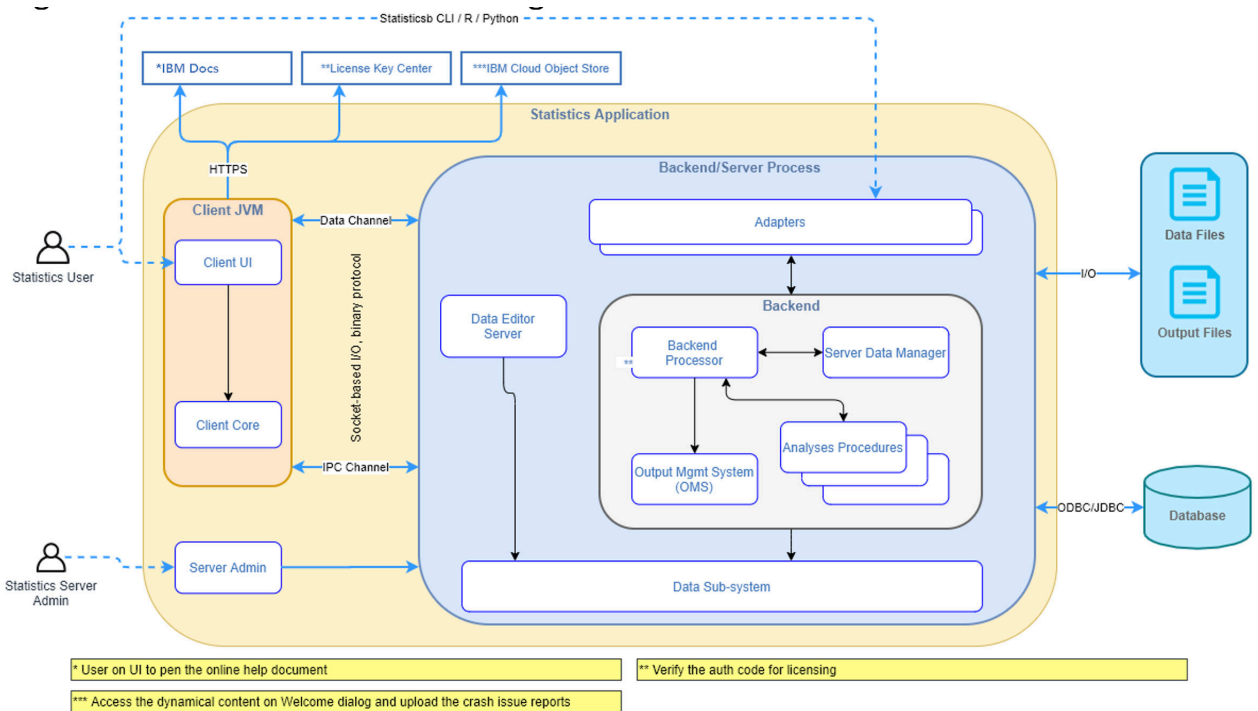
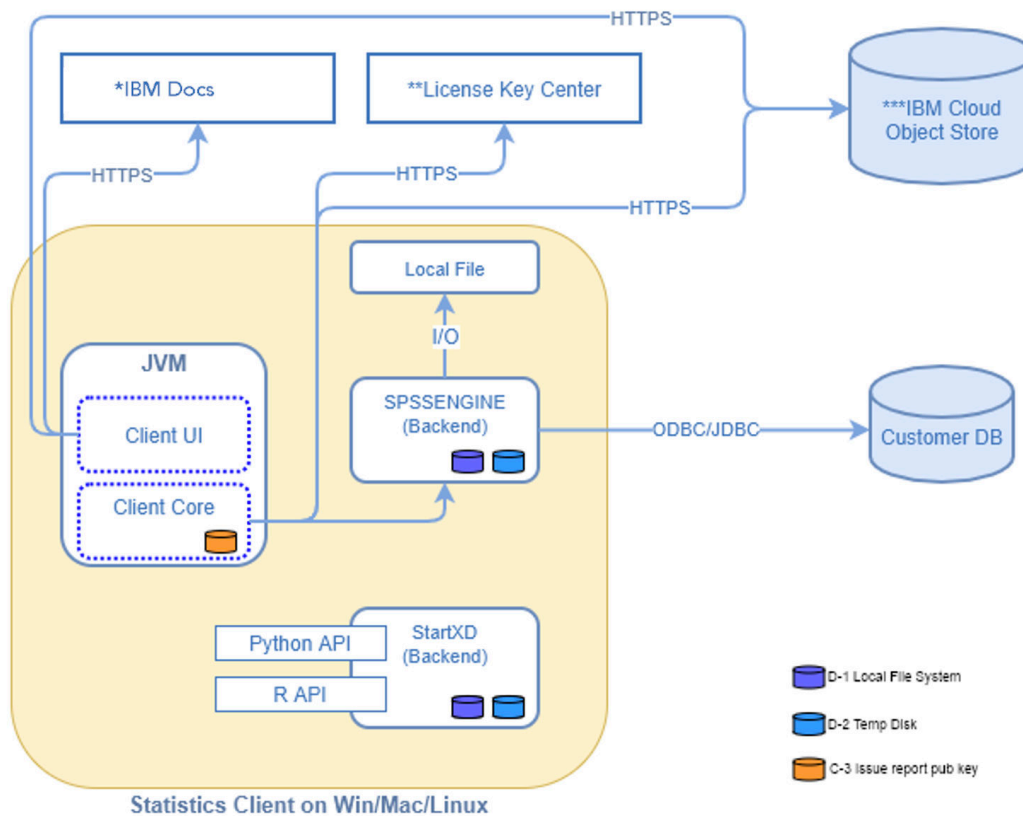


Abbildung 1. Modus für verteilte Analysen

Für Analysen, die keinen intensiven Datenzugriff oder keine numerische Verarbeitung erfordern, kann die Client-Software als eigenständige Standardanwendung verwendet werden. Im lokalen Analysemodus erfolgt der gesamte Datenzugriff und die statistische Verarbeitung auf dem Desktop-Computer des Endbenutzers.



* User on UI to pen the online help document

** Verify the auth code for licensing

*** Access the dynamical content on Welcome dialog and upload the crash issue reports

Abbildung 2. Lokaler Analysemodus

Softwarekomponenten

Wie in der Abbildung "Modus für verteilte Analyse" dargestellt, sind die Komponenten der Servertechnologie wie folgt. (Siehe Abbildung 1 auf Seite 2.)

Client-Software. Die Clientanwendung ist eine vollständige Installation des IBM Corp. -Produkts des Endbenutzers (z. B. IBM SPSS Statistics). Bei der Verwendung für verteilte Analysen werden nur die grafische Benutzerschnittstelle und die Bearbeitungsfunktionen verwendet. Wenn sie für die lokale Analyse verwendet wird, werden auch ihre Datenzugriffs- und Statistikverarbeitungsfunktionen verwendet.

Server-Software. Die Server-Software besteht aus Unterkomponenten: einem Framework, das die Client-/Serverkommunikation verwaltet, Clientprozessen, die Clientanforderungen verwalten, und Modulen, die auf Daten zugreifen und Analysen durchführen.

- **Framework** Das Framework der Server-Software ist ein Dienst (unter Windows) oder Dämon (unter UNIX). Er verarbeitet die gesamte Kommunikation zwischen der Clientanwendung und den Modulen. Das Framework wird kontinuierlich auf dem Server-Computer ausgeführt und wartet auf Clientverbindungen. Wenn ein Client eine Verbindung herstellt, startet das Framework einen Prozess, der Anforderungen für diesen Client verarbeitet.
- **Clientprozess.** Ein Clientprozess ist eine Sitzung für den Client. Für jeden Client gibt es einen Prozess. Ein Prozess wird gestartet, wenn der Client eine Verbindung herstellt, und er wird beendet, wenn der Client die Verbindung trennt. Der Prozess verwaltet die Anforderungen des Kunden für Daten und Analysen. Er lädt die Module, die für den Datenzugriff und die Datenanalyse erforderlich sind. Er entlädt Module, wenn sie nicht mehr benötigt werden.

- **Module.** Ein Modul ist eine ausführbare Datei, eine DLL oder eine gemeinsam genutzte Bibliothek, die auf Daten zugreift und Analyseprozeduren ausführt. Die Analysesoftware verfügt über mehrere Module. Module werden bei Bedarf geladen. Module können andere Module laden.

Verteilten Modus verwenden

Die folgenden Schritte treten auf, wenn ein Endbenutzer ein Produkt im Modus für verteilte Analysen ausführt:

1. **Starten Sie die Clientanwendung.** Der Endbenutzer startet die Client-Software auf seinem Desktop-Computer. Die Clientanwendung stellt eine vollständige Benutzerschnittstelle dar.
2. **Stellen Sie eine Verbindung zum Server her.** Der Endbenutzer stellt eine Verbindung zur Server-Software her, indem er sich über die Clientanwendung anmeldet. Der Service oder Dämon des Server-Frameworks ist immer aktiv und wartet auf Verbindungsanforderungen. Wenn eine Verbindung hergestellt wird, startet die Server-Software einen Prozess zum Handhaben des Endbenutzers.
3. **Auf Daten zugreifen.** Der Endbenutzer greift wie gewohnt über die Clientanwendung auf Daten zu, mit der Ausnahme, dass seine Sicht auf Datenbanktreiber, Datendateien, Verzeichnisse und Laufwerke den Computer des fernen Servers und nicht den Desktop-Computer darstellt. Der Serverprozess lädt die entsprechenden Datenzugriffsmodule und ruft die Daten ab. Ein kleines Segment der Daten wird an die Clientanwendung gesendet, damit der Endbenutzer bei der Auswahl einer Analyse darauf verweisen kann. Die meisten Daten verbleiben auf dem Server. Sie können die Server-Software auch konfigurieren, um zu verhindern, dass Daten an die Clientanwendung gesendet werden. Mit der Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird) können Sie verhindern, dass die Daten an alle Clients gesendet werden. Weitere Informationen finden Sie im Abschnitt "Benutzer" im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Sie können auch den Zugriff für jeden Benutzer oder jede Gruppe konfigurieren. Weitere Informationen finden Sie im Abschnitt IBM SPSS Statistics Server im *Deployment Manager Benutzerhandbuch*.
4. **Analysieren Sie die Daten.** Der Endbenutzer wählt über die Benutzerschnittstelle der Clientanwendung die Daten aus und fordert den gewünschten Analysetyp an. Die Anforderung wird an den Serverprozess gesendet, der die entsprechenden Datenanalysepakete lädt und die Analyse verarbeitet. Alle datenbezogenen Tasks wie das Lesen von Daten, das Transformieren von Daten, das Berechnen neuer Variablen und das Berechnen von Statistiken werden auf dem Server-Computer ausgeführt.
5. **Überprüfen Sie die Ergebnisse.** Die Server-Software sendet die Ausgabe der Clientanforderung zurück an die Clientanwendung. Nur die Ergebnisse werden gesendet, die Daten verbleiben auf dem Server. Der Endbenutzer kann dann die Clientanwendung verwenden, um die Ergebnisse zu optimieren und zu bearbeiten.

Server-Software verwalten

Dieses Handbuch richtet sich hauptsächlich an Systemadministratoren, die für die Integration der Server-Technologie in eine Netzumgebung verantwortlich sind, in der Clientanwendungen im Modus für verteilte Analysen ausgeführt werden. Zu den Verwaltungstasks gehören:

Installation. Die Server-Software ist so konzipiert, dass sie kontinuierlich ausgeführt wird und auf Anmeldungen und Anforderungen von Desktop-Computern für Endbenutzer reagiert. Wählen Sie einen geeigneten Server-Computer für die Server-Software aus - ein Computer mit geringer Ausfallzeit, der für den Endbenutzerzugriff konfiguriert ist und mit den entsprechenden Desktop-Computern vernetzt ist. Je mehr Speicher und Verarbeitungsleistung der Server-Computer hat, desto schneller werden Clientanforderungen verarbeitet. Die Clientanwendung muss auf den Desktop-Computern der Endbenutzer installiert sein. Die Clientinstallation kann von einer Netzadresse aus erfolgen. [Kapitel 2, „Installation“](#), auf Seite 7 bietet eine Übersicht über die Installation der Server-Software und der Clientanwendung. Ausführliche Installationsanweisungen finden Sie im Produkt DVD.

Datenzugriff. Wenn Sie Endbenutzern Zugriff auf Daten auf einem fernen Server erteilen müssen, während sie im verteilten Modus arbeiten, muss die Server-Software auf diese Daten zugreifen können. IBM Corp. -Produkte können über eine Vielzahl von Datendateitypen, einschließlich Datenbanken, auf Daten zugreifen. Um Ihren Job zu vereinfachen, werden IBM Corp. -Produkte mit DataDirect Connect ODBC

verteilt, um auf Daten aus einer Datenbank zuzugreifen. Kapitel 3, „Datenzugriff“, auf Seite 9 führt Datenzugriff für IBM Corp. -Produkte ein. Zusätzliche Dokumentation ist im Produkt DVD enthalten.

Konfiguration und Wartung. Da die Server-Software für einen kontinuierlichen Betrieb vorgesehen ist, sollte sie in regelmäßigen Abständen von einem Systemadministrator überwacht werden. Es gibt mehrere Konfigurationsoptionen, mit denen Sie die Funktionsweise der Server-Software steuern können. In Kapitel 4, „Belegung und Wartung konfigurieren, überwachen“, auf Seite 15 wird die Konfiguration und Überwachung der Server-Software erläutert.

Unterstützung von Endbenutzern. Endbenutzer benötigen Informationen zu Servernamen, Benutzeraccounts und zur Position von Daten. Möglicherweise müssen Sie sie auch bei der Lösung von Problemen unterstützen. In Kapitel 5, „Unterstützende Endbenutzer“, auf Seite 23 wird die Art der Unterstützung erläutert, die Endbenutzer benötigen.

Leistung. Kapitel 6, „Leistung analysieren und verbessern“, auf Seite 47 bietet Strategien zur Verbesserung der Leistung der Server-Software.

Fehlerbehebung. „Server-Software“ auf Seite 51 enthält Tipps zur Fehlerbehebung.

IBM SPSS Statistics Batch Facility (nur IBM SPSS Statistics Server). Das Produkt IBM SPSS Statistics Server enthält IBM SPSS Statistics Batch Facility für die automatisierte Erstellung von Statistikberichten. Wenn Sie IBM SPSS Statistics Server an Ihrem Standort ausführen, lesen Sie den Abschnitt Anhang B, „IBM SPSS Statistics Batch Facility“, auf Seite 53, in dem die IBM SPSS Statistics Batch Facility und die Tasks beschrieben werden, die Sie möglicherweise ausführen müssen, um sie zu unterstützen.

Verwenden dieses Dokuments

Dieses Handbuch richtet sich hauptsächlich an Systemadministratoren, die für die Installation und Wartung der Server-Software in einer Netzumgebung verantwortlich sind, in der Clientanwendungen im Modus für verteilte Analysen ausgeführt werden.

Kapitel 2. Installation

Produkte, die die Servertechnologie verwenden, sind auf mehreren Medien gepackt-ein DVD für die Server-Software und ein DVD für die Clientanwendung.

Gehen Sie wie folgt vor, um die Servertechnologie zu implementieren:

- Installieren Sie die Server-Software auf einem vernetzten Server-Computer.
- Installieren oder überwachen Sie die Installation der Clientanwendung so, dass sie über Desktop-Computer des Endbenutzers zugänglich ist.

Dieses Kapitel enthält eine Übersicht über den Installationsprozess. Ausführliche Installationsanweisungen finden Sie im Produkt DVD im Verzeichnis */Documentation/<language>/InstallationDocuments* .

Eine vollständige Liste der Serverprodukte und ihrer Clientanwendungen finden Sie unter „Produkte und Betriebssysteme“ auf Seite 1 .

Server-Software installieren

Installieren Sie die Server-Software auf einem vernetzten Server-Computer. Auf dem Server-Computer muss die entsprechende Version des Betriebssystems ausgeführt werden. Verwenden Sie nach Möglichkeit einen Server-Computer, der für eine schnelle numerische Verarbeitung und einen schnellen Datenzugriff konfiguriert und dediziert ist. Zusätzliche Verarbeitungsleistung und zusätzlicher Speicher verbessern die Leistung der Server-Software. Ausführliche Hardware- und Softwarevoraussetzungen, einschließlich Betriebssystemvoraussetzungen, finden Sie in den Installationsanweisungen.

Bei der Installation der Servertechnologie wird Software installiert, die den Zugriff auf Daten verwaltet und die für die statistische Analyse erforderlichen Berechnungen durchführt. Außerdem wird ein Dienst (unter Windows) oder Dämon (unter UNIX) installiert, der für eingehende Anmeldeanforderungen von Endbenutzern empfangsbereit ist und einen Prozess startet, der jeden Endbenutzer verarbeitet.

Befolgen Sie zur Installation der Server-Software die Anweisungen im Verzeichnis */Documentation/<language>/InstallationDocuments* auf dem Server DVD.

Clientanwendung installieren

Bei der Installation der Clientanwendung wird Software installiert, die die Benutzerschnittstelle und die Darstellung der Ergebnisse verarbeitet. Sie müssen die Installation der Clientanwendung auf dem Desktop-Computer jedes Endbenutzers installieren oder überwachen. Der Desktop-Computer muss Windows ausführen und die Mindestvoraussetzungen für Hardware und Betriebssystem erfüllen. Ausführliche Informationen zu den Voraussetzungen finden Sie in den Installationsanweisungen im Verzeichnis *' /Documentation/<language>/InstallationDocuments '* auf dem Client DVD.

Lesen Sie vor dem Lesen anderer Installationsdokumente den Abschnitt *Getting Started with Installation and Licensing.pdf*.

Kapitel 3. Datenzugriff

Wenn Sie möchten, dass Ihre Endbenutzer auf Daten auf fernen Servern, einschließlich Daten aus Datenbanken, zugreifen können, müssen Sie den Datenzugriff planen, installieren und konfigurieren. Dazu müssen Sie verstehen, wie die Anwendung entscheidet, wo nach Daten gesucht werden soll. Sie müssen auch entscheiden, ob Sie die Datenzugriffstechnologie verwenden möchten, die DataDirect Connect ODBC bietet. Sie können auch OLE DB-Datenquellen verwenden.

Ansicht der Daten

Bevor Sie mit der Planung des Datenzugriffs für die Endbenutzer beginnen, ist es wichtig zu verstehen, wie die Anwendung entscheidet, welche Daten für den Endbenutzer verfügbar sind. Die Sicht der Daten, die Endbenutzern angezeigt werden, hängt davon ab, wie sie das Programm lokal oder im verteilten Modus ausführen.

Modus für lokale Analysen. Im lokalen Analysemodus, bei dem der gesamte Datenzugriff und die Verarbeitung auf dem Desktop-Computer des Endbenutzers erfolgen, erfolgt die Ansicht von Datendateien, ODBC -Datenquellen, -Verzeichnissen und -Laufwerken aus der Perspektive des Desktop-Computers. Das heißt, wenn der Endbenutzer versucht, eine Datendatei zu öffnen, werden die Datendateien, Verzeichnisse und Netzlaufwerke auf seinem Desktop-Computer angezeigt.

Modus für verteilte Analysen. Im Modus für verteilte Analysen, in dem Datenzugriff und -verarbeitung auf einem fernen Server erfolgen, ist die Ansicht von Datendateien, ODBC -Datenquellen, -Verzeichnissen und -Laufwerken aus der Perspektive des Server-Computers, d. h., wenn der Endbenutzer versucht, eine Datendatei zu öffnen, werden die Datendateien, Verzeichnisse und angehängten Laufwerke auf dem Server-Computer angezeigt.

Ihr Job besteht darin, den Datenzugriff entweder im Modus für lokale Analysen oder im Modus für verteilte Analysen zu konfigurieren, wie vom Endbenutzer gefordert.

Datenzugriffstechnologie

Es folgt eine Kurzbeschreibung von Connect ODBC . Weitere Informationen zur Funktionsweise der Datenzugriffstechnologie mit IBM Corp. -Produkten sowie Links zur detaillierten Dokumentation für bestimmte Datenbanken finden Sie unter *IBM SPSS Data Access Pack Installationsanweisungen* im Verzeichnis */Documentation/&language>/Installationsdokumente* des Produkts DVD.

Connect ODBC

Connect ODBC ist eine umfassende Gruppe von einzelnen datenbankspezifischen Treibern, die ODBC verwenden, um Konnektivität für alle wichtigen Datenspeicher bereitzustellen, von relationalen Datenbanken bis hin zu unstrukturierten Dateidaten.

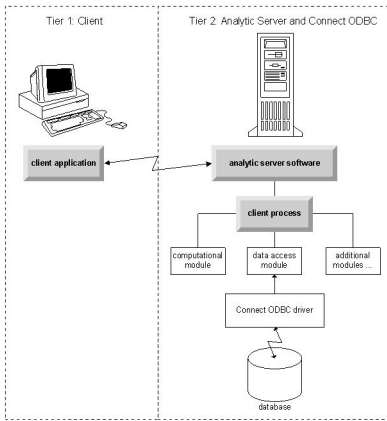


Abbildung 3. Connect ODBC im Modus für verteilte Analysen

Auf Daten zugreifen

Beachten Sie beim Einrichten des Datenzugriffs Folgendes:

Datenzugriffstechnologie. Entscheiden Sie, ob Sie eine der mit Ihrem IBM Corp. -Produkt verteilten Datenzugriffstechnologien verwenden möchten. Weitere Informationen finden Sie im Thema „[Datenzugriffstechnologie](#)“ auf Seite 9. Eine ausführlichere Beschreibung der Auswahl einer Technologie finden Sie in den *IBM SPSS Data Access Pack -Installationsanweisungen*(in /Documentation/&language>/InstallationDocuments auf dem Produkt DVD).

Analysemodus. Der Analysemodus des Endbenutzers bestimmt, auf welche Daten er zugreifen kann. Weitere Informationen finden Sie im Thema „[Ansicht der Daten](#)“ auf Seite 9.

Dateisystemleistung (nur Windows). Wenn die meisten Daten in einem proprietären Format aus IBM Corp. (z. B. .sav -Dateien) und nicht in einer Datenbank vorliegen, wird empfohlen, die Daten auf einem vernetzten Windows NTFS-Laufwerk zu speichern, damit die beste Leistung erzielt wird.

Dateiformat. Die Software verarbeitet das Öffnen und Lesen von Dateien im UNIX-Format automatisch-Sie und Ihre Endbenutzer müssen keine Maßnahmen ergreifen, um der Software mitzuteilen, dass eine Datei im UNIX-Format vorliegt.

Referenzdaten

Einige Client-Software ermöglicht es dem Endbenutzer, Verweise auf Daten und andere Dateien zu sichern. Diese Referenzen müssen aus der Perspektive des Computers geschrieben werden, der auf die Daten zugreifen wird. Wenn der Endbenutzer beispielsweise im lokalen Analysemodus ausgeführt wird, führt ein Verweis auf `C:\mydata\mydata.sav` dazu, dass die Software versucht, auf die Datei auf dem lokalen Laufwerk `C` des *Desktop-Computers* zuzugreifen. Wenn der Endbenutzer im Modus für verteilte Analysen ausgeführt wird, bewirkt derselbe Verweis auf `C:\mydata\mydata.sav`, dass die Software versucht, auf die Datei auf dem lokalen Laufwerk `C` des *-Server-Computers* zuzugreifen, was möglicherweise zu einem Fehler führt.

Windows. Wenn Sie ein Windows-System verwalten, können Sie Daten auf demselben Computer wie die Server-Software speichern. In diesem Fall wird empfohlen, dass Benutzer aus der Perspektive des Servercomputers (z. B. `C:\ServerData\mydata.sav`) auf die Position der Daten verweisen. Die Leistung ist schneller, da das Netz nicht zum Suchen der Datei verwendet wird. Wenn sich Ihre Daten auf einem anderen vernetzten Computer befinden, wird empfohlen, dass Ihre Benutzer UNC-Dateiverweise verwenden (z. B. `\\mydataserver\ServerData\mydata.sav`). UNC-Namen können nur verwendet werden, wenn die referenzierten Positionen den Namen einer *gemeinsam genutzten Ressource* im Netz enthalten. Endbenutzer, die häufig vom verteilten zum lokalen Analysemodus wechseln, sollten UNC-Dateiverweise verwenden, da sie unabhängig vom Modus arbeiten.

UNIX. Wenn Sie eine UNIX-Version der Server-Software verwalten, können Sie Dateien auf einem UNIX-Server ablegen. Endbenutzer können auf Dateien auf einem UNIX-Server verweisen und sie anweisen, die vollständige Dateispezifikation und normale Schrägstriche zu verwenden (z. B. `/FILE = '/public/da-`

ta/ourdata.txt'). Vermeiden Sie die Verwendung des Backslash-Zeichens im UNIX-Verzeichnis und in Dateinamen, die mit der Server-Software verwendet werden.

Datenzugriff steuern

Sie können den Zugriff auf Daten steuern, indem Sie mithilfe des Betriebssystems Berechtigungen nach Benutzer-IDs und Gruppen festlegen. Der Endbenutzer stellt eine Verbindung zur Server-Software her, indem er sich über die Clientanwendung anmeldet. Die Server-Software verwendet das Betriebssystem, um die Berechtigungen für diesen Benutzer durchzusetzen.

Hinweis: Zusätzliche Datensicherheit kann mit Ihrer Datenbanksoftware durchsetzbar sein—die Datenzugriffsmodule der Server-Software fordern Sie zur Eingabe von IDs und Kennwörtern auf, wenn die Datenbank sie benötigt.

Windows. Wie Sie Zugriffsberechtigungen unter Windows festlegen, hängt davon ab, wo die Daten gespeichert werden.

- Wenn sich die Dateien auf einem anderen vernetzten Computer als dem Computer befinden, auf dem die Server-Software ausgeführt wird, weisen Sie den gemeinsam genutzten Ressourcen Berechtigungen zu.
- Wenn sich die Dateien auf dem Server-Computer und einem NTFS-Laufwerk befinden, verwenden Sie Sicherheitseinstellungen. Sie können den Dateizugriff für Daten auf dem Server-Computer auf einem FAT-Laufwerk nicht steuern.

Informationen zum Festlegen von Freigabe- und Sicherheitsberechtigungen unter Windows finden Sie unter „Dateieigenschaften“ auf Seite 55 .

UNIX. Wenn der Endbenutzer über die Clientanwendung eine Verbindung zur Server-Software herstellt, übergibt die Server-Software die Anmelde-ID und das Kennwort des Benutzers an das Betriebssystem und startet einen Prozess für den Benutzer. Der gestartete Prozess verfügt über die Dateizugriffsberechtigungen des Anmeldeaccounts des Endbenutzers.

Datenquellen

ODBC

Die IBM SPSS Statistics -Serversoftware verwendet ODBC für den Zugriff auf die meisten Daten, die nicht in einem proprietären Format vorliegen, einschließlich Daten, die in Datenbanken gespeichert sind. ODBC erfordert eine ODBC -Datenquelle. Eine ODBC -Datenquelle ist eine Kombination aus:

- Ein beschreibender Name
- Ein bestimmter Treiber
- Verweis auf eine Datenbank oder einen anderen Typ von Datendatei

Für den Zugriff auf die meisten Daten müssen Sie die benötigten ODBC -Datenquellen konfigurieren oder Endbenutzer bei der Konfiguration unterstützen.

Die Position der konfigurierten Datenquelle ist kritisch. Es muss auf dem Computer konfiguriert werden, der auf die Daten zugreift und sie verarbeitet. Konfigurieren Sie daher die ODBC -Datenquelle auf dem *Server-Computer* für verteilte Analysen und auf dem *Desktop-Computer* für lokale Analysen. Vergleichen Sie beispielsweise die Position der ODBC -Treiber in den Abbildungen in „Connect ODBC“ auf Seite 9 .

Wenn Sie gerade erst mit der Verwendung der Datenzugriffstechnologie beginnen (eingeführt in „Datenzugriffstechnologie“ auf Seite 9) müssen Sie einige zusätzliche Tasks ausführen, bevor Sie eine Datenquelle konfigurieren können. Lesen Sie die *IBM SPSS Data Access Pack -Installationsanweisungen* (in / Documentation/<language>/InstallationDocuments für das Produkt DVD). Die Datenquellenkonfiguration wird in Kapitel 4, „Belegung und Wartung konfigurieren, überwachen“, auf Seite 15 dieses Handbuchs noch einmal erläutert.

UNIX-Umgebung für Datenzugriff konfigurieren

Damit die Datenzugriffstechnologie auf UNIX-Systemen funktioniert, muss das Startscript der Server-Software konfiguriert sein.

Startscript öffnen

1. Wechseln Sie im Installationsverzeichnis der Server-Software in das Unterverzeichnis `/bin`. Geben Sie beispielsweise an der UNIX-Eingabeaufforderung Folgendes ein:

```
cd /usr/local/serverproduct/bin
```

Dabei steht `/usr/local/serverproduct/bin` für das Unterverzeichnis `/bin` des Verzeichnisses, in dem die Server-Software installiert ist.

2. Öffnen Sie `statsenv.sh` mit einem Texteditor.

DataDirect-Script angeben

1. Suchen Sie nach dem ersten Kommentar, der den Text enthält:

```
MERANT_ENVIRONMENT_SCRIPT
```

2. Suchen Sie die Zeile, die die Position von `odbc.sh` definiert.
3. Bearbeiten Sie die Zeile so, dass sie den richtigen Pfad zu Ihrer Connect ODBC *-Clientinstallation* enthält, und entfernen Sie das Kommentarzeichen, falls es eines enthält. Ändern Sie beispielsweise

```
# MERANT_ENVIRONMENT_SCRIPT=/usr/s1odbc50/5_01_00/odbc.sh
```

in:

```
MERANT_ENVIRONMENT_SCRIPT=/usr/myDataAccess/s1odbc50/5_01_00/odbc.sh
```

Umgebungsvariable `odbc.ini` hinzufügen

1. Fügen Sie die folgenden Zeilen nach den obigen Zeilen hinzu, um eine Umgebungsvariable `ODBCINI` zu erstellen, die es IBM SPSS Statistics Server ermöglicht, die Datei `odbc.ini` zu finden:

```
ODBCINI=ODBCDIR/odbc.ini  
export ODBCINI
```

Dabei wird `ODBCDIR` durch den Pfad zu Ihrem ODBC Connect-Installationsverzeichnis ersetzt.

Pfade zu Datenbankbibliotheken hinzufügen

1. Fügen Sie Zeilen hinzu, die für Ihre Datenbank geeignet sind, normalerweise das *Datenbankausgangsverzeichnis* und, wenn Sie *nicht* die Data Direct Wire Protocol-Treiber verwenden, einen *Pfad zu den Datenbankbibliotheken*. Fügen Sie beispielsweise die folgenden Zeilen hinzu, wenn Sie Oracle unter Linux verwenden:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/bigdisk/oracle/product/8.1.6/lib  
export LD_LIBRARY_PATH  
ORACLE_HOME=/bigdisk/oracle/product/8.1.6  
export ORACLE_HOME
```

Dabei wird `/bigdisk/oracle/product/8.1.6` durch den Pfad zu Ihrem Oracle -Installationsverzeichnis ersetzt und `LD_LIBRARY_PATH` ist die Bibliothekspfadvariable für Ihr Betriebssystem.

Beachten Sie, dass die Data Direct Wire Protocol-Treiber nicht die Installation von Datenbankclientbibliotheken erfordern. Andere Data Direct-Treiber benötigen diese Bibliotheken jedoch.

Startscript speichern

1. Speichern Sie die Datei `statsenv.sh`.

odbc.ini bearbeiten

1. Bearbeiten Sie die ODBC -Konfigurationsdatei *odbc.ini*, sodass über IBM SPSS Statistics Server auf ODBC -Datenquellen zugegriffen werden kann. Lesen Sie den Anhang "The UNIX Environment" in DataDirect's *Referenz für DataDirect Connect ODBC* (verfügbar, wenn Sie die zusätzliche DataDirect-Dokumentation bei der Installation von Connect ODBC installiert haben) und die Kapitel für bestimmte Treiber in *odbchelp.pdf* im Unterverzeichnis *Doc* Ihres Connect ODBC -Installationsverzeichnis.

Die Änderung wird beim nächsten Start der Server-Software wirksam.

Anmerkung: Wenn Sie ODBC mit IBM SPSS Statistics Batch Facility verwenden möchten, müssen Sie das IBM SPSS Statistics Batch Facility-Startscript auf dieselbe Weise ändern.

Kapitel 4. Belegung und Wartung konfigurieren, überwachen

Konfigurieren Sie nach der Installation der Server-Software ihre Umgebung wie folgt:

- Endbenutzerkonten und -dateien verwalten
- ODBC -Datenquellen konfigurieren
- Verwaltungsanwendung (IBM SPSS Statistics Administration Console) zum Konfigurieren und Überwachen der Server-Software verwenden
- Servicestart steuern

Diese Tasks werden in den folgenden Abschnitten beschrieben.

Endbenutzerkonten und Dateien verwalten

In diesem Abschnitt erhalten Sie einen Überblick darüber, was Sie tun müssen, um Endbenutzer an Ihrem Standort zu unterstützen. Weitere Informationen hierzu finden Sie in [Kapitel 5, „Unterstützende Endbenutzer“](#), auf Seite 23.

Konten

Endbenutzer benötigen Accounts, um sich bei der Server-Software anzumelden und auf Daten zuzugreifen. Diese Konten müssen authentifiziert werden und in der Lage sein, in bestimmten Ordnern auf der Servermaschine zu lesen, zu schreiben und/oder auszuführen. Weitere Informationen zu Dateiberechtigungen finden Sie im Abschnitt [„Berechtigungen“](#) auf Seite 31. Weitere Informationen zur Authentifizierung finden Sie im Abschnitt [„Authentifizierung \(Authentication\)“](#) auf Seite 23.

Datenbankberechtigungen werden von der Datenbanksoftware durchgesetzt. Verwenden Sie Ihre üblichen Datenbankverwaltungstools, um diese Konten zu verwalten. Wenn die Datenbank eingeschränkt ist, fordern die Datenzugriffsmodule der Server-Software den Benutzer auf, sich anzumelden und diese Informationen zur Überprüfung an die Datenbank zurückzugeben, bevor er auf Daten zugreift.

Datenzugriff

Standardmäßig kann jeder Endbenutzer alle Daten anzeigen, wenn er eine Datei öffnet, während er mit der Server-Software verbunden ist. Die Anzeige aller Daten kann die Leistung beeinträchtigen und den Datenaustausch im Netz erhöhen. Sie können verhindern, dass die Clientcomputer der Endbenutzer die Daten anzeigen, indem Sie die globale Einstellung mit der Verwaltungsanwendung ändern (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird). Weitere Informationen finden Sie im Abschnitt "Benutzer" im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Sie können auch das Benutzerprofil und die Gruppeneinstellungen ändern, um den Datenzugriff für einzelne Benutzer oder Gruppen festzulegen. Weitere Informationen finden Sie im Abschnitt IBM SPSS Statistics Server im *Deployment Manager Benutzerhandbuch*.

Dateien

Die meisten Dateien, die Endbenutzer speichern müssen, sollten auf dem Desktop-Computer gespeichert werden. Sie können jedoch zulassen, dass Benutzer Datendateien auf einem vernetzten Computer speichern. Wenn sich der Endbenutzer zum ersten Mal bei der Analytic Server-Software anmeldet, ist das Installationsverzeichnis der Server-Software das Standardverzeichnis zum Öffnen und Speichern von Dateien. Dies ist eindeutig keine Position, an der Benutzer Dateien schreiben sollen. Konfigurieren Sie daher ein Verzeichnis mit Schreibberechtigung und verteilen Sie diese Position an die Endbenutzer. Sobald sie

über die Benutzerschnittstelle auf diese Position zugreifen, wird sie von der Clientanwendung gespeichert und als Standardposition für gespeicherte Dateien verwendet.

Profile

Mit der Server-Software können Sie auch Profile für Benutzer erstellen. Ein Profil kann das temporäre Verzeichnis, die UNIX-Einstellung `umask`, die CPU-Prozesspriorität, die Clientdatenzugriffseinstellung und die maximale Anzahl Threads für jeden Benutzer oder eine Benutzergruppe angeben.

ODBC -Datenquellen konfigurieren

Wenn Ihre Endbenutzer auf Daten aus Datenbanken zugreifen, während sie im Modus für verteilte Analysen arbeiten, müssen Sie ODBC -Datenquellen auf dem Computer konfigurieren, auf dem die Server-Software installiert ist.

ODBC -Datenquellen und IBM SPSS Data Access Pack

Wenn Sie die IBM Corp. -Datenzugriffstechnologie verwenden, lesen Sie den Abschnitt [Kapitel 3, „Datenzugriff“](#), auf Seite 9 in diesem Dokument. Lesen Sie die entsprechenden *Installationsanweisungen*, um eine Übersicht über die Konfiguration des Datenbankzugriffs und Links zur ausführlichen Dokumentation zum Datenzugriff für bestimmte Datenbanken zu erhalten (das Dokument befindet sich in */Documentation/&language>/InstallationDocuments* auf dem Produkt DVD).

Windows Konfigurieren Sie ODBC -Datenquellen mithilfe des ODBC -Administrators. Weitere Informationen finden Sie im Thema [„ODBC -Administrator“](#) auf Seite 56.

UNIX. Bearbeiten Sie das Startumgebungsscript für die Server-Software wie in [„UNIX-Umgebung für Datenzugriff konfigurieren“](#) auf Seite 12 beschrieben und konfigurieren Sie ODBC -Datenquellen mithilfe der Datei `odbc.ini`. Weitere Informationen finden Sie im Abschnitt [„odbc.ini“](#) auf Seite 60.

Sortierengine eines anderen Anbieters verwenden

Die Server-Software versucht standardmäßig, eine externe Engine eines anderen Anbieters zum Sortieren zu verwenden. Führen Sie die folgenden Schritte aus, um die richtige Sortierengine zu verwenden:

1. Wenn die Sortierengine eines anderen Anbieters nicht auf dem Server-Computer installiert ist, installieren Sie sie. IBM Corp. stellt die Engines nicht zur Verfügung. Sie müssen eine Engine von einem Drittanbieter erwerben und lizenzieren.
2. Stellen Sie sicher, dass sich die Bibliothek der Sortiersteuerkomponente in der Ausführungs- oder Bibliothekspfadvariablen des Systems befindet. Unter Windows ist dies die Umgebungsvariable `PATH`; unter UNIX ist dies je nach UNIX-Anbieter `LD_LIBRARY_PATH` oder `LIBPATH`. Dieser Schritt ist erforderlich, damit die Server-Software die Sortierbibliothek eines anderen Anbieters laden kann.
3. Verwenden Sie die Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird) und setzen Sie die Sortieroption auf die entsprechende Engine eines anderen Anbieters. Weitere Informationen finden Sie im Abschnitt "Benutzer" im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten).

Any procedures that require sorting (e.g., SORT) will subsequently use the third-party sorting engine. Durch Absetzen des Syntaxbefehls `SET SORT=INTERNAL` wird die Server-Software gezwungen, den internen Algorithmus zum Sortieren zu verwenden. Ein Endbenutzer kann auch explizit die Sortierung durch Dritte angeben, indem er den Befehl `SET SORT=EXTERNAL` absetzt. Dies ist jedoch nicht erforderlich, weil die Sortierung anderer Anbieter die Standardeinstellung ist.

Aktuelle Sortieroption überprüfen

Um zu prüfen, welche Sortieroption verwendet wird, können Sie den Syntaxbefehl `SET MESSAGES ON` absetzen und einen `SORT` -Job ausführen. Sie können auch den Syntaxbefehl `SHOW SORT` verwenden.

IBM SPSS Statistics-Serveradministration

IBM SPSS Statistics Administration Console bietet eine Benutzerschnittstelle für die Überwachung und Konfiguration Ihrer IBM SPSS Statistics Server-Installationen. IBM SPSS Statistics Administration Console wird als Teil von IBM SPSS Deployment Manager installiert. Die vollständige Dokumentation für IBM SPSS Statistics Administration Console ist im Abschnitt *Administrationskonsolen* von *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten) enthalten.

Xspannungen konfigurieren

Ein IBM SPSS Statistics -Serveradministrator muss Schritte ausführen, um die Xtension-Prozeduren (krr, lenr, lrr und lrr) für die Ausführung in **statsb** und SPSS Statistics Server verfügbar zu machen. Die Xtension-Prozeduren umfassen Folgendes:

- Kernel Ridge-Regression (KRR)
- Lineare Elastic Net-Regression (LENR)
- Lineare Lasso-Regression (LLR)
- Lineare Ridge-Regression (LRR)

Installieren von Xspannungen auf SPSS Statistics Server

1. Installieren Sie auf dem IBM SPSS Statistics -Client Xspannungen (im Lokalmodus) über den Erweiterungshub.
2. Stellen Sie sicher, dass die Bibliothek **sklearn** auf dem IBM SPSS Statistics Server installiert ist.

UNIX[®]

Führen Sie den folgenden Befehl als Benutzer aus, der SPSS Statistics Server installiert hat.

```
./statisticspython3 -m pip install sklearn
```

Anmerkung: statisticspython3 befindet sich im Verzeichnis bin der SPSS Statistics -Serverinstallation.

Windows[®]

Führen Sie den folgenden Befehl aus.

```
statisticspython3.bat -m pip install sklearn
```

Anmerkung: statisticspython3.bat Befindet sich im Installationsverzeichnis von SPSS Statistics Server.

3. Kopieren Sie das Verzeichnis xtensions und seinen Inhalt vom SPSS Statistics -Client (%APPDATA%\IBM\SPSS Statistics\one\xtensions\ unter Windows, \$HOME/Library/Application Support/IBM/SPSS Statistics/one/xtensions unter macOS) in das Installationsverzeichnis von SPSS Statistics Server.

SPSS Statistics Server ist jetzt bereit, die Xtension-Prozeduren auszuführen, die im Verzeichnis xtensions installiert sind.

Konfigurieren der Befehlszeilenschnittstelle des Produktionsmodus zur Übergabe von Jobs

Ab IBM SPSS Statistics Version 26 können Sie die Befehlszeilenschnittstelle von Production Facility verwenden, um Jobs an den SPSS Statistics -Server zu übergeben. Wenn die Befehlszeilenschnittstelle des Produktionsmodus in Verbindung mit dem Microsoft Windows Task Scheduler/MacOS Automator für die Terminierung von Jobs verwendet wird, können Sie IBM SPSS Collaboration and Deployment Services effektiv ersetzen, um SPSS Statistics-Jobs zu verarbeiten.

Mit dem SPSS Statistics-Befehl **INSERT HIDDEN** können Jobs ausgeführt werden, die eine Ausgabe generieren. Wenn der Befehl verwendet wird, können Benutzer nicht auf die SPSS Statistics-Quellsyntax zugreifen oder sie anzeigen.

Anmerkung: Für den Befehl **INSERT HIDDEN** ist ein SPSS Statistics-Server erforderlich. Der Befehl kann nicht auf einer eigenständigen SPSS Statistics-Clientmaschine ausgeführt werden.

INSERT HIDDEN (Funktion)

Administratoren können die Funktion **INSERT HIDDEN** über die SPSS Statistics Server-Administrationskonsole oder durch Bearbeiten der Datei <install_path>/config/statisticsd.conf (**INSERT HIDDEN = Enabled**) aktivieren. Das Feld **INSERT HIDDEN-Funktion** befindet sich auf der Registerkarte "Konfiguration des SPSS Statistics-Servers" der Verwaltungskonsole des SPSS Statistics-Servers (unter dem Abschnitt **Benutzer**).

1. Wählen Sie **Aktiviert** als Wert für **INSERT HIDDEN-Funktion** aus. Es wird ein Stern (*) auf der Registerkarte "Konfiguration des SPSS Statistics-Servers" angezeigt.
2. Speichern Sie die Änderung. Klicken Sie entweder auf das Symbol **Speichern** in der Symbolleiste oder auf "STRG-S" oder wählen Sie **Datei > Speichern** aus.
3. Starten Sie den SPSS Statistics-Server erneut.
4. Nachdem der Server auf Windows-Servern erneut gestartet wurde, wird ein Dialogfeld angezeigt, in dem der Administrator aufgefordert wird, das Kennwort für die **INSERT HIDDEN-Funktion** einzugeben. Auf Linux-Servern muss der Administrator den SPSS Statistics-Server manuell starten. Wenn der Server neu startet, wird der Administrator zur Eingabe des Kennworts aufgefordert.

Das Kennwort wird in der Systemregistry gespeichert (wie bei einem SSL-Kennwort) und alle verdeckten Syntaxdateien werden über dasselbe Kennwort verschlüsselt.

Optional kann der Administrator den Benutzerzugriff auf die **INSERT HIDDEN**-Dateien über die Dateisystemzugriffssteuerungen verweigern.

Der Dämonprozess des SPSS Statistics-Servers benötigt Lesezugriff auf die **INSERT HIDDEN**-Dateien. Mithilfe eines OMS-Befehls kann die Syntax eingeschlossen werden, um sicherzustellen, dass die Ausgabe nicht an den Ausgabebewerter gesendet wird.

```
OMS /SELECT ALL /DESTINATION VIEWER=NO.  
* - commands executed here will not output to the viewer.  
DESC ALL.  
FREQ ALL.  
OMSEND.
```

Die **INSERT HIDDEN**-Syntax ähnelt der **INSERT FILE**-Syntax. Beispiel:

```
INSERT HIDDEN  
SOURCE='source specification'  
[SYNTAX = {INTERACTIVE*}]  
  {BATCH }  
[ERROR = {CONTINUE*}]  
  {STOP }  
[ENCODING = 'encoding specification']
```

Der **INSERT HIDDEN**-Dateiautor stellt die verdeckten Dateipfade für die SPSS Statistics-Clientbenutzer bereit. Während der Laufzeit führen die Clientbenutzer die Syntax **INSERT HIDDEN SOURCE= "< Dateipfad>"** aus.

Weitere ausführliche Informationen finden Sie im *IBM SPSS Statistics-Befehlssyntaxhandbuch*.

Der Clientprozess auf dem SPSS Statistics-Server sendet den **SOURCE**-Pfad an den Dämonprozess des Servers. Der Dämonprozess verschlüsselt die Datei und gibt sie dann an den Clientprozess zur Ausführung zurück.

Der Clientprozess inaktiviert Protokolle und Journale, führt die entschlüsselte Datei aus und aktiviert dann die Protokolle und Journale erneut. Das Ergebnis ist, dass der SPSS Statistics-Ausgabebewerter keine Quellsyntaxprotokollierung enthält (er enthält Ausgabe). Das Journal enthält auch keine Quellsyntax.

Mehrere Instanzen konfigurieren

Sie können mehrere Instanzen der Server-Software erstellen, die jeweils eine eigene Portnummer haben. Diese Möglichkeit wird häufig in Verbindung mit der Gruppenberechtigung verwendet, um eine Benutzergruppe einer bestimmten Instanz zuzuordnen. Es können jedoch mehrere Instanzen unabhängig von der Gruppenberechtigung verwendet werden. Weitere Informationen zur Gruppenberechtigung finden Sie in „Gruppenberechtigung“ auf Seite 31.

Erstellen einer neuen Instanz

Wenn Sie eine Gruppeninstanz der Server-Software erstellen möchten, müssen Sie ein Script ausführen. Unter Windows müssen Sie das folgende Script über das Serverinstallationsverzeichnis ausführen.

```
create_group_service <group_name> <port_number>
```

Unter UNIX und Linux müssen Sie das folgende Script über das Unterverzeichnis `bin` des Installationsverzeichnisses ausführen.

```
create_group_configuration -group <group_name> -port <port_number>
```

< Gruppenname> ist ein eindeutiger Name für die Instanz und < Portnummer> ist die verfügbare Portnummer, die von der Instanz verwendet wird.

Nachdem Sie das Script ausgeführt haben, befindet sich auf dem System ein Konfigurationsordner, der speziell für die Instanz erstellt wurde. Suchen Sie in der Serverinstallationsrichtung nach `config_<groupname>`. Der Ordner enthält mehrere Konfigurationsdateien, z. B. `statisticsd.conf` und `UserSettings.xml`. Wenn Sie die Konfiguration für eine bestimmte Instanz aktualisieren möchten, stellen Sie sicher, dass die Konfigurationsdatei an der richtigen Position aktualisiert wird.

Starten der Serverinstanz

Unter Windows stellt die Instanz einen separaten Dienst dar, der den Namen *IBM SPSS Statistics NN.m* hat. Dabei steht *NN* für die Hauptversionsnummer und *m* für die Nebenversionsnummer. Sie können diesen Dienst wie alle anderen Windows-Dienste starten und stoppen.

Unter Linux und UNIX müssen Sie den Gruppennamen angeben, wenn Sie das Startscript ausführen:

```
./start_statistics_server -d -g <group_name>
```

Dabei ist < Gruppenname> der Name der Instanzgruppe.

Löschen einer Serverinstanz

1. Entfernen Sie unter Windows den Eintrag des Dienstes:
 - a. Öffnen Sie als Administrator eine Eingabeaufforderung.
 - b. Führen Sie den folgenden Befehl aus:

```
sc delete "IBM SPSS Statistics NN.m Server <group_name>"
```

Dabei steht *NN* für die Hauptversionsnummer, *m* für die Nebenversionsnummer und < *Gruppenname*> für die Instanzgruppe.

2. Löschen Sie das Unterverzeichnis `config_<groupname>` im Serverinstallationsverzeichnis.

Servicestart steuern

Die Server-Software verfügt über eine Frameworkkomponente, die die gesamte Kommunikation zwischen der Clientanwendung und den Modulen steuert. Unter Windows ist die Frameworkkomponente ein Ser-

vice. Unter UNIX ist die Frameworkkomponente eine Anwendung, die normalerweise als Dämon ausgeführt wird.

Windows

Standardmäßig ist der Service für den automatischen Start konfiguriert, d. h., er wird beim Neustart des Computers automatisch erneut gestartet. Wenn der Service auf diese Weise gestartet wird, wird er automatisch ausgeführt und der Servercomputer kann abgemeldet werden, ohne dass sich dies auf den Service auswirkt. Sie können die Windows-Systemsteuerung für Dienste verwenden, um die Dienststartparameter zu ändern. Weitere Informationen finden Sie im Thema „[Systemsteuerung für Services](#)“ auf Seite 56. Wenn Sie mehrere Instanzen ausführen, enthält die Serviceanzeige einen Eintrag für jede Serverinstanz.

Anmerkung: Wenn der Server-Computer die IP-Adresse des lokalen Hosts (127.0.0.1/: 1) nicht unterstützt, müssen Sie eine Systemumgebungsvariable mit dem Namen `STATS_LH_OVERRIDE` erstellen und ihren Wert auf `YES` setzen, bevor Sie den Server starten. Informationen zum Starten und Stoppen des Servers finden Sie unter „[Server-Software starten und stoppen](#)“ auf Seite 21.

platform="unix " scale="80">CrtCDSresources.sh

Das Startscript `start_statistics_server` befindet sich im Unterverzeichnis `/bin` des Installationsverzeichnisses. Das Script ruft `statsenv.sh` auf, um die Umgebung für die Server-Software zu konfigurieren, und startet anschließend die Anwendung. Sie müssen die Server-Software mit diesem Script starten. Das Startscript muss im Unterverzeichnis `/bin` ausgeführt werden. Zur Ausführung müssen Sie als **root** angemeldet sein, wenn Sie die UNIX-Standardauthentifizierung oder das Pluggable Authentication Module (PAM) verwenden. Andernfalls müssen Sie als der Benutzer angemeldet sein, der Eigentümer des Server-Software-Dämons ist. Weitere Informationen zur Authentifizierung finden Sie im Abschnitt „[Authentifizierung \(Authentication\)](#)“ auf Seite 23. Der Befehl:

```
./start_statistics_server -d
```

startet die Server-Software als Dämonprozess. Dies ist die empfohlene Methode zur Ausführung der Server-Software.

Wenn Sie mehrere Instanzen der Server-Software ausführen, startet dieser Befehl die Standardinstanz. Geben Sie zum Starten einer anderen Instanz die Instanzgruppe mit dem Switch `-g` an:

```
./start_statistics_server -d -g <groupname>
```

Dabei ist `< Gruppenname >` der Name der Instanzgruppe.

Anmerkung: Wenn der Server-Computer die IP-Adresse für den lokalen Host (127.0.0.1/:1) nicht unterstützt, müssen Sie die Umgebungsvariable `STATS_LH_OVERRIDE` vor dem Starten des Servers auf `YES` setzen. `STATS_LH_OVERRIDE` wird über das Script `statsenv.sh` festgelegt, das im Unterverzeichnis `/bin` des Installationsverzeichnisses enthalten ist. Informationen zum Starten und Stoppen des Servers finden Sie unter „[Server-Software starten und stoppen](#)“ auf Seite 21.

Befehlszeilenparameter für Startscript

Das Script `start_statistics_server` akzeptiert die folgenden Befehlszeilenparameter (in beliebiger Reihenfolge):

- **Dämon.** Führen Sie die Server-Software als Dämonprozess aus, indem Sie optional `-d` angeben. Wenn Sie `-d` nicht angeben, wird der Server als Vordergrundprozess gestartet. Verwenden Sie zum Starten der Server-Software als Dämon beispielsweise den folgenden Befehl:

```
./start_statistics_server -d
```

- **Gruppe.** Wenn Sie mehrere Instanzen der Server-Software ausführen, geben Sie die Gruppe an, die der Instanz zugeordnet ist:

```
start_statistics_server -g <groupname>
```

Hierbei gilt Folgendes:

< Gruppename> ist der entsprechende Gruppename.

- **Port.** Eine Portnummer kann optional in der Befehlszeile des Startscripts angegeben werden. Verwenden Sie beispielsweise den folgenden Befehl, um eine Portnummer anzugeben:

```
start_statistics_server -p nnnn
```

Hierbei gilt Folgendes:

nnnn ist die gewünschte Portnummer.

Geben Sie eine Portnummer nur an, wenn Sie einen Portnummernkonflikt auflösen müssen. Die Standardeinstellung funktioniert nur, wenn eine andere Anwendung auf dem Computer dieselbe Nummer verwendet. Diese Befehlszeileneinstellung überschreibt den in der Verwaltungsanwendung festgelegten Wert.

Sonstige Wartung

Entfernen Sie nicht benötigte Dateien. Überprüfen Sie regelmäßig die Position der temporären Datei und die Position der Protokolldatei auf nicht benötigte Dateien und entfernen Sie sie. Die Standorte werden mit der Verwaltungsanwendung definiert.

Aktive Prozesse überprüfen. Wenn Sie den Server-Computer nicht regelmäßig neu starten, überprüfen Sie regelmäßig die Prozesse, die auf dem Computer ausgeführt werden, und beenden Sie alle Prozesse, die nicht verwendet werden. Die Prozessnamen sind in „Server-Software starten und stoppen“ auf Seite 21 aufgelistet.

Server-Software starten und stoppen

Die Verwaltungsanwendung startet die Server-Software für Sie erneut, damit Konfigurationsänderungen festgeschrieben werden können. Es kann jedoch vorkommen, dass Sie die Server-Software über das Betriebssystem starten oder stoppen müssen. Führen Sie die folgenden Schritte für Ihr Betriebssystem aus und verwenden Sie dabei den Prozessnamen Ihres Serverprodukts. Unter Windows lautet der Standard servicename *IBM SPSS Statistics NN.m*, wobei *NN* die Hauptversionsnummer und *m* die Nebenversionsnummer ist. Wenn Sie mehrere Instanzen ausführen, lautet der Servicename *IBM SPSS Statistics NN.m < Gruppename>*, wobei *NN* die Hauptversionsnummer, *m* die Nebenversionsnummer und < Gruppename> die Gruppe der Instanz ist. Unter UNIX und Linux lautet der Dämonname *statisticsd*.

Anmerkung zur Planung: Wenn Sie den Service oder Dämon stoppen, wird die Verbindung zu Endbenutzern getrennt und die Prozesse werden beendet. Versuchen Sie daher, Konfigurations- und Verwaltungsaufgaben für eine Zeit zu planen, in der Sie erwarten, dass wenige Benutzer auf das System zugreifen (z. B. am frühen Morgen oder am späten Abend).

Service oder Dämon starten

Windows. Starten Sie den Dienst über die Systemsteuerung für Windows-Dienste. Weitere Informationen finden Sie im Thema „Systemsteuerung für Services“ auf Seite 56.

UNIX. Starten Sie den Server mit dem Startscript *start_statistics_server*, das sich im Unterverzeichnis */bin* des Installationsverzeichnisses befindet. Das Startscript muss im Unterverzeichnis */bin* ausgeführt werden. Zur Ausführung müssen Sie als **root** angemeldet sein, wenn Sie die UNIX-Standardauthentifizierung oder das Pluggable Authentication Module (PAM) verwenden. Andernfalls müssen Sie als der Benutzer angemeldet sein, der Eigner des Server-Software-Dämons ist. Weitere Informationen zur Authentifizierung finden Sie im Abschnitt „Authentifizierung (Authentication)“ auf Seite 23.

Service oder Dämon stoppen

Windows. Verwenden Sie die Systemsteuerung für Windows-Dienste, um den Dienst zu stoppen. Weitere Informationen finden Sie im Thema „Systemsteuerung für Services“ auf Seite 56.

UNIX. Beenden Sie den Serverprozess. (Ein Beispiel finden Sie in „ps und kill“ auf Seite 60 .) Der Dämon erstellt automatisch eine Datei (*statisticsd.pid*), die die Prozess-ID für den Dämon enthält. Sie können diese Datei in Verbindung mit dem Befehl kill verwenden, indem Sie im Unterverzeichnis config des Installationsverzeichnisses oder im config_<group_name> für eine andere Instanz der Server-Software Folgendes ausführen:

```
kill -9 `cat statisticsd.pid`
```

Plattformunabhängig. Verwenden Sie die Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird). Weitere Informationen finden Sie im Abschnitt zur Steuerung von IBM SPSS Statistics Server im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten).

Konfiguration zur Leistungsverbesserung

Informationen zum Ändern der Konfiguration der Server-Software zur Verbesserung der Leistung finden Sie in [Kapitel 6, „Leistung analysieren und verbessern“](#), auf Seite 47 .

Kapitel 5. Unterstützende Endbenutzer

Um Endbenutzer zu unterstützen, müssen Sie sicherstellen, dass sie über die Informationen verfügen, die sie für die Ausführung ihres IBM Corp. -Produkts im Modus für verteilte Analysen benötigen. Um die Server-Software verwenden zu können, müssen Endbenutzer Folgendes wissen:

- Herstellen einer Verbindung zur Server-Software.
- Vorgehensweise beim Zugriff auf Daten und Dateien.
- Speicherposition für Daten und Dateien.

Authentifizierung (Authentication)

Sie haben mehrere Optionen für die Authentifizierung von Benutzern. Einige Optionen erfordern, dass der Server mit Rootberechtigungen ausgeführt wird.

Tabelle 1. Authentifizierungsoptionen

| Methoden | Betriebssystemverfügbarkeit | Server muss als System/Root ausgeführt werden? |
|---|---|--|
| Standardauthentifizierung auf Betriebssystemebene (Windows-oder UNIX-Konto) | <ul style="list-style-type: none">• Windows• platform="unix " scale="80">CrtCDSresources.sh | Ja |
| Pluggable Authentication Module (PAM) | <ul style="list-style-type: none">• platform="unix " scale="80">CrtCDSresources.sh | Ja |
| Interne Authentifizierung | <ul style="list-style-type: none">• Windows• platform="unix " scale="80">CrtCDSresources.sh | Nein |
| unix2 | <ul style="list-style-type: none">• platform="unix " scale="80">CrtCDSresources.sh | Nein |
| Single Sign-on | <ul style="list-style-type: none">• Windows• platform="unix " scale="80">CrtCDSresources.sh | Nein |

Authentifizierung auf Betriebssystemebene konfigurieren

Die Authentifizierung auf Betriebssystemebene ist die Standardauthentifizierungsmethode. Verwenden Sie Ihre üblichen Systemverwaltungstools zum Erstellen und Verwalten von Standardendbenutzerkonten auf Betriebssystemebene (Informationen zum Zugriff auf den Windows-Benutzermanager finden Sie unter „Benutzermanager“ auf Seite 56).

Wenn Sie eine andere Authentifizierungsmethode versuchen und zur Authentifizierung auf Betriebssystemebene zurückkehren möchten, müssen Sie das Element *Benutzerberechtigung* in der Datei *statis-ticsd.conf* aktualisieren und den Parameter *Wert* in UNIX oder win32ändern.

Konfigurieren von PAM

Die Server-Software unter UNIX kann das Pluggable Authentication Module (PAM) verwenden, um Benutzer zu authentifizieren. Sie müssen zuerst die Server-Software für die Verwendung von PAM konfigurieren. Anschließend konfigurieren Sie PAM, indem Sie die Anweisungen Ihres UNIX-Anbieters befolgen. Schritte für Linux. Diese können je nach Version und Anbieter variieren.

Hinweis: Wenn die Server-Software aktiv ist, müssen Sie sie erneut starten, nachdem Sie alle Schritte ausgeführt haben.

Server-Software für die Verwendung von PAM konfigurieren

1. Melden Sie sich an der UNIX-Maschine als *root* an.
2. Öffnen Sie im Unterverzeichnis *config* im Installationsverzeichnis der Server-Software die Konfigurationsdatei (z. B. *statisticsd.conf*) in einem Texteditor.
3. Suchen Sie das Element *userauth* und ändern Sie den Parameter *value* von *unix* in *pam*.
4. Speichern Sie die Datei.

PAM unter Linux konfigurieren

1. Wechseln Sie in das PAM-Konfigurationsverzeichnis (z. B. */etc/pam.d*).
2. Erstellen Sie mit einem Texteditor eine Datei mit dem Namen *statisticsd*.
3. Fügen Sie die PAM-Konfigurationsinformationen hinzu, die verwendet werden sollen. Beispiel:

```
auth        include    system-auth
account     required  pam_nologin.so
account     include   system-auth
password    include   system-auth
session     optional  pam_keyinit.so force revoke
session     include   system-auth
session     required pam_loginuid.so
```

Hinweis: Diese Zeilen können je nach Konfiguration variieren. Weitere Informationen finden Sie in der Dokumentation zu Linux .

4. Speichern Sie die Datei.

Interne Authentifizierung konfigurieren

Die interne Authentifizierung ermöglicht die Ausführung der Server-Software ohne Rootberechtigung. Sie begrenzt jedoch Clientverbindungen auf denselben Plattenzugriff. Jeder Benutzer, der eine Verbindung zur Server-Software herstellt, verfügt über dieselbe Plattenzugriffssicherheit. Daher kann ein Benutzer die Datei eines anderen Benutzers löschen. Wenn dies ein Problem darstellt, wird empfohlen, stattdessen die Authentifizierungsmethode *unix2* zu verwenden. Diese Methode schränkt keine Clientverbindungen ein, da sie die UNIX-Datei *passwd* für die Authentifizierung verwendet. Weitere Informationen finden Sie in „[unix2 -authentifizierung Konfigurieren](#)“ auf Seite 25.



Warnung: Verwenden Sie keine interne Authentifizierung, wenn Sie den Dämon/Service als Stammmverzeichnis/SYSTEM ausführen. Dies entspricht der Erteilung von Root-/Systemzugriff auf Ihren Server an alle Benutzer, die eine Verbindung herstellen.

Interne Authentifizierung unter UNIX konfigurieren

1. Erstellen Sie eine Gruppe für Benutzer, die eine Verbindung zur Server-Software herstellen. Es wird empfohlen, die Gruppe **statisticsz** zu benennen.
2. Ein Mitglied dieser Gruppe muss die Server-Software installieren. Dieser Benutzer ist der Eigner des Server-Software-Dämons.
3. Ein anderes Mitglied dieser Gruppe (anders als der Dämoneigner und normalerweise der Benutzer, der die Benutzer der Server-Software verwaltet) erstellt eine Datei *statisticsusers* im Verzeichnis *config* im Installationsverzeichnis der Server-Software. Diese Datei sollte Schreib-/Lesezugriff für den Benutzer haben, der sie erstellt hat. Sie sollte Lesezugriff für die Benutzergruppe haben. Andere Benutzer soll-

ten nicht darauf zugreifen können. Wenn Sie diese Datei nicht manuell erstellen, wird sie automatisch erstellt, wenn Sie das Befehlszeilentool `statisticsuser` zum ersten Mal ausführen (siehe nächsten Schritt). Das Befehlszeilentool legt die entsprechenden Berechtigungen fest.

4. Verwenden Sie im Verzeichnis `config` das Befehlszeilentool `statisticsuser`, um Benutzer hinzuzufügen. Geben Sie als der Benutzer, der die Datei `statisticsusers` erstellt hat, `statisticsuser <username>` ein, um einen regulären Benutzer zu erstellen (z. B. `statisticsuser jdoe`). Verwenden Sie die Option `-a`, um einen Benutzer mit Administratorberechtigung zu erstellen (z. B. `statisticsuser -a jdoe`). Das Befehlszeilentool `statisticsuser` fordert Sie zur Eingabe eines Kennworts auf. Ein Endbenutzer gibt den Benutzernamen und das Kennwort ein, um eine Verbindung zur Server-Software herzustellen. Stellen Sie sicher, dass der Benutzername und die Kennwörter entsprechend verteilt werden. Verwenden Sie zum Löschen eines Benutzers die Option `-d` (z. B. `statisticsuser -d jdoe`).
5. Öffnen Sie die als Eigner des Server-Software-Dämons angemeldete Konfigurationsdatei (z. B. `statisticsd.conf`) in einem Texteditor.
6. Suchen Sie das Element `userauth` und ändern Sie den Parameter `value` von `unix` in `internal`.
7. Starten Sie den Server, der als Eigner des Server-Software-Dämons angemeldet ist.

Interne Authentifizierung unter Windows konfigurieren

1. Bearbeiten Sie den Eintrag IBM SPSS Statistics Server so, dass er als bestimmter Benutzer ausgeführt wird:
 - a. Öffnen Sie die Windows-Dienstanzeige und doppelklicken Sie auf den Eintrag für *IBM SPSS Statistics NN.m*, wobei *NN* die Hauptversionsnummer und *m* die Nebenversionsnummer ist.
 - b. Klicken Sie auf die Registerkarte **Anmelden**.
 - c. Wählen Sie unter **Anmelden als** die Option **Dieses Konto** aus.
 - d. Geben Sie die Domäne \Benutzername und das Kennwort des Benutzers ein, der Eigner des Serverprozesses ist. Dieser Benutzer benötigt die Berechtigung *Anmelden als Dienst*.
2. Derselbe Benutzer muss eine Datei `statisticsusers` im Verzeichnis `config` im Installationsverzeichnis der Server-Software erstellen. Diese Datei sollte Schreib-/Lesezugriff für den Benutzer haben, der sie erstellt hat. Keine anderen Benutzer sollten Schreibzugriff haben. Wenn Sie diese Datei nicht manuell erstellen, wird sie automatisch erstellt, wenn Sie das Befehlszeilentool `statisticsuser` zum ersten Mal ausführen (siehe nächsten Schritt).
3. Verwenden Sie im Verzeichnis `config` das Befehlszeilentool `statisticsuser`, um Benutzer hinzuzufügen. Geben Sie als Benutzer, der die Datei `statisticsusers` erstellt hat, `statisticsuser <Benutzername>` ein, um einen regulären Benutzer zu erstellen (z. B. `statisticsuser jdoe`). Verwenden Sie die Option `-a`, um einen Benutzer mit Administratorberechtigung zu erstellen (z. B. `statisticsuser -a jdoe`). Das Befehlszeilentool `statisticsuser` fordert Sie zur Eingabe eines Kennworts auf. Ein Endbenutzer gibt den Benutzernamen und das Kennwort ein, um eine Verbindung zur Server-Software herzustellen. Stellen Sie sicher, dass der Benutzername und die Kennwörter entsprechend verteilt werden. Verwenden Sie zum Löschen eines Benutzers die Option `-d` (z. B. `statisticsuser -d jdoe`).
4. Wenn Sie als Eigner des Server-Software-Dämons angemeldet sind, öffnen Sie die Konfigurationsdatei (z. B. `statisticsd.conf`) in einem Texteditor.
5. Suchen Sie das Element `userauth` und ändern Sie den Parameter `value` von `win32` in `internal`.
6. Rufen Sie die Windows-Anzeige für Dienste auf und starten Sie den Dienst.

unix2 -authentifizierung Konfigurieren

Die `unix2` -Authentifizierung ermöglicht die Ausführung der Server-Software ohne Rootberechtigung und die Authentifizierung anhand der UNIX-Datei `passwd` mit Standardbenutzerkonten. Eine ausführbare Datei (`suauth`), die mit der Server-Software installiert wird, führt die Authentifizierung durch. Damit sie ordnungsgemäß funktioniert, müssen Sie die erforderlichen Berechtigungen festlegen.

Führen Sie die folgenden Schritte aus, um die `unix2` -Authentifizierung zu konfigurieren:

1. Ändern Sie mithilfe von `setuid` und `setgid` oder der rollenbasierten Zugriffssteuerung (RBAC) die Berechtigungen der ausführbaren Datei `suauth` so, dass der Benutzer, der den Server-Software-Dämon ausführt, über die erforderlichen Rootberechtigungen verfügt. Dieser Benutzer muss in der Lage sein, den Benutzer anhand der Datei `passwd` zu authentifizieren und die Benutzer-ID und Gruppen-ID des generierten Serverprozesses für jeden Endbenutzer zu ändern. Es folgen Details zum Festlegen von Berechtigungen. Beachten Sie, dass Sie *entweder* `setuid/setgid` *oder* RBAC verwenden. Verwenden Sie nicht beide Methoden.
2. Öffnen Sie die Konfigurationsdatei (z. B. `statisticsd.conf`) in einem Texteditor.
3. Suchen Sie das Element `userauth` und ändern Sie den Parameter `value` von `unix` in `unix2`.
4. Starten Sie den Server, der als Eigner des Server-Software-Dämons angemeldet ist.

Berechtigungen mit `setuid` und `setgid` festlegen

1. Erstellen Sie eine Gruppe für den Benutzer, der die Server-Software ausführen soll. Es wird empfohlen, die Gruppe **statistics** zu benennen. Es wird außerdem empfohlen, die Gruppenzugehörigkeit auf den Benutzer zu beschränken, der den Server-Software-Dämon ausführt.
2. Ein Mitglied dieser Gruppe muss die Server-Software installieren. Dieser Benutzer ist der Eigner des Server-Software-Dämons.
3. Starten Sie eine Terminalsitzung als `root`.
4. Wechseln Sie in das Verzeichnis `bin` im Installationsverzeichnis der Server-Software.
5. Ändern Sie den Eigner der Datei `suauth` in `root`.

```
chown root suauth
```

6. Fügen Sie die `setuid`- und `setgid`-Bits zu `suauth` hinzu. Diese Bits ermöglichen es dem Benutzer in der Installationsgruppe, die Datei auszuführen und vorübergehend als `root` auszuführen. Rootberechtigungen sind aus den zuvor in diesem Abschnitt genannten Gründen erforderlich.

```
chmod 6550 suauth
```

7. Beenden Sie `root` und melden Sie sich als Eigner des Server-Software-Dämons an.

Festlegen von Berechtigungen mit rollenbasierter Zugriffssteuerung

Sie sollten auch in der Lage sein, die rollenbasierte Zugriffssteuerung (RBAC) zu verwenden, um die erforderlichen Berechtigungen festzulegen. Informationen finden Sie in der RBAC-Dokumentation Ihres Anbieters. Sie müssen Folgendes ausführen:

1. Erstellen Sie eine Autorisierung für die ausführbare Datei `suauth`.
2. Erstellen Sie eine Rolle für diese Berechtigung.
3. Ordnen Sie der Rolle den Eigner des Server-Software-Dämons zu.
4. Konfigurieren Sie die Berechtigung, um die folgenden Berechtigungen zuzulassen:
 - Lesen Sie die Datei `passwd`.
 - Benutzer-ID ändern.
 - Gruppen-ID ändern.

Single Sign-on (SSO) konfigurieren

Sie können Single Sign-on verwenden, um eine Verbindung zu einem Server herzustellen, der auf einer beliebigen unterstützten Plattform ausgeführt wird. Sie müssen zuerst Ihren IBM SPSS Statistics -Server, den IBM SPSS Statistics -Client und die IBM SPSS Collaboration and Deployment Services -Maschinen konfigurieren. Die interne Authentifizierung ermöglicht die Ausführung der Server-Software ohne Rootberechtigung.

Wenn Sie Single Sign-On verwenden, um die Verbindung sowohl zu IBM SPSS Statistics Server als auch zu IBM SPSS Collaboration and Deployment Services herzustellen, müssen Sie zuerst die Verbindung zu IBM

SPSS Collaboration and Deployment Services herstellen, bevor Sie die Verbindung zu IBM SPSS Statistics Server herstellen.

Zur Interaktion mit den meisten modernen, sicheren Active Directory-Installationen müssen Sie das Softwarepaket für starke Verschlüsselung für Java installieren, da die erforderlichen Verschlüsselungsalgorithmen nicht standardmäßig unterstützt werden. Sie müssen das Softwarepaket für den Client und den Server installieren. Eine Fehlermeldung wie `Illegal key size` (Unzulässige Schlüsselgröße) wird auf dem Client angezeigt, wenn eine Serververbindung aufgrund eines nicht installierten Softwarepakets fehlschlägt. Siehe „[Installieren der Verschlüsselung mit unbegrenzter Stärke](#)“ auf Seite 40.

Anmerkung: Bevor Sie SPSS Statistics Server-, SPSS Statistics -Client- und IBM SPSS Collaboration and Deployment Services -Maschinen für Single Sign-on konfigurieren, müssen Sie sicherstellen, dass die Maschinen Zugriff auf den Domänencontroller-Server haben.

Informationen zur Konfiguration von IBM SPSS Collaboration and Deployment Services für Single Sign-on finden Sie unter [IBM SPSS Collaboration and Deployment Services -SSO-Services-Übersicht](#).

Server für Single Sign-on konfigurieren

Server unter Windows konfigurieren

1. Stellen Sie sicher, dass die Windows-Servermaschine Mitglied der AD-Domäne (Active Directory) ist.
2. Suchen Sie im Installationsverzeichnis von IBM SPSS Statistics Server nach dem Ordner `config`.
3. Erstellen Sie im Ordner `config` einen Unterordner namens `sso`.
4. Erstellen Sie im Ordner `sso` die Datei `krb5.conf`. Anweisungen zum Erstellen der Datei `krb5.conf` finden Sie unter http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html.
Nachfolgend sehen Sie ein Beispiel für eine Datei `krb5.conf` :

```
[libdefaults]
    default_realm = STATISTICSSSO.COM
    dns_lookup_kdc = true
    dns_lookup_realm = true

[realms]
    STATISTICSSSO.COM = {
        kdc = statisticssso.com:88
        admin_server = statisticssso.com:749
        default_domain = STATISTICSSSO.COM
    }

[domain_realm]
    .statisticssso.com = STATISTICSSSO.COM
```

Server unter UNIX konfigurieren

Zum Konfigurieren von Single Sign-on für UNIX-Servermaschinen können Sie die UNIX-Maschine zur Windows AD-Domäne hinzufügen und anschließend die Anweisungen zum Konfigurieren von Single Sign-on unter Windows befolgen. Alternativ können Sie die folgenden Schritte ausführen:

1. Erstellen Sie einen Domänenbenutzeraccount für die UNIX-Maschine.
2. Ändern Sie den Hostnamen. Wenn Sie RedHat Linux verwenden, öffnen Sie die Datei `/etc/sysconfig/network` und ändern Sie `HOSTNAME` in das Format `<name>.<realm>`. Dies ermöglicht es AD, die Serverberechtigungsnachweise zu finden.
3. Führen Sie einen der folgenden Schritte aus, um den DNS-Server für die Suche nach der UNIX-Maschine zu aktivieren:
 - Öffnen Sie die Datei `%windows%/system32/drivers/etc/hosts` und fügen Sie die IP-Adresse/Hostzuordnung hinzu. Beispiel:

```
192.168.1.102 test.statisticssso.com test
```

Oder

- Fügen Sie einen neuen Reverse-Lookup-Zoneneintrag hinzu. Dadurch wird eine IP/Host-Zuordnung auf dem DNS-Server hinzugefügt.

Wenn der DNS-Eintrag für die UNIX-Maschine nicht korrekt ist, können Sie den Reverse-Lookup-Eintrag manuell auf dem DNS-Server hinzufügen.

Client für Single Sign-on konfigurieren

Diese Schritte gelten für alle Clients mit Ausnahme der Schritte, auf die speziell für Windows hingewiesen wird.

1. Stellen Sie sicher, dass die lokale Windows-Maschine, auf der IBM SPSS Statistics ausgeführt wird, ein Mitglied der AD-Domäne (Active Directory) ist.
2. Fügen Sie den Domänenbenutzer als Administrator auf der lokalen Maschine hinzu.
3. Aktivieren Sie Windows für den Zugriff auf den TGT-Sitzungsschlüssel:
 - a. Klicken Sie im Menü **Start** auf **Ausführen**.
 - b. Geben Sie `regedit` ein und klicken Sie auf **OK**, um den **Registry-Editor** zu öffnen.
 - c. Navigieren Sie zur folgenden Registry-Position:


```
My Computer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
```
 - d. Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Neu > DWORD** aus. Der Name des neuen Wertes sollte `allowtgtsessionkey` lauten.
 - e. Setzen Sie den Wert für `allowtgtsessionkey` auf den Hexadezimalwert `1`, also `0x0000001`.
 - f. Schließen Sie den **Registrierungseditor**.
 - g. Führen Sie `kinit.exe` aus, das sich in `<IBM SPSS Statistics installation location>\jre\bin` befindet.
4. Erstellen Sie im Ordner `config` des IBM SPSS Statistics-Installationsverzeichnisses den Ordner `sso`.
5. Kopieren Sie die Datei `krb5.conf` vom Server in den Ordner `sso`.
6. Starten Sie die Clientmaschine und die Servermaschine neu.

Service Principle Name (SPN) registrieren

Jede Serverinstanz muss zur eigenen Identifizierung einen eindeutigen *Namen des Service-Principals* (SPN - Service Principal Name) registrieren und der Client muss denselben SPN angeben, wenn er eine Verbindung zum Server herstellt.

Ein SPN für eine Instanz der Server-Software hat folgendes Format:

```
statisticsserver/<host>:<port>
```

Beispiel:

```
statisticsserver/jdoemachine.ibm.com:3023
```

Beachten Sie, dass der Hostname mit seiner DNS-Domäne qualifiziert werden muss (in diesem Beispiel `ibm.com`) und die Domäne dem Kerberos -Realm zugeordnet werden muss.

Die Kombination aus Hostname und Portnummer stellt die Eindeutigkeit des SPN sicher (da jede Instanz auf einem Host auf einem anderen Port empfangsbereit sein muss). Da sowohl Client als auch Server bereits Hostnamen und Portnummer aufweisen, sind sie in der Lage, den jeweiligen SPN für die Instanz zu bilden. Als zusätzlicher Konfigurationsschritt muss der SPN in der Kerberos-Datenbank registriert werden.

Registrieren des SPN unter Windows

Wenn Sie Active Directory als Kerberos-Implementierung nutzen, verwenden Sie den Befehl `setspn`, um den SPN zu registrieren. Zum Ausführen des Befehls müssen die folgenden Bedingungen erfüllt sein:

- Sie müssen an einem Domänencontroller angemeldet sein
- Sie müssen die Eingabeaufforderung mit erweiterten Berechtigungen (als Administrator) ausführen
- Sie müssen ein Mitglied der Gruppe der Domänenadministratoren sein (oder über die entsprechende, Ihnen von einem Domänenadministrator delegierte Berechtigung verfügen)

Weitere Informationen finden Sie in den folgenden Artikeln:

- [Referenz für Setspn-Befehlszeile](#)
- [Delegating Authority to Modify SPNs](#)

Für die Standardinstanz, die am Standardport (z. B. 3023 für Version 23) empfangsbereit ist und unter dem Konto des lokalen Systems ausgeführt wird, müssen Sie den SPN für den Namen des Servercomputers registrieren. Beispiel:

```
setspn -s statisticsserver/jdoemachine.spss.com:3023 jdoemachine
```

For each subsequent server instance, listening on a custom port (for example, 3099) and running under an arbitrary user account (for example, johndoe) with the option userauth set to `internal` (that is, using internal authentication), you must register the SPN against the service user account name:

```
setspn -s statisticsserver/jdoemachine.spss.com:3099 jdoe
```

Beachten Sie, dass in diesem Fall (wenn als Dienstkonto nicht "Lokales System" verwendet wird), es nicht ausreicht, den SPN zu registrieren, damit ein Client eine Verbindung herstellen kann. Weitere Konfigurationsschritte werden im nächsten Abschnitt beschrieben.

So zeigen Sie die für das Konto `jdoe` registrierten SPNs an:

```
setspn -l jdoe
```

Registrieren des SPN unter UNIX

Wenn Sie Active Directory als Kerberos -Implementierung verwenden, verwenden Sie den Befehl `setspn` wie im vorherigen Abschnitt zu Windows beschrieben. Dies setzt voraus, dass Sie den Computer oder den Benutzeraccount bereits im Verzeichnis erstellt haben. Sie können auch bei Bedarf mit `ktpassexperimentieren` (siehe [Ktpass-Befehlszeilenreferenz](#)).

Wenn Sie eine andere Kerberos -Implementierung verwenden, verwenden Sie Ihr bevorzugtes Kerberos -Verwaltungstool, um den Service-Principal zur Kerberos -Datenbank hinzuzufügen. Um den SPN in einen Kerberos-Principal umzuwandeln, müssen Sie den Namen des Kerberos-Realms anhängen. Beispiel:

```
statisticsserver/jdoemachine.ibm.com:3023@ibm.com
```

Fügen Sie diesen Principal und das Kennwort dem Chiffrierschlüssel des Servers hinzu. Der Chiffrierschlüssel muss für jede auf dem Host ausgeführte Instanz einen Eintrag enthalten.

SSO bei Ausführung als Nicht-Root/System konfigurieren

Wenn der Server-Service/Dämon als beliebiger Benutzer ausgeführt wird (nicht Root unter UNIX und nicht System unter Windows), müssen Sie den Service-/Dämonaccount registrieren. Sie benötigen den SPN, den Sie zuvor erstellt haben.

1. Erstellen Sie das Verzeichnis `<STATISTICSSERVER>\config\sso`.
2. Kopieren Sie die Datei `krb5.conf` aus dem Client-SSO-Verzeichnis in das in Schritt 1 erstellte Server-SSO-Verzeichnis.
3. Erstellen Sie mithilfe des folgenden Befehls die Datei `krb5.keytab` im SSO-Verzeichnis des Servers:

```
<STATISTICSSERVER>\jre\bin\ktab -a <spn>@<realm> -k krb5.keytab
```

Beispiel:

```
"..\jre\bin\ktab.exe" -a statisticserver/jdoemachi  
ne.ibm.com:3023@ibm.com  
-k krb5.keytab
```

Daraufhin werden Sie zur Angabe eines Kennworts aufgefordert. Als Kennwort müssen Sie das Kennwort des Dienstkontos eingeben. Beim Dienstkonto jdoe zum Beispiel, müssen Sie das Kennwort für den Benutzer jdoe eingeben.

Das Dienstkonto selbst wird im Chiffrierschlüssel nicht genannt, allerdings haben Sie zuvor den SPN mithilfe von setspn für dieses Konto registriert. Dies bedeutet, der Dienstprincipal und das Dienstkonto haben ein und dasselbe Kennwort.

Für jede neue Serverinstanz, die Sie erstellen, müssen Sie den SPN für diese Instanz (mit setspn) registrieren und eine Chiffrierschlüsseldatei erstellen. Die Chiffrierschlüsseldatei muss in das Unterverzeichnis config_<group_name>/sso im Serverinstallationsverzeichnis kopiert werden. Die Standardinstanz benötigt keine Chiffrierschlüsseldatei.

So prüfen Sie, ob im Chiffrierschlüssel eine Instanz angegeben ist:

```
ktab.exe -l -e -k krb5.keytab
```

Möglicherweise werden für jeden Principal mehrere Einträge mit verschiedenen Verschlüsselungstypen angezeigt, dies ist jedoch normal.

Gruppenzugehörigkeit konfigurieren

Wenn Sie Gruppenberechtigung verwenden, können Sie IBM SPSS Collaboration and Deployment Services so konfigurieren, dass ein LDAP-Provider abgefragt wird, um die Gruppe zu ermitteln, zu der ein authentifizierter Benutzer gehört. Weitere Informationen zur Gruppenberechtigung finden Sie im Abschnitt „Gruppenberechtigung“ auf Seite 31.

Damit die Gruppensuche ordnungsgemäß funktioniert, müssen Sie zunächst Ihr Repository konfigurieren, um einen LDAP-oder Active Directory -Provider hinzuzufügen, und anschließend SSO mit diesem Provider aktivieren.

1. Starten Sie den IBM SPSS Deployment Manager-Client und wählen Sie **Datei > Neu > Verbindung zu verwaltetem Server ...** aus, um eine Verbindung zu einem verwalteten Server für Ihr Repository zu erstellen (falls noch keine vorhanden ist).
2. Melden Sie sich bei der Verbindung zum verwalteten Server an und erweitern Sie den Ordner **Konfiguration**.
3. Klicken Sie mit der rechten Maustaste auf **Sicherheitsprovider**, wählen Sie **Neu > Sicherheitsproviderdefinition ...** aus und geben Sie die entsprechenden Werte ein. Klicken Sie im Dialogfeld auf **Hilfe**, um weitere Informationen zu erhalten.
4. Erweitern Sie den Ordner **Single Sign-on-Provider**, klicken Sie mit der rechten Maustaste auf **Kerberos-SSO-Provider** und wählen Sie **Öffnen** aus.
5. Klicken Sie auf **Aktivieren**, wählen Sie Ihren Sicherheitsprovider aus und klicken Sie dann auf **Speichern**. Sie müssen hier keine weiteren Angaben machen, es sei denn, Sie möchten den SSO nutzen (die Aktivierung des Providers allein reicht aus, um Gruppensuchen zu ermöglichen).

Wichtig: Damit die Gruppensuche ordnungsgemäß funktioniert, müssen Sie hier den gleichen Kerberos-Provider konfigurieren, der auch für IBM SPSS Statistics Server konfiguriert wurde. Insbesondere ist zu beachten, dass die Provider innerhalb desselben Kerberos-Realms eingesetzt werden müssen. Wenn sich ein Benutzer über SSO am Server anmeldet und ihn als jdoe@ibm.com identifiziert (wobei ibm.com der Realm ist), erwartet der Sicherheitsprovider in IBM SPSS Collaboration and Deployment Services, dass er diesen Benutzerprinzipalnamen erkennt und die entsprechende Gruppenzugehörigkeit aus dem LDAP-Verzeichnis zurückgibt.

SSO für Datenquellen konfigurieren

In IBM SPSS Statistics haben Sie die Möglichkeit, über Single Sign-on eine Verbindung zu Datenbanken herzustellen. Wenn Sie eine Datenbankverbindung über Single Sign-on erstellen wollen, müssen Sie zuerst mithilfe Ihrer ODBC-Verwaltungssoftware eine Datenquelle und ein Single-Sign-on-Token ordnungsgemäß konfigurieren. Wenn dann in IBM SPSS Statistics eine Verbindung zu einer Datenbank hergestellt wird, verwendet IBM SPSS Statistics dieses Single-Sign-on-Token und der Benutzer wird nicht aufgefordert, sich an der Datenquelle anzumelden.

Wurde die Datenquelle jedoch nicht ordnungsgemäß für Single Sign-on konfiguriert, fordert IBM SPSS Statistics den Benutzer auf, sich an der Datenquelle anzumelden. Nach Angabe der gültigen Berechtigungsnachweise kann der Benutzer weiter auf die Datenquelle zugreifen.

Detaillierte Informationen zur Konfiguration von ODBC-Datenquellen auf Ihrem System bei aktiviertem Single Sign-on finden Sie in der Dokumentation Ihres Datenbankanbieters. Nachfolgend sind beispielhaft allgemeine Schritte aufgeführt, die möglicherweise durchzuführen sind:

1. Konfigurieren Sie Ihre Datenbank so, dass sie Kerberos-Single Sign-on unterstützt.
2. Erstellen Sie auf der Servermaschine eine ODBC und testen Sie sie. Für die DSN-Verbindung sollte keine Benutzer-ID und kein Kennwort benötigt werden.
3. Stellen Sie über Single Sign-on eine Verbindung zum Server her und beginnen Sie mit der Verwendung der in Schritt 2 erstellten ODBC -Datenquelle.

Berechtigungen

Wenn Sie keine interne Authentifizierung oder Gruppenberechtigung mit Single Sign-on verwenden, startet die Server-Software einen Prozess für den Endbenutzer und übergibt die Benutzer-ID und das Kennwort an das Betriebssystem. Der gestartete Prozess verfügt über die Dateizugriffsberechtigungen des Endbenutzeraccounts. Ein Benutzer, der eine Verbindung zur Server-Software herstellt, muss sich mit einem Konto anmelden, das über die folgenden Berechtigungen verfügt:

- Lese- und Ausführungsberechtigungen für das Installationsverzeichnis des Servers und dessen Unterverzeichnisse
- Lese-, Ausführungs- und Schreibberechtigungen für die Verzeichnisposition für temporäre Dateien

Für die interne Authentifizierung und die einmalige Anmeldung verfügt der verbindende Clientbenutzer über die Berechtigungen, die dem Benutzer zugeordnet sind, der den Service/Dämon gestartet hat.

Sie können die Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird) verwenden, um die Standardposition der temporären Dateien zu ändern. Weitere Informationen finden Sie im Abschnitt zu Dateipositionen im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Sie können auch die Position einzelner Benutzer oder Gruppen ändern. Weitere Informationen finden Sie im Abschnitt IBM SPSS Statistics Server im *Deployment Manager Benutzerhandbuch*.

Berechtigungen auf Administratorebene

Standardmäßig ist die Administratorgruppe für die Server-Software die Administratorgruppe für die Maschine, auf der die Server-Software ausgeführt wird. Sie können die Administratorgruppe für die Server-Software ändern, indem Sie sie im Textfeld 'Admin Group' (Verwaltungsgruppe) in der Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird) angeben. Weitere Informationen finden Sie im Abschnitt "Benutzer" im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Wenn Sie die interne Authentifizierung unter UNIX verwenden, können Sie Administratoren direkt erstellen. Weitere Informationen finden Sie im Thema „Interne Authentifizierung konfigurieren“ auf Seite 24.

Gruppenberechtigung

Sie können die Server-Software für die Unterstützung von Gruppenberechtigungen konfigurieren. Für jede berechtigte Benutzergruppe wird eine separate Instanz des Service/Dämons ausgeführt.

Konfigurieren von Gruppenberechtigung

1. Erstellen Sie für jede Gruppe eine Serverinstanz. Weitere Informationen zum Erstellen von Serverinstanzen finden Sie in „[Mehrere Instanzen konfigurieren](#)“ auf Seite 19.
2. Erstellen Sie die Gruppen in IBM SPSS Collaboration and Deployment Services und weisen Sie den Gruppen Benutzer zu.
3. Öffnen Sie die Verwaltungsanwendung und aktualisieren Sie den Wert von **Gruppenautorisierungs-service-URL** mit der URL für IBM SPSS Collaboration and Deployment Services. Stellen Sie sicher, dass Sie die Portnummer einschließen (z. B. `http://myserver.mydomain.com:9080`).

Steuern des DSN-Zugriffs nach Gruppe

Bei der Mehrfaktorauthentifizierung (MFA - Multi-Factor Authentication) muss das Set an ODBC-Datenquellennamen (DSN - Data Source Name), auf das Benutzer je nach ihrer Gruppenzugehörigkeit Zugriff haben, eingeschränkt werden können.

1. Öffnen Sie die Verwaltungsanwendung und setzen Sie **Datenbankzugriff beschränken** auf Ja.
2. Geben Sie in das Feld **Zulässige Datenbankenquellen** eine durch Semikolons (;) begrenzte Liste mit Namen der Datenquellen ein, die zum Zugriff berechtigt sind (z. B. `Betrug - Analyse;Betrug - Betrieb`).

Wenn diese Einschränkung angewendet wird, führt dies zu folgenden Ergebnissen:

- Wenn ein Benutzer im Datenbankassistenten nach Datenquellen sucht, werden ihm nicht alle auf dem Serversystem definierten Datenquellennamen angezeigt, sondern nur das von der Verwaltungsanwendung definierte Subset der Datenquellennamen. Beachten Sie, dass der Pfad möglicherweise Datenquellennamen enthält, die nicht auf dem Server definiert sind. Diese werden ignoriert und dem Benutzer werden diese Namen nicht angezeigt.
- Wenn ein Benutzer die `GET DATA /TYPE=ODBC` -Syntax ändert, die einen DSN angibt, der nicht von der Verwaltungsanwendung angegeben wird, wird die Syntax nicht ausgeführt und dem Benutzer wird ein Fehler ähnlich dem folgenden angezeigt: **Zugriff verweigert auf Datenquelle: < X >**.

Profile

Mit der Server-Software können Sie Profile einzelner Benutzer und Benutzergruppen erstellen. Mit diesen Benutzerprofilen und Gruppen können Sie Einstellungen für bestimmte Benutzer definieren.

Client-und Serverversionen

Ab Version 20.0.1 muss die Client-Software nicht dasselbe Release-Level aufweisen wie die Server-Software, zu der sie eine Verbindung herstellt. Der Client der Version 20.0.1 kann beispielsweise eine Verbindung zur 21 Server-Software und der Client der Version 21 eine Verbindung zu einem Server der Version 20.0.1 herstellen. Beachten Sie, dass Sie auch mehrere Versionen der Server-Software auf einem Server-Computer ausführen können.

Das Mischen von Release-Levels ist nur zur Vereinfachung von Upgrades zulässig. Release-Level können während des Upgradezeitraums gestaffelt werden und Clients müssen nicht gleichzeitig aktualisiert werden. Es wird jedoch nicht empfohlen, diese Konfiguration über längere Zeit beizubehalten. Wenn der Server neuer ist als der Client, erstellt er möglicherweise Ausgaben, die nicht vom Client gelesen werden können. Wenn der Client neuer ist als der Server, wird die vom Client übermittelte Syntax möglicherweise nicht vom Server erkannt. Daher sollten Sie ein Upgrade für die Client-oder Server-Software so schnell wie möglich durchführen, je nachdem, welche Version dem anderen entspricht.

Wenn Sie Verbindungsinformationen an Endbenutzer verteilen, denken Sie daran, welche Version der Client-Software ausgeführt wird, und stellen Sie sicher, dass sie über die Verbindungsinformationen für eine übereinstimmende Serverversion verfügen.

Benutzer über eine Firewall verbinden

Wenn Sie eine **Firewall** verwenden, um Ihr Netz vor Eindringlingen zu schützen, können Sie Ihre Firewall und die Server-Software so konfigurieren, dass Endbenutzer außerhalb der Firewall den Client mit der Server-Software verbinden können. Ihre Firewall kann **NAT** (Network Address Translation) verwenden, dies ist jedoch nicht erforderlich.

Das typische Szenario für die Verbindung von Endbenutzern über eine Firewall, die NAT verwendet, sieht wie folgt aus:

1. Der Endbenutzer verbindet die Clientanwendung mit der Server-Software unter Verwendung der **maskierten IP** (der IP-Adresse, die NAT nach außen darstellt) und der Portnummer des Servers. Der Endbenutzer stellt beispielsweise eine Verbindung mit IP 10.10.10.2 und der Portnummer 3016 her.
2. Die Firewall lässt die Verbindung zu, da sie so konfiguriert wurde, dass Verbindungen von der maskierten IP-Adresse akzeptiert werden.
3. Die Firewall leitet die maskierte IP an die reale interne IP des Servers um. Die Verbindung wird zugelassen, da der Port (z. B. 3016) in der Firewall aktiviert ist.
4. Der Server generiert einen Prozess für die Clientverbindung des Endbenutzers und ordnet ihm eine Portnummer aus der Liste in der Systemumgebungsvariablen `STATISTICS_CLIENT_PORTS` zu. Der Prozess kommuniziert beispielsweise über Port 3287.
5. Die Firewall ermöglicht die Kommunikation über diesen Port (z. B. 3287), weil sie in der Firewall aktiviert ist.

Verbindungen über eine Firewall konfigurieren

Einführung

Der IBM SPSS Statistics -Server verwendet dieselbe Portnummer für Clientverbindungen. Dies bedeutet, dass nur zwei Ports über die Firewall offen sein müssen: der SPSS Statistics -Dämon oder der Empfangsport (standardmäßig 3028, kann aber bei Bedarf geändert werden) und der Antwortport, über den SPSS Statistics -Clients mit ihren untergeordneten SPSS Statistics Server-Prozessen kommunizieren.

Anmerkung: Die Wiederverwendung von Ports ist an die Funktion zur Wiederherstellung der Clientverbindung gebunden. Standardmäßig ist `client-reconnect` für 100 Sekunden aktiviert. Wenn Clientwiederverbindung aktiviert ist, hat SPSS Statistics Server ein 1:1-Verhältnis von verbundenen Clients zu offenen Antwortports. Um die Wiederverwendung von Ports zu ermöglichen, müssen Sie zuerst die Option `client-reconnect` inaktivieren. Bearbeiten Sie dazu die Einstellung **reconnect-timeout** in `<Statistics Install Path>/config/statisticsd.conf`. Beispiel:

```
<reconnect-timeout desc="The timeout in minutes that the server uses to drop disconnected clients (default: 100)." value="0"/>
```

In einer Umgebung mit vielen möglichen Client/Server-Verbindungen können Sie mehrere Clientantwortports konfigurieren. Wenn ein SPSS Statistics -Client gerade eine Verbindung zum SPSS Statistics -Server herstellt, ist der Client-Port im Wesentlichen gesperrt und kann nur von einem Client verwendet werden, bis der Verbindungsprozess abgeschlossen ist. Die Verbindungsdauer liegt im Bereich von 1 bis 3 Sekunden (diese Zeit kann je nach Systembelastung variieren). Wenn ein zweiter oder dritter SPSS Statistics -Client versucht, während dieser Zeit eine Verbindung herzustellen, werden die Clients blockiert, bis der Client-Port verfügbar ist. Das Öffnen mehrerer Client-Ports verringert die Wartezeit beim Herstellen einer Verbindung in einer Umgebung, in der viele Benutzer gleichzeitig SPSS Statistics -Sitzungen einleiten.

Beispiel

Angenommen, in der Systemumgebungsvariablen **STATISTICS_CLIENT_PORTS** sind fünf Client-Ports aufgelistet (Ports 40001-40005) und es gibt vier mögliche Clients. Ein Benutzer leitet eine Verbindung zum SPSS Statistics -Server ein und der erste Kontakt wird über den Empfangsport (3028) hergestellt.

Der Server generiert einen untergeordneten Prozess und setzt die Kommunikation über den ersten verfügbaren Client-Port (4001) fort. Wenn Port 40001 nicht gesperrt ist (weil die Kommunikation mit einem anderen Client gerade gestartet wurde) wird der Port wiederverwendet. Wenn Port 40001 gesperrt ist, wird die Kommunikation mit dem nächsten Port (4002) fortgesetzt, vorausgesetzt, er ist nicht gesperrt usw.

Nachdem alle vier Clients verbunden sind, verwenden sie wahrscheinlich alle dieselbe Portnummer (40001). Es besteht eine geringe Chance, dass ein oder mehrere Clients Port 40002 verwenden, eine geringere Chance, dass ein Client Port 40003 verwendet, und eine noch geringere Chance, dass ein oder mehrere Clients Port 40004 verwenden. Es besteht keine Chance, dass ein Client Port 40005 verwendet, da es nur vier Clients gibt und der Algorithmus bei der ersten verfügbaren Portnummer beginnt, die in der Systemumgebungsvariablen `STATISTICS_CLIENT_PORTS` aufgelistet ist.

Es gibt zwei empfohlene Methoden zum Konfigurieren von SPSS Statistics -Serververbindungen durch eine Firewall.

Firewall so konfigurieren, dass Prozesse zugelassen werden

Stellen Sie mithilfe Ihrer Firewall-Software sicher, dass die folgenden Prozesse Netzverbindungen akzeptieren dürfen.

statisticsproc.exe

Der Prozess `statisticsproc.exe` öffnet, schließt und verwendet die Antwortports (oder Ports, die in `STATISTICS_CLIENT_PORTS` definiert sind).

statisticssrvr.exe (Microsoft Windows) oder statisticsd (UNIX oder Linux)

Der Prozess ist der Windows-Hauptdienst oder der UNIX/Linux -Dämon und verwaltet den Empfangsport.

Die Bereitstellung des Zugriffs auf die Prozesse ermöglicht effektiv jeden Port, den der Prozess verwendet wird.

Anmerkung: Die folgenden Bedingungen gelten, wenn das Zeitlimit für die Verbindungswiederholung größer als 0 ist und `statisticsproc.exe` Netzverbindungen akzeptieren darf:

- `STATISTICS_CLIENT_PORTS` ist außer bei Diagnoseprogrammen irrelevant. Jeder Port kann verwendet werden.
- Es gibt keine Begrenzung für die Anzahl der Verbindungen, sofern keine Ports in `STATISTICS_CLIENT_PORTS` definiert sind. Die Anzahl der definierten `STATISTICS_CLIENT_PORTS` -Ports begrenzt effektiv die von SPSS Statistics Server verwendeten Ports.

Firewall durch manuelles Öffnen von Ports konfigurieren

Gehen Sie wie folgt vor, um die Server-Software und die Firewall manuell zu konfigurieren:

1. Installieren Sie die Server-Software wie gewohnt. Sie müssen die IP-Adresse des Computers, auf dem der Server installiert ist, sowie die Portnummer kennen, die die Server-Software für die Kommunikation verwendet. Installieren Sie beispielsweise den Server unter `202.123.456.78` am Empfangsport `3028`.
2. Konfigurieren Sie die Systemumgebungsvariable `STATISTICS_CLIENT_PORTS`, indem Sie mindestens eine Portnummer angeben. Die Umgebungsvariable listet die Ports auf, die verwendet werden, um Clientverbindungen zum Server fortzusetzen (**RESPONSE** -Ports). Bei Bedarf können Sie eine durch Kommas begrenzte Liste und einen Portbereich angeben (z. B. `4001, 4002, 4003-4005`).

Wichtig:

- Wenn Sie das Zeitlimit für die automatische Verbindungswiederholung auf einen Wert größer als 0 setzen, definiert `STATISTICS_CLIENT_PORTS` die maximale Anzahl zulässiger gleichzeitiger Client- und Serververbindungen.
- Listen Sie den Port **LISTEN** (3028) nicht in der Umgebungsvariablen `STATISTICS_CLIENT_PORTS` auf.

Microsoft® Windows™

Verwenden Sie die Windows-Systemeigenschaften, um die Umgebungsvariable zu erstellen und zu konfigurieren. Anweisungen finden Sie in „Systemeigenschaften“ auf Seite 55 .

platform="unix " scale="80">CrtCDSresources.sh

Bearbeiten Sie das Umgebungsript statsenv . shder Server-Software, das sich im Unterverzeichnis /bin des Installationsverzeichnisses befindet. Definieren Sie den Port, der von den Clientprozessen verwendet werden kann, die der Server startet. Fügen Sie beispielsweise die folgenden Zeilen hinzu:

```
STATISTICS_CLIENT_PORTS=4001
```

```
STATISTICS_CLIENT_PORTS exportieren
```

3. Wenn Sie NAT (Network Address Translation, Netzadressumsetzung) verwenden, erstellen und ordnen Sie IPs zu. Erstellen Sie mit Ihrer Firewall-Software eine maskierte IP-Adresse für die externe Verwendung und ordnen Sie sie der internen IP-Adresse des Servers zu. Erstellen Sie beispielsweise eine Maskierungs-IP 10 . 10 . 10 . 2 und ordnen Sie sie 202 . 123 . 456 . 78zu.
4. Aktivieren Sie mithilfe Ihrer Firewall-Software Portnummern in der Firewall:
 - Die **LISTEN** -Portnummer des Servers. Aktivieren Sie beispielsweise Port 3028.
 - Die Portnummern, die Sie in der Umgebungsvariablen STATISTICS_CLIENT_PORTS angegeben haben Aktivieren Sie beispielsweise Port 4001.
5. Verteilen Sie Verbindungsinformationen an die Benutzer, die von außerhalb der Firewall eine Verbindung zur Server-Software herstellen.
 - Falls verwendet, die maskierte IP des Computers, auf dem die Server-Software installiert ist (verteilen Sie nicht die interne IP des Servers). Verteilen Sie beispielsweise 10 . 10 . 10 . 2 als IP-Adresse des Servers.
 - Verteilen Sie die Portnummer der Server-Software wie gewohnt. Verteilen Sie beispielsweise 3028 als **LISTEN** -Portnummer des Servers.

Benutzer mit PPTP verbinden

Endbenutzer können einen fernen Client-Computer mit der Analytic Server-Software mit **Point-to-Point-Tunneling Protocol** (PPTP) verbinden. PPTP ist ein Netzprotokoll, das virtuelle private Netze mit mehreren Protokollen (VPNs) unterstützt. Es ermöglicht fernen Endbenutzern den sicheren Zugriff auf Ihr Netz über das Internet.

PPTP-Verbindungen verwenden:

1. **Konfigurieren Sie einen Fernzugriffsserver für PPTP.** Stellen Sie sicher, dass Sie genügend IP-Adressen für die Clients erstellen, da die Server-Software mehrere Clientverbindungen unterstützt. Für jede Clientverbindung ist eine eigene IP-Adresse erforderlich.
2. **Konfigurieren Sie den Client-Desktop-Computer.** Verwenden Sie die Windows-Netzsteuerkonsole, um eine private Netzverbindung mit PPTP hinzuzufügen. Geben Sie eine IP-Adresse ein, die der Fernzugriffsserver als PPTP-Verbindung erkennt.
3. **Aktivieren Sie die PPTP-Verbindung auf dem Client-Desktop-Computer.** Wenn Endbenutzer von einem fernen Standort aus eine Verbindung zur Server-Software herstellen möchten, aktivieren sie die PPTP-Verbindung und verwenden dann die Client-Software, um wie üblich eine Verbindung zum Server herzustellen.

Verwenden von SSL zur sicheren Datenübertragung

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

Funktionsweise von SSL

SSL beruht auf dem öffentlichen und privaten Schlüssel des Servers sowie einem 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.

Aktivieren von SSL mit GSKit

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

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

1. Beziehen und installieren Sie das SSL-Zertifikat und die Schlüssel.
2. Aktivieren und konfigurieren Sie eine spezielle Konfigurationsdatei, die sich im IBM SPSS Statistics Server-Installationsverzeichnis befindet.

Anmerkung: IBM SPSS Statistics Server unterstützt das Protokoll TLSv1.2. GSKit unterstützt derzeit keine anderen Versionen.

3. Bei Verwendung von Verschlüsselungszertifikaten mit einer Stärke von mehr als 2048 Bit installieren Sie auf den Client-Computern Verschlüsselung mit unbegrenzter Stärke.
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 Repository für Collaboration and Deployment Services aufbaut. In diesem Fall ist IBM SPSS Statistics-Server der *Client*.

Beziehen und Installieren von SSL-Zertifikat und -Schlüssel

Zur Konfiguration der SSL-Unterstützung müssen Sie zuerst die folgenden Schritte durchführen:

1. Beziehen Sie ein SSL-Zertifikat und eine Schlüsseldatei. Es gibt verschiedene Möglichkeiten, dies zu tun:
 - Erwerben Sie Zertifikat und Schlüsseldatei von einer öffentlichen Zertifizierungsstelle (z. B. VeriSign, Thawte oder Entrust). Die öffentliche Zertifizierungsstelle signiert das Zertifikat, um den Server zu verifizieren, der es verwendet.
 - Rufen Sie die Schlüssel- und Zertifikatsdateien von einer unabhängigen Zertifizierungsstelle ab. Bei diesem Ansatz muss das *.pfx -Stammzertifikat der unabhängigen Zertifizierungsstelle in die Key-store-Datei des Servers importiert werden (siehe unten).
 - Generieren Sie Schlüssel- und Zertifikatsdateien mithilfe einer internen Zertifizierungsstelle für selbst signierte Zertifikate. Hierfür sind die folgenden Schritte erforderlich:
 - a. Bereiten Sie eine Schlüsseldatenbank vor. Weitere Informationen finden Sie im Thema [„Erstellen einer SSL-Schlüsseldatenbank“](#) auf Seite 38.
 - b. Erstellen Sie das selbst signierte Zertifikat. Weitere Informationen finden Sie im Thema [„Erstellen eines selbst signierten SSL-Zertifikats“](#) auf Seite 38.

2. Kopieren Sie bei Zertifikaten einer Zertifizierungsstelle (CA) oder selbst signierten Zertifikaten die Dateien `.kdb` und `.sth` aus Schritt 1 in ein Verzeichnis, in das der IBM SPSS Statistics Server Rufen Sie auf und geben Sie den Pfad zu diesem Verzeichnis in der Datei `statisticsd.conf` an. Die Datei `statisticsd.conf` befindet sich in `<Statistics Server installation directory>/config/`. Kopieren Sie für Zertifikate anderer Anbieter die Dateien `.pfx` und `.sth` aus Schritt 1.

3. Legen Sie die folgenden Parameter in der Datei `statisticsd.conf` fest:

Für Zertifizierungsstellen (CA) oder selbst signierte Zertifikate:

- `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, wobei `<value>` entweder 0 oder 1 ist, um anzugeben, ob GSKit aktiviert werden soll.
- `<gsk-keystore desc="GSKSSL Key store database filename." value="<filename>.kdb"/>`, wobei `<filename>` der Name der Schlüsseldatenbankdatei ist.
- `<gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>`, wobei `<filename>` der Name der Kennwort-Stashdatei der Schlüsseldatenbank ist.
- `<gsk-cert-label desc="GSKSSL certificate label." value=""/>`, wobei `<label>` die Bezeichnung Ihres Zertifikats ist.

Für Zertifikate anderer Anbieter:

- `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, wobei `<value>` entweder 0 oder 1 ist, um anzugeben, ob GSKit aktiviert werden soll.
- `<gsk-keystore = "<*.pfx_file_location>"`, wobei `<*.pfx_file_location>` die Position und den Namen der `*.pfx`-Stammzertifikatsdatei ist.
- `<gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>`, wobei `<filename>` der Name der Kennwort-Stashdatei der Schlüsseldatenbank ist.
- `<gsk-cert-label desc="GSKSSL certificate label." value=""/>`, wobei `<label>` die Bezeichnung Ihres Zertifikats ist.

4. Für Zertifikate anderer Anbieter:

a. Extrahieren Sie die Datei `root.pem` aus der Datei `*.pfx`, indem Sie den folgenden GSK-Befehl als Beispiel verwenden:

```
gsk8capi64.exe -cert -extract -db C:\SSL\<certificate_name>.pfx -stashed -label  
<cert-certificate_issuing_server.com> -target C:\SSL\root.pem
```

b. Kopieren Sie `root.pem` in den Ordner `C:\ProgramData\IBM\SPSS\certificates` (Windows) oder `/Library/Application Support/IBM/SPSS/certificates` (macOS) auf dem Client.

c. Legen Sie auf dem Client die Verbindung mit dem vollständig qualifizierten Domännennamen (z. B. `cert-certificate_issuing_server.com`) " im Feld **Servername** fest und aktivieren Sie die Option **SSL**.

5. Für selbst signierte Zertifikate installieren Sie das Zertifikat auf Clientsystemen. Für gekaufte Zertifikate öffentlicher Zertifizierungsstellen oder Zertifikate anderer Anbieter ist dieser Schritt nicht erforderlich. Stellen Sie sicher, dass Zugriffsberechtigungen ein zufälliges Anzeigen des Verzeichnisses verhindern, das das Zertifikat enthält. Weitere Informationen finden Sie im Thema „Installieren eines selbst signierten SSL-Zertifikats“ auf Seite 39.

Konfigurieren der Umgebung für die GSKit-Ausführung

GSKCapiCmd ist ein nicht auf Java basierendes Befehlszeilentool, und Java™ muss nicht auf Ihrem System installiert sein, um dieses Tool zu verwenden. Es befindet sich im Ordner `<Statistics Server installation directory>/bin`. Der Prozess, mit dem Sie Ihre Umgebung für die Ausführung von IBM Global Security Kit (GSKit) konfigurieren, variiert je nach verwendeter Plattform.

Fügen Sie zur Konfiguration für Linux/Unix das Verzeichnis für gemeinsam genutzte Bibliotheken `<Statistics Server installation directory>/lib` zu Ihrer Umgebung hinzu:

```
$export <Shared library path environment variable>=<Statistics_server_install_path>/lib:<Shared library
```

```
path environment variable>
$export PATH=$PATH:<Statistics_server_install_path>/bin
```

Der Variablenname für den Pfad für die gemeinsam genutzte Bibliothek hängt von Ihrer Plattform ab:

- Linux verwendet den Variablennamen LD_LIBRARY_PATH.

Um beispielsweise die Umgebung unter Linux festzulegen, verwenden Sie Folgendes:

```
$export LD_LIBRARY_PATH=/opt/IBM/SPSS/StatisticsServer/25/lib:$LD_LIBRARY_PATH
$export PATH=$PATH:/opt/IBM/SPSS/StatisticsServer/25/bin
```

Kontozugriff auf Dateien

Stellen Sie sicher, dass Sie die richtigen Berechtigungen für die Konten erteilen, die auf die SSL-Dateien zugreifen:

1. Erteilen Sie allen von IBM SPSS Statistics zur Verbindung verwendeten Konten Lesezugriff auf die SSL-Dateien.

Anmerkung: Dies gilt auch für den Benutzer *Anmelden als*, der im IBM SPSS Statistics Server-Service definiert ist. Unter UNIX oder Linux gilt dies für den Benutzer, als der Sie den Server starten.

2. Unter Windows reicht es nicht aus, dass sich die Konten in der Gruppe "Administratoren" befinden und dieser Gruppe die Berechtigung erteilt wird, wenn die Benutzerzugriffssteuerung (UAC - User Access Control) aktiviert ist. Zusätzlich müssen Sie eine der folgenden Aktionen ausführen:

- Erteilen Sie den Konten separat Berechtigungen.
- Erstellen Sie eine neue Gruppe, fügen Sie dieser neuen Gruppe Konten hinzu und erteilen Sie der Gruppe die Berechtigung für den Zugriff auf die SSL-Dateien.
- Inaktivieren Sie UAC.

Erstellen einer SSL-Schlüsseldatenbank

Verwenden Sie das GSKCapiCmd-Tool, um Ihre Schlüsseldatenbank zu erstellen. Vor der Verwendung des Tools müssen Sie Ihre Umgebung konfigurieren (weitere Informationen hierzu finden Sie in „[Konfigurieren der Umgebung für die GSKit-Ausführung](#)“ auf Seite 37).

Um die Schlüsseldatenbank zu erstellen, führen Sie GSKit aus und geben Sie den folgenden Befehl ein:

```
gsk<ver>capiCmd[_64] -keydb -create -populate -db <filename>.kdb -pw <password> -stash
```

Dabei ist <ver> die GSKit-Versionsnummer, <filename> ist der Name, den Sie für die Schlüsseldatenbankdatei verwenden möchten, und <password> ist das Kennwort für die Schlüsseldatenbank.

Die Option `-stash` erstellt im Pfad für die Schlüsseldatenbank eine Stashdatei mit der Dateierweiterung `.sth`. GSKit ruft mithilfe der Stashdatei das Kennwort für die Schlüsseldatenbank ab, sodass es nicht jedes Mal in die Befehlszeile eingegeben werden muss.

Anmerkung: Sie sollten für die Datei `.sth` einen starken Dateisystemschutz verwenden.

Erstellen eines selbst signierten SSL-Zertifikats

Mit dem folgenden Befehl können Sie ein selbst signiertes Zertifikat generieren und in der Schlüsseldatenbank speichern:

```
gsk<ver>capiCmd[_64] -cert -create -db <filename>.kdb -stashed -dn "CN=myserver,OU=mynet[
work,0=mycompany,
C=mycountry" -label <label> -expire <Number of days certificate is valid>
```

Dabei ist <ver> die GSKit-Versionsnummer, <filename> ist der Name der Schlüsseldatenbankdatei, <Number of days certificate is valid> ist die Anzahl der Tage, an denen das Zertifikat gültig ist, und <label> ist eine Beschriftung, mit deren Hilfe Sie die Datei leichter finden (z. B. können Sie eine Beschriftung wie `myselfsigned` verwenden).

Installieren eines selbst signierten SSL-Zertifikats

Für die Clientsysteme, die über SSL eine Verbindung zu Ihrem Server herstellen, müssen Sie den öffentlichen Teil des Zertifikats an die Clients verteilen, damit er in deren Schlüsseldatenbanken gespeichert werden kann. Führen Sie hierzu die folgenden Schritte aus:

Anmerkung: Überspringen Sie diesen Schritt, wenn Sie ein Zertifikat verwenden, das von einer Zertifizierungsstelle signiert wurde. Wenn Sie ein selbst signiertes Zertifikat verwenden, müssen Sie die vertrauenswürdige CA-Datei auf die Client-Computer kopieren. Beachten Sie, dass ein Server-Computer auch als Client agieren kann. Ein Beispiel ist IBM SPSS Statistics-Server, der eine Verbindung zu IBM SPSS Repository für Collaboration and Deployment Services herstellt. In diesem Fall ist der IBM SPSS Statistics-Server der Client. Daher müssen Sie das Zertifikat für den IBM SPSS Repository für Collaboration and Deployment Services-Server auf IBM SPSS Statistics-Server kopieren.

1. Extrahieren Sie den öffentlichen Teil einer Datei mithilfe des folgenden Befehls:

```
gsk<ver>capicmd[_64] -cert -extract -db <filename>.kdb -stashed -label <label> -target root.pem
```

2. Verteilen Sie `root.pem` an die Clients. Wenn Sie mehrere vertrauenswürdige CA-Dateien haben, kopieren Sie diese in eine einzige Datei `root.pem`. Vertrauenswürdige CA-Dateien sind Textdateien, sodass Sie die Zertifikate kopieren und einfügen können. Kopieren Sie `root.pem` an die folgende Position auf den Client-Computern. Wenn Sie bereits für ein anderes IBM Produkt eine Datei `root.pem` auf den Client kopiert haben, fügen Sie den Inhalt der vertrauenswürdigen CA-Datei der vorhandenen Datei `root.pem` hinzu. Standardmäßig suchen alle IBM Clientprodukte an dieser Position nach selbst signierten Zertifikatsdateien. Wenn Sie einen anderen Speicherort verwenden wollen, müssen Sie eine `SSL_CERT_DIR`-Umgebungsvariable erstellen und den Wert der Variablen auf den Speicherort setzen.

- Windows 7 und höher: `C:\ProgramData\IBM\SPSS\certificates`
- Mac OS: `/Library/Application Support/IBM/SPSS/certificates`
- UNIX und Linux: `/opt/IBM/SPSS/certificates`

Clientzertifikate konfigurieren

Wenn SPSS Statistics Server für die Verwendung einer SSL-Verbindung konfiguriert ist und Sie ein selbst signiertes Zertifikat verwenden, müssen Sie die anerkannte Zertifizierungsstelle auf alle Client-Workstations kopieren und konfigurieren.

Ein Beispiel wäre, wenn IBM SPSS Collaboration and Deployment Services einen Job an eine Instanz von SPSS Statistics Server übergibt (in der SSL aktiviert ist). In dieser Situation ist IBM SPSS Collaboration and Deployment Services der Client. Die anerkannte Zertifizierungsstelle (`root.pem` auf SPSS Statistics Server) muss auf alle Maschinen mit IBM SPSS Collaboration and Deployment Services kopiert und konfiguriert werden.

Konfigurieren der Zertifikatsdateien für IBM SPSS Collaboration and Deployment Services

Die Unterstützung von IBM SPSS Collaboration and Deployment Services kann auf einem Webanwendungsserver (zum Beispiel IBM WebSphere und RedHat JBoss EAP) bereitgestellt werden.

Der erste Schritt bei der Konfiguration von Zertifikatsdateien für die IBM SPSS Collaboration and Deployment Services -Unterstützung ist das Abrufen der SPSS Statistics Server `root.pem`-Datei von Ihrem Administrator.

Der Prozess der Konfiguration eines SSL-Zertifikats hängt davon ab, auf welchem Webanwendungsserver die Bereitstellung erfolgt.

IBM WebSphere und RedHat JBoss EAP

Die folgenden Anweisungen gelten sowohl für IBM WebSphere als auch für RedHat JBoss EAP.

Hinweis für RedHat JBoss EAP: Wenn IBM GSKit SSL durch SPSS Statistics Server verwendet wird, müssen Sie das IBM JDK beim Konfigurieren von IBM SPSS Collaboration and Deployment Services auf JBoss EAP verwenden.

1. Verteilen Sie die Datei `root.pem` an die IBM SPSS Collaboration and Deployment Services Server-Maschine. Wenn Sie über mehrere vertrauenswürdige Zertifizierungsstellen verfügen, kopieren Sie sie in eine einzelne `root.pem`-Datei (vertrauenswürdige Zertifizierungsstellen sind Textdateien, sodass Sie die Zertifikate kopieren und einfügen können). Kopieren Sie `root.pem` an die folgende Position auf dem IBM SPSS Collaboration and Deployment Services Server.

Wenn Sie bereits für ein anderes IBM Produkt eine Datei `root.pem` auf den Client kopiert haben, fügen Sie den Inhalt der vertrauenswürdigen CA-Datei der vorhandenen Datei `root.pem` hinzu. Erstellen Sie die Umgebungsvariable `SSL_CERT_DIR` und legen Sie den Wert der Variablen auf die gewünschte Serverposition, die die Datei `root.pem` enthält, fest.

2. Prüfen Sie, ob der IBM SPSS Collaboration and Deployment Services-Serverbenutzer die Umgebungsvariable `SSL_CERT_DIR` hinzufügt.

Anmerkung: Der IBM SPSS Collaboration and Deployment Services-Server muss nach dem Hinzufügen der Umgebungsvariablen erneut gestartet werden.

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.

1. 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`.
2. Ersetzen Sie die vorhandenen Dateien `US_export_policy.jar` und `local_policy.jar` durch die beiden Dateien, die Sie heruntergeladen und extrahiert haben.

Anweisung an Benutzer, SSL zu aktivieren

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

Aktivieren von SSL mithilfe von OpenSSL

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

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

1. Installieren Sie OpenSSL auf dem Server-Computer.
2. Beziehen und installieren Sie das SSL-Zertifikat und die Schlüssel.
3. Aktivieren und konfigurieren Sie SSL in der Serververwaltungsanwendung (IBM SPSS Deployment Manager).

Anmerkung: IBM SPSS Statistics Server unterstützt das TLSv1-Protokoll. SSLv3 weist nachweislich eine Sicherheitslücke auf und sollte daher nicht verwendet werden.

4. Bei Verwendung von Verschlüsselungszertifikaten mit einer Stärke von mehr als 2048 Bit sollten Sie auf den -Client-Computern Verschlüsselung mit unbegrenzter Stärke installieren.
5. Wenn Sie ein selbst signiertes Zertifikat verwenden, kopieren Sie es auf den Client-Computer.
6. Weisen Sie Benutzer an, bei der Verbindung zum Server SSL zu aktivieren.

Anmerkung: Gelegentlich fungiert ein Serverprodukt als Client. Als Beispiel dient der IBM SPSS Statistics Server, der eine Verbindung zum IBM SPSS Repository für Collaboration and Deployment Services herstellt. In this case, IBM SPSS Statistics Server is the *client*.

Installieren von OpenSSL

Wenn OpenSSL noch nicht auf dem Server verfügbar ist, müssen Sie es installieren.

1. Laden Sie OpenSSL von <http://www.openssl.org/> herunter. Stellen Sie sicher, dass Sie die Version von OpenSSL verwenden, die für Ihre Serverversion geeignet ist:

| <i>Tabelle 2. OpenSSL-Versionen</i> | |
|--|--|
| Serverprodukt | Kompatible OpenSSL-Version |
| IBM SPSS Statistics 29 | 1.1.1f oder höher |
| IBM SPSS Statistics 28 | 1.1.1f oder höher |
| IBM SPSS Statistics 27.0.1 | 1.1.1f oder höher Anmerkung: Das unsichere SSLv3 -Protokoll wird nicht mehr unterstützt. |
| IBM SPSS Statistics 26-27 | 1.0.2 oder höher |
| IBM SPSS Statistics 24-25 | 1.0.1f oder höher |
| IBM SPSS Statistics 20-23 | 1.0.0 |
| IBM SPSS Statistics 17-19 (<i>nicht Linux® on System z®</i>) | 0.9.8 und Unterversionen (0.9.8a, 0.9.8b usw.) |
| IBM SPSS Statistics 19 (Linux® on System z®) | 1.0.0 |

2. Befolgen Sie die Anweisungen für die Installation und Konfiguration der Software. Es wird empfohlen, gemäß den folgenden Anleitungen OpenSSL selbst zu erstellen:

Windows. OpenSSL muss mit DLLs (die standardmäßig mehrere Threads verwenden) erstellt werden.

UNIX. OpenSSL muss mehrere Threads (was nicht immer standardmäßig der Fall ist) und gemeinsam verwendete Bibliotheken unterstützen.

3. Stellen Sie sicher, dass sich die OpenSSL-Module im Systempfad befinden.

Anmerkung: Wenn mehr als eine Version der OpenSSL-Module auf dem Server-Computer vorhanden ist, kopieren Sie die OpenSSL-Module für IBM SPSS Statistics Server in das Verzeichnis, in dem IBM SPSS Statistics Server installiert ist.

Beziehen und Installieren von SSL-Zertifikat und -Schlüssel

1. Beziehen Sie ein SSL-Zertifikat und eine Schlüsseldatei. Dazu haben Sie zwei Möglichkeiten.

- Erwerben Sie sie von einer öffentlichen Zertifizierungsstelle (z. B. Comodo, Symantec oder GoDaddy). Die öffentliche Zertifizierungsstelle signiert das Zertifikat, um den Server zu verifizieren, der es verwendet. Hierbei handelt es sich um die empfohlene Methode.
- Generieren Sie Schlüssel und Zertifikatsdateien mithilfe einer internen Zertifizierungsstelle für selbstsignierte Zertifikate. OpenSSL bietet ein Zertifikatverwaltungstool für diesen Zweck. Alternativ können Sie im Internet nach Anweisungen zur Erstellung von selbstsignierten SSL-Zertifikaten suchen.

2. Kopieren Sie Zertifikat und Schlüsseldateien in ein lokales Verzeichnis bzw. in lokale Verzeichnisse auf dem Server. Der öffentliche und der private Schlüssel können in separaten Verzeichnissen gespeichert werden. Sie können auch zusammen in einer Datei gespeichert werden. Stellen Sie sicher, dass sich

der private Schlüssel nicht an einer Position befindet, die beim gelegentlichen Durchsuchen des Dateisystems auftreten kann.

3. Kopieren Sie die anerkannte Zertifizierungsstelle mit dem Namen *root.pem* an den folgenden Speicherort auf dem Server-Computer. Wenn Sie eine andere Position verwenden wollen, erstellen Sie eine Umgebungsvariable `SSL_CERT_DIR` und setzen Sie den Wert der Variablen auf die Position.

Windows 7 und höher: `C:\ProgramData\IBM\SPSS\certificates`

Mac: `/Library/Application Support/IBM/SPSS/certificates`

UNIX und Linux: `/opt/IBM/SPSS/certificates`

Aktivieren und Konfigurieren von SSL in IBM SPSS Deployment Manager

1. Starten Sie die Serververwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wurde) und stellen Sie eine Verbindung zum Server her.
2. Stellen Sie auf der Konfigurationsseite die Option **Secure Sockets Layer** auf Ja ein.
3. Geben Sie in **SSL-Datei - öffentlicher Schlüssel** den vollständigen Pfad zur Datei mit dem öffentlichen Schlüssel an.
4. Geben Sie in **SSL-Datei - privater Schlüssel** den vollständigen Pfad zur Datei mit dem privaten Schlüssel an.

Hinweis: Wenn öffentlicher und privater Schlüssel in einer Datei gespeichert werden, geben Sie in **SSL-Datei - öffentlicher Schlüssel** und **SSL-Datei - privater Schlüssel** dieselbe Datei an.

5. Wählen Sie in den Menüs Folgendes aus:

Datei > Speichern

6. Starten Sie den Serverdienst oder -dämon neu. Beim Neustart werden Sie zur Eingabe des SSL-Kennworts aufgefordert. Unter Windows können Sie **Kennwort speichern** wählen, um das Kennwort sicher zu speichern. Damit ist es nicht mehr nötig, bei jedem Serverstart das Kennwort einzugeben.

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.

1. 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`.
2. Ersetzen Sie die vorhandenen Dateien `US_export_policy.jar` und `local_policy.jar` durch die beiden Dateien, die Sie heruntergeladen und extrahiert haben.

Kopieren der Zertifikatsdatei auf Client-Computer

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

Wenn Sie ein selbstsigniertes Zertifikat verwenden, müssen Sie die anerkannte Zertifizierungsstelle auf die *Client*-Computer kopieren. Beachten Sie, dass ein Server-Computer auch als Client agieren kann. Ein Beispiel ist ein IBM SPSS Statistics-Server, der eine Verbindung zum IBM SPSS Repository für Collaboration and Deployment Services aufbaut. In diesem Fall handelt es sich bei dem IBM SPSS Statistics Server um den *Client*. Daher müssen Sie das Zertifikat für den IBM SPSS Repository für Collaboration and Deployment Services-Server auf den IBM SPSS Statistics Server kopieren.

1. Erstellen Sie eine anerkannte Zertifizierungsstelle mit dem Namen *root.pem*. Wenn Sie beispielsweise die anerkannte Zertifizierungsstelle mit OpenSSL erstellt haben, geben Sie mit dem Switch `-out` als Ausgabedatei *root.pem* an. Wenn Sie über mehrere anerkannte Zertifizierungsstellen verfügen, kopie-

ren Sie sie in eine gemeinsame *root.pem*-Datei. Anerkannte Zertifizierungsstellen sind Textdateien. Daher können Sie das Zertifikat bzw. die Zertifikate kopieren und einfügen.

2. Kopieren Sie *root.pem* an die folgende Position auf den Client-Computern. Wenn Sie bereits eine *root.pem*-Datei für ein anderes IBM Corp. Produkt auf den Client kopiert haben, hängen Sie die Informationen zu der anerkannten Stammzertifizierungsstelle von Ihrer Berechtigung an die vorhandene *root.pem*-Datei an. Standardmäßig suchen alle IBM Corp. Clientprodukte an diesem Speicherort nach vertrauenswürdigen selbstsignierten Zertifikatsdateien. Wenn Sie eine andere Position verwenden wollen, erstellen Sie eine Umgebungsvariable `SSL_CERT_DIR` und setzen Sie den Wert der Variablen auf die Position.

Windows 7 und höher: `C:\ProgramData\IBM\SPSS\certificates`

Mac: `/Library/Application Support/IBM/SPSS/certificates`

UNIX und Linux: `/opt/IBM/SPSS/certificates`

Anweisung an Benutzer, SSL zu aktivieren

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

Ländereinstellung festlegen

Die Server-Software und der Client, der eine Verbindung zu ihr herstellt, müssen mit demselben Zeichensatz, derselben Codierung und derselben Ländereinstellung ausgeführt werden. Die Server-Software ruft ihre Ländereinstellung vom Client ab. Standardmäßig ist dies die Ländereinstellung des Clients *system*. Der Client kann jedoch den Standardwert überschreiben, um Datendateien in anderen Ländereinstellungen zu verarbeiten. Durch Überschreiben der Standardeinstellung weist der Benutzer die Server-Software an, in einer angegebenen Ländereinstellung ausgeführt zu werden, ohne die Systemländereinstellung des Clients zu ändern.

Syntax

Der Benutzer überschreibt den Standardwert mit dem Syntaxbefehl `SET LOCALE :`

```
SET LOCALE="localeid"
```

localeid ist eine Zeichenfolge, die die Ländereinstellung angibt, in der die Server-Software ausgeführt wird. `SET LOCALE` schreibt einen Registrierungseintrag auf die Clientmaschine. Dieser Eintrag bleibt bestehen, damit IBM SPSS Statistics beim nächsten Start von IBM SPSS Statistics auf der Clientmaschine mit dieser Ländereinstellung ausgeführt wird.

Die Namenskonvention für die Ländereinstellungs-ID kann zwischen Plattformen und Anbietern variieren. Daher ist eine XML-Datei mit dem Server installiert, die Clientländereinstellungen den Serverländereinstellungen zuordnet. Diese Datei *loclmap.xml* befindet sich unter Windows im Serverinstallationsverzeichnis und unter UNIX im Unterverzeichnis */bin*.

loclmap.xml

Das Stammelement in *loclmap.xml* lautet wie folgt. Das Stammelement gibt auch die Schemaposition an.

```
<locale-map xmlns="http://xml.spss.com/spss/mls"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xml.spss.com/spss/mls
http://xml.spss.com/spss/mls/locale-map-1.0.xsd">
```

Das Stammelement enthält `<client-locale>`-Elemente mit einem Attribut `name`, das die Clientländereinstellung angibt. Die `<client-locale>`-Elemente enthalten mindestens ein `<server-locale>`-Element. Jedes Element `<server-locale>` hat ein Attribut `name`, das eine Serverländereinstellung angibt, die der Clientländereinstellung entspricht. Die Server-Software übersetzt die Clientländereinstel-

lungs-ID in eine, die auf der Servermaschine verwendet werden kann. Er überprüft jede Serverländereinstellung in der angegebenen Reihenfolge, bis er eine auf der Servermaschine gültige Ländereinstellung findet.

Keine der Standardserverländereinstellungen in der Datei *loclmap.xml* sind Windows-Ländereinstellungen. Ländereinstellungen für Windows-Systeme werden im Allgemeinen nicht benötigt, weil die Server-Software zuerst versucht, dieselbe Ländereinstellung wie die Systemländereinstellung des Clients zu verwenden. Ein Windows-Server sollte die Ländereinstellung haben, die der Clientländereinstellung entspricht. Sie können jedoch Ländereinstellungen für Windows-Server zu *loclmap.xml* hinzufügen, wenn Sie eine andere, aber ähnliche Windows-Ländereinstellung ersetzen müssen.

Sie können *loclmap.xml* nach Bedarf ändern. Beachten Sie lediglich, dass Ihre XML-Elemente anhand des Schemas validiert werden müssen.

Beispiel

Das folgende Beispiel zeigt den Inhalt von *loclmap.xml*:

```
<client-locale name="French">
  <server-locale name="fr_FR.cp1252"></server-locale>
  <server-locale name="fr_FR.IBM-1252@euro"></server-locale>
  <server-locale name="fr_FR.IBM-1252"></server-locale>
  <server-locale name="fr_FR.8859-15"></server-locale>
  <server-locale name="fr_FR.ISO8859-15"></server-locale>
  <server-locale name="fr_FR.iso885915@euro"></server-locale>
  <server-locale name="fr_FR@euro"></server-locale>
  <server-locale name="fr_FR"></server-locale>
  <server-locale name="fr"></server-locale>
  <server-locale name="fr_FR.iso88591"></server-locale>
  <server-locale name="fr_FR.ISO8859-1"></server-locale>
  <server-locale name="fr_FR.windows-1252"></server-locale>
  <server-locale name="fr_FR.utf8"></server-locale>
  <server-locale name="fr_FR.UTF-8"></server-locale>
  <server-locale name="French_France.1252"></server-locale>
</client-locale>
```

In diesem Fall überprüft die Server-Software zuerst `fr_FR.cp1252`, wenn der Benutzer `SET LOCALE="French"` ausgibt. Betrachten Sie den Fall eines AIX-Servers. Die `fr_FR.cp1252`-Ländereinstellung funktioniert unter AIX nicht. Daher setzt die Server-Software die Überprüfung fort, bis sie `fr_FR.windows-1252` erreicht, was unter AIX funktioniert.

Serverländereinstellung verwenden

Wenn der Benutzer `SET LOCALE` mit einer Serverländereinstellungs-ID ausgibt, die auf der Clientmaschine nicht erkannt wird, verwendet die Clientmaschine *loclmap.xml*, um die Clientländereinstellungs-ID zu suchen, die einer Serverländereinstellungs-ID zugeordnet ist. Diese Ländereinstellungs-ID wird in die Registry geschrieben. Wenn der Benutzer beispielsweise `SET LOCALE="fr_FR.windows-1252"` ausgibt, wird French in die Registry geschrieben. Um festzustellen, welcher Eintrag in *loclmap.xml* für den Client gilt, können Sie den Befehl `SHOW LOCALE` im lokalen Modus ausführen.

Potenzielle Probleme

Beachten Sie, dass die Verwendung des Befehls `SET LOCALE` in einigen Fällen zu funktionalen Problemen führen kann:

- Die aktuellen Variablennamen sind in der neuen Codepage möglicherweise nicht zulässig.
- Namensübereinstimmungen ohne Beachtung der Groß-/Kleinschreibung können fehlschlagen. Der Fehler kann auftreten, da Zeichenfolgen in Großbuchstaben konvertiert werden, wenn die Groß-/Kleinschreibung bei Namensübereinstimmungen nicht beachtet wird (z. B. beim Vergleich von Variablennamen). Ist die Ländereinstellung falsch, würde diese Konvertierung das Zeichen ändern (z. B. in der mitteleuropäischen Codepage 1250).
- Einige Bytes können fälschlicherweise als führende Bytes interpretiert werden, und es kann ein Problem auftreten, weil ein unerwartetes Trailbyte aufgetreten ist.
- `SET LOCALE` ändert nicht die Ländereinstellung des Clientsystems. Wenn also die IBM SPSS Statistics-Ländereinstellung, die `SET LOCALE` zugeordnet ist, von der Systemländereinstellung des Clients abweicht, treten Anzeige Probleme an verschiedenen Stellen auf. In dieser Situation kann ein Benutzer

auch keinen Editor für Eingabemethoden (Input Method Editor, IME) verwenden, um nationale Sonderzeichen einzugeben.

- Die IBM SPSS Statistics -Ländereinstellung, die OLANG-Einstellung und die für die Daten verwendete Codierung müssen kompatibel sein. Andernfalls kann die Ausgabe unbrauchbar und nicht lesbar sein.

Verbindung zur Server-Software herstellen

Der Endbenutzer stellt eine Verbindung zur Server-Software her, indem er sich über die Clientanwendung anmeldet. Für die Anmeldung eines Endbenutzers benötigen Sie die folgenden Informationen:

- **Computernamen oder IP-Adresse.** Wenn Endbenutzer eine Verbindung zur Server-Software herstellen, melden sie sich über die Clientanwendung an. Dazu muss der Name des Computers, auf dem die Server-Software ausgeführt wird, korrekt angegeben werden. Der Servercomputer kann durch einen alphanumerischen Namen (z. B. myserver) oder durch eine IP-Adresse identifiziert werden, die dem Servercomputer zugeordnet ist (z. B. 202 . 123 . 456 . 78)-je nachdem, was Sie bevorzugen. Wenn Sie die Server- und Client-Desktop-Computer für die Verwendung von Secure Sockets Layer (SSL) konfigurieren, muss der Endbenutzer einen vollständig qualifizierten Domännennamen (z. B. myserver.mycompany.com) verwenden.
- **Portnummer.** Endbenutzer müssen den Port, an dem die Server-Software für Verbindungen empfangsbereit ist, korrekt angeben. Die Portnummer ist der Standardwert für den Server bzw. die Angabe, die Sie bei der Konfiguration der Server-Software angegeben haben.
- **Domänenname (nur Windows)** Endbenutzer müssen möglicherweise auch einen Domännennamen angeben. Ein Domänenname ist nur erforderlich, wenn sich der Server-Computer in einer anderen Domäne als die Desktop-Computer der Endbenutzer befindet.
- **Benutzername und Kennwort.** Endbenutzer müssen sich am Server-Computer anmelden. Dazu benötigen die Benutzer einen gültigen Account mit entsprechenden Berechtigungen für den Computer, auf dem die Server-Software ausgeführt wird.
- **Secure Socket Layer (SSL).** Wenn Sie SSL verwenden, um die Kommunikation zu verschlüsseln, die auftritt, wenn Endbenutzer eine Verbindung zur Server-Software herstellen, weisen Sie die Benutzer an, SSL zu aktivieren, wenn sie die Serververbindung einrichten. Die Clients müssen nicht wissen, welches SSL-Protokoll vom Server verwendet wird. Die Client-Software versucht beides und verwendet das, was funktioniert.

Zugriff auf Daten und Dateien

Wenn Endbenutzer eine Verbindung zur Analyseserver-Software herstellen, erfolgt ihre Ansicht der Datenquellen und Dateien aus der Perspektive des Server-Computers, nicht aus der Perspektive der Desktop-Computer.

- **ODBC-Datenquellen.** Wenn Ihre Endbenutzer Zugriff auf ODBC -Datenquellen benötigen, die auf dem Server-Computer definiert sind, verteilen Sie die Namen, Beschreibungen und Anmeldeinformationen für diese Datenquellen. Eine Beschreibung des Datenbankzugriffs über die Server-Software finden Sie in Kapitel 3, „Datenzugriff“, auf Seite 9 .
- **Dateizugriff.** Verteilen Sie die Namen und Positionen der Dateien auf dem Server-Computer, auf den Endbenutzer zugreifen sollen. Weitere Informationen hierzu finden Sie in „Referenzdaten“ auf Seite 10.

Daten und Dateien speichern

Wenn Endbenutzer Dateien speichern, während sie mit der Server-Software verbunden sind, ist die Standardposition für die Sicherung das Verzeichnis, von dem aus die Datei geöffnet wurde. In vielen Fällen ist dies der lokale Desktop-Computer. Bei Datendateien ist es jedoch häufig eine schreibgeschützte Position auf dem Server-Computer. Teilen Sie Benutzern mit, wo Datendateien gespeichert werden sollen. In der Regel ist die Position das Ausgangsverzeichnis des Benutzers in Ihrem Netz.

UNIX-Hinweis: Sagen Sie den Endbenutzern, dass sie beim Speichern von Dateien die vollständige Dateispezifikation und Schrägstriche verwenden sollen (z. B. /public/myhome/myserverdata/data.sav). Vermei-

den Sie die Verwendung des umgekehrten Schrägstrichs im UNIX-Verzeichnis und in Dateinamen, die mit der Server-Software verwendet werden.

Kapitel 6. Leistung analysieren und verbessern

Wenn Sie die Leistung der Server-Software verbessern müssen, finden Sie in diesem Kapitel verschiedene Strategien, von Konfigurationsänderungen bis hin zu Hardware-Upgrades. Bevor Sie diese Änderungen vornehmen, rufen Sie Leistungsinformationen ab, damit Sie wissen, welche Bereiche problematisch sind.

Wir bieten auch ein Whitepaper, das zusätzliche Informationen zur Verbesserung der Leistung enthält. Rufen Sie <http://www.ibm.com/developerworks/spssdevcentral> auf und suchen Sie nach dem Link zu "Bücher und Artikel".

Leistungsinformationen abrufen

Um die Leistung zu überprüfen, vergleichen Sie die Nutzung in den folgenden Bereichen, wenn der Server nicht genutzt wird, wenn er stark ausgelastet ist.

- Plattenbelegung
- CPU-Nutzung
- Speichernutzung
- Netzauslastung

Protokollierung

Die Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird) ermöglicht Ihnen, die Server-Software für die Protokollierung von Leistungsinformationen zu konfigurieren. Mithilfe des Knotens **Leistungsprotokollintervall** können Sie angeben, wie oft die Server-Software Leistungsinformationen in das Protokoll schreibt. Weitere Informationen finden Sie im Abschnitt zur Protokollierung im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Sie können Leistungsinformationen auch direkt vom Betriebssystem abrufen.

Leistungsdaten unter Windows abrufen

Unter Windows können Sie mithilfe des Leistungsmonitors Leistungsinformationen abrufen.

| Tabelle 3. Windows-Leistungsinformationen | | |
|---|--------------------------------|---|
| Bereich | Windows-Leistungsmonitorobjekt | Nützlicher Zähler |
| Plattenbelegung | Physische Platte | % Leerlaufzeit |
| CPU-Nutzung | Prozessor | % Prozessorzeit |
| Speicherbelegung | Speicher | Zugesicherte Byte |
| Netzauslastung | Netzschnittstelle | Gesamtzahl Byte/Sek. für jede physische Schnittstelleninstanz (nicht die MS TSP-Loopback-Schnittstelle) |

Leistungsdaten unter UNIX abrufen

Unter UNIX gibt es je nach Hersteller verschiedene Befehle zum Abrufen von Leistungsinformationen.

Tabelle 4. UNIX-Leistungsinformationen

| Bereich | Anbieter | Befehl | Hinweis |
|------------------|----------|------------------|---|
| Plattenbelegung | Linux | Iostat -x | Überprüfen Sie die Spalte %util . |
| Plattenbelegung | AIX | iostat -d | Überprüfen Sie die Spalte % tm_actl . |
| CPU-Nutzung | Linux | oberer Grenzwert | Mit dem interaktiven Befehl P können Sie nach CPU-Belastung sortieren. |
| CPU-Nutzung | AIX | Zusatzspeicher | Leiten Sie an den Befehl <code>sort</code> weiter, um nach der Spalte %CPU zu sortieren. |
| CPU-Nutzung | Alle | Uptime | Überprüfen Sie den Lastdurchschnitt. |
| Speicherbelegung | Linux | oberer Grenzwert | Mit dem interaktiven Befehl M können Sie nach CPU-Belastung sortieren. |
| Speicherbelegung | AIX | Zusatzspeicher | Verwenden Sie die Pipe zum Befehl <code>sort</code> , um nach der Spalte RSS zu sortieren. |
| Netzauslastung | Alle | Netsat | Verwenden Sie die Switches <code>-i</code> und <code>-s</code> für Informationen. |

Nächster Schritt

Nach dem Zusammenstellen dieser Informationen sollten Sie in der Lage sein, die problematischen Bereiche zu identifizieren. In den folgenden Abschnitten werden mögliche Lösungen und Empfehlungen für jeden Bereich beschrieben.

Plattenbelegung verbessern

Beachten Sie Folgendes, um die Plattenbelegung zu verbessern.

space. Lassen Sie ausreichend Plattenspeicherplatz zu. Jeder Benutzer benötigt normalerweise temporären Plattenspeicherplatz, der doppelt so groß ist wie die verwendete Datendatei (SAV) (der benötigte Speicherplatz reicht von 1 bis 2,5 Mal). Ein Benutzer, der eine Datei sortiert, benötigt möglicherweise mehr als die dreifache Größe der Datei. Wenn beispielsweise sechs gleichzeitig angemeldete Benutzer auf eine Datei zugreifen und zwei gleichzeitig sortieren, benötigen sie möglicherweise bis zu 17 Mal die Größe der Datei. In der Praxis wird die maximale Nutzung nicht gleichzeitig erreicht, sodass die Größe der Datei 12-mal ausreicht.

Hardware. Verwenden Sie SCSI-Platten für die schnellste Leistung. Verwenden Sie keine IDE.

Systemkonfiguration. Temporäre Dateien auf einer separaten Spindel aufbewahren. Sie können auch mehrere temporäre Dateipositionen mit der Verwaltungsanwendung definieren. Stellen Sie sicher, dass sich jede Position auf einer separaten Spindel befindet. Wenn Sie RAID verwenden, verwenden Sie RAID0 für die temporäre Dateispindel. Die Geschwindigkeit von RAID0 für Arbeitsdateien wird gegenüber der Redundanz von RAID1 bevorzugt. Wenn Ihre CPU kein Problem darstellt und der Server-Computer Wind-

ows ausführt, können Sie auch das Datenverzeichnis oder die Datendateien auf der Platte komprimieren. Ordnen Sie keinen weiteren virtuellen Speicher zu.

IBM SPSS Statistics -Konfiguration. Wenn der Speicher kein Problem, aber die Plattenbelegung ist, erhöhen Sie den Arbeitsbereich in IBM SPSS Statistics, um die Leistung zu verbessern. Versuchen Sie es, indem Sie die Menge des Arbeitsspeichers auf dem Server-Computer durch die erwartete Anzahl gleichzeitig angemeldeter Benutzer dividieren. Wenn der Server-Computer beispielsweise über 1 GB RAM verfügt, setzen Sie den Arbeitsbereich auf 0,25 GB RAM.

Verzeichnis für temporäre Dateien. Ändern Sie das Benutzerprofil oder die Gruppeneinstellungen so, dass sich die temporären Dateiverzeichnisse für jeden Benutzer auf verschiedenen physischen Laufwerken befinden.

Cachekomprimierung. Wenn Ihre Benutzer konsistent mit großen Datendateien arbeiten (insbesondere wenn die Größe der Dateien größer als die Hälfte des RAM des Servers ist), versuchen Sie, die Cachekomprimierung in der Verwaltungsanwendung zu aktivieren.

Verbessern der CPU-Belastung

Beachten Sie Folgendes, um die CPU-Auslastung zu verbessern:

Nummer Fügen Sie weitere Prozessoren hinzu. Wenn Sie sich der Geschwindigkeit nähern möchten, die ein Benutzer beim lokalen Ausführen von IBM SPSS Statistics erreichen würde, versuchen Sie, einen Prozessor für jeweils zwei gleichzeitig angemeldete Benutzer zu haben. Verwenden Sie auch Prozessoren, die so schnell oder schneller sind als der Prozessor auf dem Desktop-Computer. Wenn Sie beispielsweise einen Durchschnitt von vier gleichzeitig angemeldeten Benutzern erwarten, konfigurieren Sie den Server-Computer mit zwei schnellen Prozessoren.

Hardware. Verwenden Sie schnelle Prozessoren. Das Hinzufügen einiger wirklich schneller Prozessoren ist besser als das Hinzufügen vieler langsamer Prozessoren. Wenn die CPU-Auslastung weiterhin ein Problem mit schnellen Prozessoren ist, sollten Sie in Betracht ziehen, Ihrem System weitere Server-Computer hinzuzufügen.

Positionen der SAV-Dateien und Zugriff. Wenn bestimmte Dateien häufig von vielen gleichzeitig angemeldeten Benutzern verwendet werden, ziehen Sie in Betracht, die Dateien auf mehrere Server zu verschieben, um die Benutzerlast auszugleichen. Wenn beispielsweise *TestScores.sav* und *GPA.sav* stark ausgelastet sind, stellen Sie sie auf separate Server. Steuern Sie den Zugriff auf die Dateien mit den Betriebssystemberechtigungen (pro Gruppe oder pro Benutzer), anstatt den Zugriff über Serverkonten zu steuern.

CPU-Priorität. Wenn bestimmte Benutzer eine höhere CPU-Priorität als andere Benutzer benötigen (z. B. Benutzer, die Schnelljobs ausführen, im Vergleich zu Benutzern, die lange Jobs ausführen), ändern Sie das Benutzerprofil oder die Gruppeneinstellungen.

Cachekomprimierung. Die Cachekomprimierung hat einen gewissen CPU-Aufwand für die Komprimierung und Dekomprimierung von Arbeitsdateien. Wenn Ihre Benutzer nicht mit großen Datendateien arbeiten, kann es sinnvoll sein, diese auszuschalten.

Speicherbelegung verbessern

Beachten Sie Folgendes, um die Speicherbelegung zu verbessern:

Betrag. Fügen Sie so viel RAM wie möglich hinzu. Versuchen Sie, 128 MB RAM für jeden gleichzeitig angemeldeten Benutzer zu haben. Sind also vier gleichzeitig angemeldete Benutzer vorhanden, konfigurieren Sie den Server mit 512 MB RAM.

IBM SPSS Statistics -Konfiguration. Verkleinern Sie den Arbeitsbereich in IBM SPSS Statistics.

Netzauslastung verbessern

Beachten Sie Folgendes zur Verbesserung der Netzauslastung:

Systemkonfiguration. Planen Sie netzintensive Operationen für Zeiten, in denen die Server-Software nicht verwendet wird (z. B. Systemsicherungen über Nacht ausführen). Wenn Sie ein Problem mit dem Netzwerkverkehr auf einem Computer identifizieren, auf dem der Server ausgeführt wird, arbeitet IBM Corp. mit Ihnen zusammen, um das Problem weiter zu diagnostizieren.

IBM SPSS Statistics Effizient Verwenden

Neben der Konzentration auf bestimmte Problembereiche können Sie auch die Leistung verbessern, indem Sie die folgenden Richtlinien für die effiziente Verwendung von IBM SPSS Statistics einhalten.

Datenmanagement. Wenn Sie große Datendateien haben, die regelmäßig aktualisiert werden müssen und von Benutzern gemeinsam genutzt werden, sollten Sie die Aktualisierungen einmal durchführen und dann die Dateien für die Benutzer zur Analyse freigeben. Wenn Sie beispielsweise regelmäßig monatliche Daten zu einer Datei hinzufügen, sortieren und Transformationen durchführen, bestimmen Sie eine Person für die Ausführung des Jobs für die Datei. Die anderen Benutzer können die Daten abrufen, die sie benötigen, ohne die Zusammenführung, Sortierung und Transformationen wiederholen zu müssen.

Interaktive vs. Batch. Wenn Sie über regelmäßige, zeitaufwendige Operationen mit IBM SPSS Statistics verfügen, sollten Sie in Betracht ziehen, diese über IBM SPSS Statistics Batch Facility und nicht über einen Client auszuführen, der mit dem Server verbunden ist. Verwenden Sie den Client zum Erstellen der Berichte und führen Sie sie über IBM SPSS Statistics Batch Facility aus, wenn die Berichte bereit sind.

Anhang A. Fehlerbehebung

Server-Software

Portnummernkonflikt. Bei einem Portnummernkonflikt kann die Server-Software möglicherweise nicht gestartet werden. Beheben Sie das Problem mithilfe der Verwaltungsanwendung (IBM SPSS Statistics Administration Console, die als Teil von IBM SPSS Deployment Manager installiert wird), um die Portnummer zu ändern. Weitere Informationen finden Sie im Abschnitt "Verbindungen" im *Deployment Manager Benutzerhandbuch* (in der Hilfe für IBM SPSS Collaboration and Deployment Services enthalten). Achten Sie darauf, die neue Portnummer an die Endbenutzer zu verteilen.

Erratisches Verhalten. Die Server-Software kann sich unberechenbar verhalten, wenn die zugehörige Konfigurationsdatei (z. B. *statisticsd.conf*) beschädigt ist oder fehlt. Stellen Sie zum Beheben des Problems die Konfigurationsdatei aus Ihrer Sicherungskopie wieder her. Kopieren Sie sie an die in der Verwaltungsanwendung oder in der Umgebungsvariablen der Konfigurationsdatei angegebene Position und starten Sie die Server-Software erneut. Informationen zum Neustart finden Sie im Abschnitt „Server-Software starten und stoppen“ auf Seite 21 in.

Die Verwaltungsanwendung funktioniert nicht (nur UNIX). Wenn Sie die Verwaltungsanwendung zum Steuern oder Konfigurieren der Server-Software verwenden und diese nicht funktioniert (z. B. wenn Sie den Server nicht stoppen können), kann dies daran liegen, dass Sie die Server-Software nicht mit dem von IBM Corp. bereitgestellten Startscript gestartet haben. Beheben Sie das Problem, indem Sie die Server-Software mit dem Startscript *start_statistics_server* starten. Weitere Informationen finden Sie im Thema „Service oder Dämon stoppen“ auf Seite 21. Wenn beim Versuch, die Server-Software zu steuern oder zu konfigurieren, eine Fehlermeldung angezeigt wird, liegt dies möglicherweise daran, dass Sie mit einem Konto verbunden sind, das keine Administratorberechtigungen hat.

Position temporärer Dateien kann nicht geändert werden (nur UNIX) Wenn Sie die Verwaltungsanwendung verwenden, um die Position von temporären Dateien zu ändern, und die Änderung nicht wirksam ist, kann dies daran liegen, dass die neue Position nicht über ausreichende Dateiberechtigungen für die Endbenutzer verfügt. Wählen Sie eine Position mit **read**-, **write**- und **execute** -Zugriff für alle Benutzer aus, die eine Verbindung zur Server-Software herstellen.

Server wird nicht gestartet (nur UNIX). Wenn die Server-Software nicht gestartet wird, kann dies daran liegen, dass Sie nicht über die erforderlichen Programmkorrekturen für das Betriebssystem verfügen. Um das Problem zu beheben, laden Sie die entsprechende Programmkorrektur herunter und installieren Sie sie. Die erforderlichen Programmkorrekturen sind in den UNIX-Installationsanweisungen für Ihr Serverprodukt aufgelistet.

Client-Software

Endbenutzer kann keine Verbindung zum Server herstellen. Möglicherweise verfügt der Benutzer nicht über die entsprechenden Berechtigungen oder die Firewall blockiert die Server-Software. Informationen zu Benutzerberechtigungen finden Sie unter „Berechtigungen“ auf Seite 31 . Informationen zur Konfiguration der Firewall finden Sie unter „Verbindungen über eine Firewall konfigurieren“ auf Seite 33 .

Die Endbenutzeranmeldung schlägt mit der Nachricht "Der angegebene ferne Server-Computer wurde nicht gefunden" fehl. Der Service oder Dämon ist möglicherweise nicht aktiv. Bestätigen Sie dies, indem Sie den Status der Server-Software überprüfen. Starten Sie den Service oder Dämon erneut, um das Problem zu beheben. Weitere Informationen hierzu finden Sie in „Server-Software starten und stoppen“ auf Seite 21.

Die Anmeldung des Endbenutzers schlägt mit der Nachricht "Error connecting to package" fehl. Der Endbenutzer hat den Namen oder die IP-Adresse eines Server-Computers angegeben, der sich nicht im Netz befindet. Um das Problem zu beheben, bitten Sie den Endbenutzer, einen gültigen Servernamen einzugeben.

Die DataDirect- ODBC -Datenquelle schlägt mit der Nachricht "not licensed" fehl. Die DataDirect-Datenzugriffstechnologie wird mit IBM Corp. -Produkten verteilt. Es funktioniert nur mit neueren IBM Corp. -Produkten-es funktioniert nicht mit früheren Versionen, noch funktioniert es mit Nicht-IBM Corp. -Anwendungen. Wenn Endbenutzer versuchen, DataDirect-Datenquellen mit einem älteren oder nicht lizenzierten Produkt zu verwenden, erhalten sie eine Nachricht mit dem Text **You are not licensed to use the DataDirect ODBC Driver**. Führen Sie ein Upgrade Ihrer Benutzer auf eine aktuelle Version durch, um das Problem mit dem Produkt IBM Corp. zu beheben. Um das Problem mit nicht lizenzierten Produkten zu beheben, führen Sie ein Upgrade Ihrer Lizenzierung mit DataDirect durch oder bitten Sie Endbenutzer, nicht zu versuchen, die Datenquellen zu verwenden, die Sie für IBM Corp. -Produkte mit nicht lizenzierten Anwendungen definiert haben.

Endbenutzer kann keine Datendatei oder ODBC -Datenquelle finden. Wenn Endbenutzer im Modus für verteilte Analysen ausgeführt werden, haben sie nur Zugriff auf Datendateien und ODBC -Datenquellen auf dem Computer, auf dem die Server-Software ausgeführt wird. Wenn Endbenutzer im lokalen Analysemodus ausgeführt werden, haben sie nur Zugriff auf Datendateien und ODBC -Datenquellen auf ihren Desktop-Computern. Um das Problem zu beheben, bitten Sie den Endbenutzer, die Clientanwendung im entsprechenden Modus auszuführen.

Endbenutzer kann keine Statistikprozedur ausführen (nur IBM SPSS Statistics Server) Wenn Endbenutzer mit der Server-Software verbunden sind, haben sie nur Zugriff auf die IBM SPSS Statistics -Optionen, die während der Installation von IBM SPSS Statistics Server installiert wurden. Um das Problem zu beheben, den Endbenutzer bitten, die Prozedur im lokalen Analysemodus auszuführen oder die angeforderte Prozedur auf dem Server-Computer zu installieren.

Anhang B. IBM SPSS Statistics Batch Facility

Hinweis: IBM SPSS Statistics Batch Facility ist ein Dienstprogramm zur Stapelverarbeitung, das in **IBM SPSS Statistics Server** enthalten ist.

Normalerweise wird der Client für IBM SPSS Statistics Server IBM SPSS Statistics auf einem Desktop-Computer ausgeführt. IBM SPSS Statistics Batch Facility ist jedoch eine alternative Methode, die Leistung von IBM SPSS Statistics Server zu nutzen, und wird auf dem Server-Computer ausgeführt. IBM SPSS Statistics Batch Facility ist für die **automatisierte Produktion** von Statistikberichten konzipiert. Die automatisierte Produktion bietet die Möglichkeit, Analysen ohne Benutzereingriff auszuführen. Die automatisierte Produktion ist von Vorteil, wenn Benutzer an Ihrem Standort regelmäßig eine Reihe von zeitaufwendigen Analysen benötigen, z. B. wöchentliche Berichte.

IBM SPSS Statistics Batch Facility verwendet als Eingabe eine Berichtsanforderung, die in einer **Befehlsyntax** enthalten ist. IBM SPSS Statistics Batch Facility erstellt dann automatisch die in der Syntax angegebenen Statistikberichte.

Was Sie wissen müssen

. IBM SPSS Statistics Batch Facility ist derzeit für alle IBM SPSS Statistics Server, UNIX und Windows verfügbar.

Installation. IBM SPSS Statistics Batch Facility wird automatisch im Installationsverzeichnis von IBM SPSS Statistics Server unter Windows und im Unterverzeichnis *bin* des Installationsverzeichnisses unter UNIX installiert.

Aufruf. IBM SPSS Statistics Batch Facility wird über die Befehlszeile mit der ausführbaren Datei *statisticsb* ausgeführt. Er wird unabhängig von IBM SPSS Statistics Server-IBM SPSS Statistics Server ausgeführt und muss nicht gestartet werden, damit er ausgeführt werden kann. Es kann auch gleichzeitig mit IBM SPSS Statistics Server ausgeführt werden.

Betriebsarten. Befehle werden an IBM SPSS Statistics Batch Facility im **Stapelmodus** oder im **interaktiven Modus** übergeben. Im Stapelmodus übergibt der Analyst oder IT-Experte eine Befehlssyntaxdatei zur Ausführung an IBM SPSS Statistics Batch Facility. Die Befehle in der Datei werden gelesen und als Stapel verarbeitet und die Ausgabe wird in eine Datei übertragen. IBM SPSS Statistics Batch Facility wird unbeaufsichtigt ausgeführt und nach Ausführung des letzten Befehls beendet. Dies ist die typische Methode für die Verwendung von IBM SPSS Statistics Batch Facility. Im interaktiven Modus gibt der Analyst Befehle nacheinander an einer Eingabeaufforderung ein. Die Befehle werden sofort ausgeführt und die Ausgabe wird im Fenster angezeigt. IBM SPSS Statistics Batch Facility wartet auf den nächsten Befehl.

Dokumentation. Das Benutzerhandbuch, das für die Analysten und IT-Spezialisten an einer Site geschrieben wurde, die IBM SPSS Statistics Batch Facility verwenden werden, befindet sich auf dem IBM SPSS Statistics Server DVD in */Documentation/<language>/Handbücher*. Das Referenzhandbuch zur Befehlsyntax, das Analysten benötigen, um Befehlssyntaxdateien für IBM SPSS Statistics Batch Facility zu erstellen, befindet sich auf dem IBM SPSS Statistics Server DVD in */Documentation/<language>/Manuals*. IBM SPSS Statistics Batch Facility for UNIX wird auch mit der manuellen Seite *statisticsb.1* verteilt, die sich im Unterverzeichnis */bin* des IBM SPSS Statistics Server-Installationsverzeichnisses befindet. Wenn Sie ein UNIX-System verwalten, kopieren Sie es an die Position, an der Sie Ihre Handbuchseiten behalten.

Zusätzliche Dokumentation. Das IBM SPSS Statistics Batch Facility Benutzerhandbuch enthält ausreichende Informationen für einen Analysten, der Erfahrung mit der Befehlssyntaxsprache IBM SPSS Statistics hat, um Befehlssyntaxdateien für IBM SPSS Statistics Batch Facility zu erstellen. Wenn die Analysten an Ihrem Standort IBM SPSS Statistics neu sind, benötigen sie möglicherweise zusätzliche Dokumentation. Ist dies der Fall, leiten Sie sie an unsere Website unter <http://www.ibm.com/software/analytics/spss/> weiter oder bitten Sie sie, sich an Ihren Vertriebsbeauftragten zu wenden.

Anhang C. Tasks für das Betriebssystem Windows

Sie können die meisten Verwaltungsaufgaben mit der Verwaltungsanwendung ausführen. Einige Tasks müssen jedoch möglicherweise mit dem Betriebssystem Windows ausgeführt werden. Verwenden Sie die folgenden Betriebssystemfunktionen, um Server-Software unter Windows zu verwalten:

- **Dateieigenschaften.** Wird verwendet, um den Endbenutzerzugriff auf das Installationsverzeichnis der Server-Software, die temporäre Dateiposition und Datendateien festzulegen.
- **Systemeigenschaften.** Wird verwendet, um Umgebungsvariablen zu erstellen
- **Benutzermanager.** Wird zum Erstellen von Endbenutzerkonten verwendet
- **Systemsteuerung für Dienste.** Wird zum Starten, Stoppen und Konfigurieren des Service verwendet.
- **ODBC Administrator.** Dient zur Konfiguration von Datenquellen.

Dateieigenschaften

Verwenden Sie Dateieigenschaften, um Berechtigungen für Dateien festzulegen. Bei Datendateien hängt die Vorgehensweise davon ab, wo die Daten gespeichert werden. Wenn Sie Daten auf demselben Computer wie die Server-Software speichern, steuern Sie den Zugriff auf das Datenverzeichnis, indem Sie Berechtigungen für ein Verzeichnis auf einem NTFS-Laufwerk definieren.

Auf dem Server-Computer, angemeldet als Administrator:

1. Navigieren Sie mit dem Windows-Explorer zum Datenverzeichnis.
2. Klicken Sie auf das Verzeichnis, klicken Sie mit der rechten Maustaste und klicken Sie im Kontextmenü auf **Teilen**.
3. Klicken Sie auf die Registerkarte **Sicherheit** und konfigurieren Sie die Berechtigungen.

Anmerkung: Die Registerkarte "Sicherheit" ist nur auf NTFS-Laufwerken verfügbar. Wenn Sie nicht sicher sind, welchen Dateisystemtyp Ihre Hardware verwendet, führen Sie die folgenden Schritte aus:

4. Verwenden Sie den Windows Explorer, um zum Laufwerk zu navigieren.
5. Klicken Sie auf das Laufwerk, klicken Sie mit der rechten Maustaste und klicken Sie im Kontextmenü auf **Eigenschaften**.
6. Klicken Sie auf die Registerkarte **Allgemein** und sehen Sie sich den Wert für das Dateisystem an.

Wenn Sie Daten auf einem Computer in Ihrem Netz speichern, können Sie den Zugriff auf das Datenverzeichnis steuern, indem Sie eine gemeinsam genutzte Ressource erstellen und die Berechtigungen entsprechend festlegen.

Auf dem vernetzten Computer als Administrator angemeldet:

7. Navigieren Sie mit dem Windows-Explorer zum Datenverzeichnis.
8. Klicken Sie auf das Verzeichnis, klicken Sie mit der rechten Maustaste und klicken Sie im Kontextmenü auf **Teilen**.
9. Klicken Sie im Dialogfeld auf die Registerkarte **Freigeben**, klicken Sie auf **Gemeinsam genutzt als**, geben Sie einen Freigabennamen ein und legen Sie den entsprechenden Zugriff fest.

Systemeigenschaften

Verwenden Sie Systemeigenschaften, um Umgebungsvariablen zu erstellen.

Auf dem Server-Computer, angemeldet als Administrator:

1. Klicken Sie auf dem Windows-Desktop mit der rechten Maustaste auf das Symbol für den Computer. Klicken Sie beispielsweise mit der rechten Maustaste auf **Arbeitsplatz**.
2. Wählen Sie im Menü **Eigenschaften** aus.

3. Klicken Sie auf die Registerkarte **Erweitert** und anschließend auf **Umgebungsvariablen**.
4. Klicken Sie auf **Neu**.
5. Geben Sie den Namen der neuen Variablen ein.
6. Geben Sie den Wert für die neue Variable ein.

Benutzermanager

Verwenden Sie den Benutzermanager, um Endbenutzerkonten zu erstellen.

Auf dem Server-Computer, angemeldet als Administrator:

1. Wählen Sie im Windows-Startmenü Folgendes aus:
 - Programme > Verwaltung**
 - Wählen Sie **Computerverwaltung** und anschließend **Lokale Benutzer und Gruppen** aus.
2. Erstellen Sie die Benutzerkonten.

Systemsteuerung für Services

Verwenden Sie die Systemsteuerung für Windows-Dienste, um:

- Stoppen und starten Sie den Service.
- Ändern Sie die Servicestartparameter.
- Überprüfen Sie den Serverstatus.

Gehen Sie wie folgt vor, um die Systemsteuerung für Dienste aufzurufen und zu verwenden:

1. Wählen Sie im Windows-Startmenü Folgendes aus:
 - Einstellungen > Systemsteuerung**
2. Wählen Sie **Verwaltung** und anschließend **Dienste** aus.
3. Wählen Sie den Service aus. Sie können jetzt den Status überprüfen, starten oder stoppen und die Startparameter bearbeiten.

Anmerkung: Sie können den Status der Server-Software mit der Verwaltungsanwendung starten, stoppen und überprüfen.

Task-Manager

Verwenden Sie den Task-Manager, um anzuzeigen, wie viele serverbezogene Prozesse ausgeführt werden.

1. Öffnen Sie den Windows-Task-Manager, indem Sie Strg-Alt-Entf drücken und **Task-Manager** wählen.
2. Klicken Sie auf die Registerkarte **Prozesse**.
3. Klicken Sie auf **Bildname**, um die Prozesse alphabetisch zu sortieren.
4. Suchen Sie nach dem Dateinamen des Serverprozesses (*statisticsrvr.exe*).
5. Suchen Sie nach dem Dateinamen des Clientprozesses (*statisticsproc.exe*). Für jeden Endbenutzer, der momentan mit der Server-Software verbunden ist, gibt es einen Prozess.

Hinweis: Sie können Server und Clientprozesse mit der Verwaltungsanwendung überwachen.

ODBC -Administrator

Verwenden Sie den ODBC -Administrator, um System- und Benutzerdatenquellen für die Verwendung mit der Server-Software zu konfigurieren.

Wie die ODBC -Datenquelle erstellt wird, wirkt sich darauf aus, wer sie anzeigen und verwenden kann. Verwenden Sie *System* -DSNs, wenn Sie allgemeinen Zugriff auf die Datenquelle zulassen möchten.

Verwenden Sie DSNs des Typs *Benutzer* , wenn Sie den Zugriff auf sensible Informationen einschränken oder den DSN für einen bestimmten Benutzer anpassen wollen.

So konfigurieren Sie einen System-DSN

Systemdatenquellennamen können von jedem verwendet werden, der an dem Computer angemeldet ist, auf dem sie definiert sind. System-DSNs sind einfacher zu konfigurieren und zu verwalten, da Sie es nur einmal für alle Benutzer tun.

Auf dem Computer, auf dem sich die Datenquelle befinden soll, als Administrator angemeldet:

1. Wählen Sie im Windows-Startmenü Folgendes aus:

Einstellungen > Systemsteuerung

2. Wählen Sie **Verwaltung** und dann **Datenquellenaus**.

3. Klicken Sie die Registerkarte **System-DSN** an.

4. Klicken Sie auf **Hinzufügen**.

5. Wählen Sie einen Treiber aus der Liste aus. Wenn Sie eine Datenquelle konfigurieren, die die IBM Corp. -Datenzugriffstechnologie verwendet, werden die Namen der Connect ODBC -Treiber mit dem Text IBM Corp. OEM gekennzeichnet.

6. Klicken Sie auf **Fertigstellen**.

7. Geben Sie die entsprechenden Informationen im Dialogfenster **Treiberkonfiguration** ein.

8. Klicken Sie auf **OK**.

So konfigurieren Sie einen Benutzer-DSN

Benutzer-DSNs können nur vom Account des Benutzers verwendet werden, der sie erstellt hat. Konfigurieren Sie DSNs für Benutzer, wenn Sie den Zugriff auf sensible Informationen einschränken oder den DSN für einen bestimmten Benutzer anpassen wollen.

Melden Sie sich als Benutzer an und befolgen Sie die Schritte für einen System-DSN mit der folgenden Ausnahme:

- Klicken Sie auf die Registerkarte **Benutzer-DSN** anstelle der Registerkarte **System-DSN** .

Anhang D. UNIX-Betriebssystemtasks

Sie können die meisten Verwaltungstasks mit der Verwaltungsanwendung ausführen. Einige Tasks müssen jedoch möglicherweise mit dem Betriebssystem UNIX ausgeführt werden. Verwenden Sie die folgenden Betriebssystemfunktionen, um Server-Software unter UNIX zu verwalten:

- **chmod** Wird verwendet, um den Endbenutzerzugriff auf Datendateien festzulegen.
- **env** Wird verwendet, um die Werte von Umgebungsvariablen zu überprüfen
- **Scripts**. Wird verwendet, um die Server-Software zu starten und ihre Umgebung zu konfigurieren.
- **ps** und **kill**. Wird zum Prüfen und Stoppen von Serverprozessen verwendet.
- **odbc.ini**. Wird zum Konfigurieren von ODBC -Datenquellen verwendet.

Chmod

Mit dem Befehl `chmod` (oder `chown`) können Sie den Berechtigungsmodus für Verzeichnisse und Datendateien ändern oder zuordnen. Geben Sie beispielsweise Folgendes ein, um das Verzeichnis `/usr/data` für alle Benutzer auf 'schreibgeschützt' zu setzen:

1. Melden Sie sich als Superuser oder als Eigner des Verzeichnisses an.
2. Geben Sie an der UNIX-Eingabeaufforderung Folgendes ein:

```
chmod a-w /usr/data
```

Umschlag

Mit dem Befehl `env` können Sie die aktuellen Werte von Umgebungsvariablen überprüfen. Wenn Sie beispielsweise `env` verwenden möchten, um die aktuellen Werte von Umgebungsvariablen für die Server-Software zu überprüfen:

1. Melden Sie sich mit dem Account an, der den Dämon gestartet hat, normalerweise `root`.
2. Geben Sie an der UNIX-Eingabeaufforderung Folgendes ein:

Umgebung

3. Überprüfen Sie die Einstellungen für die gewünschte (n) Variable (n).

Scripts

Um den Wert von Umgebungsvariablen zu ändern, bearbeiten Sie das Umgebungsvariablen-script, das von dem Script aufgerufen wird, das die Server-Software startet. So bearbeiten Sie das Umgebungsvariablen-script:

1. Öffnen Sie mit einem Texteditor das Script `statsenv.sh`, das sich im Unterverzeichnis `/bin` des IBM SPSS Statistics Server-Installationsverzeichnis befindet. Öffnen Sie beispielsweise `/usr/local/my-serverproduct/bin/statsenv.sh`.
2. Entfernen Sie bei Bedarf die Kommentarzeichen für die Zeile, die die Variable definiert, und geben Sie dann den neuen Wert für die Variable ein.
3. Speichern Sie die Datei.

`statsenv.sh` wird vom Script `start_statistics_server` aufgerufen. Umgebungsvariablen, die in `statsenv.sh` festgelegt und exportiert werden, wirken sich nur auf die Prozesse aus, die mit dem Script `start_statistics_server` gestartet werden.

ps und kill

Verwenden Sie den Befehl `ps`, um Informationen zu den Serverprozessen abzurufen, die gerade ausgeführt werden, und um den Prozessstatus zu melden. Beispiel:

1. Geben Sie an der UNIX-Eingabeaufforderung Folgendes ein:

```
ps -efl.
```

2. Suchen Sie nach dem Dateinamen des Dämonprozesses (z. B. *statisticsd*). Dieser Prozess hat die **UID** des Benutzers, der den Server-Software-Dämonprozess gestartet hat (normalerweise *root*).
3. Suchen Sie nach dem Dateinamen des Clientprozesses *statisticsproc.exe*. Für jeden Endbenutzer, der momentan mit der Server-Software verbunden ist, gibt es einen Prozess. In der Spalte *UID* wird die Anmelde-ID des Endbenutzers angezeigt, der Eigner des Clientprozesses ist.

Mit dem Befehl `kill` können Sie einen Prozess beenden. Beispiel:

4. Melden Sie sich als der Benutzer an, der den Dämon gestartet hat.
5. Geben Sie an der UNIX-Eingabeaufforderung Folgendes ein:

```
kill -9 PID
```

Dabei ist *pid* die Prozess-ID des Prozesses.

Der Server-Software-Dämon erstellt auch automatisch eine Datei, die seine Prozess-ID enthält. Anstatt die PID manuell mit dem Befehl `ps` zu suchen, können Sie diese Datei in Verbindung mit dem Befehl `kill` direkt verwenden, um den Dämonprozess direkt zu beenden:

```
kill -9 `cat statisticsd.pid`
```

Hinweis: Wenn Sie die Verwaltungsanwendung zum Überwachen und Beenden von Prozessen verwenden wollen, müssen Sie die Server-Software mit dem Startscript starten, das von IBM Corp. bereitgestellt wird. Weitere Informationen hierzu finden Sie in „Servicestart steuern“ auf Seite 19.

odbc.ini

Möglicherweise müssen Sie ODBC -Datenquellen auf dem Server-Computer konfigurieren, wenn:

- Sie verwenden IBM Corp. Data Access Pack

und

- Die Server-Software muss auf Datenbanken zugreifen

Unter UNIX ist kein ODBC -Administrator vorhanden. Um eine ODBC -Datenquelle unter UNIX zu konfigurieren, bearbeiten Sie eine Textdatei mit Systeminformationen, *odbc.ini*. *Odbc.ini* wird installiert, wenn Sie das Datenzugriffspaket für UNIX installieren. Installationsanweisungen finden Sie in *IBM Corp. Data Access Pack Installation Instructions for Unix.pdf* (das Dokument befindet sich im Verzeichnis `/Documentation/<language>/InstallationDocuments` auf dem Produkt). DVD). Installieren Sie die zusätzliche Dokumentation, damit Sie auf die unten aufgeführten Dokumente zugreifen können.

Connect ODBC. Ausführliche Anweisungen zum Bearbeiten der Datei *odbc.ini* und zum Festlegen wichtiger Umgebungsvariablen finden Sie im Abschnitt "Configuring Drivers and Data Sources" im Kapitel "Installation on UNIX" in den *Connect ODBC -Installationsanweisungen*.

Die DataDirect-Produktdokumentation für Connect ODBC ist standardmäßig als Bestandteil der IBM SPSS Data Access Pack-Installation im Lieferumfang enthalten. Das Installationsprogramm erstellt den Eintrag "IBM SPSS OEM Connect and ConnectXE for ODBC" zusammen mit den Einträgen für Ihre anderen Programme im Startmenü. Der Zugriff auf die DataDirect-Produktdokumentation erfolgt über dieses Menüelement.

Die DataDirect-Produktdokumentation für Connect ODBC befindet sich in dem Verzeichnis, in dem Sie die Dateien extrahiert haben.

Hinweis: Sie können auch über die DataDirect-Homepage unter <http://www.datadirect.com> auf die Dokumentation zugreifen.

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 ist eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich.

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

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

IBM Director of Licensing

IBM Europe, Middle East & Africa

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

France

Bei Lizenzanforderungen zu Double-Byte-Information (DBCS) wenden Sie sich bitte an die IBM Abteilung für geistiges Eigentum in Ihrem Land oder senden Sie Anfragen schriftlich an folgende Adresse:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. -->

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 als IBM 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 Europe, Middle East & Africa

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

France

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

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

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

Alle Informationen zu Produkten anderer Anbieter als IBM 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 Aussage zu Leistung, Kompatibilität und anderen Merkmalen von Produkten anderer Anbieter als IBM machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter als IBM 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 Geschäftsablaufes. 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 Quellsprache geschrieben sind und Programmieretechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme ohne Zahlung an IBM 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.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© Copyright IBM Corp. 2021. Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet.

© Copyright IBM Corp. 1989 - 2021. All rights reserved.

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- oder Servicenamen können Marken von IBM oder anderen Her-

stellern 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 eingetragene 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.

Index

A

Arbeitsbereich [48, 49](#)
Arbeitsbereich IBM SPSS Statistics [48, 49](#)
Arbeitsspeicher (RAM) [49](#)
authentication
 intern [24](#)
 OS [23](#)
 PAM [24](#)
 Single Sign-on [26](#)
 unix2 [25](#)
automatisierte Produktion mit IBM SPSS Statistics Server [53](#)

B

Benutzer-ID und Kennwort
 Wissenswertes für Endbenutzer [45](#)
Benutzerprofile [32](#)
Berechtigungen [31](#)
Berechtigungen auf Administratorebene [31](#)
Betriebssystemtasks, UNIX
 Dateiberechtigungen mit dem Befehl 'chmod' festlegen [59](#)
 Datenquellen mit odbc.ini konfigurieren [60](#)
 Scripts zum Festlegen von Umgebungsvariablen verwenden [59](#)
 Serverprozesse mit dem Befehl kill stoppen [60](#)
 Serverprozesse mit dem Befehl ps überprüfen [60](#)
 Umgebungsvariablen mit dem Befehl env überprüfen [59](#)
Betriebssystemtasks, Windows
 Benutzermanager verwenden [56](#)
 Dateieigenschaften festlegen [55](#)
 ODBC -Administrator verwenden [56](#)
 Task-Manager verwenden [56](#)
 über die Systemsteuerung für Dienste [56](#)
 Umgebungsvariablen erstellen [55](#)

C

Clientanwendung
 Fehlerbehebung [51](#)
 Installation von [7](#)
Computername
 Wissenswertes für Endbenutzer [45](#)
Connect ODBC
 Architektur [9](#)
 Einrichten der UNIX-Umgebung für [12](#)
 Übersicht [9](#)
CPU-Nutzung
 verbessern [49](#)

D

Datenansicht [15](#)
Datenquellen
 Single Sign-on [31](#)

Datenzugriff
 Connect ODBC [9](#)
 Daten aus Client-Software referenzieren [10](#)
 Konfigurieren von ODBC Datenquellen für [16](#)
 ODBC -Datenquelle für [10](#)
 Steuerung [10](#)
 unter UNIX [12](#)
 Zu berücksichtigende Faktoren [10](#)
Datenzugriffstechnologie [9](#)
Domänenname
 Wissenswertes für Endbenutzer [45](#)
DSN-Zugriff [31](#)

E

Endbenutzer
 Benutzer-ID und Kennwort [45](#)
 Computername [45](#)
 Domänenname [45](#)
 Liste der erforderlichen Informationen [23](#)
 ODBC-Datenquellen [45](#)
 Portnummer [45](#)
 Unterstützung [23](#)
 Zugriff auf Datendateien [45](#)

F

Fehlerbehebung
 Clientanmeldung [51](#)
 Clientanwendung [51](#)
 Konfigurationsdatei [51](#)
 ODBC-Datenquellen [51](#)
 Portnummer [51](#)
 Server-Software [51](#)
Firewall [33](#)

G

Gruppenberechtigung [19, 31](#)

I

IBM SPSS Collaboration and Deployment Services
 Ersatz [17](#)
IBM SPSS Statistics Administration Console [17](#)
IBM SPSS Statistics Batch Facility
 Einführung [53](#)
 Was Sie wissen müssen, [53](#)
IDE [48](#)
INSERT HIDDEN
 Produktionsmodus [17](#)
Installation
 Clientanwendung [7](#)
 Server-Software [7](#)

K

- Konfigurationsdatei
 - Fehlerbehebung [51](#)
- Konfigurieren
 - X-Spannungen [17](#)
 - Zertifikate [39](#)
- Konten [15](#)

L

- Ländereinstellung [43](#)
- Leistung
 - verbessern [47](#)
- Leistung verbessern [47](#)
- Leistungsinformationen [47](#)
- Lokaler Analysemodus
 - Datenansicht [9](#)
 - definiert [1](#)

M

- Modus für verteilte Analysen
 - Datenansicht [9](#)
 - definiert [1](#)
 - Schritte zur Verwendung [1](#)

N

- Netzadressumsetzung [33](#)
- Netzauslastung
 - verbessern [49](#)

O

- ODBC -Datenquellen, UNIX
 - in odbc.ini definiert [60](#)
- ODBC -Datenquellen, Windows
 - Benutzer-DSNs [56](#)
 - System-DSNs [56](#)
- ODBC-Datenquellen
 - Fehlerbehebung [51](#)
 - Konfigurieren [16](#)
 - und Server-Software [11](#)
 - Wissenswertes für Endbenutzer [45](#)
- ohne Rootberechtigungen ausführen [24–26](#)

P

- PAM [24](#)
- platform="unix " scale="80">CrtCDSresources.sh
 - Dateiberechtigungen festlegen [59](#)
 - ODBC -Datenquellen erstellen und konfigurieren [60](#)
 - Serverprozesse stoppen [60](#)
 - Serverprozesse überprüfen [60](#)
 - Umgebungsvariablen definieren [59](#)
 - Umgebungsvariablen überprüfen [59](#)
- Plattenbelegung
 - verbessern [48](#)
- Pluggable Authentication Module [24](#)
- Portnummer
 - Fehlerbehebung [51](#)
 - Wissenswertes für Endbenutzer [45](#)

- PPTPComment [35](#)
- Produkte und Betriebssysteme [1](#)
- Produktionsmodus
 - INSERT HIDDEN [17](#)
- Profile [32](#)
- Prozessnamen nach Produkt [21](#)
- Prozessoren [49](#)
- Punkt-zu-Punkt-Tunnelprotokoll [35](#)

R

- RAID [48](#)
- Rollenbasierte Zugriffssteuerung [25](#)
- Rootberechtigungen [24–26](#)

S

- SCSI [48](#)
- Secure Sockets Layer [35](#)
- Server-Software
 - Administratoren [31](#)
 - Architektur [1](#)
 - definiert [1](#)
 - Endbenutzerkonten und Dateien verwalten [15](#)
 - Fehlerbehebung [51](#)
 - Installation von [7](#)
 - Komponenten von [1](#)
 - Konfiguration [15](#)
 - Mehrere Instanzen [19](#)
 - ODBC -Datenquellen konfigurieren [16](#)
 - Produkte [1](#)
 - Prozessnamen nach Produkt [21](#)
 - Routinewartung [21](#)
 - Start steuern [19](#)
 - starten und stoppen [21](#)
 - UNIX-Startscript verwenden [19](#)
- Server-Software konfigurieren [15](#)
- Service-Principalname [28, 29](#)
- Sicherheit
 - SSL [35](#)
- Single Sign-on
 - Client konfigurieren [28](#)
 - Datenquellen [31](#)
 - Gruppenmitgliedschaft [30](#)
 - Server konfigurieren [27](#)
 - Service-Principalname [28, 29](#)
- sortieren [16](#)
- Sortierung anderer Anbieter [16](#)
- Speicherbelegung
 - verbessern [49](#)
- Speicherplatz [48](#)
- SSL
 - Kommunikation schützen [36, 40](#)
 - Übersicht [36](#)
- SSO [26](#)
- start_statistics_server [19](#)
- Statistiksb [53](#)
- Synchronisationsortierung [16](#)
- Systemadministratoren
 - Übersicht über Verwaltungstasks [4](#)
 - Wissenswertes für Endbenutzer [23](#)

U

UNC-Dateiverweise [45](#)
UNIX-Umgebung und Datenzugriff [12](#)

V

Verschlüsselung
 SSL [35](#)
Versionen [32](#)
Verteilte Architektur [1](#)
Verwaltung [17](#)
Verwaltungsanwendung [17](#)

W

Windows
 Dateiberechtigungen festlegen [55](#)
 Endbenutzerkonten erstellen [56](#)
 ODBC -Datenquellen erstellen und konfigurieren [56](#)
 Parameter für den Servicestart ändern [56](#)
 Serverprozesse überprüfen [56](#)
 Services starten und stoppen [56](#)
 Servicestatus überprüfen [56](#)
 Umgebungsvariablen erstellen [55](#)

X

X-Spannungen
 Konfigurieren [17](#)

Z

Zertifikate
 Konfigurieren [39](#)
Zugriff auf Datendateien
 Wissenswertes für Endbenutzer [45](#)

