pitney bowes

Spectrum™ Technology Platform

Version 12.0 SP2

Spectrum Spatial-Administratorhandbuch

Inhalt

1 - Einführung

2 - Konfigurieren Ihres Systems

3 - Verwalten von Sicherheit

4 - Überwachen Ihres Systems

5 - Leistungsoptimierung

6 - Verwalten eines Clusters

7 - Verwenden der Administrationsumgebung

8 - Enterprise Routing-Modul

9 - Beheben von Fehlern in Ihrem System

1 - Einführung

In this section

Inhalt dieses Handbuchs

Willkommen im *Spectrum Spatial-Administratorhandbuch*. Befolgen Sie die Schritte in diesem Handbuch, um mithilfe zahlreicher Webservices, Funktionen, Tools und Beispielcodes eine Web-Mapping-Anwendung zu erstellen oder Mapping in eine vorhandene Anwendung einzubinden.

In diesem Handbuch wird Folgendes behandelt:

- Konfigurieren Ihres Systems, indem Sie die Standardportnummer oder Datenbank ändern, Zugriff auf die Datenbank, Zugreifen auf und Hochladen von Ressourcen, Konfigurieren von Webservices und Ausführen von Spectrum™ Technology Platform als Linux-Dienst
- Verwalten der Sicherheit mithilfe der Management Console, einschließlich wie Benutzer und Rollen hinzugefügt werden und wie Außerkraftsetzungen der Sicherheitsentität angewendet werden
- Überwachen Ihres Systems, einschließlich Protokollierung, Anzeigen von Versions- und Lizenzinformationen, Überwachen der Leistung über die JMX Console und Überwachen der Speicherauslastung
- Verwalten von Speicher und Threads, einschließlich JVM-Leistungsoptimierung, Anpassen der Poolgröße und Vergrößern des Heapspeichers
- Lastenausgleich von Geodatendiensten für Zuverlässigkeit und hohe Kapazität
- Beheben von Fehlern in Ihrem System, einschließlich Neuerstellen eines beschädigten Datenbankindex und Überwachen der Speichernutzung auf einem nicht reagierenden Server

Zusätzliche Dokumentationen zu Spectrum™ Technology Platform und Location Intelligence-Modul finden Sie online unter **support.pb.com**.

2 - Konfigurieren Ihres Systems

In this section

Ändern der HTTP-Portnummer für Spectrum Spatial

Der HTTP-Port wird verwendet, um über REST oder SOAP auf alle Spectrum™ Technology Platform-Webservices und auf die Begrüßungsseite, Beispielanwendungen und Spatial Manager zuzugreifen.

Nachdem Sie Spectrum™ Technology Platform installiert haben, können Sie die vorhandenen Porteinstellungen, die während der Installation zugewiesen wurden, ändern, indem Sie die globale Konfigurationsdatei sowie die Konfigurationsdateien für Start und für einzelne Dienste von Hand ändern. Es gibt verschiedene Gründe, warum Sie möglicherweise die Portnummer ändern müssen:

- Nach der Installation tritt ein Portkonflikt auf.
- Sie möchten eine neue Version von Spectrum™ Technology Platform ausprobieren, ohne die alte Version zu entfernen. Da Sie nicht beide nebeneinander installieren können, können Sie die vorhandene Version deaktivieren und ein Spectrum™ Technology Platform-Abbild installieren, das einen anderen Port verwendet.
- Sie benötigen einen Proxy auf Port 8080, müssen jedoch eine begrenzte Anzahl von Ports extern verfügbar machen. Sie möchten Spectrum™ Technology Platform verschieben, ohne Ihre gesamten Einstellungen und Datenflüsse neu zu erstellen.

> **Anmerkung:** Diese Aufgabe sollte nur von erfahrenen Administratoren durchgeführt werden, die aus dem Umgang mit Anwendungsservern Erfahrung mit dem Ändern von Portnummern haben, da Netzwerkportkonflikte dazu führen können, dass Modulkomponenten nicht starten. Ein Anzeichen dafür, dass eine Komponente nicht gestartet wurde, ist, dass sie nicht in der Management Console angezeigt wird. Um dieses Problem zu beheben, sehen Sie im Wrapper-Protokoll des Spectrum™ Technology Platform-Servers nach. In diesem Protokoll wird aufgeführt, welcher Port das Problem verursacht. Sie finden das Wrapper-Protokoll unter: `<install_folder>\server\app\repository\logs\wrapper.log`.

Damit Spectrum™ Technology Platform über den neuen HTTP-Port läuft, müssen einige Einträge in Eigenschafts- und Konfigurationsdateien geändert werden. Sie müssen auf dem Server Dateibearbeitung über WebDAV aktiviert haben, um die Dienstkonfigurationen ändern zu können. WebDAV ist für Windows- und Linux-Server verfügbar, muss aber möglicherweise installiert werden.

So ändern Sie die Portnummer:

1. Ändern Sie in der Datei „spectrum-container.properties“ den Wert von `spectrum.http.port` auf die neue Portnummer. Diese Datei befindet sich in `<install_folder>/server/app/conf`.
2. Ändern Sie in der Datei „java.properties“ alle Ports für `repository.host` und `image.webapp.url`. Diese Datei befindet sich unter `<install_folder>/server/modules/spatial`..
3. Ändern Sie in die Portnummern in diesen Dienstkonfigurationen:

- Mapping (nur erforderlich, wenn auf den Mapping-Dienst per SOAP zugegriffen wird und der ReturnImage-Parameter für eine RenderMap-Anforderung "false" ist)
- WFS
- WMS
- WMTS

Weitere Informationen finden Sie im Spatial Manager-Handbuch im Abschnitt „Dienstprogramme“ des *Spectrum Spatial-Handbuchs*.

Wenn Sie den Server verschieben, sodass er einen anderen Port verwenden kann, läuft der Spectrum™ Technology Platform-Server wahrscheinlich nicht. Sie werden die Dienstkonfigurationsdateien nicht bearbeiten können, bis der Server läuft. Sie müssen den Server starten, die Konfigurationen bearbeiten und dann den Server neu starten.

4. Starten Sie Spectrum™ Technology Platform neu, damit die Änderungen an Ports und Eigenschaften wirksam werden.

Ändern des Typs Ihrer Repository-Datenbank

Das Location Intelligence-Modul speichert benannte Ressourcen (Karten, Layer, Tabellen und Stile), geografische Metadaten und Konfigurationen in einem Repository. In der standardmäßigen Installation eines einzelnen Servers wird eine integrierte Datenbank verwendet, um diese Ressourcen auf dem lokalen Server zu speichern. Es gibt verschiedene Gründe, warum Sie möglicherweise eine andere Datenbank als die integrierte Derby-Datenbank verwenden müssen:

- Erstellen einer skalierbaren Lösung, die eine zuverlässige, unabhängige Datenbank verwendet
- Verwenden einer unternehmensinternen Datenbank, die von Ihrer Firma bevorzugt wird oder vorgeschrieben ist

In dieser Version werden die Repository-Datenbanken Oracle, PostGreSQL/PostGIS und Microsoft SQL Server unterstützt. Anweisungen finden Sie unter **Einrichten einer allgemeinen Repository-Datenbank** auf Seite 88.

Konfigurieren der Webservices

Sie können das erwünschte Verhalten der Location Intelligence-Modul-Webservices über Einstellungen in der jeweiligen Konfigurationsdatei eines Webservice ausdrücklich spezifizieren und müssen dies auch oft tun. Die Konfigurationsdateien für Webservices des Location Intelligence-Moduls befinden sich als benannte Konfigurationen in der Location Intelligence-Modul-Datenbank.

Anmerkung: Benannte Konfigurationen verhalten sich nicht wie andere benannte Ressourcen in der Datenbank. Sie können nicht den Named Resource-Dienst für den Zugriff auf benannte Konfigurationen verwenden. Stattdessen müssen Sie ein WebDAV-Tool wie WebFolders verwenden.

Konfigurationsdateien für die Mapping-, Feature-, Map Tiling-, WFS-, WMS- und WMTS-Dienste werden in der Datenbank vorgeladen. Diese Konfigurationsdateien befinden sich unter `http://hostname:port/RepositoryService/repository/default/Configuration/`.

Weitere Informationen zu Namen und Speicherort der benannten Konfigurationen der einzelnen Webservices in der Datenbank sowie eine Liste der Konfigurationsparameter für jeden Webservice finden Sie im Kapitel „Arbeiten mit Geodatendiensten“ im *Spectrum Spatial Developer-Handbuch*.

Steuern der Darstellung von Geometrieknoten

Das Location Intelligence-Modul und das Routing-Modul bieten eine Eigenschaft, mit der Sie die Anzahl von Stellen steuern können, mit denen in einer Webservice-Antwort zurückgegebene Geometrieknoten dargestellt werden. Geometrien werden standardmäßig ohne festgelegtes Limit für die Anzahl von Stellen zurückgegeben. Dies könnten bis zu 16 Stellen sein. Die zusätzlichen Stellen werden unnötigerweise zur Nutzlast einer JSON- oder SOAP-Antwort hinzugefügt. Dies ist insbesondere dann der Fall, wenn große Polygone oder viele Datensätze zurückgegeben werden. Zudem entsteht möglicherweise eine Genauigkeitserwartung, die in den Daten nicht widergespiegelt wird. Der Unterschied zu einer am wenigsten signifikanten Stelle kann ein Wert von einem Milliardstel eines Meters sein. 3989657,014543291 und 3989657,014543292 unterscheiden sich beispielsweise um ein Milliardstel eines Meters. Spatial Data weisen selten einen Wert auf, der nah an dieser Genauigkeit liegt. Durch Festlegen der Eigenschaft auf „true“ werden die Werte in der Regel auf 9 oder 10 signifikante Stellen gekürzt. Mit Blick auf das vorherige Beispiel wird der Wert als 3989657,01 zurückgegeben. Dies entspricht einer Genauigkeit von einem Zentimeter.

Fügen Sie zum Kürzen der Knotenwerte folgende Eigenschaft zur Datei „%Spectrum%\server\bin\wrapper\wrapper.conf“ hinzu und starten Sie den Server neu.

```
wrapper.java.additional.xx=-Dcom.pb.midev.service.output.geometry.useprecision=true
```

Dabei steht `xx` für die Zahl der nächsten verfügbaren Zeile im Abschnitt.

Die Koordinatenwerte werden bei allen Geometrien über Dienste gleich behandelt, unabhängig davon, ob es sich um SOAP- oder REST-Aufrufe handelt. Darin inbegriffen sind auch über einen Datenfluss verfügbar gemachte Dienste. Zu den Diensten zählen der Feature-Dienst des Location Intelligence-Moduls, der Mapping-Dienst, der Geometry-Dienst, der Map Tiling-Dienst sowie die WMS-, WMTS- und WFS- und Enterprise Routing-Dienste.

Anwendungen, in denen Polygondaten über die Webservices bearbeitet werden, sollten diese Eigenschaft nicht verwenden, wenn die Möglichkeit besteht, dass durch das Rückschreiben gekürzter

Geometrien kleine Überlappungen oder Lücken mit angrenzenden Geometrien erstellt werden könnten.

Deaktivieren von Genauigkeitsdateien für Datumstransformationen

Spectrum Spatial unterstützt Konvertierungen zwischen bestimmten Datumswerten. Dabei kommen Algorithmen zum Einsatz, die eine genauere Verschiebung der Koordinaten unterstützen. Standardmäßig wird für jede Datumstransformation eine separate JAR-Datei installiert, die diese Algorithmen enthält. Sie befinden sich im Verzeichnis *Spectrum-Installationsspeicherort*\server\app\types:

- midev-core-coordsys-irishtm-*Versionsnummer*-onprem.jar für Irish Transverse Mercator
- midev-core-coordsys-jgd2000-*Versionsnummer*-onprem.jar (aktiviert auch die aktuelle Version JGD2011) für japanische Datumswerte
- midev-core-coordsys-nadcon-*Versionsnummer*-onprem.jar für US Nad27-Nad83
- midev-core-coordsys-ntv2-*Versionsnummer*-onprem.jar für NTV2, das verschiedene Konvertierungen für viele Länder enthält

  Anmerkung: Eine XML-Datei in diesem JAR steuert, welche Konvertierungen verwendet werden. Stoppen Sie den Server und extrahieren Sie die XML-Datei aus dem JAR, um bestimmte Konvertierungen zu deaktivieren. Verwenden Sie einen Editor, um den Eintrag für jede zu deaktivierende Konvertierung auf „false“ festzulegen. Fügen Sie die bearbeitete XML-Datei dem JAR hinzu und starten Sie dann den Server neu. Wenn Sie die Konvertierung aktivieren möchten, müssen Sie die Einträge ebenfalls auf „true“ festlegen. Einzelheiten finden Sie unter **Aktivieren der NTv2-Transformation**.

- midev-core-coordsys-rgf93-*Versionsnummer*-onprem.jar für French Lambert-Konvertierungen

Standardmäßig werden alle dieser JAR-Dateien geladen, doch kann deren Verwendung die Leistung bestimmter Vorgänge beeinträchtigen. Sie können diese Konvertierung in einigen Fällen deaktivieren, beispielsweise wenn Sie einen bestimmten Konvertierungstyp (wie den für japanische Datumswerte) nicht benötigen oder der Leistungszuwachs die Vorteile der Genauigkeit in höheren Zoomstufen aufwiegt.

So deaktivieren Sie eine bestimmte Transformation:

1. Stoppen Sie den Server.
2. Entfernen Sie das JAR aus dem Verzeichnis. Alternativ können Sie die Dateierweiterung der JAR-Datei umbenennen (zum Beispiel zu „.jar~“), wodurch diese nicht mehr geladen wird.
3. Starten Sie den Server neu.

KonKonfigurieren von Timeouts bei Anforderungen

In Spectrum Spatial können Sie für SOAP- und REST-Vorgänge als Teil einer Anforderung an den Mapping- und den Feature-Dienst einen Timeout festlegen. Der Timeout ist standardmäßig mit einem Wert von 300 Sekunden (5 Minuten) aktiviert.

Um den Timeout anzuwenden, müssen Sie Einstiegs- und Zwischenpunkte konfigurieren. Dies erledigen Sie in der aop.xml unter server/modules/spatial/. Die Datei enthält mehrere Implementierungen, die Sie verwenden können. Der Einstiegspunkt ist der Punkt, an dem der Timeout beginnt, die Zeit zu messen. An den Zwischenpunkten überprüft der Timeout, ob bei dem Vorgang eine Zeitüberschreitung aufgetreten ist.

Verwenden Sie dies, wenn Sie beispielsweise einen Timeout auf die SOAP- und REST-renderMap-Methoden und einige Zwischenschritte (Datenbankaufrufe, Durchsuchen von Tabellen, Abrufen von Kandidaten) anwenden möchten.

Bearbeiten Sie die Timeouteigenschaft des Mapping- und/oder des Feature-Dienstes in den java.properties unter /server/modules/spatial, um den standardmäßigen Timeoutwert von 300 Sekunden anzupassen.

```
timeout.mapping.value=300
```

```
timeout.feature.value=300
```

Wenn der angegebene Timeoutwert <= 0 ist, wird der Timeout deaktiviert.

Starten Sie Spectrum™ Technology Platform neu, nachdem Sie einen Timeoutwert geändert haben.

Konfigurieren des Attributs „Veränderlich“ für benannte Tabellen

Veränderlichkeit ist ein Anzeichen für Spectrum Spatial, dass sich Informationen aus einer Datenquelle jederzeit ändern können. Der Standardwert für TAB-, SAP HANA- und JDBC-basierte (Oracle, SQL Server und PostGIS) benannte Tabellen ist „wahr“, was bedeutet, dass Spectrum Spatial die Datenquelle für jeden Datenzugriffsvorgang wie Abfragen oder Einfügen daraufhin überprüft, ob die Tabelle veränderlich ist und – wenn dies der Fall ist – ob sich die Daten geändert haben. Wenn sich die Daten geändert haben, wird der Cache geleert und die Tabelle wird neu geladen, bevor der Datenzugriffsvorgang fortgesetzt wird. Wenn sich die Tabelle nicht geändert hat, wird die Abfrage oder ein anderer Vorgang mit den Daten im Cache durchgeführt. Weitere

Informationen darüber, was eine Änderung für die einzelnen Datenquellen auslöst, finden Sie unter **Unterstützte Datenquellen** im Abschnitt „Ressourcen und Daten“ des *Spectrum Spatial-Handbuchs*.

Veränderlichkeit wird für benannte Tabellen aktiviert (auf „wahr“ gesetzt), die über **Map Uploader** von MapInfo Professional hochgeladen werden. Die Veränderlichkeit ist auch für alle benannten Tabellen, die mit **Spatial Manager** erstellt wurden, aktiviert. Ältere benannte Tabellen im Repository gelten als veränderlich, doch wird dies unter den Tabellendetails im Spatial Manager nicht angezeigt.

Sie sollten Veränderlichkeit nur bei Tabellen deaktivieren, die sich nicht ändern. Wenn Sie beispielsweise Kacheln aus veränderlichen TAB-Dateien generieren, wird dieser Vorgang sehr langsam ausgeführt. Auch wenn Sie PostGIS verwenden, können Sie in Betracht ziehen, Veränderlichkeit zu deaktivieren, um Verbindungsfehler in Spatial Manager zu vermeiden (wenn Sie zum Beispiel die Beispielzeilen auf der Seite mit den Tabellendetails anzeigen).

Veränderlichkeit kann auf der Tabellendetailsseite in Spatial Manager deaktiviert werden. Weitere Informationen zum Erstellen und Ändern von benannten Tabellen in Spatial Manager finden Sie im Abschnitt „Dienstprogramme“ im *Spectrum Spatial-Handbuch*.

Sie müssen den Server neu starten, wenn Sie die Einstellung für die Veränderlichkeit bei einer vorhandenen benannten Tabelle ändern oder wenn Sie eine neue benannte Tabelle erstellen, die auf einer Datenbanktabelle basiert, die zuvor auf „falsch“ festgelegt (und Veränderlichkeit somit deaktiviert) war.

> **Anmerkung:** Verwenden Sie nicht den Vorgang updateNamedResource im Named Resource-Dienst, um diesen Wert zu ändern. Bearbeiten Sie auch nicht die Definition der benannten Tabelle, auf die Sie über WebDAV zugegriffen haben, in einem Texteditor.

Ausführen vAusführen von Spectrum™ Technology Platform als Linux-Dienst

In dieser Einführung erfahren Sie, welche Schritte Sie ausführen müssen, um Spectrum™ Technology Platform als Linux-Dienst auszuführen.

Wie Sie Spectrum™ Technology Platform als Linux-Dienst ausführen

Diese Anweisungen beschreiben, wie Sie Spectrum™ Technology Platform als Linux-Dienst ausführen.

1. Ändern Sie das zur Verfügung gestellte Skript `pbspectrum`, das sich an folgendem Speicherort befindet: **PBSpectrum-Skript** auf Seite 14.
   a) Ändern Sie in Zeile 5 den Parameter `chkconfig`. Dieser Parameter ist standardmäßig `# chkconfig: 35 90 10`.

Bei dem ersten Wert (35) handelt es sich um den „runlevel“. Verwenden Sie „man init“, um weitere Informationen zu erhalten.

Bei dem zweiten Wert (90) handelt es sich um die Startpriorität.

Bei dem dritten Wert (10) handelt es sich um die Stoppppriorität.

Sie sollten Start- und Stoppppriorität entsprechend den abhängigen Diensten festlegen. Wenn Oracle Server beispielsweise auf demselben Computer ausgeführt und von Spectrum™ Technology Platform verwendet wird, sollte die Startpriorität von Spectrum™ Technology Platform unterhalb der des Oracle-Dienstes und die Stoppppriorität oberhalb der des Oracle-Dienstes liegen. Verwenden Sie „man chkconfig“, um weitere Informationen zu erhalten.

b) Ändern Sie die Variable „SPECTRUM_ROOT“ in Zeile 11 auf Ihr Installationsverzeichnis von Spectrum™ Technology Platform.
c) Wenn Sie SUSE Linux verwenden, müssen Sie den standardmäßig bevorzugten Benutzer von `su` zu `runuser` ändern.

2. Kopieren Sie das geänderte Skript `pbspectrum` entweder nach `/etc/rc.d/init.d` unter RedHat Linux oder nach `/etc/init.d` unter Suse Linux.
3. Machen Sie das Skript `pbspectrum` ausführbar. Verwenden Sie `/etc/rc.d/init.d` unter RedHat Linux oder `/etc/init.d` unter Suse Linux.

   Führen Sie abhängig von Ihrer Linux-Version `cd /etc/init.d` oder `cd /etc/rc.d/init.d` aus.

   Führen Sie `chmod +x pbspectrum` aus.

4. Führen Sie `chkconfig --add pbspectrum` aus.
5. Überprüfen Sie, ob das Skript funktioniert, indem Sie den Rechner neu starten. Verwenden Sie `shutdown -r now`, um von der Shell neu zu starten.

Nach Abschluss können Sie auch folgende Befehle verwenden:

- `service pbspectrum start`, um Spatial Server zu starten
- `service pbspectrum stop`, um Spatial Server zu beenden
- `service pbspectrum restart`, um Spatial Server neu zu starten

Anmerkung: Das zur Verfügung gestellte Skript führt den Befehl „ulimit -n 8192“ aus, der erforderlich ist, um die Anzahl der offenen Dateien unter Linux zu erhöhen.

PBSpectrum-Skript

Für diesen Vorgang wird das folgende Skript als Basis verwendet: **Wie Sie Spectrum™ Technology Platform als Linux-Dienst ausführen** auf Seite 12.

```
   #! /bin/bash
#
#  pbspectrum Bring up/down PB Spectrum platform
#
# chkconfig: 35 90 10
# description: Starts and stops the spectrum
#
# /etc/rc.d/init.d/pbspectrum
# See how we were called.

SPECTRUM_ROOT=/root/PBSpectrum

start() {
        su - spectrum -c ". $SPECTRUM_ROOT/server/bin/setup;
  ulimit -n 8192;
  $SPECTRUM_ROOT/server/bin/server.start"
        RETVAL=$?
        return $RETVAL
}

stop() {
        su - spectrum -c ". $SPECTRUM_ROOT/server/bin/setup;
        $SPECTRUM_ROOT/server/bin/server.stop"
        RETVAL=$?
        return $RETVAL
}

# See how we were called.
case "$1" in
  start)
        start
        ;;
  stop)
        stop
        ;;
  restart)
        stop
        start
        ;;
  *)
        echo $"Usage: pbspectrum {start|stop|restart}"
        exit 1
esac
```

```
exit $RETVAL
```

Konfigurieren eines Linux-Rechners für MRR

Um in einer Linux-Umgebung MRR-Dateien (Multi Resolution Raster) in Spectrum Spatial zu verwenden, muss ein Upgrade von GCC und LIBC auf die korrekten Versionen durchgeführt werden.

So konfigurieren Sie einen Linux-Rechner für MRR:

1. Installieren Sie das UUID-Paket, das LIBC v.2.17 installiert.

   So installieren Sie beispielsweise UUID auf Cent OS:

   - `wget http://ftp.riken.jp/Linux/centos/6/os/x86_64/Packages/libuuid-2.17.2-12.18.el6.x86_64.rpm`
   - `sudo yum -y install libuuid-2.17.2-12.18.el6.x86_64.rpm`
   - `sudo yum -y install libuuid-devel`

2. Installieren Sie devtoolset-3, das GCC v.4.9 installiert. Anweisungen finden Sie unter **https://www.softwarecollections.org/de/scls/rhscl/devtoolset-3/**.
3. Überprüfen Sie, ob GCC v.4.9 und LIBC v.2.17 (oder höher) installiert sind.
4. Stellen Sie sicher, dass alle Abhängigkeiten in obigen Schritten aufgelöst wurden. Wenn eine Abhängigkeit nicht aufgelöst wurde, installieren Sie sie und wiederholen Sie Schritt 2.

   Als Beispiel finden Sie unten einige der erforderlichen Abhängigkeiten für einen Rechner mit OEL 6.5:

   - `wget https://www.softwarecollections.org/en/scls/mizdebsk/maven30-rhel-6/epel-6-x86_64/download/mizdebsk-maven30-rhel-6-epel-6-x86_64.noarch.rpm`
   - `sudo yum -y install mizdebsk-maven30-rhel-6-epel-6-x86_64-1-2.noarch.rpm`
   - `wget https://www.softwarecollections.org/en/scls/rhscl/maven30/epel-6-x86_64/download/rhscl-maven30-epel-6-x86_64.noarch.rpm`
   - `sudo yum -y install rhscl-maven30-epel-6-x86_64-1-2.noarch.rpm`
   - `sudo yum -y install maven30`
   - `wget https://www.softwarecollections.org/en/scls/mbooth/eclipse-luna/fedora-20-x86_64/download/mbooth-eclipse-luna-fedora-20-x86_64.noarch.rpm`
   - `sudo yum -y install mbooth-eclipse-luna-fedora-20-x86_64-1-2.noarch.rpm`
   - `sudo yum -y install --skip-broken eclipse-luna`

Deaktivieren von Standard-HTTP-Cache-Control-Headern

Die Spectrum™ Technology Platform-Webservices verwenden standardmäßig die folgenden HTTP-Headers für das Caching:

```
Cache-Control: no-cache,no-store,no-transform,must-revalidate
Expires: Wed, 07 Jan 2015 15:38:03 GMT //48 hours in the past
Pragma: no-cache
```

Diese HTTP-Header eignen sich nicht für den Map Tiling-Dienst; Sie können diese Standard-HTTP-Header allerdings deaktivieren und stattdessen das HTTP-Cache-Verhalten in den Headern festlegen, die in den einzelnen Webservices definiert sind.

> **Anmerkung:** Wenn Sie diese Änderung auf ein Cluster anwenden, müssen Sie die folgende Vorgehensweise für jeden Knoten im Cluster wiederholen.

So deaktivieren Sie die Standard-HTTP-Cache-Control-Header:

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
2. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumFolder\server\app\conf\spectrum-advanced.properties
3. Ändern Sie die folgende Eigenschaft von „true“ in „false“:

   ```
   spectrum.cache.control.headers.enable=false
   ```
4. Speichern Sie die Eigenschaftsdatei und schließen Sie sie.
5. Starten Sie den Spectrum™ Technology Platform-Server.

3 - Verwalten von Sicherheit

Das Location Intelligence-Modul verwendet dasselbe rollenbasierte Sicherheitsmodell, wie es für Spectrum™ Technology Platform zum Einsatz kommt. Da die Sicherheit auf Plattformebene umgesetzt wird, können Sie die Management Console verwenden, um alle Sicherheitsaktivitäten des Location Intelligence-Moduls zu verwalten.

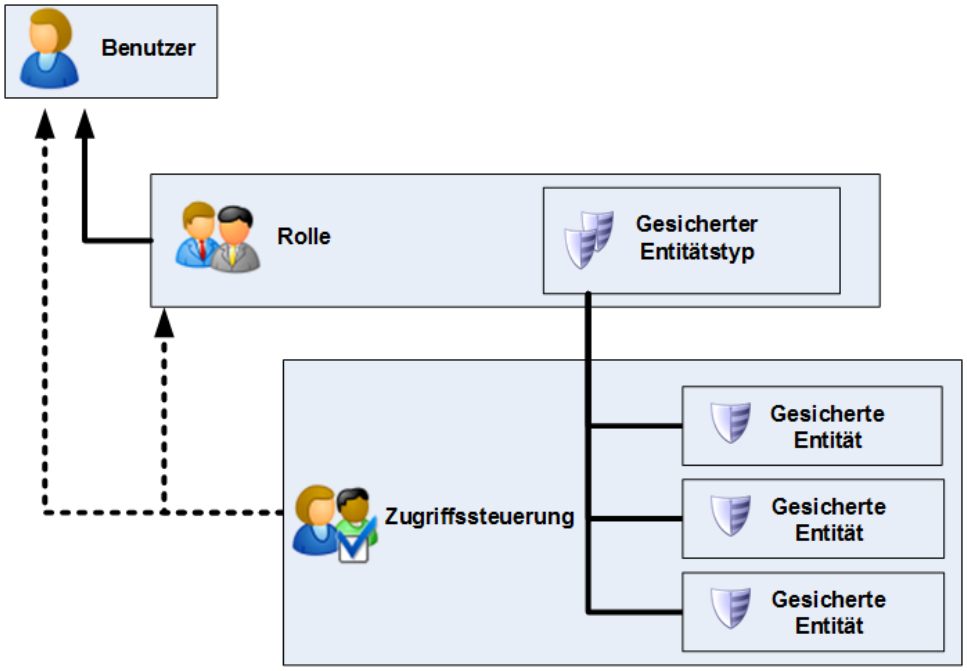
In this section

SicherheitSicherheit für Spectrum™ Technology Platform

Die Themen in diesem Abschnitt behandeln das Sicherheitsmodell und die Prozeduren auf Plattformebene, die für alle Module gelten. Unter **Sicherheit für das Location Intelligence-Modul** auf Seite 53 finden Sie weitere Informationen zu modulspezifischer Sicherheit.

Sicherheitsmodell

Spectrum™ Technology Platform Verwendet für die Steuerung des Zugriffs auf das System ein rollenbasiertes Sicherheitsmodell. Das folgende Diagramm veranschaulicht die wichtigsten Konzepte im Spectrum™ Technology Platform-Sicherheitsmodell:



Ein *Benutzer* ist ein einer Einzelperson zugewiesenes Konto, über das sich die Person bei Spectrum™ Technology Platform authentifiziert, und zwar entweder bei einem der Client-Tools, wie z. B. der Enterprise Designer oder die Management Console, oder beim Aufrufen eines Dienstes über Webdienste oder die API.

Einem Benutzer ist mindestens eine Rolle zugewiesen. Eine *Rolle* ist eine Sammlung von Berechtigungen, die den Zugriff auf verschiedene Teile des Systems gewähren oder verweigern. Rollen spiegeln in der Regel die Art der Interaktionen wider, die zwischen einem bestimmten Benutzertyp und dem System bestehen. Beispiel: Sie verfügen über eine Rolle für Datenfluss-Designer, die Zugriff zum Erstellen und Ändern von Datenflüssen gewährt, sowie über

eine weitere Rolle für Personen, die lediglich Daten über vorhandene Datenflüsse verarbeiten müssen.

Eine Rolle gewährt Berechtigungen für gesicherte Entitätstypen. Ein *gesicherter Entitätstyp* stellt eine Kategorie von Elementen dar, für die der Zugriff gewährt oder verweigert werden soll. Es gibt beispielsweise den gesicherten Entitätstyp „Datenflüsse“, der die Standardberechtigungen für alle Datenflüsse auf dem System steuert.

Wenn Sie eine Feinabstimmung für den Zugriff vornehmen müssen, können Sie die Einstellungen in der Rolle oder dem Benutzer optional durch Konfigurieren der Zugriffssteuerung überschreiben. Die Berechtigungen für einen Benutzer werden über Zugriffssteuerungseinstellungen zusammen mit Rollen definiert. Durch Rollen werden die Berechtigungen für Entitätskategorien definiert, z. B. alle Datenflüsse oder alle Datenbankressourcen, und durch Zugriffssteuerungseinstellungen werden die Berechtigungen für bestimmte Entitäten definiert, so genannte *gesicherte Entitäten*. Zu Beispielen für gesicherte Entitäten zählen bestimmte Aufträge oder bestimmte Datenbankverbindungen. Das Definieren von Zugriffssteuerungseinstellungen ist optional. Wenn Sie keine Zugriffssteuerungseinstellungen definieren, werden die Berechtigungen des Benutzers durch die in der Rolle definierten Berechtigungen gesteuert.

Die Berechtigungen für einen Benutzer werden über Zugriffssteuerungseinstellungen zusammen mit Rollen definiert. Durch Rollen werden die Berechtigungen für Entitätskategorien definiert, z. B. alle Datenflüsse oder alle Datenbankressourcen, und durch Zugriffssteuerungseinstellungen werden die Berechtigungen für bestimmte Entitäten definiert, so genannte *gesicherte Entitäten*. Zu Beispielen für gesicherte Entitäten zählen bestimmte Aufträge oder bestimmte Datenbankverbindungen. Beispiel: Sie verfügen über eine Rolle, die für den gesicherten Entitätstyp „Datenflüsse“ die Berechtigung zum Ändern gewährt hat. Sie möchten jedoch verhindern, dass Benutzer einen bestimmten Datenfluss ändern. Dies ist möglich, indem Sie die Berechtigung zum Ändern für den bestimmten Datenfluss über die Zugriffssteuerung entfernen. Sie können Zugriffssteuerungseinstellungen für Benutzer und Rollen angeben. Durch die Zugriffssteuerungseinstellungen eines Benutzers werden die von den Benutzerrollen gewährten Berechtigungen dieses bestimmten Benutzers überschrieben. Zugriffssteuerungseinstellungen für Rollen gelten für alle Benutzer mit dieser Rolle.

Benutzer

In Spectrum™ Technology Platform-Benutzerkonten werden die Arten von Aktionen gesteuert, die Benutzer auf dem System ausführen können. Benutzerkonten sind für folgende Aktionen erforderlich:

- Verwenden von Tools wie Management Console, Enterprise Designer, Metadata Insights und Befehlszeilentools
- Ausführen von Aufträgen in einem Zeitplan
- Ausführen von Aufträgen über die Befehlszeile
- Zugriff auf Dienste über Webservices oder die API

Im Lieferumfang des Systems ist ein Administratorkonto mit dem Namen **admin** enthalten. Dieses Konto verfügt über Vollzugriff. Das ursprüngliche Kennwort lautet „admin“.

Wichtig: Sie sollten das Kennwort „admin“ sofort nach der Installation von Spectrum™ Technology Platform ändern, um einen nicht autorisierten Administratorzugriff auf Ihr System zu verhindern.

Sie können so viele Benutzerkonten wie gewünscht erstellen.

Hinzufügen eines Benutzers

In dieser Prozedur wird beschrieben, wie ein Spectrum™ Technology Platform-Benutzerkonto erstellt wird und wie dem Konto eine Rolle zugewiesen wird.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Klicken Sie auf die Schaltfläche „Hinzufügen“  .
4. Lassen Sie den Schalter **Aktiviert** weiter **Eingeschaltet**, wenn dieses Benutzerkonto zur Verwendung verfügbar sein soll.
5. Geben Sie im Feld **Benutzername** den Benutzernamen ein.

   Anmerkung: Benutzernamen dürfen nur ASCII-Zeichen enthalten. Bei Benutzernamen muss die Groß-/Kleinschreibung beachtet werden.

6. Geben Sie im Feld **E-Mail-Adresse** die E-Mail-Adresse des Benutzers ein. Die E-Mail-Adresse wird von einigen Modulen verwendet, um Benachrichtigungen an Benutzer zu senden.
7. Geben Sie im Feld **Beschreibung** eine Beschreibung des Benutzers ein.
8. Geben Sie das Kennwort des Benutzers ein und bestätigen Sie es.
9. Wählen Sie die Rollen aus, die Sie diesem Benutzer erteilen möchten.

   Sie können Ihre eigenen Rollen erstellen oder eine der Standardrollen verwenden. Die Standardrollen sind:

Administrator	Diese Rolle hat auf alle Teile des Systems Vollzugriff.
Designer	Diese Rolle ist für Benutzer vorgesehen, die Datenflüsse und Prozessflüsse im Enterprise Designer erstellen. Sie bietet die Möglichkeit, Datenflüsse zu entwerfen und auszuführen.
Integrator	Diese Rolle ist für Benutzer vorgesehen, die Daten über Spectrum™ Technology Platform verarbeiten müssen, jedoch keine Datenflüsse erstellen oder ändern müssen. Sie ermöglicht es Benutzern, über Webservices und die API auf Dienste zuzugreifen und Aufträge auszuführen.
Benutzer	Dies ist die Standardrolle. Sie bietet keinen Zugriff auf das System. Benutzer mit dieser Rolle können nur dann auf das System zugreifen, wenn Sie über Änderungen gesicherter Entitäten eine Berechtigung erteilen.

   Informationen zum Erstellen von Rollen finden Sie unter **Erstellen einer Rolle** auf Seite 25.

10. Klicken Sie auf **Speichern**.

Ändern eines Kennworts

In dieser Prozedur wird beschrieben, wie das Kennwort eines Benutzers geändert wird.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Wählen Sie einen Benutzer aus und klicken Sie anschließend auf die Schaltfläche „Bearbeiten“  .
4. Klicken Sie auf **Kennwort ändern**.
5. Geben Sie das neue Kennwort ein und geben Sie es zur Bestätigung ein zweites Mal ein.
6. Klicken Sie auf **Speichern**.

Festlegen einer minimalen Kennwortlänge

Beim Erstellen oder Ändern eines Kennworts wird die minimale Kennwortlänge erzwungen. Vorhandene Kennwörter, die die minimale Länge nicht erreichen, sind weiterhin gültig.

1. Öffnen Sie einen Webbrowser, und rufen Sie Folgendes auf:`http://server:port/jmx-console`

   Dabei gilt Folgendes:

   server ist die IP-Adresse oder der Hostname Ihres Spectrum™ Technology Platform-Servers.

   port ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der Standardwert ist 8080.
2. Melden Sie sich mit dem Administratorkonto an.
3. Klicken Sie unter „Domäne: com.pb.spectrum.platform.config“ auf **com.pb.spectrum.platform.config:manager=AccountConfigurationManager**.
4. Legen Sie im Vorgang **updatePasswordPolicy** die Option **enableAdvanceControl** auf **Wahr** fest.
5. Geben Sie im Feld **minLength** die minimale Kennwortlänge ein.
6. Klicken Sie auf **Aufrufen**.
7. Klicken Sie auf **Zurück zur MBean-Ansicht**, um zum Bildschirm „Kontokonfigurationsmanager“ zurückzukehren.

Ändern Ihrer E-Mail-Adresse

Die mit Ihrem Konto verbundene E-Mail-Adresse wird von einigen Modulen verwendet, um Ihnen Benachrichtigungen zu senden. Wenn Sie Ihre E-Mail-Adresse ändern möchten, führen Sie die folgenden Schritte aus.

1. Melden Sie sich an der Management Console an.
2. Klicken Sie auf das Benutzermenü oben rechts.
3. Wählen Sie **Profil** aus.

4. Geben Sie im Feld **E-Mail** Ihre neue E-Mail-Adresse ein.
5. Klicken Sie auf **Speichern**.

Deaktivieren eines Benutzerkontos

Sie können ein Benutzerkonto deaktivieren, damit darüber nicht auf Spectrum™ Technology Platform zugegriffen werden kann. Alle in einem Zeitplan mit einem deaktivierten Benutzerkonto ausgeführten Aufträge werden nicht ausgeführt.

Anmerkung: Das Benutzerkonto „Admin“ kann nicht deaktiviert werden.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Aktivieren Sie das Kästchen neben dem zu ändernden Benutzer und klicken Sie anschließend auf die Schaltfläche „Bearbeiten“ .
4. Stellen Sie den Schalter **Aktiviert** auf **Deaktiviert** um.
5. Klicken Sie auf **Speichern**.

Das Benutzerkonto ist jetzt deaktiviert und kann nicht für den Zugriff auf Spectrum™ Technology Platform verwendet werden.

Löschen eines Benutzers

In dieser Prozedur wird beschrieben, wie ein Spectrum™ Technology Platform-Benutzerkonto dauerhaft gelöscht werden kann.

Tipp: Benutzerkonten können auch deaktiviert werden. Auf diese Weise wird verhindert, dass das Konto für den Zugriff auf das System verwendet wird, ohne dass das Konto gelöscht werden muss.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Aktivieren Sie das Kästchen neben dem zu löschenden Benutzer und klicken Sie anschließend auf die Schaltfläche „Löschen“ .

Anmerkung: Das Benutzerkonto „Admin“ kann nicht gelöscht werden.

Sperren von Benutzerkonten

Als Sicherheitsmaßnahme werden Benutzerkonten nach fünf nicht erfolgreichen Authentifizierungsversuchen in Folge deaktiviert. Dies umfasst nicht erfolgreiche Authentifizierungsversuche im Enterprise Designer, in der Management Console, in Webservices und in der Client-API.

Als Administrator können Sie ein Benutzerkonto wieder aktivieren, indem Sie sich bei der Management Console anmelden, den Benutzer bearbeiten und den Schalter **Aktiviert** auf **Ein**

stellen. Benutzerkonten können auch über die Administrationsumgebung wieder aktiviert werden. Benutzer können ihre eigenen Konten nicht entsperren.

> **Anmerkung:** Wenn Sie LDAP oder Active Directory für die Authentifizierung verwenden, finden die Regeln dieser Dienste zum Sperren von Konten Anwendung. Ihre LDAP- oder Active Directory-Regeln lassen unter Umständen mehr oder weniger nicht erfolgreiche Anmeldeversuche zu als Spectrum™ Technology Platform.

Entsperren des Kontos „Admin“

Benutzer werden nach mehreren, nicht erfolgreichen Anmeldeversuchen gesperrt. Die meisten Benutzerkonten können über die Management Console entsperrt werden, das Konto „Admin“ jedoch nicht. Stattdessen müssen Sie zum Entsperren des Kontos „Admin“ ein Skript auf dem Server ausführen.

1. Melden Sie sich auf dem Server an, auf dem Spectrum™ Technology Platform ausgeführt wird.

   Melden Sie sich bei einem beliebigen Knoten an, wenn Sie Spectrum™ Technology Platform in einem Cluster ausführen. Sie müssen das Skript zum Entsperren nur auf einem der Knoten ausführen.

2. Öffnen Sie eine Eingabeaufforderung und rufen Sie den Ordner `*Spectrum Folder*\server\bin` auf.
3. (Nur unter Unix und Linux) Führen Sie den folgenden Befehl aus:

   ```
   . ./setup
   ```

4. Führen Sie das Skript „enableadmin“ aus, indem Sie den folgenden Befehl eingeben:

   Unter Windows:

   ```
   enableadmin.bat -h Host und Port -p Admin-Kennwort [-s]
   ```

   Unter Unix und Linux:

   ```
   ./enableadmin.sh -h Host und Port -p Admin-Kennwort [-s]
   ```

   Wo:

Host und Port	Der in Spectrum™ Technology Platform verwendete Hostname und HTTP-Port. Beispiel: `spectrumserver:8080`.
Admin-Kennwort	Das Kennwort für das Konto „Admin“. Wenn Ihnen das Kennwort für das Konto „Admin“ nicht bekannt ist und das Konto „Admin“ gesperrt wurde, wenden Sie sich an den technischen Support von Pitney Bowes.
-s	Geben Sie `-s` an, wenn Spectrum™ Technology Platform für die Verwendung von HTTPS konfiguriert wurde.

Automatische Abmeldung aufgrund von Inaktivität

Benutzer des Enterprise Designer und Webclients wie die Management Console, der Relationship Analysis Client, das Business Steward Portal und andere werden nach 30 Minuten Inaktivität automatisch abgemeldet.

Rollen

Eine *Rolle* ist eine Sammlung von Berechtigungen, die den Zugriff auf verschiedene Teile des Systems gewähren oder verweigern. Rollen spiegeln in der Regel die Art der Interaktionen wider, die zwischen einem bestimmten Benutzertyp und dem System bestehen. Beispiel: Sie verfügen über eine Rolle für Datenfluss-Designer, die Zugriff zum Erstellen und Ändern von Datenflüssen gewährt, sowie über eine weitere Rolle für Personen, die lediglich Daten über vorhandene Datenflüsse verarbeiten müssen.

In Spectrum™ Technology Platform sind folgende Rollen bereits definiert:

Administrator	Diese Rolle hat auf alle Teile des Systems Vollzugriff.
Designer	Diese Rolle ist für Benutzer vorgesehen, die Datenflüsse und Prozessflüsse im Enterprise Designer erstellen. Sie bietet die Möglichkeit, Datenflüsse zu entwerfen und auszuführen.
Integrator	Diese Rolle ist für Benutzer vorgesehen, die Daten über Spectrum™ Technology Platform verarbeiten müssen, jedoch keine Datenflüsse erstellen oder ändern müssen. Sie ermöglicht es Benutzern, über Webservices und die API auf Dienste zuzugreifen und Aufträge auszuführen.
Benutzer	Dies ist die Standardrolle. Sie bietet keinen Zugriff auf das System. Benutzer mit dieser Rolle können nur dann auf das System zugreifen, wenn Sie über Änderungen gesicherter Entitäten eine Berechtigung erteilen.

Anmerkung: Weitere Informationen zu den vordefinierten Rollen für das Location Intelligence-Modul finden Sie unter **Sicherheit für das Location Intelligence-Modul** auf Seite 53.

Öffnen Sie die Management Console und die Option **Sicherheit**, und klicken Sie auf **Rollen**, um die für die einzelnen Rollen erteilten Berechtigungen anzuzeigen. Wählen Sie anschließend die Rolle aus, die angezeigt werden soll, und klicken Sie auf **Anzeigen**.

Tipp: Die vordefinierten Rollen können nicht geändert werden. Sie können jedoch neue Rollen erstellen und dabei die vordefinierten Rollen als Startpunkt verwenden.

Erstellen einer Rolle

Eine Rolle ist eine Sammlung von Berechtigungen, die einem Benutzer zugewiesen werden. Wenn die in Spectrum™ Technology Platform enthaltenen vordefinierten Rollen nicht den Bedürfnissen Ihrer Organisation entsprechen, können Sie Ihre eigenen Rollen erstellen.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Klicken Sie auf **Rollen**.
4. Klicken Sie auf die Schaltfläche „Hinzufügen“  .

   Tipp: Wenn Sie eine Rolle erstellen möchten, die einer vorhandene Rolle ähnelt, können Sie die vorhandene Rolle kopieren, indem Sie das Kästchen neben der zu kopierenden Rolle aktivieren und anschließend auf die Schaltfläche „Kopieren“ klicken  . Anschließend können Sie die neue Rolle bearbeiten und mit den folgenden Schritten fortfahren.

5. Geben Sie im Feld **Rollenname** den gewünschten Namen für diese Rolle ein. Sie können den Namen frei wählen.
6. Optional: Da die Liste der gesicherten Entitätstypen lang sein kann, können Sie auch nur eine bestimmte Gruppe gesicherter Entitätstypen anzeigen. Dies kann hilfreich sein, wenn Sie die gleichen Berechtigungen auf alle Entitäten in einer Gruppe anwenden möchten. Wenn Sie beispielsweise die Berechtigung zum Ändern aus allen Datenbankressourcen entfernen möchten, könnten Sie die Liste so filtern, dass nur die Gruppe „Datenbankressourcen“ angezeigt wird. Gehen Sie wie folgt vor, um nur eine Gruppe anzuzeigen und zu ändern:
   a) Aktivieren Sie das Kästchen **Gruppenfilterung aktivieren**.
   b) Klicken Sie in der im Header der Spalte **Gruppe** auf das Trichtersymbol und wählen Sie die Gruppe aus, die Sie anzeigen möchten.
   c) Aktivieren oder deaktivieren Sie im Header der Spalte das Kästchen bei der Berechtigung, die angewendet werden soll.
   d) Klicken Sie auf das Filtersymbol, wählen Sie **(Alle)** aus und deaktivieren Sie anschließend das Kästchen **Gruppenfilterung aktivieren**, um zur vollständigen Liste der gesicherten Entitätstypen zurückzukehren.
7. Wählen Sie die Berechtigungen aus, die Sie für die einzelnen Entitätstypen erteilen möchten. Es gibt folgende Berechtigungen:

   Anzeige Ermöglicht es dem Benutzer, im Entitätstyp enthaltene Entitäten anzuzeigen. Wenn Sie beispielsweise für den Entitätstyp „JDBC-Verbindung“ die Berechtigung zum Anzeigen erteilen, können Benutzer mit dieser Rolle Datenbankverbindungen in der Management Console anzeigen.

   Ändern Ermöglicht es dem Benutzer, im Entitätstyp enthaltene Entitäten zu ändern. Wenn Sie beispielsweise für den Entitätstyp „JDBC-Verbindung“ die Berechtigung zum Ändern erteilen, können Benutzer mit dieser Rolle Datenbankverbindungen in der Management Console ändern.

Erstellen Ermöglicht es dem Benutzer, Entitäten zu erstellen, die in die Kategorie dieses Entitätstyps fallen. Wenn Sie beispielsweise für den Entitätstyp „JDBC-Verbindung“ die Berechtigung zum Erstellen erteilen, können Benutzer mit dieser Rolle in der Management Console neue Datenbankverbindungen erstellen.

Löschen Ermöglicht es dem Benutzer, im Entitätstyp enthaltene Entitäten zu löschen. Wenn Sie beispielsweise für den Entitätstyp „JDBC-Verbindung“ die Berechtigung zum Löschen erteilen, können Benutzer mit dieser Rolle Datenbankverbindungen in der Management Console löschen.

Ausführen Ermöglicht es dem Benutzer, die Verarbeitung von Aufträgen, Diensten und Prozessflüssen einzuleiten. Wenn Sie beispielsweise für den Entitätstyp „Auftrag“ die Berechtigung zum Ausführen erteilen, können Benutzer mit dieser Rolle Batchaufträge ausführen. Wenn Sie für den Entitätstyp „Dienst“ die Berechtigung zum Ausführen erteilen, können Benutzer mit dieser Rolle auf Dienste zugreifen, die in Spectrum™ Technology Platform über die API oder Webservices ausgeführt werden.

8. Klicken Sie auf **Speichern**.

Die Rolle kann jetzt einem Benutzer zugewiesen werden.

Löschen einer Rolle

Eine Rolle kann gelöscht werden, wenn sie keinem Benutzer mehr zugewiesen ist.

> **Anmerkung:** Folgende Rollen können nicht gelöscht werden: Administrator, Benutzer, Designer und Integrator.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Stellen Sie auf der Registerkarte **Benutzer** sicher, dass die Rolle, die gelöscht werden soll, keinem Benutzer zugewiesen ist. Eine Rolle kann nicht gelöscht werden, wenn sie einem Benutzer zugewiesen ist.
4. Klicken Sie auf **Rollen**.
5. Aktivieren Sie das Kästchen neben der zu löschenden Rolle und klicken Sie anschließend auf die Schaltfläche „Löschen“  .

Deaktivieren der rollenbasierten Sicherheit

Die rollenbasierte Sicherheit ist standardmäßig aktiviert. Dies bedeutet, dass die den Benutzern über Rollen zugewiesenen Sicherheitseinschränkungen erzwungen werden. Wenn Sie die rollenbasierte Sicherheit deaktivieren möchten, werden die den Benutzern zugewiesenen Sicherheitseinschränkungen nicht erzwungen, sodass alle Benutzer Zugriff auf alle Teile des Systems haben. Beachten Sie, dass für den Zugriff auf Dienste immer ein gültiges Benutzerkonto erforderlich ist, selbst dann, wenn Sie die rollenbasierte Sicherheit deaktivieren.

In dieser Prozedur wird beschrieben, wie die rollenbasierte Sicherheit deaktiviert wird.

Warnung: Wenn Sie diese Prozedur befolgen, haben alle Benutzer Vollzugriff auf Ihr Spectrum™ Technology Platform-System.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Stellen Sie den Schalter **Zugriff nach Rolle beschränken** auf **Deaktiviert** um.

Gesicherte Entitätstypen – Plattform

Ein Entitätstyp stellt eine Kategorie von Elementen dar, für die der Zugriff gewährt oder verweigert werden soll. Es gibt beispielsweise den Entitätstyp „Datenflüsse“, der Berechtigungen für alle Datenflüsse auf dem System steuert. Plattformentitätstypen gelten für alle Spectrum™ Technology Platform-Installationen, während modulspezifische Entitätstypen nur gelten, wenn Sie bestimmte Module installiert haben. Die Entitätstypen auf Plattformebene lauten wie folgt:

Überwachungsprotokoll	Steuert den Zugriff auf den Bereich **System** > **Protokolle** > **Prüfprotokoll** in der Management Console.
Datenflüsse	Steuert den Zugriff auf alle Datenflusstypen (Aufträge, Dienste und Unterflüsse) im Enterprise Designer. **Anmerkung:** Wenn ein Benutzer nicht über die Berechtigung zum Bearbeiten verfügt, werden ihm im Bereich „**Versionen**“ im Enterprise Designer nur die verfügbar gemachte Version und die zuletzt gespeicherte Version angezeigt.
Datenflüsse – verfügbar machen	Steuert die Möglichkeit, Datenflüsse zur Ausführung zur Verfügung zu stellen. **Anmerkung:** Um die zuletzt gespeicherte Version des Datenflusses (die Version, die im Bereich „**Versionen**“ im Enterprise Designer immer oben steht) verfügbar zu machen, muss der Benutzer zusätzlich zur Berechtigung zum Bearbeiten für den gesicherten Entitätstyp **Datenflüsse – verfügbar machen** über die Berechtigung zum Bearbeiten für den gesicherten Entitätstyp **Datenflüsse** verfügen. Der Grund dafür ist, dass zunächst die zuletzt gespeicherte Version als Version gespeichert werden muss, bevor sie verfügbar gemacht werden kann. Dies macht die Berechtigung zum Bearbeiten für den Datenfluss erforderlich.
Flussstandardwerte – Datentypkonvertierung	Steuert den Zugriff auf den Bereich **Flüsse** > **Standardwerte** > **Datentypkonvertierungen** in der Management Console. Alle Benutzer haben Ansichtszugriff auf alle Optionen für Datentypkonvertierungen. Der Ansichtszugriff kann nicht entfernt werden.

Flussstandardwerte – falsch formatierte Datensätze	Steuert den Zugriff auf den Bereich **Flüsse** > **Standardwerte** > **Falsch formatierte Datensätze** in der Management Console. Alle Benutzer haben Ansichtszugriff auf Optionen für falsch formatierte Datensätze. Der Ansichtszugriff kann nicht entfernt werden.
Flussstandardwerte – Berichte	Steuert den Zugriff auf den Bereich **Flüsse** > **Standardwerte** > **Berichte** in der Management Console. Alle Benutzer haben Ansichtszugriff auf Berichtsoptionen. Der Ansichtszugriff kann nicht entfernt werden.
Flussstandardwerte – Sortierleistung	Steuert den Zugriff auf den Bereich **Flüsse** > **Standardwerte** > **Sortierleistung** in der Management Console. Alle Benutzer haben Ansichtszugriff auf Optionen für die Sortierleistung. Der Ansichtszugriff kann nicht entfernt werden.
Flussverlauf – Aufträge	Steuert den Ansichtszugriff auf den Ausführungsverlauf von Aufträgen im Enterprise Designer und in der Management Console.
Flussverlauf – Prozessflüsse	Steuert den Zugriff auf den Ausführungsverlauf von Prozessflüssen in der Management Console und im Enterprise Designer.
Flussverlauf – Transaktionen	Steuert den Zugriff auf den Bereich **Flüsse** > **Verlauf** > **Transaktionen** in der Management Console.
Flussplanung	Steuert den Zugriff auf den Bereich **Fluss** > **Zeitpläne** in der Management Console.
Aufträge	Steuert die Möglichkeit, Aufträge im Enterprise Designer, in der Management Console, im Job Executor und in der Administrationsumgebung auszuführen.
Benachrichtigung – Lizenzablauf	Steuert den Zugriff für die Konfiguration von Benachrichtigungs-E-Mails über einen Lizenzablauf in der Management Console.
Benachrichtigung – SMTP-Einstellungen	Steuert den Zugriff auf den Bereich **System** > **Mailserver** in der Management Console.
Prozessflüsse	Steuert den Zugriff auf Prozessflüsse im Enterprise Designer. **Anmerkung:** Wenn ein Benutzer nicht über die Berechtigung zum Bearbeiten verfügt, werden ihm im Bereich „**Versionen**“ im Enterprise Designer nur die verfügbar gemachte Version und die zuletzt gespeicherte Version angezeigt.
Prozessflüsse – verfügbar machen	Steuert die Möglichkeit, im Enterprise Designer Prozessflüsse zur Ausführung zur Verfügung zu stellen. **Anmerkung:** Um die zuletzt gespeicherte Version des Datenflusses (die Version, die im Bereich „**Versionen**“ im Enterprise Designer immer oben steht) verfügbar zu machen, muss der Benutzer zusätzlich zur Berechtigung zum Bearbeiten für den gesicherten Entitätstyp **Prozessflüsse – verfügbar machen** über die Berechtigung zum Bearbeiten für den gesicherten Entitätstyp **Prozessflüsse** verfügen. Der Grund dafür ist, dass zunächst die zuletzt gespeicherte Version als Version gespeichert werden muss, bevor sie verfügbar gemacht

werden kann. Dies macht die Berechtigung zum Bearbeiten für den Datenfluss erforderlich.

Ressourcen – Datenbankverbindungen	Steuert die Möglichkeit, Datenbankverbindungen in der Management Console zu konfigurieren.
Ressourcen – Externe Webservices	Steuert den Zugriff auf verwaltende externe Webservices in der Management Console.
Ressourcen – Dateiserververbindungen	Steuert die Möglichkeit, Dateiserver in der Management Console zu konfigurieren.
Ressourcen – JDBC-Treiber	Steuert die Möglichkeit, JDBC-Treiber in der Management Console zu konfigurieren.
Ressourcen – Remoteserver	Steuert den Zugriff auf den Bereich **Ressourcen** > **Remoteserver** in der Management Console.
Sicherheit – Zugriffssteuerung	Steuert den Zugriff auf Zugriffssteuerungseinstellungen im Bereich **System** > **Sicherheit** > **Zugriffssteuerung** in der Management Console.
Sicherheit – Zugriffstoken	Steuert die Möglichkeit, Token von Benutzern anzuzeigen und zu löschen. Ein Token ermöglicht die Authentifizierung zwischen einem Client und dem Server. Mit der Berechtigung zum Lesen können Sie eine Liste der aktiven Token anzeigen, von denen jedes eine aktive Sitzung repräsentiert. Mit der Berechtigung zum Löschen können Sie Token von Benutzern löschen, wodurch ihre Sitzung beendet wird.
Sicherheit – Verzeichniszugriff	Steuert die Möglichkeit, Einschränkungen in Serververzeichnisressourcen über den Bereich **System** > **Sicherheit** > **Verzeichniszugriff** in der Management Console zu aktivieren oder zu deaktivieren.
Sicherheit – Verzeichnispfade	Steuert die Möglichkeit, Serververzeichnisressourcen im Bereich **System** > **Sicherheit** > **Verzeichniszugriff** in der Management Console zu konfigurieren.
Sicherheit – Optionen	Steuert die Möglichkeit, die Sicherheit im Bereich **System** > **Sicherheit** > **Rollen** in der Management Console zu aktivieren und zu deaktivieren.
Sicherheit – Rollen	Steuert den Zugriff auf die Rollenkonfiguration im Bereich **System** > **Sicherheit** > **Rollen** in der Management Console.
Sicherheit – Verzeichnispfade	Steuert die Möglichkeit, Serververzeichnisressourcen im Bereich **System** > **Sicherheit** > **Verzeichniszugriff** in der Management Console zu konfigurieren.
Sicherheit – Benutzer	Steuert den Zugriff für die Verwaltung von Benutzerkonten im Bereich **System** > **Sicherheit** > **Benutzer** in der Management Console.
Dienste	Steuert die Möglichkeit, Dienste über die API und über Webservices auszuführen.
Schritten	Steuert, ob verfügbar gemachte Unterflüsse im Enterprise Designer als Schritte in Datenflüssen verfügbar sind.

System – Lizenzierung	Steuert den Zugriff auf Lizenzinformationen, die im Bereich **System** > **Lizenzierung und Ablauf** in der Management Console angezeigt werden.
System – Versionsinformationen	Steuert den Zugriff auf den Bereich **System** > **Version** in der Management Console.
Systemprotokoll	Steuert den Zugriff auf das Systemprotokoll in der Management Console.

Gesicherte Entitätstypen – Location Intelligence-Modul

Ein Entitätstyp stellt eine Kategorie von Elementen dar, für die der Zugriff gewährt oder verweigert werden soll. Das Location Intelligence-Modul umfasst folgende modulspezifische Entitätstypen:

Benannte Ressourcen	Steuert Berechtigungen für alle benannten Ressourcen im Location Intelligence-Modul. Benutzer der Location Intelligence-Moduldienste müssen für die von Ihnen verwendeten Ressourcen und alle abhängigen Ressourcen mindestens über Berechtigungen zum Lesen verfügen. Bei der Erstellung einer benannten Ressource (mit einem beliebigen Tool, Spatial Manager, die Administrationsumgebung, den Named Resource-Dienst und WebDAV inbegriffen) wird für die benannte Ressource automatisch eine neue gesicherte Entität vom Typ „LocationIntelligence.Named Resource“ erstellt.
Dataset.DML	Steuert Berechtigungen für im Location Intelligence-Modul verwendete Datasets, die benannten Tabellen zugeordnet sind. Bei der Erstellung oder dem Hochladen einer benannten Tabelle (mit einem beliebigen Tool, Spatial Manager, die Administrationsumgebung, den Named Resource-Dienst und WebDAV inbegriffen) wird für das zugeordnete Dataset der benannten Tabelle automatisch eine neue gesicherte Entität vom Typ „LocationIntelligence.Dataset“ erstellt. Ein Benutzer muss für eine benannte Tabelle über Berechtigungen zum Anzeigen *und* für das Dataset über Berechtigungen zum Erstellen/Ändern/Löschen verfügen, um DML-Vorgänge in beschreibbaren (JDBC-basierten) Tabellen ausführen zu können. DML-Vorgänge beinhalten das Einfügen, Aktualisieren und Löschen ausgeführter Vorgänge unter Verwendung des „Write Spatial Data“-Schrittes oder des Feature-Dienstes.

Zugriffssteuerung

Die Berechtigungen für einen Benutzer werden über Zugriffssteuerungseinstellungen zusammen mit Rollen definiert. Durch Rollen werden die Berechtigungen für Entitätskategorien definiert, z. B. alle Datenflüsse oder alle Datenbankressourcen, und durch Zugriffssteuerungseinstellungen werden die Berechtigungen für bestimmte Entitäten definiert, so genannte *gesicherte Entitäten*. Zu Beispielen für gesicherte Entitäten zählen bestimmte Aufträge oder bestimmte Datenbankverbindungen. Beispiel: Sie verfügen über eine Rolle, die für den gesicherten Entitätstyp „Datenflüsse“ die Berechtigung zum Ändern gewährt hat. Sie möchten jedoch verhindern, dass Benutzer einen bestimmten Datenfluss ändern. Dies ist möglich, indem Sie die Berechtigung zum Ändern für den bestimmten Datenfluss über die Zugriffssteuerung entfernen. Sie können Zugriffssteuerungseinstellungen für Benutzer und Rollen angeben. Durch die Zugriffssteuerungseinstellungen eines Benutzers werden die von den

Benutzerrollen gewährten Berechtigungen dieses bestimmten Benutzers überschrieben. Zugriffssteuerungseinstellungen für Rollen gelten für alle Benutzer mit dieser Rolle.

Konfigurieren der Zugriffssteuerung

Die Berechtigungen für einen Benutzer werden über Zugriffssteuerungseinstellungen zusammen mit Rollen definiert. Durch Rollen werden die Berechtigungen für Entitätskategorien definiert, z. B. alle Datenflüsse oder alle Datenbankressourcen, und durch Zugriffssteuerungseinstellungen werden die Berechtigungen für bestimmte Entitäten definiert, z. B. bestimmte Aufträge oder Datenbankverbindungen.

Um Zugriffssteuerungen konfigurieren zu können, müssen Sie über Berechtigungen zum Anzeigen und Ändern dieser gesicherten Entitätstypen verfügen:

- Sicherheit – Zugriffssteuerung
- Sicherheit – Rollen
- Sicherheit – Benutzer

Gehen Sie wie folgt vor, um eine Zugriffssteuerung zu konfigurieren:

1. Klicken Sie in der Management Console auf **System** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Zugriffssteuerung**.
3. Klicken Sie auf die Schaltfläche „Hinzufügen“ .
4. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Rolle**, wenn Sie Zugriffssteuerungen für eine Rolle angeben möchten. Die von Ihnen angegebenen Zugriffssteuerungsberechtigungen haben auf alle Benutzer Auswirkungen, die über die von Ihnen ausgewählte Rolle verfügen.
   - Klicken Sie auf **Benutzer**, wenn Sie Zugriffssteuerungen für einen einzelnen Benutzer angeben möchten. Die von Ihnen angegebenen Zugriffssteuerungsberechtigungen haben nur Auswirkungen auf den von Ihnen ausgewählten Benutzer.
5. Wählen Sie die Rolle oder den Benutzer aus, für die bzw. für den Sie Zugriffssteuerungen definieren möchten.
6. Klicken Sie auf die Schaltfläche „Hinzufügen“ .
7. Wählen Sie den gesicherten Entitätstyp aus, der die von Ihnen gewünschte gesicherte Entität enthält. Wenn Sie beispielsweise eine Zugriffssteuerung für einen Datenfluss konfigurieren möchten, wählen Sie „Plattorm.Dataflows“ aus.
8. Wählen Sie die gesicherte Entität aus, für die Sie Zugriffssteuerungen konfigurieren möchten, und klicken Sie dann auf die Schaltfläche **>>**, um sie zur Liste **Ausgewählte Entitäten** hinzuzufügen.
9. Klicken Sie auf **Hinzufügen**.

   Die von Ihnen ausgewählten gesicherten Entitäten werden angezeigt. Die Kästchen geben die gültigen Berechtigungen für die ausgewählte Rolle oder den ausgewählten Benutzer an.

10. Geben Sie die Berechtigungen an, die Sie für die einzelnen gesicherten Entitäten erteilen möchten. Die einzelnen gesicherten Entitäten können über folgende Berechtigungen verfügen:

	Die Berechtigung wird von der Rolle geerbt.
	Die Berechtigung wird von der Rolle geerbt und kann nicht außer Kraft gesetzt werden.
	Die Berechtigung wird erteilt und dabei wird die für den Benutzer oder die Rolle angegebene Berechtigung außer Kraft gesetzt.
	Die Berechtigung wird verweigert und dabei wird die für den Benutzer oder die Rolle angegebene Berechtigung außer Kraft gesetzt.

Beispiel für Zugriffssteuerungen

Im Folgenden werden Zugriffssteuerungseinstellungen für die Rolle „RetentionDepartmentDesigner“ angezeigt.

In diesem Beispiel ist der gesicherte Entitätstyp „Plattform.Datenfluss“ so festgelegt, dass die Berechtigungen zum Anzeigen und Ändern erteilt werden, die Berechtigung zum Löschen jedoch nicht. Folglich würde jeder Benutzer mit der Rolle „RetentionDepartmentDesigner“ für alle Datenflüsse über diese Berechtigungen verfügen. Sie möchten jedoch verhindern, dass Benutzer mit dieser Rolle nur den Datenfluss „Beispielauftrag 1“ ändern können. In diesem Fall müssen Sie das Kästchen bei „Beispielauftrag 1“ in der Spalte „Ändern“ deaktivieren. Jetzt können Benutzer mit dieser Rolle diesen Datenfluss nicht ändern, sie können aber weiterhin andere Datenflüsse ändern.

Löschen von Zugriffssteuerungseinstellungen

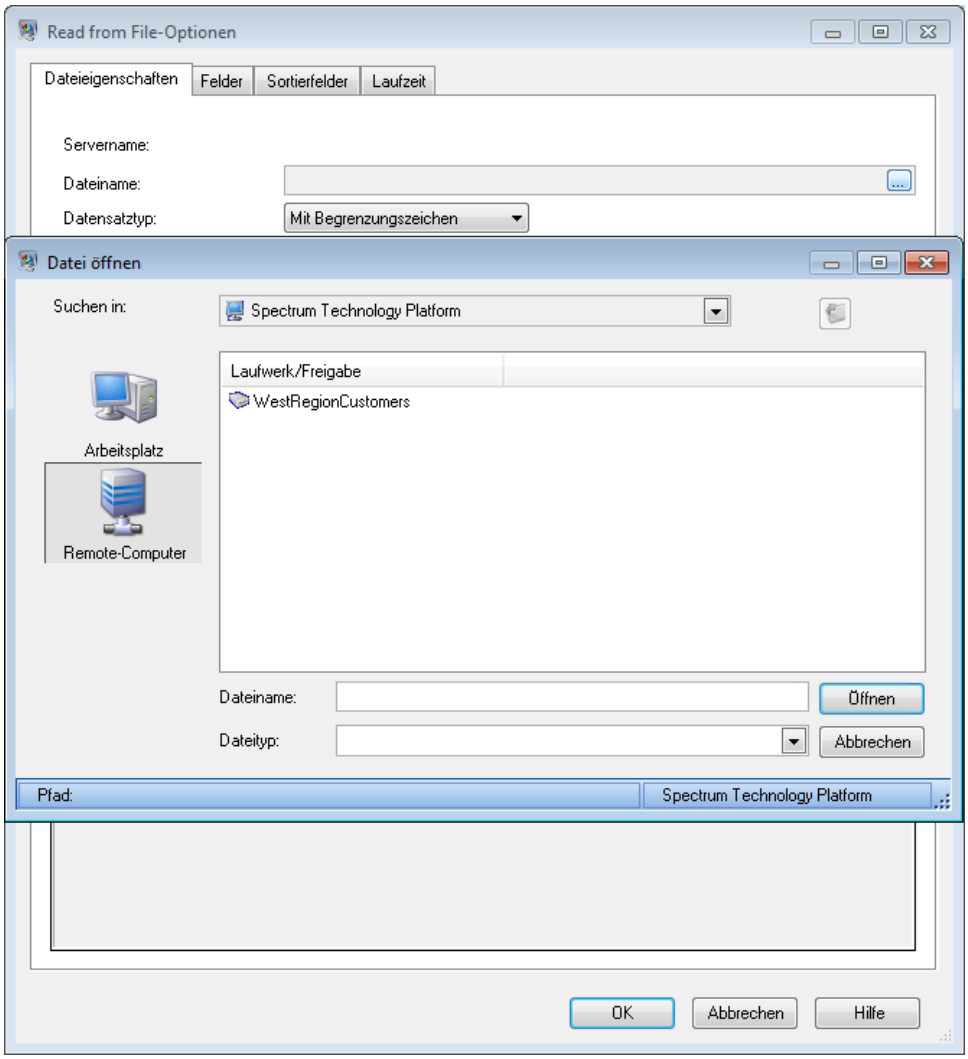
Wenn Sie Zugriffssteuerungseinstellungen für einen Benutzer oder eine Rolle löschen, werden die in den Zugriffssteuerungseinstellungen definierten Außerkraftsetzungen der Berechtigungen aus dem Bereich des Benutzers oder der Rolle entfernt. Dies bedeutet für Benutzer, dass die durch die Rolle eines Benutzers erteilten Berechtigungen ohne Außerkraftsetzungen wirksam werden. Für Rollen bedeutet dies, dass die in der Rolle selbst definierten Berechtigungen ohne Außerkraftsetzungen wirksam werden.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Klicken Sie auf **Zugriffssteuerung**.
4. Aktivieren Sie das Kästchen neben dem Benutzer oder der Rolle, bei dem bzw. bei der Sie eine Zugriffssteuerung entfernen möchten, und klicken Sie anschließend auf die Schaltfläche „Löschen“  .

Begrenzen des Serververzeichniszugriffs

Wenn Benutzer Aufgaben ausführen, für die sie eine Datei auswählen müssen, können sie die Ordner des Spectrum™ Technology Platform-Servers durchsuchen. So können Benutzer beispielsweise den Server durchsuchen, wenn sie eine Eingabe- oder Ausgabedatei in einem Quell- oder Datenladungsschritt im Enterprise Designer auswählen. Als Administrator möchten Sie eventuell den Zugriff beschränken, sodass empfindliche Teile des Servers nicht durchsucht oder geändert werden können.

Eine Möglichkeit, den gesamten Zugriff auf das Dateisystem des Servers zu unterbinden, ist, sicherzustellen, dass Benutzer nicht über die Plattform-Sicherheitsberechtigung **Sicherheit – Verzeichnispfade** verfügen. So verhindern Sie den Zugriff auf alle Ordner auf dem Server. Sie können außerdem den Zugriff auf einige Ordner auf dem Server verhindern, während Sie den Zugriff auf andere Ordner gewähren. Wenn Sie eingeschränkten Zugriff gewähren, werden die Ordner, auf die Sie Zugriff gewähren, in den obersten Ordnern in den Fenstern zum Durchsuchen der Dateien angezeigt. Wenn Sie Benutzern z. B. erlauben, nur auf einen Ordner auf dem Server „WestRegionCustomers“ zuzugreifen, würden die Benutzer beim Durchsuchen des Servers nur diesen Ordner sehen, wie hier dargestellt:



Wichtig: Es gibt zwei Situationen, bei denen Benutzer das gesamte Dateisystem des Server anzeigen können, auch wenn Sie nur eingeschränkten Zugriff gewährt haben:

- Benutzer durchsuchen den Server während der Erstellung einer Spectrum-Datenbank in der Management Console nach einer Datenbankdatei.
- Benutzer durchsuchen den Server während der Erstellung eines Treibers in der Management Console nach einer JDBC-Treiberdatei.

Um Benutzer daran zu hindern, das gesamte Dateisystem des Servers zu durchsuchen, verwenden Sie Rollen, um den Zugriff von Benutzern auf Spectrum-Datenbanken und JDBC-Treiber zu beschränken.

Um Zugriff auf einige Ordner auf dem Server zu gewähren und gleichzeitig den Zugriff auf andere einzuschränken, folgen Sie dieser Prozedur.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.

3. Klicken Sie auf **Verzeichniszugriff**.
4. Stellen Sie den Schalter **Zugriff auf Serververzeichnisse beschränken** auf **Ein**.
5. Klicken Sie auf die Schaltfläche „Hinzufügen“  .
6. Geben Sie in das Feld **Name** einen aussagekräftigen Namen für den Ordner ein, für den Sie den Zugriff gewähren.

   Der hier angegebene Name wird Benutzern als Stammname des Verzeichnisses angezeigt, wenn sie den Server durchsuchen. Im Beispiel zu Beginn dieses Themas lautete der Name des zugänglichen Verzeichnisses „WestRegionCustomers“.
7. Legen Sie im Feld **Pfad** den Ordner fest, auf den Sie den Zugriff gewähren möchten. Benutzer können dann auf alle Dateien und Unterordner im angegebenen Ordner zugreifen.
8. Klicken Sie auf **Speichern**.
9. Wenn Sie den Zugriff auf weitere Ordner gewähren möchten, wiederholen Sie die vorherigen Schritte nach Bedarf.

Benutzer haben nun nur Zugriff auf die von Ihnen angegebenen Ordner. Beachten Sie, dass Benutzer über die Plattform-Sicherheitsberechtigung **Sicherheit – Verzeichnispfade** verfügen müssen, um auf Serververzeichnisse zugreifen zu können.

> **Anmerkung:** Wenn es Datenflüsse gibt, die zuvor auf Dateien zugegriffen haben, die aufgrund von Einschränkungen nicht mehr verfügbar sind, schlagen diese Datenflüsse fehl.

Konfigurieren der HTTPS-Kommunikation

Standardmäßig verwendet der Spectrum™ Technology Platform-Server HTTP für die Kommunikation mit dem Enterprise Designer, Browseranwendungen wie die Management Console und Metadata Insights sowie für die Verarbeitung von Webservice-Anforderungen und API-Aufrufen und für die Remote-Serverkommunikation. Sie können Spectrum™ Technology Platform zur Verwendung von HTTPS konfigurieren, wenn Sie diese Netzwerkkommunikation schützen möchten.

> **Anmerkung:** Spectrum™ Technology Platform verwendet TLS 1.2 zur Verschlüsselung der Kommunikation. Anwendungen, die auf Spectrum™ Technology Platform-Webservices oder die API zugreifen, müssen TLS 1.2 unterstützen, um eine Verbindung über HTTPS herzustellen.

In dieser Prozedur wird beschrieben, wie Sie die HTTPS-Kommunikation bei einer Einzelserverinstallation von Spectrum™ Technology Platform aktivieren. Wenn Sie HTTPS verwenden möchten und Spectrum™ Technology Platform in einem Cluster ausführen, führen Sie nicht diese Prozedur aus. Konfigurieren Sie stattdessen den Load Balancer, HTTPS für die Kommunikation mit Clients zu verwenden. Die Kommunikation zwischen dem Load Balancer und den Spectrum™ Technology Platform-Knoten sowie zwischen den Knoten untereinander erfolgt unverschlüsselt, da Spectrum™ Technology Platform-Clustering HTTPS nicht unterstützt. Der Load Balancer und die

Spectrum™ Technology Platform-Server im Cluster müssen sich hinter einer Firewall befinden, um eine sichere Umgebung zu bieten.

So konfigurieren Sie die HTTPS-Kommunikation für eine Einzelserverinstallation von Spectrum™ Technology Platform:

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
   - Klicken Sie dazu unter Windows auf das Spectrum™ Technology Platform-Symbol auf der Windows-Taskleiste und wählen Sie **Spectrum™ stoppen** aus. Wahlweise können Sie auch die Option „Dienste“ in der Windows-Systemsteuerung verwenden und den Pitney Bowes Spectrum™ Technology Platform-Dienst stoppen.
   - Beziehen Sie unter Unix oder Linux das Skript *SpectrumLocation*`/server/bin/setup` und führen Sie dann das Skript *SpectrumLocation*`/server/bin/server.stop` aus.
2. Erstellen Sie ein durch eine vertrauenswürdige Zertifizierungsstelle (CA) signiertes Zertifikat.

   Anmerkung: Das Zertifikat muss die Anforderungen für Verschlüsselung und Länge der von Spectrum™ Technology Platform verwendeten Java-Version erfüllen. Um die Java-Version herauszufinden, öffnen Sie die Management Console und navigieren Sie zu **System** > **Version**. Weitere Informationen finden Sie unter **java.com/en/jre-jdk-cryptoroadmap.html**.
3. Laden Sie das Zertifikat in einen JSSE-Schlüsselspeicher. Weitere Informationen finden Sie unter **www.eclipse.org/jetty/documentation/current/configuring-ssl.html#loading-keys-and-certificates**.
4. Erstellen Sie eine XML-Datei mit dem Namen `spectrum-override-container-ssl.xml` und folgendem Inhalt:

```
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:util="http://www.springframework.org/schema/util"
    xsi:schemaLocation="http://www.springframework.org/schema/beans
      http://www.springframework.org/schema/beans/spring-beans-3.0.xsd

       http://www.springframework.org/schema/util
      http://www.springframework.org/schema/util/spring-util-3.0.xsd">


    <bean id="defaultWebServerConnector"
class="org.eclipse.jetty.server.ServerConnector">
        <constructor-arg ref="webServer"/>
        <constructor-arg>
          <bean class="org.eclipse.jetty.util.ssl.SslContextFactory">

                <property name="keyStorePath"
value="/SpectrumKeystore"/>
              <property name="keyManagerPassword" value="password"/>

                <property name="keyStorePassword" value="password"/>
```

```
            </bean>
        </constructor-arg>
        <property name="host" value="${spectrum.bind.address}"/>
        <property name="port" value="${spectrum.http.port}"/>
        <property name="idleTimeout" value="-1"/>
    </bean>
</beans>
```

5. Ändern Sie die folgenden Zeilen nach Bedarf, damit sie Ihrer Umgebung entsprechen:

`<property name="keyStorePath" value="/SpectrumKeystore"/>`	Ändern Sie den Wert, damit er den vollständigen Pfad zum Java-Schlüsselspeicher angibt.
`<property name="keyManagerpassword" value="password"/>`	Ändern Sie den Wert, damit er das Kennwort für den Schlüsselspeicher angibt.
`<property name="keyStorePassword" value="password"/>`	Ändern Sie den Wert, damit er das Kennwort für den Schlüssel innerhalb des Schlüsselspeichers angibt.

6. Speichern Sie die Datei `spectrum-override-container-ssl.xml` in *`SpectrumLocation`*`/server/app/conf/spring`.
7. Öffnen Sie in einem Texteditor die Datei `spectrum-container.properties`, die sich in *`SpectrumLocation`*`/server/app/conf` befindet. Entfernen Sie die Kommentarzeichen und legen Sie die folgenden Eigenschaften fest:

   ```
   spectrum.http.port=port
   spectrum.runtime.port=port
   spectrum.runtime.hostname=dnsname
   ```

   Dabei steht *port* für den Netzwerkport für die Kommunikation mit den Clients (z. B. 8443) und *dnsname* für den Hostnamen des Spectrum™ Technology Platform-Servers. Der angegebene Port muss für `spectrum.http.port` und `spectrum.runtime.port` identisch sein.

8. Wenn Sie HTTPS-Kommunikation für das Location Intelligence-Modul und die Spectrum-Geodatendienste konfigurieren, müssen Sie eine zusätzliche Konfiguration vornehmen, bevor Sie den Spectrum™ Technology Platform-Server neu starten.
   a) Ändern Sie die Datei `java.properties` (*`SpectrumLocation`*`\server\modules\spatial`), indem Sie alle Hostnamen und Ports ändern, sodass sie identisch mit den für den Spectrum™ Technology Platform-Server verwendeten sind. Der Hostname muss mit dem DNS-Namen des Servers und dem CN-Wert

im Zertifikat übereinstimmen. Setzen Sie die Eigenschaft `repository.useSecureConnection` auf true. Beispiel:

```
repository.host=www.spectrum.com
repository.port=8443
repository.useSecureConnection=true
```

b) Ändern Sie in die URLs in diesen Dienstkonfigurationen, um HTTPS zu verwenden:

- Mapping (nur erforderlich, wenn auf den Mapping-Dienst per SOAP zugegriffen wird und der ReturnImage-Parameter für eine RenderMap-Anforderung "false" ist)
- WFS
- WMS
- WMTS

Weitere Informationen finden Sie im Spatial Manager-Handbuch im Abschnitt „Dienstprogramme“ des *Spectrum Spatial-Handbuchs*.

9. Starten Sie den Spectrum™ Technology Platform-Server.
   - Klicken Sie dazu unter Windows auf das Spectrum™ Technology Platform-Symbol auf der Windows-Taskleiste und wählen Sie **Spectrum™ starten** aus. Wahlweise können Sie auch die Option „Dienste“ in der Windows-Systemsteuerung verwenden und den Pitney Bowes Spectrum™ Technology Platform-Dienst starten.
   - Führen Sie unter Unix oder Linux das Skript *SpectrumLocation*`/server/bin/server.start` aus.

Webservice-Authentifizierung

Bei Spectrum™ Technology Platform-Webservices ist es erforderlich, dass der anfordernde Benutzer gültige Anmeldeinformationen angibt. Es sind zwei Methoden für die Authentifizierung vorhanden: Standardauthentifizierung und Token-Authentifizierung.

Standardauthentifizierung

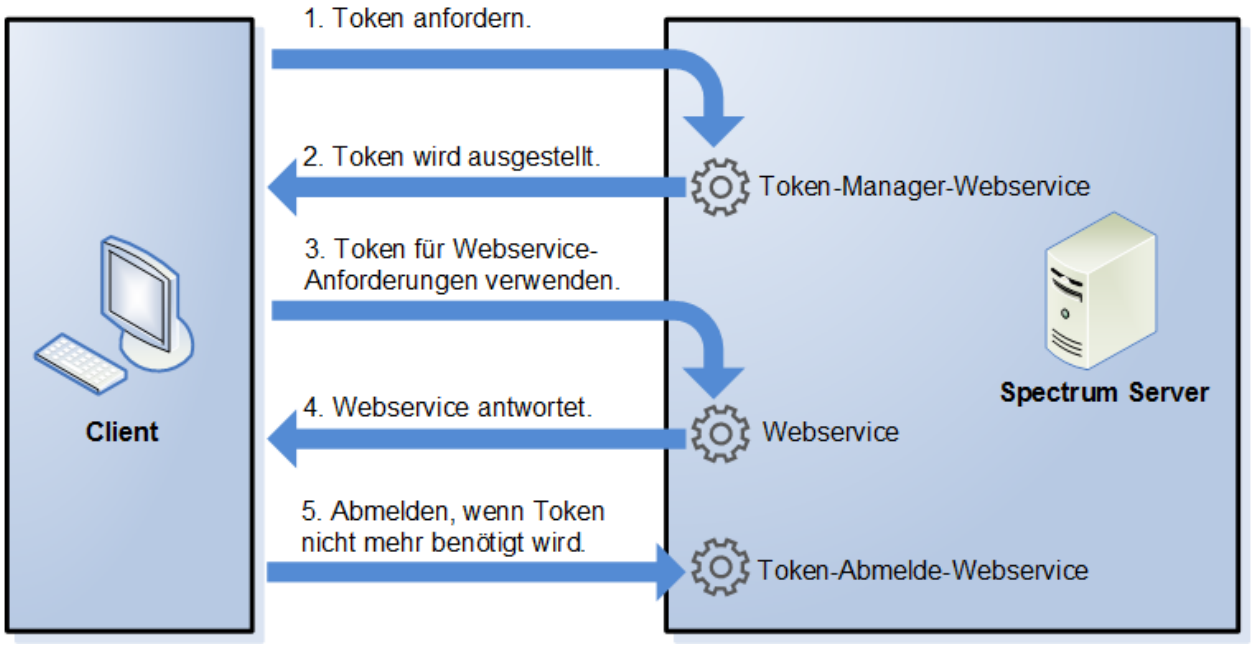
Bei der Standardauthentifizierung werden die Benutzerkennung und das Kennwort im HTTP-Header jeder Anforderung an den an den Webservice an Spectrum™ Technology Platform gesendet. Standardmäßig ist die Standardauthentifizierung aktiviert. Ihr Administrator deaktiviert die Standardauthentifizierung jedoch eventuell. Wenn die Standardauthentifizierung deaktiviert ist, müssen Sie per Token-Authentifizierung auf die Webservices zugreifen.

Token-Authentifizierung

Bei der Token-Authentifizierung ruft der anfordernde Benutzer ein Token über den Spectrum™ Technology Platform-Server ab und verwendet das Token anschließend, wenn er eine Anforderung an den Webservice sendet. Statt Anmeldeinformationen in jeder Anforderung zu senden, wird das

Token an den Server gesendet. Der Server ermittelt anschließend, ob es sich um ein gültiges Token handelt.

Im folgenden Diagramm wird der Prozess veranschaulicht:



1. Rufen Sie ein Token über den Spectrum™ Technology Platform-Server ab, indem Sie eine Anforderung an den Token-Verwaltungsdienst senden.
2. Der Token-Verwaltungsdienst stellt ein Token aus. Wenn Sie ein Sitzungstoken angefordert haben, wird außerdem eine Sitzungskennung ausgestellt.
3. Senden Sie eine Anforderung an den gewünschten Webservice, und geben Sie das Token im HTTP-Header an. Geben Sie bei Sitzungstokens die Sitzungskennung im HTTP-Header an.
4. Der Webservice stellt eine Antwort aus. Mithilfe des Token können Sie weitere Webservice-Anforderungen entweder an denselben Webservice oder einen beliebigen anderen Webservice auf dem Spectrum™ Technology Platform-Server senden. Die Anzahl der Webservice-Anforderungen, die Sie mit einem Token senden können, unterliegt keinen Begrenzungen. Wenn das Token jedoch ein Ablauflimit (auch als Gültigkeitsdauer bezeichnet) hat, ist es nicht länger gültig, nachdem die Gültigkeitsdauer abgelaufen ist. Wenn es sich bei dem Token um ein Sitzungstoken handelt, wird es nach 30 Minuten der Inaktivität ungültig.
5. Wenn Sie das Token nicht mehr benötigen, sollten Sie sich abmelden, indem Sie eine Anforderung an den Abmeldungs-Webservice für Token senden. Dadurch wird das Token aus der Liste der gültigen Tokens auf dem Spectrum™ Technology Platform-Server entfernt.

Deaktivierung der Standardauthentifizierung für Webservices

Spectrum™ Technology Platform unterstützt zwei Typen der Authentifizierung für Webservice-Anforderungen: Standardauthentifizierung und Token-Authentifizierung. Standardmäßig sind beide Methoden aktiviert. Wenn Webservice-Anforderungen die Token-Authentifizierung statt

der Standardauthentifizierung verwenden sollen, können Sie die Standardauthentifizierung deaktivieren. Führen Sie dafür die folgenden Schritte aus.

> **Anmerkung:** Beachten Sie, dass vorhandene Clients durch die Deaktivierung der Standardauthentifizierung fehlschlagen. WMS-, WMTS- und WFS-Clients erwarten beim Location Intelligence-Modul entweder die Standardauthentifizierung oder keine Authentifizierung. Wenn nur die Token-Authentifizierung aktiviert ist, schlagen diese Clients voraussichtlich fehl.

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
2. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumLocation/server/app/conf/spectrum-container.properties

3. Setzen Sie die folgende Eigenschaft auf „False“:

```
spectrum.security.authentication.webservice.basicauth.enabled=false
```

4. Starten Sie den Server.

Deaktivierung der Authentifizierung für Webservices

Für alle von Spectrum™ Technology Platform verwendeten Dienste und für den Zugriff auf Ressourcen ist die Authentifizierung standardmäßig aktiviert.

Die Authentifizierung auf Dienstebene kann für alle SOAP- oder REST-Webservices (oder beide) deaktiviert werden. Dies ist nützlich, wenn in Ihrer Lösung eine hohe Authentifizierungsebene integriert ist, die beispielsweise die Dienste des Location Intelligence-Moduls verwendet.

So deaktivieren Sie die Authentifizierung für Spectrum™ Technology Platform-Webservices:

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
2. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumLocation\server\app\conf\spectrum-container.properties

3. Ändern Sie den Wert jeder Eigenschaft nach Bedarf. So deaktivieren Sie beispielsweise die Authentifizierung für alle SOAP-Dienste:

```
spectrum.security.authentication.webservice.enabled.REST=true
spectrum.security.authentication.webservice.enabled.SOAP=false
```

   > **Anmerkung:** Im Falle des Location Intelligence-Moduls umfassen REST-Dienste auch OGC-Webservices.

4. Speichern Sie die Eigenschaftsdatei und schließen Sie sie.
5. Starten Sie den Spectrum™ Technology Platform-Server.

Nach Abschluss des Vorgangs wird die Authentifizierung für den angegebenen Typ von Webservices deaktiviert.

Aktivieren von CORS

Bei Cross-Origin Resource Sharing (CORS) handelt es sich um einen W3C-Standard, anhand dessen Sie Daten zwischen Domänen teilen können. Mithilfe von CORS können Webanwendungen, die in einer Domäne ausgeführt werden, auf Daten einer anderen Domäne zugreifen. Wenn Sie CORS auf Ihrem Spectrum™ Technology Platform-Server aktivieren, können Sie auf einer anderen Domäne gehosteten Webanwendungen erlauben, auf die Spectrum™ Technology Platform-Webservices zuzugreifen.

Nehmen wir beispielsweise an, dass Ihre Webanwendung über **webapp.example.com** gehostet wird. Diese Webanwendung enthält eine JavaScript-Funktion, die einen über **spectrum.example.com** gehosteten Spectrum™ Technology Platform-Webservice aufruft. Ohne CORS müssten Sie einen Proxyserver verwenden, um diese Anforderung zu ermöglichen. Somit würde Ihre Implementierung komplizierter werden. Die Verwendung eines Proxyservers ist mit CORS nicht erforderlich. Stattdessen können Sie **webapp.example.com** die Kennzeichnung „Zulässiger Ursprung“ geben. Dementsprechend erlauben Sie Spectrum™ Technology Platform, auf Webservice-Anforderungen zu antworten, die über die Domäne **webapp.example.com** gesendet werden.

So aktivieren Sie CORS auf Ihrem Spectrum™ Technology Platform-Server:

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
2. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumLocation`/server/app/conf/spectrum-advanced.properties`

3. Bearbeiten Sie die folgenden Parameter.

   spectrum.jetty.cors.enabled

   Setzen Sie diese Eigenschaft auf true, um CORS zu aktivieren. Der Standardwert ist false.

   spectrum.jetty.cors.allowedOrigins

   Eine durch Kommas getrennte Liste der Ursprünge, die auf Ressourcen auf dem Spectrum™ Technology Platform-Server zugreifen können. Der Standardwert lautet http://localhost:8080,http://localhost:443. Hierüber wird der Zugriff auf Ressourcen über den HTTP-Standardport 8080 und den HTTPS-Standardport 443 gewährt.

   Wenn ein zulässiger Ursprung ein oder mehrere Sternchen („*“) enthält, z. B. http://*.domain.com, werden Sternchen in .* umgewandelt und Punktzeichen („.“) werden in Escape-Zeichen „\.“ gesetzt. Der daraus folgende zulässige Ursprung wird als regulärer Ausdruck interpretiert. Zulässige Ursprünge können dementsprechend komplexere Ausdrücke wie https?://*.domain.[a-z]{3} sein, die HTTP oder HTTPS, mehreren Unterdomänen und jeder dreistelligen Domäne der obersten Ebene (.com, .net, .org usw.) entsprechen.

   spectrum.jetty.cors.allowedMethods

Eine durch Kommas getrennte Liste der HTTP-Methoden, die beim Zugriff auf Ressourcen auf dem Spectrum™ Technology Platform-Server verwendet werden können. Der Standardwert ist POST,GET,OPTIONS,PUT,DELETE,HEAD.

spectrum.jetty.cors.allowedHeaders

Eine durch Kommas getrennte Liste der HTTP-Header, die beim Zugriff auf Ressourcen auf dem Spectrum™ Technology Platform-Server zugelassen sind. Der Standardwert ist X-PINGOTHER, Origin, X-Requested-With, Content-Type, Accept. Wenn der Wert ein einzelnes Sternchen („*“) ist, werden alle Header zugelassen.

spectrum.jetty.cors.preflightMaxAge

Die Anzahl an Sekunden, während der Preflight-Anforderungen durch den Client zwischengespeichert werden können. Der Standardwert beträgt 1800 Sekunden oder 30 Minuten.

spectrum.jetty.cors.allowCredentials

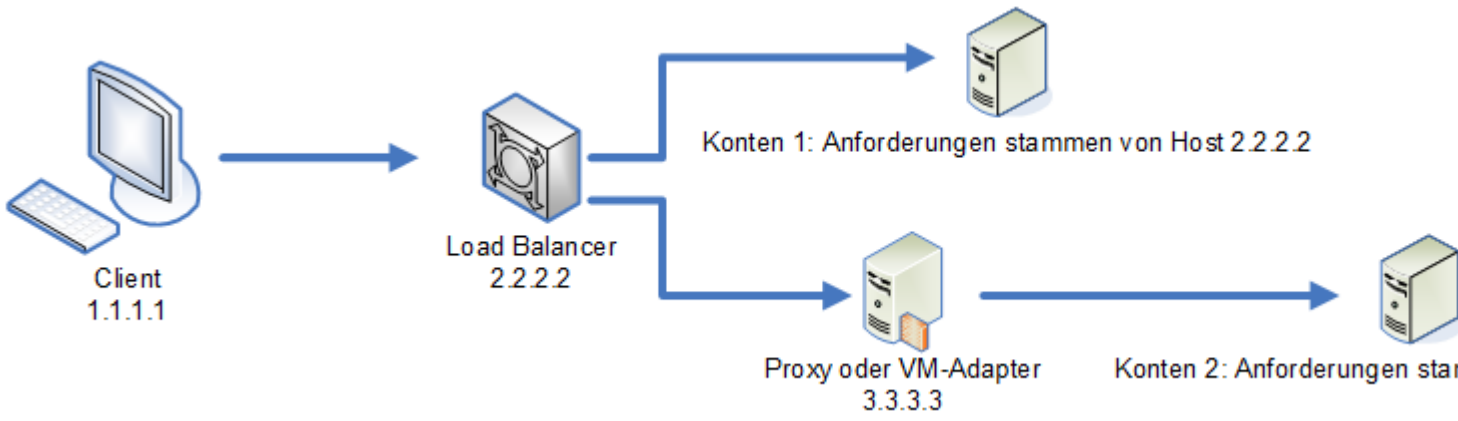
Gibt an, ob die Ressource Anforderungen mit Anmeldeinformationen zulässt. Der Standardwert ist true.

4. Speichern Sie die Datei und schließen Sie sie.
5. Starten Sie den Spectrum™ Technology Platform-Server.

Deaktivieren von Host-Überprüfungen bei der Token-Authentifizierung

Bei der Token-Authentifizierung prüft der Spectrum™ Technology Platform-Server das vom Client bereitgestellte Token, bevor er auf die Anforderung antwortet. Der Server überprüft das Token, um festzustellen, ob es abgelaufen ist, ob es korrekt verschlüsselt wurde und ob es dem korrekten Host entstammt. Bei Sitzungstokens überprüft der Server zudem die Sitzungskennung. Wenn eine dieser Prüfungen fehlschlägt, wird das Token abgelehnt und der Server antwortet nicht auf die Anforderung.

In einer Cluster-Umgebung werden Anforderungen eventuell so weitergeleitet, dass die Anforderungen von einem anderen Host zu kommen scheinen als demjenigen, der im Token angegeben ist. Als Folge wird die Fehlermeldung „Ungültiges Token“ angezeigt. Nehmen wir beispielsweise an, dass Ihnen ein Cluster mit zwei Knoten gemäß der folgenden Darstellung vorliegt:



Nehmen wir weiterhin an, dass der Client eine Anforderung sendet und diese Anforderung an Knoten 1 geleitet wird. Ein Token wird erstellt und an den Host 2.2.2.2 (den Lastenausgleich) geknüpft, da die Anforderung für den Knoten aus dem Lastenausgleich gesendet wurde. Wenn die nächste Anforderung von dem Client zum Knoten 2 geleitet wird, bleibt das Token an den Host 2.2.2.2 geknüpft. Allerdings scheint die Anforderung dann von dem Proxyserver 3.3.3.3 gesendet worden zu sein. In diesem Fall lehnt der Knoten das Token ab, da es scheint, dass es nicht mit dem Host verknüpft ist, von dem die Anforderung gesendet wurde.

Konfigurieren Sie den Spectrum™ Technology Platform-Server dann entsprechend, damit er die im Token enthaltenen Hostinformationen ignoriert. Diese Konfiguration sollte nur dann vorgenommen werden, wenn Ihre Umgebung über unterschiedliche Netzwerkgeräte zwischen dem Lastenausgleich und den Knoten verfügt. Wenn alle Knoten demselben Netzwerkgerät angehören, muss die Hostüberprüfung nicht deaktiviert werden.

> **Anmerkung:** Wenn Sie dieses Verfahren anwenden, werden Clienttokens zu Open-Tokens, da die Hostüberprüfung deaktiviert wird. Sitzungstokens sind weiterhin an eine spezifische Sitzungskennung geknüpft, jedoch an keinen spezifischen Host.

1. Öffnen Sie die folgende Eigenschaftsdatei auf dem Spectrum™ Technology Platform-Server:

   SpectrumLocation`/server/app/conf/spectrum-container.properties`

2. Setzen Sie die folgende Eigenschaft auf false.

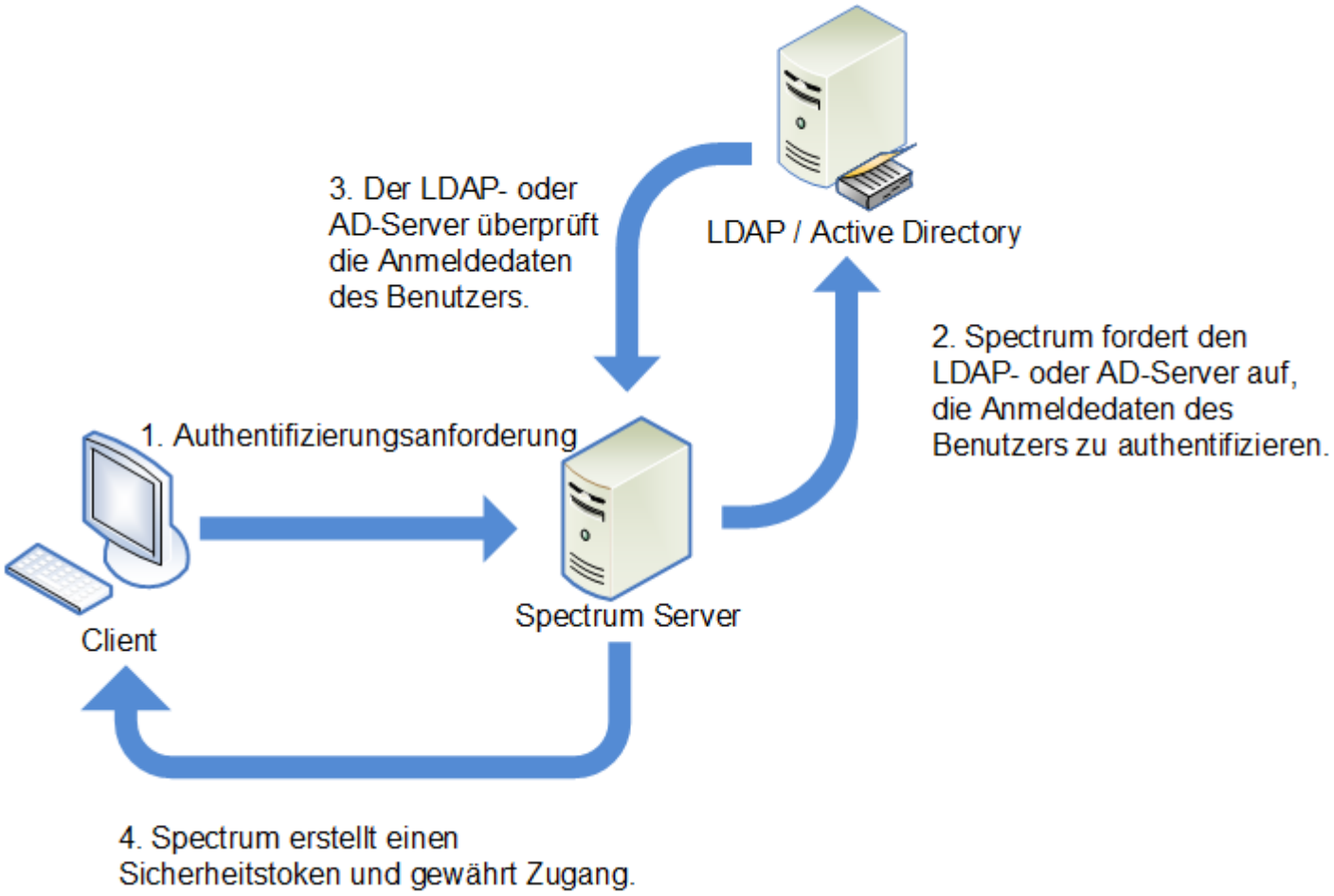
   ```
   spectrum.security.authentication.token.remoteClientCheck.enabled=false
   ```

3. Speichern Sie die Eigenschaftsdatei und schließen Sie sie.
4. Wiederholen Sie diesen Vorgang auf allen Knoten im Cluster.

Verwenden von LDAP oder Active Directory zur Authentifizierung

Sie können Spectrum™ Technology Platform konfigurieren, einen LDAP- oder Active Directory-Server zur Authentifizierung zu verwenden. Wenn sich ein Benutzer bei Spectrum™ Technology Platform anmeldet, werden die Anmeldeinformationen des Benutzers unter Verwendung von LDAP oder AD verifiziert. Das System überprüft dann, ob ein Spectrum™ Technology Platform-Benutzer mit demselben Namen vorhanden ist. Wenn das der Fall ist, wird der Benutzer angemeldet. Andernfalls wird automatisch ein Spectrum™ Technology Platform-Benutzerkonto für den Benutzer erstellt, dem dann die Rolle `Benutzer` zugewiesen wird.

Im folgenden Diagramm wird dieser Prozess veranschaulicht:



Bevor Sie Spectrum™ Technology Platform konfigurieren, einen Verzeichnisdienst zur Authentifizierung zu verwenden, vergewissern Sie sich, dass Ihr Verzeichnisdienst die folgenden Voraussetzungen erfüllt:

- Für LDAP muss der Verzeichnisserver mit LDAP Version 3 kompatibel sein.
- Für Active Directory-Server gibt es keine speziellen Voraussetzungen.

Anmerkung: Wir empfehlen Ihnen, den technischen Support oder Professional Services von Pitney Bowes zu kontaktieren, um Sie durch diesen Prozess zu leiten.

Anmerkung: Wenn Sie Spectrum mit LDAP oder STS oder SSO_STS einrichten und die Eigenschaft standardmäßig `spectrum.security.account.createNonExisting=true` ist, werden Active Directory-Benutzer nach ihrer ersten Anmeldung bei Spectrum automatisch in Spectrum™ Technology Platform erstellt. Wenn Sie die Eigenschaft deaktivieren (`spectrum.security.account.createNonExisting=false`), werden LDAP-/Active Directory-Benutzer erst dann für Spectrum™ Technology Platform authentifiziert, wenn der Administrator Benutzer manuell erstellt.

1. Wenn in der Management Console vorhandene Benutzer konfiguriert sind und Sie diese weiterverwenden möchten, nachdem Sie LDAP- oder Active Directory-Authentifizierung aktiviert

haben, erstellen Sie diese Benutzer in Ihrem LDAP- oder Active Directory-System. Achten Sie darauf, denselben Benutzernamen wie in Spectrum™ Technology Platform zu verwenden.

> **Anmerkung:** Sie müssen den Benutzer „admin“ nicht in LDAP oder Active Directory erstellen, da dieser Benutzer weiterhin Spectrum™ Technology Platform zur Authentifizierung verwenden wird, nachdem Sie LDAP- oder Active Directory-Authentifizierung aktiviert haben.

2. Stoppen Sie den Spectrum™ Technology Platform-Server.
3. Aktivieren Sie LDAP oder Active Directory-Authentifizierung:
   a) Öffnen Sie folgende Konfigurationsdatei in einem Texteditor:

      ```
      server\app\conf\spectrum-container.properties
      ```

   b) Legen Sie die Eigenschaft `spectrum.security.authentication.basic.authenticator` auf LDAP fest:

      ```
      spectrum.security.authentication.basic.authenticator=LDAP
      ```

      Die Einstellung `LDAP` wird verwendet, um sowohl Active Directory als auch LDAP zu aktivieren.

   c) Speichern Sie die Datei und schließen Sie sie.
4. Konfigurieren Sie die Verbindungseigenschaften:
   a) Öffnen Sie folgende Konfigurationsdatei in einem Texteditor:

      ```
      server\app\conf\spring\security\spectrum-config-ldap.properties
      ```

   b) Ändern Sie diese Eigenschaften.

      spectrum.ldap.url

      Dies ist die URL einschließlich Port des LDAP- oder Active Directory-Servers. Beispiel:

      ```
      spectrum.ldap.url=ldap://ldapserver.example.com:389/
      ```

      spectrum.ldap.dn.format

      Dies ist das Format, das zur Suche nach dem Benutzerkonto in LDAP oder Active Directory verwendet wird. Verwenden Sie die Variable `%s` für den Benutzernamen. Beispiel:

      LDAP:

      ```
      spectrum.ldap.dn.format=uid=%s,ou=users,dc=example,dc=com
      ```

      Active Directory:

      ```
      spectrum.ldap.dn.format=%s@example.com
      ```

      spectrum.ldap.dn.base

Dies ist der eindeutige Name (Distinguished Name, dn) über den in LDAP oder Active Directory nach Benutzerkonten gesucht wird. Beispiel:

LDAP:

```
spectrum.ldap.dn.base=ou=users,dc=example,dc=com
```

Active Directory:

```
spectrum.ldap.dn.base=cn=Users,dc=example,dc=com
```

spectrum.ldap.search.filter

Dies ist ein Suchfilter, der verwendet wird, wenn nach Attributen wie Rolle gesucht wird. Der Suchfilter kann die folgenden Variablen enthalten:

- `{user}` ist der Benutzername für die Anmeldung bei Spectrum™ Technology Platform.
- `{dn}` ist der eindeutige Name, der in `spectrum.ldap.dn.base` angegeben ist.

Beispiel:

LDAP:

```
spectrum.ldap.search.filter=uid={user}
```

Active Directory:

```
spectrum.ldap.search.filter=userPrincipalName={dn}
```

spectrum.ldap.attribute.roles

Optional: Gibt das LDAP- oder Active Directory-Attribut an, das den Namen der Spectrum™ Technology Platform-Rolle für den Benutzer enthält. Der Rollenname, den Sie im LDAP- oder Active Directory-Attribut angeben, muss mit dem in Spectrum™ Technology Platform definierten Rollennamen übereinstimmen.

Um beispielsweise die im Attribut `spectrumgecos` definierten Rollen anzuwenden, müssen Sie Folgendes angeben:

```
spectrum.ldap.attribute.roles=spectrumroles
```

Wenn dieses Attribut eine Rolle namens `Designer` enthält, wird dem Benutzer die Rolle `Designer` zugewiesen.

Sie können nur ein Attribut spezifizieren, doch kann das Attribut mehrere Rollen enthalten. Wenn Sie mehrere Rollen in einem Attribut angeben möchten, trennen Sie diese durch ein Komma. Sie können außerdem ein Multiwertattribut spezifizieren, bei dem jede Instanz des Attributs eine andere Rolle enthält. Nur die in diesem einen Attribut spezifizierten Rollen werden in Spectrum™ Technology Platform verwendet.

Andere LDAP- oder Active Directory-Attribute haben keine Auswirkungen auf Spectrum™ Technology Platform-Rollen.

Wenn dem Benutzer in Spectrum™ Technology Platform Rollen zugewiesen sind, setzen sich die Berechtigungen des Benutzers aus den Rollen aus LDAP oder Active Directory und den Rollen aus Spectrum™ Technology Platform zusammen.

> **Anmerkung:** Wenn sich ein Benutzer zum ersten Mal anmeldet und nicht nicht über ein Spectrum™ Technology Platform-Benutzerkonto verfügt, wird automatisch eins erstellt. Der Benutzer erhält die Rolle `Benutzer`. Die effektiven Berechtigungen des Benutzers setzen sich aus den Berechtigungen der Rolle `Benutzer` und denen der Rollen zusammen, die in den in der Eigenschaft `spectrum.ldap.attribute.roles` aufgelisteten Attributen spezifiziert sind.
>
> **Anmerkung:** Wenn Sie die Rollen des Benutzers in der Management Console anzeigen, werden die Rollen, die dem Benutzer über die Eigenschaft `spectrum.ldap.attribute.roles` zugewiesen wurden, nicht angezeigt.

spectrum.ldap.pool.min

Gibt die Mindestgröße des Verbindungspools für Verbindungen zum LDAP- oder Active Directory-Server.

spectrum.ldap.pool.max

Gibt die maximale Anzahl der gleichzeitigen Verbindungen zum LDAP- oder Active Directory-Server.

spectrum.ldap.timeout.connect

Gibt in Millisekunden an, wie lange auf die Verbindungsherstellung zum LDAP- oder Active Directory-Server zu warten ist. Der Standardwert ist 1000 Millisekunden.

spectrum.ldap.timeout.response

Gibt in Millisekunden an, wie lange auf eine Antwort vom LDAP- oder Active Directory-Server zu warten ist, nachdem die Verbindung hergestellt wurde. Der Standardwert ist 5000 Millisekunden.

spectrum.ldap.retry.count

Die Anzahl an Versuchen, die der Spectrum™ Technology Platform-Server durchführen wird, um eine Verbindung zum LDAP- oder Active Directory-Server herzustellen, wenn der erste Verbindungsversuch fehlschlägt. Setzen Sie diesen Wert auf 0, wenn Sie nur einen Verbindungsversuch zulassen möchten.

Tipp: Wenn Ihre LDAP- oder Active Directory-Server geclustert sind, empfehlen wir, diesen Wert auf 1 oder höher festzulegen, damit die Verbindungsanforderung über den LDAP- oder Active Directory-Lastausgleich zu einem anderen Server umgeleitet werden kann, wenn der Server des ersten Verbindungsversuchs nicht verfügbar ist.

spectrum.ldap.retry.wait

Die Anzahl an Millisekunden, die zwischen Verbindungsversuchen gewartet werden soll.

spectrum.ldap.retry.backoff

Der Multiplikator, der verwendet wird, um die Wartezeit nach jedem fehlgeschlagenen Verbindungsversuch zu erhöhen.

Beispiel:

```
spectrum.ldap.timeout.connect=1000
...
spectrum.ldap.retry.count=5
spectrum.ldap.retry.wait=500
spectrum.ldap.backoff=2
```

In diesem Beispiel beträgt die Wartezeit für den ersten Verbindungsversuch 1.000 Millisekunden. Die Wartezeit für jeden der fünf nachfolgenden Verbindungsversuche wird um den Faktor 2 erhöht, woraus folgende Wartezeiten für die Verbindungsversuche resultieren:

Erneuter Verbindungsversuch 1: 500 Millisekunden
Erneuter Verbindungsversuch 2: 1.000 Millisekunden
Erneuter Verbindungsversuch 3: 2.000 Millisekunden
Erneuter Verbindungsversuch 4: 4.000 Millisekunden
Erneuter Verbindungsversuch 5: 8.000 Millisekunden

c) Speichern Sie die Eigenschaftsdatei und schließen Sie sie.

5. Wenn Sie das Location Intelligence-Modul verwenden und planen, Rollen (wie in **Zuordnen von LDAP-Attributwerten zu Rollen** auf Seite 49 beschrieben) zuzuordnen, ist eine zusätzliche manuelle Konfiguration der Konfigurationsdatei von Jackrabbit (unter *SpectrumFolder*\server\modules\spatial\jackrabbit\workspaces\default\workspace.xml) erforderlich, damit Spectrum Spatial alle dynamisch zugewiesenen LDAP- oder Active Directory-Rollen erkennt. Fügen Sie den Parameter `checkRoles` hinzu, wie unten dargestellt:

```
<!--
 Spectrum ACL provider.
-->
<WorkspaceSecurity>
 <AccessControlProvider class="com.mapinfo.repository.jackrabbit.acl

  .AccessControlProviderImpl">
  <param name="checkRoles" value="true"/>
 </AccessControlProvider>
</WorkspaceSecurity>
```

6. Starten Sie den Spectrum™ Technology Platform-Server.

Wenn Spectrum™ Technology Platform bei Ihnen in einem Cluster läuft, ändern Sie einfach die Dateien `spectrum-container.properties` und `spectrum-config-ldap.properties` auf jedem Server im Cluster. Beenden Sie den Server, bevor Sie die Dateien ändern, und starten Sie den Server anschließend wieder. Wenn Sie ein LDAP-Attribut einer Rolle zugeordnet haben, wird diese Zuordnung zu allen Knoten im Cluster repliziert. Sie müssen also die Zuordnungsprozedur in der JMX-Konsole nicht wiederholen.

Zuordnen von LDAP-Attributwerten zu Rollen

Vor Ausführen dieser Prozedur müssen Sie die LDAP-Authentifizierung aktivieren. Wenn Sie das Location Intelligence-Modul verwenden, müssen Sie zudem die Konfigurationsdatei von Jackrabbit ändern. Weitere Informationen finden Sie unter **Verwenden von LDAP oder Active Directory zur Authentifizierung** auf Seite 43.

Wenn Sie Spectrum™ Technology Platform zur Verwendung von LDAP oder Active Directory für die Authentifizierung konfigurieren, spezifiziert eine der von Ihnen konfigurierten Konfigurationseigenschaften (die Eigenschaft `spectrum.ldap.attribute.roles` in der Datei `spectrum-config-ldap.properties`) ein LDAP-Attribut, dessen Wert die Rolle festlegt, die einem Benutzer gewährt wird. Standardmäßig müssen die Attributwerte genau mit dem Spectrum™ Technology Platform-Rollennamen übereinstimmen, damit die Rolle gewährt wird. Um beispielsweise die Rolle designer zu gewähren, muss das von Ihnen angegebene Attribut den Wert designer enthalten.

Wenn der LDAP-Attributwert, den Sie verwenden möchten, nicht mit dem Rollennamen in Spectrum™ Technology Platform übereinstimmt, können Sie den LDAP-Attributwert einem Rollennamen zuordnen. Sie können auch einen LDAP-Attributwert, der denselben Namen aufweist wie eine Spectrum™ Technology Platform-Rolle, einer anderen Rolle zuordnen. Beispielsweise ist designer eine der integrierten Rollen. Wenn Sie über einen LDAP-Attributwert namens designer verfügen, ihn aber einer anderen Rolle zuordnen möchten, können Sie eine Zuordnung erstellen.

1. Öffnen Sie einen Webbrowser, und rufen Sie Folgendes auf:`http://server:port/jmx-console`

   Dabei gilt Folgendes:

   server ist die IP-Adresse oder der Hostname Ihres Spectrum™ Technology Platform-Servers.

   port ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der Standardwert ist 8080.

2. Klicken Sie auf folgende Eigenschaft:

   `com.pb.spectrum.platform.common.security.ldap:mappings`

   > **Anmerkung:** Diese Eigenschaft ist nur sichtbar, wenn Sie LDAP-Authentifizierung aktiviert haben und der Server vollständig gestartet ist. Wenn Sie LDAP-Authentifizierung nicht aktiviert haben, lesen Sie weiter unter **Verwenden von LDAP oder Active Directory zur Authentifizierung** auf Seite 43.

3. Geben Sie im Bereich **addMapping** in das Feld **ldapValue** den LDAP-Attributwert ein, den Sie einer Spectrum™ Technology Platform-Rolle zuordnen möchten.
4. Geben Sie in das Feld **roleName** die Spectrum™ Technology Platform-Rolle ein, die Sie dem LDAP-Attributwert zuordnen möchten.
5. Klicken Sie auf **Invoke**.

Benutzern mit diesem LDAP-Attribut wird nun die von Ihnen angegebene Rolle gewährt, wenn sie sich in Spectrum™ Technology Platform anmelden.

Um die Zuordnung zu entfernen, geben Sie das LDAP-Attribut, für das Sie die Zuordnung aufheben möchten, in das Feld **ldapValue** im Bereich **removeMapping** ein.

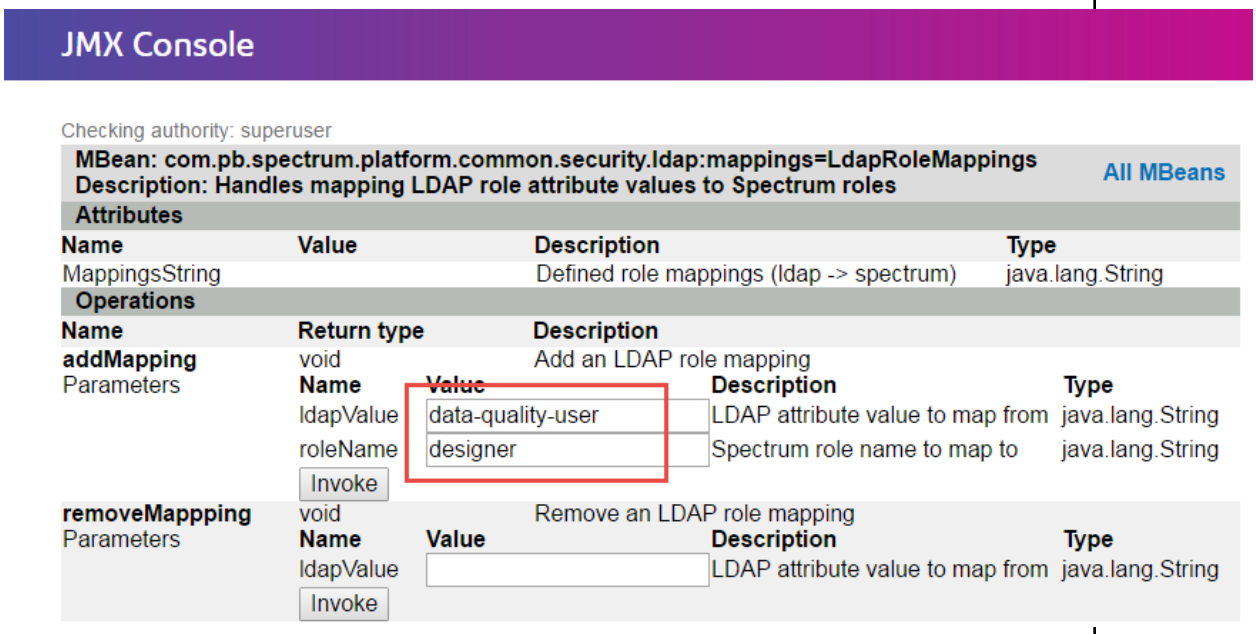
Beispiel

Sie möchten beispielsweise einen Wert im Attribut `gecos` verwenden, um in Spectrum™ Technology Platform eine Rolle zuzuweisen. `gecos` enthält den Wert data-quality-user, doch möchten Sie, dass dem Benutzer die Rolle designer gewährt wird, wenn er sich in Spectrum™ Technology Platform anmeldet.

Dazu müssen Sie das Attribut `gecos` in der Datei `spectrum-config-ldap.properties` als das Attribut angeben, das zur Zuweisung der Rollen verwendet wird:

```
spectrum.ldap.attribute.roles=gecos
```

Danach müssen Sie in der JMX-Konsole den Wert data-quality-user der Rolle designer zuordnen:



Als Ergebnis wird jedem Benutzer, der den Wert data-quality-user im Attribut `gecos` aufweist, die Rolle designer gewährt.

Aktivieren der SSL-Kommunikation mit LDAP

Die Kommunikation zwischen Spectrum™ Technology Platform und einem LDAP- oder Active Directory-Server erfolgt standardmäßig über TCP. Sie können Spectrum™ Technology Platform konfigurieren, LDAP über SSL zu verwenden, wenn Sie die Kommunikation zwischen dem Spectrum™ Technology Platform-Server und dem LDAP- oder Active Directory-Server sicher machen möchten.

1. In folgenden Fällen müssen Sie möglicherweise das Zertifikat zum von Spectrum™ Technology Platform verwendeten Java TrustStore hinzufügen:

   - Der standardmäßige Java TrustStore enthält keinen Eintrag für die Zertifizierungsautorität, die Sie verwenden.
   - Sie verwenden ein selbstsigniertes Zertifikat. Beachten Sie bitte, dass die Verwendung eines selbstsignierten Zertifikats in einer Produktionsumgebung nicht empfohlen wird.

   Falls einer dieser Fälle auf Sie zutrifft, fügen Sie das Zertifikat zum Java TrustStore hinzu, indem Sie die folgenden Schritte ausführen:

   a) Beschaffen Sie eine Kopie des Zertifikats. Sie können eine Kopie des Zertifikats von Ihrem LDAP-Administrator erhalten oder ein Tool wie LDAP Admin verwenden, um das Zertifikat anzeigen zu lassen und zu speichern.
   b) Fügen Sie das Zertifikat unter Verwendung des im JDK enthaltenen Dienstprogramms `keytool` zu einem neuen oder einem vorhandenen TrustStore hinzu.

      Beispiel:

      ```
      keytool -import -file X509_certificate_ldap.cer -alias
      server.example.com -keystore ldapTrustStore
      ```

      In der Dokumentation zu Java finden Sie weitere Informationen.

      Anmerkung: Das Zertifikat muss die Anforderungen für Verschlüsselung und Länge der von Spectrum™ Technology Platform verwendeten Java-Version erfüllen. Um die Java-Version herauszufinden, öffnen Sie die Management Console und navigieren Sie zu **System** > **Version**. Weitere Informationen finden Sie unter **java.com/en/jre-jdk-cryptoroadmap.html**.

2. Stoppen Sie den Spectrum™ Technology Platform-Server.

   - Klicken Sie dazu unter Windows auf das Spectrum™ Technology Platform-Symbol auf der Windows-Taskleiste und wählen Sie **Spectrum™ stoppen** aus. Wahlweise können Sie auch die Option „Dienste“ in der Windows-Systemsteuerung verwenden und den Pitney Bowes Spectrum™ Technology Platform-Dienst stoppen.
   - Beziehen Sie unter Unix oder Linux das Skript *SpectrumLocation*`/server/bin/setup` und führen Sie dann das Skript *SpectrumLocation*`/server/bin/server.stop` aus.

3. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumLocation`\server\app\conf\spring\security\spectrum-config-ldap.properties`

4. Konfigurieren Sie die folgenden Eigenschaften:

   spectrum.ldap.url

   Geben Sie die URL des LDAP-Servers an. Achten Sie darauf, die SSL-Portnummer anzugeben, die normalerweise 636 ist. Beispiel:

   ```
   spectrum.ldap.url=ldap://server.example.com:636
   ```

   Anmerkung: Sie dürfen am Ende der URL keinen Schrägstrich (/) angeben.

   spectrum.ldap.useSSL

   Geben Sie true an, um die SSL-Kommunikation mit LDAP zu aktivieren.

   spectrum.ldap.trustStore

   Geben Sie den Speicherort des TrustStore an, der das für die SSL-Kommunikation mit LDAP zu verwendende Zertifikat enthält. Unter Windows beispielsweise:

   ```
   spectrum.ldap.trustStore=file:D:\\Certs\\MyTrustStore
   ```

   Unter Linux und Unix:

   ```
   spectrum.ldap.trustStore=file://Certs//MyTrustStore
   ```

   spectrum.ldap.trustStore.password

   Geben Sie das TrustStore-Kennwort an.

Wichtig: Wenn Spectrum™ Technology Platform bei Ihnen in einem Cluster läuft, wiederholen Sie diese Prozedur auf jedem Server im Cluster.

Deaktivieren der SSL-Kommunikation mit LDAP

Wenn Sie Spectrum™ Technology Platform konfiguriert haben, SSL-Kommunikation mit LDAP oder Active Directory zu verwenden, und auf die Verwendung von TCP zurückwechseln müssen, gehen Sie wie folgt vor.

1. Stoppen Sie den Spectrum™ Technology Platform-Server.
   - Klicken Sie dazu unter Windows auf das Spectrum™ Technology Platform-Symbol auf der Windows-Taskleiste und wählen Sie **Spectrum™ stoppen** aus. Wahlweise können Sie auch die Option „Dienste“ in der Windows-Systemsteuerung verwenden und den Pitney Bowes Spectrum™ Technology Platform-Dienst stoppen.
   - Beziehen Sie unter Unix oder Linux das Skript *SpectrumLocation*`/server/bin/setup` und führen Sie dann das Skript *SpectrumLocation*`/server/bin/server.stop` aus.
2. Öffnen Sie die folgende Datei in einem Texteditor:

   SpectrumLocation`\server\app\conf\spring\security\spectrum-config-ldap.properties`

3. Konfigurieren Sie die folgenden Eigenschaften:

spectrum.ldap.url

Ändern Sie die URL des LDAP-Servers auf die Verwendung des TCP-Ports anstelle des SSL-Ports. Der Standardwert ist 389. Beispiel:

```
spectrum.ldap.url=ldap://ldapserver.example.com:389/
```

Anmerkung: Sie müssen am Ende der URL einen Schrägstrich (/) angeben.

spectrum.ldap.useSSL

Geben Sie false an, um die SSL-Kommunikation mit LDAP zu deaktivieren.

spectrum.ldap.trustStore

Kommentieren Sie diese Eigenschaft aus.

spectrum.ldap.trustStore.password

Kommentieren Sie diese Eigenschaft aus.

Sicherheit für das Location Intelligence-Modul

Das Location Intelligence-Modul verwendet die rollenbasierte Sicherheit, wie sie für Spectrum™ Technology Platform zum Einsatz kommt. Da die Sicherheit auf Plattformebene umgesetzt wird, können Sie die Management Console verwenden, um alle Sicherheitsaktivitäten des Location Intelligence-Moduls zu verwalten. Dies schließt das Festlegen von Berechtigungen für benannte Ressourcen zusätzlich zum Verwalten von Benutzerkonten (erstellen, ändern und löschen von Benutzerkonten) mit ein.

Vordefinierte Geodatenrollen

Sobald Sie das Location Intelligence-Modul installiert haben, stehen in der Management Console drei vordefinierte Rollen zur Verfügung:

spatial-admin	Die Rolle „spatial-admin“ bietet volle Berechtigungen (Erstellen/Anzeigen/Ändern/Löschen) für alle benannten Ressourcen und Datasets, die zu benannten Tabellen gehören. Diese Berechtigungen werden über die gesicherten Entitätstypen des Location Intelligence-Moduls, „Location Intelligence.Named Resources“ und „Location Intelligence.Dataset.DML“, gesteuert. Benutzer der Location Intelligence-Moduldienste müssen für die von Ihnen verwendeten Ressourcen und alle abhängigen Ressourcen mindestens über Berechtigungen zum Anzeigen verfügen. Weitere Informationen zum Steuern von Berechtigungen für Datasets finden Sie unter **Zugriffssteuerung für Datasets** auf Seite 63.

spatial-user	Die Rolle „spatial-user“ bietet nur Anzeigeberechtigungen für benannte Ressourcen. Diese Berechtigungen werden über den gesicherten Entitätstyp des Location Intelligence-Moduls „Location Intelligence.Named Resources“ gesteuert. Benutzer der Location Intelligence-Moduldienste müssen für die von Ihnen verwendeten Ressourcen und alle abhängigen Ressourcen mindestens über Berechtigungen zum Anzeigen verfügen.
spatial-dataset-editor	Die Rolle „spatial-dataset-editor“ bietet volle Berechtigungen (Erstellen/Anzeigen/Ändern/Löschen) für Datasets. Diese Berechtigungen werden über den gesicherten Entitätstyp des Location Intelligence-Moduls „Location Intelligence.Dataset.DML“ gesteuert. Weitere Informationen zu dieser Rolle und zum Steuern von Berechtigungen für Datasets finden Sie unter **Zugriffssteuerung für Datasets** auf Seite 63.

Datenfluss-Designern, die Zugriff auf benannte Ressourcen benötigen, müssen Sie zusätzliche Berechtigungen über die der Rolle „designer“ hinaus gewähren. Anweisungen zum Erstellen einer Rolle „spatial-dataflow-designer“ finden Sie unter **Erstellen eines Geodaten-Datenfluss-Designers** auf Seite 66.

Benutzerdefinierte Geodatenrollen und Zugriffssteuerungseinstellungen

Sie können benutzerdefinierte Rollen erstellen, die auf den vordefinierten Geodatenrollen basieren. Sie können diese dann Benutzerkonten zuweisen und den Zugriff auf benannte Ressourcen für diese Rollen und Benutzer anpassen, indem Sie Zugriffssteuerungseinstellungen (Außerkraftsetzungen) auf einzelne benannte Ressourcen, Datasets, Ordner oder Verzeichnisse anwenden. Ein typisches Szenario und gleichzeitig eine Best Practice für das Einrichten der Sicherheit für das Location Intelligence-Modul beinhaltet das Erstellen einer Rolle ohne Berechtigungen, das Anwenden von Zugriffssteuerungseinstellungen für diese Rolle (beispielsweise Gewähren der Berechtigungen Ändern und Löschen von benannten Ressourcen in einem angegebenen Ordner) und das Zuweisen dieser benutzerdefinierten Rolle sowie auch einer der vordefinierten Geodatenrollen zu einem Benutzer. Außerkraftsetzen von Berechtigungen eines einzelnen Benutzers ist ein weiteres typisches Szenario. Dabei wird beispielsweise ein Benutzerkonto erstellt, das nur über Berechtigungen zur Anzeige von benannten Ressourcen verfügt, dann werden Zugriffssteuerungseinstellungen angewendet, sodass der Benutzer benannte Ressourcen in einem bestimmten Ordner ändern und löschen kann.

Ordner

Ordnerberechtigungen werden an enthaltene Ressourcen und untergeordnete Ordnern vererbt, solange diese Ressourcen und Ordner über keine besonderen Zugriffssteuerungseinstellungen verfügen, die diese Berechtigungen außer Kraft setzen. Dies ist nützlich, wenn Sie die Berechtigungen für einen Satz an Ressourcen festlegen möchten. Sie können den Zugriff auf einen Ordner auf bestimmte Benutzer oder Rollen beschränken. Andere Benutzer können weder diesen Ordner noch dessen Inhalte sehen. Bei dem Entitätstyp „Location Intelligence.Named Resources“ sind alle aufgelisteten Ressourcen, die mit einem Schrägstrich (/) enden, Ordner oder Verzeichnisse in der Datenbank.

Berechtigungen auf Ordnerebene setzen jedoch nicht Berechtigungen, die auf der untergeordneten Ebene einzelner Ressourcen festgelegt wurden, außer Kraft. Wenn bei einem Ordner beispielsweise

die Berechtigung zum Erstellen für eine bestimmte Rolle oder einen bestimmten Benutzer festgelegt wurde, aber eine einzelne Ressource in dem Ordner (wie eine benannte Tabelle) über eine Zugriffssteuerungseinstellung verfügt, die für dieselbe Rolle oder denselben Benutzer die Berechtigung zum Anzeigen festlegt, hat die Berechtigung zum Anzeigen (schreibgeschützt) für die einzelne Ressource Vorrang vor der Berechtigung zum Erstellen für den Ordner.

Verstehen von ACLs

Übersicht

Die Zugriffssteuerungsliste (ACL) in Spectrum Spatial ist eine Liste von Berechtigungen, die an Named Resources oder an Ordner im Spectrum Spatial-Repository angehängt sind. Berechtigungen können erteilt werden, damit Benutzer Karten rendern, Features abfragen oder bearbeiten oder Ordner und Ressourcen im Repository verwalten können. Berechtigungen können entweder Benutzern oder Rollen zugewiesen werden. Benutzer erben alle Berechtigungen von den Rollen, zu denen sie gehören.

Die Art und Weise, wie Berechtigungen definiert werden, wurde in dieser Version vollständig überarbeitet. Wenn Sie frühere Versionen von Spectrum aktualisieren, werden die Berechtigungen auf das neue Modell migriert. Neu in dieser Version ist, dass es jetzt auch möglich ist, Berechtigungen für Repository-Ordner zu erteilen, damit andere Benutzer als „admin“ bestimmte Ordner im Repository verwalten können. Benutzer mit diesen Berechtigungen werden als Unteradministratoren bezeichnet. Es wurde eine neue ACL-Dienst-API bereitgestellt, um das Auflisten, Hinzufügen und Entfernen von Berechtigungen zu erleichtern. In künftigen Releases von Spectrum wird eine neue Benutzeroberfläche in Spectrum Spatial Manager zur Verwaltung von Berechtigungen bereitgestellt, die die Benutzeroberfläche in der Spectrum Management Console ersetzt. Zu diesem Zeitpunkt können sich Unteradministratoren auch beim Spectrum Spatial Manager anmelden und diesen verwenden. In dieser Version können Unteradministratoren nur Ressourcen und ihre ACL über die REST-APIs verwalten.

Die Verwaltung der Benutzer und Rollen erfolgt weiterhin über die Spectrum Management Console. Der ACL-Dienst bietet keine Vorgänge zum Verwalten von Benutzern oder Rollen.

ACL und Repository

Die ACL-Berechtigungen, die mithilfe der ACL-Dienste erteilt werden können, lassen sich in drei Kategorien einteilen.

- **Ordner-ACL:** Erteilt Berechtigungen zum Verwalten des Inhalts des Repositorys (einschließlich Hochladen, Erstellen und Löschen von Named Resources und Festlegen weiterer Berechtigungen für diese). Diese Berechtigungen werden für Repository-Ordner erteilt. Benutzer mit diesen Berechtigungen können Named Resources in den Ordnern anzeigen oder ändern, für die ihnen Berechtigungen erteilt wurden. Benutzer mit Berechtigungen für einen oder mehrere Ordner werden als Unteradministratoren bezeichnet, da sie eine Untergruppe des Repositorys verwalten können. Unteradministratoren haben Zugriff auf die Named Resource- und ACL-Dienste. In

zukünftigen Versionen können sie sich auch beim Spatial Manager und Map Uploader anmelden, um Ressourcen zu verwalten.

- **Ressourcen-ACL:** Erteilt Berechtigungen zum Rendern bestimmter benannter Kacheln, benannter Karten und benannter Layer. Diese Berechtigungen werden für die benannten Ressourcen selbst erteilt. Benutzer mit diesen Berechtigungen können die Mapping- und Tiling-Dienste zum Rendern von Karten und Layern verwenden. Benutzer, die Unteradministratoren sind, erben auch die Ressourcenberechtigungen, um alle Karten und Layer in ihren Ordnern zu rendern.
- **Dataset-ACL:** Erteilt Berechtigungen zum Abfragen oder Bearbeiten bestimmter benannter Tabellen (d. h. CRUD-Vorgänge zum Erstellen, Lesen, Aktualisieren, Löschen). Diese Berechtigungen werden für die benannten Tabellenressourcen selbst erteilt. Benutzer mit diesen Berechtigungen können Features aus den Tabellen abfragen oder Features einfügen/aktualisieren/löschen. Benutzer, die Unteradministratoren sind, erben auch Dataset-Berechtigungen, um Tabellen abzufragen.. Sie erben jedoch nicht die Dataset-Einfügungs-, Aktualisierungs- oder Löschungsberechtigungen. Um Tabellen bearbeiten zu können, müssen ihnen zusätzlich zu den Ordnerberechtigungen auch diese Berechtigungen erteilt werden.

Die folgende Tabelle fasst die drei Kategorien, die Named Resources, auf die sie sich beziehen, und die spezifischen Berechtigungen zusammen, die in jeder Kategorie erteilt werden können. Es gibt auch einige Named Resources, für die keine Berechtigungen erteilt werden. Diese sind ebenfalls in der Tabelle aufgeführt.

Tabelle 1: Zusammenfassung der ACL-Berechtigungen

Art der Berechtigung	Erteilt für	Berechtigungen, die mithilfe von ACL-Diensten festgelegt wurden	**Berechtigungen, die für Spectrum Platform übernommen werden**	Aktivitäten, die Benutzer ausführen können
Ordnerberechtigung	Repository-Ordner	READ	NamedResource.EXECUTE NamedResource.VIEW	Der Benutzer kann Ordner, Unterordner und deren Inhalt als Unteradministrator anzeigen. Der Benutzer kann beliebige Karten und Layer in seinen Ordnern rendern. Der Benutzer kann beliebige Tabellen in seinen Ordnern abfragen.
		WRITE	NamedResource.CREATE NamedResource.DELETE NamedResource.MODIFY	Der Benutzer kann Ressourcen in seinen Ordnern erstellen, löschen oder ändern, einschließlich des Hochladens von Ressourcen und des Festlegens neuer ACL-Berechtigungen für sie.
Ressourcenberechtigung	Benannte Kacheln, benannte Karten, benannte Layer und benannte Beschriftungsquellen	EXECUTE	NamedResource.EXECUTE	Der Benutzer kann die Karten und Layer rendern, für die er diese Berechtigung hat.

Art der Berechtigung	Erteilt für	Berechtigungen, die mithilfe von ACL-Diensten festgelegt wurden	**Berechtigungen, die für Spectrum Platform übernommen werden**	Aktivitäten, die Benutzer ausführen können
Dataset-Berechtigung	Benannte Tabellen und benannte Ansichtstabellen	EXECUTE	NamedResource.EXECUTE	Der Benutzer kann die Daten aus den Tabellen abfragen, für die er diese Berechtigung hat.
		CREATE	Dataset.DML.CREATE	Der Benutzer kann neue Datensätze in die Tabellen einfügen, für die er diese Berechtigung hat.
		DELETE	Dataset.DML.DELETE	Der Benutzer kann Datensätze aus den Tabellen löschen, für die er diese Berechtigung hat.
		ÄNDERN	Dataset.DML.MODIFY	Der Benutzer kann Datensätze in den Tabellen aktualisieren, für die er diese Berechtigung hat.
Keine Berechtigungen erforderlich	Benannte Stile	Auf die benannten Stile wird keine ACL angewendet. Auf jeden benannten Stil, auf den in einem Layer oder WMS verwiesen wird, kann beim Rendern des Layers zugegriffen werden.		
	Benannte Verbindungen	Auf die benannten Verbindungen wird keine ACL angewendet. Es kann eine beliebige benannte Verbindung verwendet werden, wenn Daten aus einer benannten Tabelle abgefragt werden. Benannte Verbindungen können jedoch nur von Benutzern, die Unteradministratoren sind (d. h. die über Ordnerberechtigungen verfügen), über den Named Resource-Dienst angezeigt werden.		
	Metadaten-Ressourcen	Auf Named Resource-Metadaten wird keine ACL angewendet. Derzeit können diese nur von den Administratoren oder den Benutzern, die Unteradministratoren sind (d. h. die über Ordnerberechtigungen verfügen), über den Named Resource-Dienst angezeigt werden.		

ACL und Zugreifen auf Dienste und Anwendungen

Der Zugriff auf Dienste und Anwendungen ist abhängig von der jeweiligen ACL. Die folgende Liste beschreibt die Berechtigungen, die von Benutzern benötigt werden. Ausführliche Informationen finden Sie unter den einzelnen Dienstmethoden im REST- und SOAP-Handbuch für jeden Dienst.

- **Mapping-Dienst (REST und SOAP):** Benutzer können die Karten und Layer auflisten, beschreiben und rendern, für die sie über die Ausführungsberechtigung für Ressourcen verfügen. Für die zugrunde liegenden Ressourcen ist keine Berechtigung erforderlich, um eine bestimmte Karte oder einen bestimmten Layer zu rendern. Eine solche ist jedoch erforderlich, wenn eine Clientanwendung auch die zugrunde liegenden Ressourcen beschreiben oder darauf zugreifen muss, wenn sie den Benutzern angezeigt werden.
- **Map Tiling-Dienst (REST und SOAP):** Benutzer können die benannten Kacheln auflisten, beschreiben und rendern, für die sie die Ausführungsberechtigung für Ressourcen haben. Für die zugrunde liegenden Ressourcen ist keine Berechtigung erforderlich, um eine bestimmte Kachel zu rendern. Eine solche ist jedoch erforderlich, wenn eine Clientanwendung auch die zugrunde liegenden Ressourcen beschreiben oder darauf zugreifen muss, wenn sie den Benutzern angezeigt werden.
- **Feature-Dienst (REST und SOAP):** Benutzer können Features aus den benannten Tabellen und Ansichten, für die sie die Ausführungsberechtigung für Datasets haben, auflisten, beschreiben und abfragen. Benutzer können Features aus den benannten Tabellen einfügen, aktualisieren und löschen, für die sie über die Berechtigung CREATE, MODIFY oder DELETE für Datasets verfügen
- **Named Resource-Dienst (SOAP):** Um einen Vorgang im Named Resource-Dienst verwenden zu können, muss ein Benutzer über Ordnerberechtigungen für mindestens einen Ordner verfügen (und er muss lese- oder schreibberechtigt für die Ordner sein, um die Ressourcen anzuzeigen oder zu verwalten)
- **ACL Service (REST):** listDatasetPermissions und listFolderPermissions im ACL-Dienst stehen allen Benutzern zur Verfügung. Um die anderen ACL-Vorgänge zu verwenden (um Ressourcen-, Ordner- oder Dataset-Berechtigungen aufzulisten, hinzuzufügen oder zu löschen), muss ein Benutzer über Ordnerberechtigungen für mindestens einen Ordner verfügen (und er muss lese- oder schreibberechtigt für die Ordner sein, um die Ressourcen anzuzeigen oder zu verwalten).
- **WMTS:** Auf benannte WMTS-Kacheln werden keine ACL-Berechtigungen angewendet. Wenn eine benannte WMTS-Kachel erstellt wird, ist der Lesezugriff darauf über den WMTS-Dienst impliziert. Es sind keine ACL-Berechtigungen für die zugrunde liegenden Ressourcen erforderlich. Der Benutzer kann über den WMTS-Dienst auf die Kachel zugreifen (jedoch nicht über die anderen Dienste, es sei denn, er verfügt über bestimmte Ressourcenberechtigungen).
- **WMS:** Beim WMS-Dienst bedeutet das Hinzufügen eines Layers zum Dienst Lesezugriff darauf über den WMS-Dienst. ACL-Berechtigungen sind für die zugrunde liegende Named Layer-Ressource nicht erforderlich. Der Layer wird in der Capabilities-Datei aufgelistet, und Benutzer können die Karte und die Legende rendern und Feature-Informationen über den WMS-Dienst abrufen (jedoch nicht über die anderen Dienste, sofern sie nicht über bestimmte Ressourcenberechtigungen verfügen).
- **WFS:** Beim WFS-Dienst bedeutet das Hinzufügen einer Tabelle zum Dienst Lesezugriff darauf über den WFS. Es sind keine ACL-Berechtigungen für die zugrunde liegende Named

Table-Ressource erforderlich. Die Tabelle wird in der Capabilities-Datei aufgelistet, und Benutzer können Features über den WFS-Dienst abfragen (jedoch nicht über die anderen Dienste, es sei denn, sie verfügen über bestimmte Ressourcenberechtigungen).

- **Spatial Manager:** Zum Verwalten von Ressourcen in der Spatial Manager-Anwendung muss ein Benutzer über „spatial-admin“-Berechtigungen verfügen. Derzeit können Benutzer, die Unteradministratoren sind, Ressourcen mithilfe der Dienst-APIs verwalten.
- **Map Uploader:** Für Uploads mit dem Map Uploader muss ein Benutzer über „spatial-admin“-Berechtigungen verfügen. Derzeit können Benutzer, die Unteradministratoren sind, Ressourcen mithilfe der Dienst-APIs verwalten.
- **Datenflüsse im Enterprise Designer:** Um Datenflüsse ausführen zu können, muss ein Benutzer über „admin“ oder „spatial-admin“ sowie „designer“-Berechtigungen verfügen. Der Benutzer muss Ausführungsberechtigungen für benannte Tabellen und Berechtigungen zum Erstellen/Ändern/Löschen für das Dataset haben, um DML-Vorgänge für die unterstützte beschreibbare Tabelle ausführen zu können.

ACL-Verwaltung

Es wird empfohlen, die ACL-Dienste zum Hinzufügen und Entfernen von ACL zu verwenden, anstatt die Spectrum Management Console zu verwenden. Die ACL-Dienst-APIs sind im REST-API-Abschnitt des Spectrum Spatial-Handbuchs dokumentiert. Die Dienste stellen sicher, dass die korrekte Kombination von Berechtigungen für Spectrum Platform übernommen wird.

Die ACL-Dienste können auch Berechtigungen an die abhängigen Ressourcen weitergeben (wiederholen). Dies ist wichtig, wenn Sie Spectrum Spatial mit Clientanwendungen (z. B. Spectrum Spatial Analyst) verwenden, bei denen Benutzer Karten rendern bzw. die Layer rendern müssen, auf die die Karten verweisen, und auch Berechtigungen für die Abfrage von Features für die von den Layern referenzierten Tabellen benötigen.

Die Spectrum Management Console kann verwendet werden, um die erteilten Berechtigungen anzuzeigen. Wenn die Spectrum Management Console zum Ändern von Berechtigungen verwendet wird, müssen folgende Regeln befolgt werden, um die Konsistenz der erteilten Berechtigungen zu gewährleisten:

- Es sollte keine verweigerten Berechtigungen für Ressourcen oder Ordner geben. Das Verweigern von Berechtigungen verhindert Folgendes:
  - Dass Benutzer Berechtigungen von Rollen erben
  - Dass Unteradministratoren Berechtigungen von Ordnern erben
- Um Render- und Abfragezugriff auf Named Resources zu ermöglichen, sollte nur NamedResource.EXECUTE erteilt werden. Erteilen Sie NamedResource.VIEW, NamedResource.CREATE, NamedResource.DELETE oder NamedResource.MODIFY niemals direkt der Named Resource (diese Berechtigungen übermitteln Unteradministratorrechte und sollten nur für Ordner erteilt werden).
- Um Dataset-Bearbeitungsberechtigungen für benannte Tabellen bereitzustellen, erteilen Sie je nach Bedarf die Dataset.DML.CREATE-, Dataset.DML.DELETE- oder Dataset.DML.MODIFY-Berechtigung.

- Um Unteradministratoren Lesezugriff auf Repository-Ordner zu geben, erteilen Sie sowohl NamedResource.EXECUTE als auch NamedResource.VIEW für die Ordner. Diese Berechtigungen sollten immer zusammen erteilt werden. Dies ist wichtig.
- Um Unteradministratoren Schreibzugriff auf Repository-Ordner zu geben, erteilen Sie die Berechtigungen NamedResource.CREATE, NamedResource.DELETE und NamedResource.MODIFY. Diese drei Berechtigungen sollten immer zusammen erteilt werden. Dies ist wichtig.
- Erteilen Sie keine Berechtigungen für benannte Verbindungen, benannte Stile, benannte WMTS-Kacheln oder Metadatenressourcen.
- Wenn Clientanwendungen auf Karten, Layer und Tabellen zugreifen, müssen Berechtigungen für alle abhängigen benannten Ressourcen festgelegt werden, die verwendet werden sollen.

Aktualisieren mit ACL

Migration auf 12.0 SP2

Beim Upgrade auf 12.0 SP2 wird das ACL-Modell auf ein neues Sicherheitsmodell aktualisiert. Das Migrationsskript wird als Teil der Installation ausgeführt, kann jedoch auch unabhängig vom Installationsvorgang ausgeführt werden.

> **Anmerkung:** Wenn Sie das CLI exportieren, werden die Berechtigungen nicht geändert. Diese Berechtigung muss migriert werden. Zum Beispiel verfügen die Ressourcen aus 12.0 SP1 und davor über die Anzeigeberechtigung. Wenn Sie jedoch auf 12.0 SP2 aktualisieren, ändert das Migrationsskript die Anzeige- in die Ausführungsberechtigung.

Das Migrationsskript wird ausgeführt, wenn der Spectrum-Server zum ersten Mal gestartet wird, nachdem auf 12.0 SP2 aktualisiert wurde. Es wird nur einmal ausgeführt. Das Migrationsskript führt Folgendes aus:

- Alle Berechtigungen für Ordner werden entfernt.
- Alle Berechtigungen für Ressourcen werden entfernt.
- Die neue Ausführungsberechtigung wird angewendet, wenn die Anzeigeberechtigung für Ressourcen vorhanden ist.
- Alle vorhandenen verweigerten Berechtigungen werden entfernt.
- Die Anzeigeberechtigung für Datasets wird entfernt. Andere Berechtigungen für Datasets wie die zum Erstellen, Ändern und Löschen bleiben erhalten, wenn sie vor der Aktualisierung vorhanden waren.
- NamedResourceMetadata-Ressourcen haben vorerst keine ACL.

> **Anmerkung:** Nach dem Hinzufügen der neuen Ausführungsberechtigung ist die Erneuerung von Spectrum abgeschlossen.

Grundlegendes zu CLI-Änderungen für ACL

Mit dem neuen ACL-Sicherheitsmodell verfügt das CLI über aktualisierte Berechtigungen. In diesem Abschnitt werden die Änderungen beschrieben, die am CLI-Tool zum Importieren und Exportieren des neuen ACL-Modells vorgenommen wurden, das importiert und exportiert werden kann.

Arbeiten mit dem CLI

Nur ein „admin“- oder „spatial-admin“-Benutzer kann das CLI-Dienstprogramm ausführen. Bei Version 12.2 können Sie mit minimalen Berechtigungen Exporte durchführen: Sie benötigen lediglich die Anzeigeberechtigung für eine Ressource. Zum Importieren sind dann Berechtigungen zum Erstellen für den Zielordner erforderlich. Im Allgemeinen sollten jedoch nur Administratoren und Unteradministratoren bei Version 12.2 Im- und Exporte durchführen können.

- Ein Benutzer kann die Ressourcen exportieren, wenn er die Berechtigung zum Anzeigen hat.
- Ein Benutzer kann die Ressourcen importieren, wenn er die Berechtigung zum Erstellen in dem Ordner im Repository hat.

Exportieren

Der exportierende Benutzer muss Anzeigeberechtigungen (Ressourcenberechtigungen) für alle zu exportierenden Ressourcen haben, andernfalls wird eine Ausnahme (Zugriff verweigert) ausgelöst und der Exportvorgang beendet.

Wenn Sie mit der Option „--a“ exportieren, nachdem alle Ressourcen erfolgreich exportiert wurden, wird auch die ACL aller exportierten Ressourcen exportiert (einschließlich Entitäten aller anderen Benutzer/Rollen).

Importieren

Ein Benutzer muss über Berechtigungen zum Erstellen (Ressourcenberechtigungen) für den Zielordner im Repository verfügen, andernfalls wird eine Ausnahme (Zugriff verweigert.) ausgelöst und der Importvorgang beendet.

Wenn Sie mit der Option „--a“ importieren, werden alle ACLs in vorhandene ACLs, die im System registriert sind (wie in früheren Versionen), zusammengeführt.

Wenn Sie Ressourcen importieren, die aus einer älteren Version unter Angabe von „--a“ exportiert wurden, wird die ACL auf Basis der folgenden Regeln aktualisiert, bevor sie mit einer vorhandenen ACL im System zusammengeführt wird:

- Alle Berechtigungen für Ordner werden ignoriert.
- Alle Berechtigungen für Ressourcen werden ignoriert.
- Die Ausführungsberechtigung wird hinzugefügt, wenn eine Ressource über Anzeigeberechtigung verfügte.
- Alle verweigerten Berechtigungen werden ignoriert.
- Alle Dataset-Berechtigungen werden wie zuvor zusammengeführt.

Zugriffssteuerung für Datasets

Was ist ein Dataset?

Ein Dataset ist eine Sammlung von Datenwerten in tabellarischer Form, die typischerweise aus Spalten (oder Datensätzen) und Zeilen besteht. Im Location Intelligence-Modul kann ein Dataset in Form einer TAB-Datei, einer Shape-Datei, einer GeoPackage-Datei oder einer JDBC-basierten Tabelle wie eine MS SQL Server-Tabelle vorhanden sein.

Vorteile von Zugriffssteuerung für Datasets

Über die Zugriffssteuerung für Datasets können Administratoren die Berechtigungen für eine benannte Tabelle von den Bearbeitungsberechtigungen des Datasets, auf das die benannte Tabelle verweist, abtrennen. Sie können als Administrator beispielsweise volle Bearbeitungsberechtigungen (Erstellen/Ändern/Löschen) für ein Dataset erteilen, während Sie die schreibgeschützten Berechtigungen (Ausführen) für die benannte Tabelle beibehalten. Wenn ein Benutzer versucht, einen DML-Vorgang (Data Manipulation Language, Datenmanipulationssprache) durchzuführen (wie einen Einfüge-, Aktualisierungs- oder Löschvorgang mithilfe des Feature-Dienstes oder des „Write Spatial Data“-Schrittes), werden die Berechtigungen des Benutzers nicht nur gegenüber der angegebenen benannten Tabelle im Entitätstyp „Location Intelligence.Named Resources“ überprüft, sondern auch gegenüber dem Entitätstyp „Location Intelligence.Dataset.DML“. Wenn die Ausführungsberechtigungen nicht erteilt sind, erscheint die benannte Tabelle nicht im Repository des Benutzers.

Was ist eine Dataset-gesicherte Entität?

Der gesicherte Entitätstyp „LocationIntelligence.Dataset.DML“ ist einer von zwei Typen gesicherter Entitäten für das Location Intelligence-Modul. Er steuert DML-Berechtigungen für Datasets, die mit benannten Tabellen verbunden sind. Bei der Erstellung oder dem Hochladen einer benannten Tabelle (mit einem beliebigen Tool, Spatial Manager, die Administrationsumgebung, den Named Resource-Dienst und WebDAV inbegriffen) wird für das zugeordnete Dataset der benannten Tabelle automatisch eine neue gesicherte Entität vom Typ „LocationIntelligence.Dataset.DML“ erstellt. Ein Benutzer muss für eine benannte Tabelle über Berechtigungen zum Ausführen *und* für das Dataset über Berechtigungen zum Erstellen/Ändern/Löschen verfügen, um DML-Vorgänge in beschreibbaren (JDBC-basierten) Tabellen ausführen zu können. DML-Vorgänge beinhalten das Einfügen, Aktualisieren und Löschen ausgeführter Vorgänge unter Verwendung des „Write Spatial Data“-Schrittes oder des Feature-Dienstes.

> **Anmerkung:** Obwohl Sie Berechtigungen zum Erstellen/Ändern/Löschen für Dataset-gesicherte Entitäten für schreibgeschützte Datasets wie TAB-Dateien oder Shape-Dateien festlegen können, können Sie trotzdem keine DML-Vorgänge mit diesen Datasets ausführen.

Tipp: Die Ausführungsberechtigung für die gesicherte Entität für das Dataset hat keine Auswirkung auf dessen Berechtigungen. Wenn Sie bei einer Dataset-gesicherten Entität die Ausführungsberechtigung deaktivieren, können Sie die Daten in der Tabelle immer noch anzeigen.

Wenn Sie nicht möchten, dass ein Benutzer eine Tabelle anzeigt, entfernen Sie stattdessen die Ausführungsberechtigungen auf der gesicherten Entität für die Named Resource.

Wenn eine benannte Tabelle umbenannt, verschoben oder gelöscht wird, benennt Spectrum Spatial die zugehörige gesicherte Entität für das Dataset um oder löscht sie.

Geodatenrollen und Dataset-Zugriff

Rollen werden verwendet, um Zugriff auf verschiedene Teile des Systems zu gewähren oder zu verweigern, und machen die Berechtigungsverwaltung einfacher. In der Management Console sind drei vordefinierte Rollen für Benutzer des Location Intelligence-Moduls verfügbar:

spatial-admin Die Rolle „spatial-admin“ bietet volle Berechtigungen (Ausführen/Erstellen/Ändern/Löschen) für alle Named Resources und Datasets. Ein Benutzer mit der Rolle „spatial-admin“ kann benannte Ressourcen anzeigen und Datasets bearbeiten.

> **Anmerkung:** Außerdem ist Dateiserverzugriff erforderlich, um den Quellordner für benannte Verbindungen, die dateisystembasiert sind, zu erstellen oder zu bearbeiten, wie auch bestimmte Einstellungen in Dienstkonfigurationsdateien (wie das Bildverzeichnis für den Mapping-Dienst). Weitere Informationen finden Sie unter **Erstellen eines Administrators für benannte Ressourcen** auf Seite 64.

spatial-user Die Rolle „spatial-user“ bietet nur Ausführungsberechtigungen für Named Resources. Ein Benutzer mit der Rolle „spatial-user“ kann Ressourcen anzeigen, aber nicht Datasets bearbeiten.

spatial-dataset-editor Die Rolle „spatial-dataset-editor“ bietet volle Berechtigungen (Ausführen/Erstellen/Ändern/Löschen) für Datasets. Ein Administrator kann beispielsweise volle Berechtigungen für Datasets gewähren, indem er bei einem Benutzer, der derzeit die Rolle „spatial-user“ hat, die Rolle „spatial-dataset-editor“ hinzufügt.

Diese vordefinierten Rollen können nicht geändert werden. Sie können allerdings benutzerdefinierte Rollen erstellen, die auf den vordefinierten Geodatenrollen basieren. Sie können diese dann Benutzerkonten zuweisen und den Zugriff in diesen Rollen und für die Benutzern anpassen, indem Sie Zugriffssteuerungseinstellungen (Änderungen) auf Datasets, einzelne benannte Ressourcen oder Ordner mit benannten Ressourcen anwenden. Weitere Informationen finden Sie unter **Konfigurieren der Zugriffssteuerung** auf Seite 31.

Erstellen eines Administrators für benannte Ressourcen

Um die benannten Ressourcen im Repository mithilfe von Spatial Manager und der Management Console zu verwalten, muss ein Benutzer über eine zugewiesene Rolle verfügen, die zusätzlich zum Zugriff, der über die vordefinierten Geodatenrollen gewährt wird, vollen Zugriff auf diese Ressourcen gestattet. Die vordefinierten Geodatenrollen können nicht geändert werden, und eine

vordefinierte Rolle „Administrator für benannte Ressourcen“ wird von Spectrum™ Technology Platform nicht zur Verfügung gestellt. Sie können jedoch unter Verwendung einer vordefinierten Geodatenrolle als Grundlage eine solche Rolle erstellen.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Sicherheit**.
3. Klicken Sie auf **Rollen**.
4. Aktivieren Sie das Kästchen neben der Rolle „spatial-admin“, um diese als Ausgangspunkt zu verwenden, und klicken Sie dann auf die Schaltfläche „Kopieren“  . Die Rolle „spatial-admin“ bietet die Berechtigungen Anzeigen, Ändern, Erstellen und Löschen für die gesicherten Entitätstypen „Location Intelligence Module.Named Resources“ und „Location Intelligence Module.Dataset“.
5. Geben Sie in das Feld **Rollenname** den gewünschten Namen für diese Rolle ein (beispielsweise „resource-admin“).
6. Legen Sie zusätzliche Berechtigungen für diese gesicherten Entitätstypen wie folgt fest:

   Datenbankressourcen:

   - **Centrus-Datenbankressourcen** für Anzeigen/Ändern/Erstellen/Löschen/Ausführen (falls erforderlich)
   - **Enterprise Routing** für Anzeigen/Ändern/Erstellen/Löschen/Ausführen (falls erforderlich)

   Plattform:

   - **Dienste** für Anzeigen/Ändern/Ausführen
   - **System – Versionsinformationen** für Anzeigen

   Resourcenverbindung:

   - **Ressourcen – Dateiserververbindungen** für Anzeigen
   - **Ressourcen – JDBC-Treiber** für Anzeigen

7. Klicken Sie auf **Speichern**, um die neue Rolle „resource-admin“ zu speichern.
8. Klicken Sie auf **Benutzer**.
9. Wählen Sie entweder einen vorhandenen Benutzer aus, und klicken Sie auf die Schaltfläche „Bearbeiten“  , um ihn zu bearbeiten, oder klicken Sie auf die Schaltfläche „Hinzufügen“  , um einen neuen Benutzer zu erstellen.
10. Weisen Sie dem Benutzerkonto die neue Rolle „resource-admin“ zu, um dem Benutzer zu gestatten, benannte Ressourcen zu verwalten.

Der Benutzer verfügt nun über den erforderlichen Zugriff, um benannte Ressourcen in Spatial Manager und der Management Console zu verwalten.

Erstellen eines Geodaten-Datenfluss-Designers

Ein Benutzer muss über die Rollen „designer“ und „spatial-user“ verfügen, um Datenflüsse für Schritte und Dienste des Location Intelligence-Moduls zu erstellen. Die Rolle „spatial-user“ bietet Zugriff zum Anzeigen benannter Ressourcen des gesicherten Entitätstyps „Location Intelligence.Named Resources“. Die Rolle „designer“ bietet den erforderlichen Zugriff auf Entitätstypen wie Datenflüsse, die auf Plattformebene gesichert sind.

1. Klicken Sie in der Management Console auf **System** > **Sicherheit**.
2. Wählen Sie entweder einen vorhandenen Benutzer aus, und klicken Sie auf die Schaltfläche „Bearbeiten“  , oder klicken Sie auf die Schaltfläche „Hinzufügen“  , um einen neuen Benutzer zu erstellen.
3. Weisen Sie im Abschnitt „Rollen“ sowohl die Rolle „designer“ als auch die Rolle „spatial-user“ dem Benutzerkonto zu.

Der Benutzer verfügt nun über die Berechtigung, benannte Ressourcen anzuzeigen und Datenflüsse zu entwerfen sowie diese Ressourcen für Schritte und Dienste des Location Intelligence-Moduls zu verwenden.

Einschränken des WebDAV-Zugriffs auf die Datenbank

WebDAV wird als ein Protokoll verwendet, um auf Ressourcen innerhalb der Spectrum Spatial-Datenbank zuzugreifen. Standardmäßig ist der Zugriff auf die Datenbank über WebDAV nicht auf einen bestimmten Server eingeschränkt, sondern steht allen Servern mit Zugriff auf die Datenbank offen. Sie können den Zugriff auf bestimmte Server einschränken, indem Sie die räumliche Java-Eigenschaftendatei ändern. Fügen Sie hierfür die folgende Eigenschaft hinzu, in der eine Liste von Hostnamen (IP) enthalten ist, für die WebDAV verfügbar ist (durch Komma getrennt). Nach der Änderung müssen Sie den Spectrum™ Technology Platform-Server neu starten.

So schränken Sie den Datenbankzugriff über WebDAV ein:

1. Öffnen Sie die Datei `modules/spatial/java.properties` in einem Editor.
2. Fügen Sie der Datei die folgende Eigenschaft hinzu.

```
repository.accesscontrol.allows=
```

3. Geben Sie eine Liste von IP-Adressen an, die auf WebDAV zugreifen dürfen. Sie können mehrere Server hinzufügen. Verwenden Sie dafür eine durch Kommas getrennte Liste von IP-Adressen. Wenn Sie die Eigenschaft leer lassen, wird der Zugriff über WebDAV für alle

Server mit Ausnahme des Rechners, auf dem Spectrum™ Technology Platform installiert ist, deaktiviert.

```
repository.accesscontrol.allows=192.168.2.1,192.168.2.2
```

4. Starten Sie den Server neu.

Sobald Sie den Vorgang abgeschlossen haben, ist der WebDAV-Zugriff auf die Datenbank eingeschränkt.

Verwendung von WebDAV mit HTTPS

Bei der Kommunikation mit dem Server über HTTPS zwecks Zuordnung eines Laufwerks zur Datenbank ist ein WebDAV-Client erforderlich, um das TLS v1.2-Protokoll verwenden zu können. Bei Client-Rechnern mit den Betriebssystemen Windows 7 SP1, Windows Server 2008 R2 SP1 und Windows Server 2012 müssen Sie einen Sicherheitspatch anwenden und die Registry aktualisieren, um dieses Protokoll nutzen zu können.

1. Wenden Sie den für das Betriebssystem geeigneten Patch aus der Microsoft Knowledge Base auf dem Clientcomputer an: **https://support.microsoft.com/en-us/kb/3140245**
2. Befolgen Sie die Anweisungen im KB-Artikel, um die Registry zu aktualisieren, damit diese TLS v1.2 unterstützt. Der Wert von DefaultSecureProtocols muss mindestens 0x00000800 sein.
3. Starten Sie den Clientcomputer neu, nachdem Sie den Registrierungseintrag geändert haben.

4 - Überwachen Ihres Systems

In this section

Anzeigen von Systemereignissen

Das Systemprotokoll zeigt Nachrichten aus dem Wrapper-Protokoll des Spectrum™ Technology Platform-Servers an. Diese Nachrichten umfassen Informationen zu Servervorgängen und zu Anforderungen an Dienste, die über die API oder über Webservices erstellt wurden. Zeigen Sie das Systemprotokoll an, wenn Probleme auftreten und Sie nach Informationen zu möglichen Ursachen suchen.

Wenn Sie Spectrum™ Technology Platform in einem Cluster ausführen, stammt das von Ihnen abgerufene Systemprotokoll aus dem Knoten, mit dem Sie verbunden sind. Sie können das Systemprotokoll für einen bestimmten Knoten anzeigen, indem Sie die folgende Datei mit einem Texteditor in dem gewünschten Knoten öffnen:
ServerLocation\server\app\repository\logs\wrapper.log.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Protokolle**.
3. Klicken Sie auf das Symbol „Herunterladen“  , um die Systemprotokolldatei herunterzuladen.
4. Öffnen Sie die heruntergeladene Datei in einem Texteditor.

Festlegen von Protokollierungsebenen für Dienste

Sie können die Standardprotokollierungsebene und Protokollierungsebenen für die einzelnen Dienste in Ihrem System angeben. Wenn Sie Protokollierungsebenen ändern, spiegelt sich diese Änderung nicht in den Protokolleinträgen wider, die vor der Änderung gemacht wurden.

> **Anmerkung:** Die von Ihnen angegebenen Protokollierungsebenen für Dienste haben keine Auswirkungen auf das Überwachungsprotokoll. Sie steuern nur die Protokollierungsebene für das Ereignisprotokoll, das Sie in der Management Console anzeigen können. Zu diesem Zeitpunkt können Sie das Ereignisprotokoll in der Webversion der Management Console nicht anzeigen.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Protokolle**.
3. Wählen Sie im Feld **Standardprotokollierungsebene des Systems** eine Standardereignisprotokollierungsebene für Dienste in Ihrem System aus.

Deaktiviert	Es ist keine Ereignisprotokollierung aktiviert.
Schwerwiegend	Minimale Protokollierung. Nur schwerwiegende Fehler werden protokolliert. Schwerwiegende Fehler sind Fehler, durch die das System unbrauchbar gemacht wird.

Fehler	Fehler und schwerwiegende Fehler werden protokolliert. Fehler deuten auf ein isoliertes Problem hin, durch das ein Teil des Systems unbrauchbar wird. Ein Problem, durch das ein einzelner Dienst nicht funktioniert, würde beispielsweise einen Fehler generieren.
Warnen	Ereigniswarnungen, Fehler und schwerwiegende Fehler werden protokolliert. Warnungen deuten auf Probleme hin, bei denen das System aber weiterhin arbeiten kann. Wenn beispielsweise ein Dienst geladen wird, bei dem ein Parameter einen ungültigen Wert aufweist, wird eine Warnung ausgegeben und der Standardparameter verwendet. Wenn während der Verwendung eines Dienstes Ergebnisse zurückgegeben werden, jedoch ein Problem vorliegt, wird eine Warnung protokolliert.
Info	Systeminformationen der obersten Ebene werden protokolliert. Dies ist die detaillierteste, für die Produktion geeignete Protokollierungsebene. Informationsereignisse werden in der Regel während des Starts und der Initialisierung angezeigt und enthalten Informationen, wie z. B. Versionsinformationen und Informationen darüber, welche Dienste geladen wurden.
Debuggen	Eine sehr detaillierte Protokollierungsebene, die für Fehlerbehebungsprobleme mit dem System geeignet ist.
Ablauf verfolgen	Die detaillierteste Protokollierungsebene, auf der die Programmausführung nachverfolgt wird (Methodeneingabe und Beenden). Sie enthält zur Fehlerbehebung detaillierte Informationen zum Programmfluss.

Jede Protokollierungsebene beinhaltet die in der Liste darüber aufgeführten Ebenen. Anders ausgedrückt: Wenn „Warnung“ als Protokollierungsebene ausgewählt wird, werden auch Fehler und schwerwiegende Fehler protokolliert. Wenn „Info“ ausgewählt wird, werden Informationsmeldungen, Warnungen, Fehler und schwerwiegende Fehler protokolliert.

> **Anmerkung:** Eine Auswahl der intensivsten Protokollierungsebene kann die Systemleistung beeinträchtigen. Daher sollten Sie die am wenigsten intensive Einstellung auswählen, die Ihre bestimmten Protokollierungsanforderungen erfüllt.

4. Wenn Sie für jeden Dienst eine andere Protokollierungsebene angeben möchten, wählen Sie die gewünschte Protokollierungsebene aus.

ProtoProtokollieren von Spatial

Die Datei „logback.xml“ ermöglicht Ihnen, das Protokollierungsverhalten zu steuern. Standardmäßig wird die Ausgabe zur Konsole gesendet, die sie dann zur Datei „wrapper.log“ umleitet. Sie können die Ausgabe jedoch stattdessen zu einer Protokolldatei senden lassen. Sie können außerdem über

die Protokollierungsebene die Protokollierung vollständig deaktivieren oder nur schwerwiegende Fehler protokollieren lassen.

Standardmäßige Datei „logback.xml“
(`<Installed>\Pitney Bowes\Spectrum\server\modules\spatial\logback.xml`)

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
======================================================================================
 -->
<!-- Logger configuration for remote components
                    -->
<!--
                    -->
<!-- log to console, redirected to Platform log
(server\app\repository\logs\wrapper.log) -->
<!-- log to files, redirected to (server\modules\spatial\spatial.XXX.log)
                 -->
<!--
                    -->
<!-- for general information about the configuration file, check out
the logback manual  -->
<!-- at http://logback.qos.ch/manual/configuration.html
                    -->
<!--
======================================================================================
 -->
<configuration>
 <appender name="CONSOLE-SPATIAL"
class="ch.qos.logback.core.ConsoleAppender">
  <encoder>
   <pattern>[Spatial] - [%thread] %-5level %logger{35} - %msg%n</pattern>

  </encoder>
 </appender>
 <!--appender name="FILE-SPATIAL"
class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${g1.server.modules.dir}/spatial/${component.name}.log</file>
  <encoder>
   <pattern>%d [%thread] %-5level %logger{35} - %msg%n</pattern>
  </encoder>
  <append>true</append>
  <triggeringPolicy
class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
   <maxFileSize>10MB</maxFileSize>
  </triggeringPolicy>
  <rollingPolicy
class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
   <fileNamePattern>${component.name}.log.%i</fileNamePattern>
   <maxIndex>1</maxIndex>
  </rollingPolicy>
```

```
 </appender-->
 <!-- Level: OFF, ERROR, WARN, INFO, DEBUG -->
 <logger name="com.mapinfo.midev" level="INFO" additivity="false">
  <appender-ref ref="CONSOLE-SPATIAL"/>
  <!-- appender-ref ref="FILE-SPATIAL"/ -->
 </logger>
</configuration>
```

Option	Werte
Stufe	• OFF: Protokollierung deaktivieren • ERROR: Laufzeitfehler oder unerwartete Fehler protokollieren • WARN: nur Warnungen protokollieren, beispielsweise die Verwendung einer veralteten API • INFO: Laufzeitereignisse wie Start oder Herunterfahren protokollieren [Standard] • DEBUG: detaillierte Informationen zur Fehlersuche protokollieren
Ausgabe	• CONSOLE-SPATIAL: Protokollinformationen zur Konsole senden [Standard] • FILE-SPATIAL: Protokollinformationen zu einer auf der Komponente basierenden Protokolldatei senden (Nicht mehr verfügbar: Spectrum Spatial verfügt über eine einzelne Remote-Komponente.)

Konfigurieren eines Mailservers

Spectrum™ Technology Platform Kann E-Mail-Warnungen senden, um Sie über wichtige Ereignisse zu informieren. E-Mail-Benachrichtigungen können aufgrund von Bedingungen in Datenflüssen und Prozessflüssen gesendet werden und wenn der Ablauf zeitbasierter Lizenzen, Datenbanken und anderer zeitbasierter Elemente bevorsteht.

Spectrum™ Technology Platform verfügt über keinen integrierten Mailserver. Zur Aktivierung von E-Mail-Benachrichtigungen müssen Sie so konfigurieren, dass ein externer SMTP-Server verwendet wird.

1. Öffnen Sie die Management Console.

2. Öffnen Sie **System** > **Mailserver**.
3. Geben Sie im Feld **Host** den Hostnamen oder die IP-Adresse des SMTP-Servers ein, den Sie zum Senden der E-Mail-Benachrichtigungen verwenden möchten.
4. Geben Sie im Feld **Port** eine Portnummer oder einen Bereich ein, die bzw. der für die Netzkommunikation zwischen dem Spectrum™ Technology Platform-Server und dem SMTP-Server verwendet werden soll.

   Der Standardort ist 25.

5. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldeinformationen ein, die der Spectrum™ Technology Platform-Server für die Authentifizierung am SMTP-Server verwenden sollte.
6. Geben Sie im Feld **Absenderadresse** die E-Mail-Adresse ein, von der aus die Benachrichtigungs-E-Mail gesendet wird.
7. Um sicherzustellen, dass Sie einen Mailserver ordnungsgemäß konfiguriert haben, können Sie eine Test-E-Mail senden. Geben Sie im Feld **Testadresse** die E-Mail-Adresse ein, an die die Test-E-Mail gesendet werden soll, und klicken Sie anschließend auf **Testen**.
8. Klicken Sie auf **Speichern**.

Der Spectrum™ Technology Platform-Server ist jetzt mit einem SMTP-Server verbunden und kann über diesen Server Benachrichtigungs-E-Mails senden.

Beispiel: Konfigurieren eines Mailservers

Sie verfügen über einen SMTP-Server mit dem Namen mail.beispiel.com. Sie möchten diesen Mailserver verwenden, um vom Spectrum™ Technology Platform-Server gesendete E-Mail-Benachrichtigungen zu verarbeiten. Sie haben auf dem SMTP-Server ein Konto mit dem Namen „Spectrum123“ und dem Kennwort „Beispiel123“ erstellt, und die E-Mail-Adresse für dieses Konto lautet spectrum.notification@beispiel.com.

Um eine Benachrichtigung mit diesen Informationen zu konfigurieren, müssen Sie die Felder wie folgt ausfüllen:

Host	mail.beispiel.com
Absenderadresse	spectrum.notification@beispiel.com
Benutzername	Spectrum123
Kennwort	Beispiel123

Auswählen von Elementen für Ablaufbenachrichtigungen

Spectrum™ Technology Platform Kann eine E-Mail-Benachrichtigung senden, wenn eine Lizenz, Datenbank oder Softwarekomponente bald abläuft. Dadurch können Sie die notwendigen Maßnahmen ergreifen, um sicherzustellen, dass Ihre Geschäftsprozesse nicht durch einen Ablauf unterbrochen werden. Zu den Komponenten mit Ablaufdatum zählen folgende:

- Lizenzen

  Anmerkung: Für transaktionsbasierte Lizenzen sind keine E-Mail-Benachrichtigungen verfügbar. Wenn Sie sich der maximalen Anzahl von Transaktionen für eine Lizenz nähern, wird im Systemprotokoll in der Management Console eine Nachricht angezeigt.

- Datenbanken, wie z. B. postalische US-Datenbanken, die für die CASS-Verarbeitung verwendet werden
- Bestimmte Softwarekomponenten, wie z. B. das für die Validierung von US-Adressen Im Universal Addressing-Modul verwendete Modul

Tipp: Um die Elemente mit Ablaufdatum anzuzeigen, öffnen Sie die Management Console und **System** > **Lizenzierung und Ablauf**.

Sie können auswählen, zu welchen Elementen Sie Benachrichtigungen erhalten möchten, damit Sie nur zu den für Sie relevanten Elemente Benachrichtigungen erhalten.

1. Öffnen Sie die Management Console.
2. Öffnen Sie **System** > **Lizenzierung und Ablauf**.
3. Aktivieren Sie das Kästchen in der Spalte **Benachrichtigung senden**, um eine Ablaufbenachrichtigungs-E-Mail zu einem Element zu erhalten. Geben Sie die Anzahl der Tage an, die Sie vor dem Ablauf benachrichtigt werden möchten, wenn Sie früher oder später als standardmäßig festgelegt benachrichtigt werden möchten.

Anzeigen von Versionsinformationen

1. Öffnen Sie die folgende URL in einem Webbrowser:

   http://*server*:*port*/managementconsole

   Dabei steht *Server* für den Servernamen oder die IP-Adresse Ihres Spectrum™ Technology Platform-Servers, und *Port* ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der HTTP-Port ist standardmäßig auf 8080 eingestellt.

2. Klicken Sie auf **System** > **Version**.

Anzeigen und Exportieren von Lizenzinformationen

Sie können Informationen zu Ihrer Lizenz in eine XML-Datei exportieren. Dies kann erforderlich sein, wenn Lizenzprobleme mit dem technischen Support gelöst werden sollen.

1. Öffnen Sie die folgende URL in einem Webbrowser:

   http://*server*:*port*/managementconsole

   Dabei steht *Server* für den Servernamen oder die IP-Adresse Ihres Spectrum™ Technology Platform-Servers, und *Port* ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der HTTP-Port ist standardmäßig auf 8080 eingestellt.

2. Klicken Sie auf **System** > **Lizenzierung und Ablauf**.
3. Klicken Sie auf das Exportsymbol.

Ihre Lizenzinformationen werden in einer XML-Datei mit der Erweiterung `.lic` gespeichert.

Überwachen der Leistung mit der JMX Console

Bei der JMX Console handelt es sich um ein browserbasiertes Tool, das ein Tool für die Leistungsüberwachung bereitstellt. Dieses Tool zeichnet für jeden Schritt in einem Datenfluss Leistungsstatistiken auf.

1. Öffnen Sie einen Webbrowser, und rufen Sie Folgendes auf:`http://server:port/jmx-console`

   Dabei gilt Folgendes:

   server ist die IP-Adresse oder der Hostname Ihres Spectrum™ Technology Platform-Servers.

   port ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der Standardwert ist 8080.

2. Melden Sie sich mit dem Administratorkonto an.
3. Klicken Sie unter „Domäne: com.pb.spectrum.platform.performance“ auf **com.pb.spectrum.platform.performance:service=PerformanceMonitorManager**.
4. Klicken Sie neben **aktivieren** auf die Schaltfläche **Aufrufen**.
5. Klicken Sie auf **Zurück zur MBean-Ansicht**, um zum Bildschirm „PerformanceMonitorManager“ zurückzukehren.

Die Leistungsüberwachung ist jetzt aktiviert. Wenn ein Datenfluss ausgeführt wird, wird die Leistungsstatistik oben auf dem Bildschirm „PerformanceMonitorManager“ angezeigt. Beachten Sie Folgendes:

- Sie müssen den Bildschirm aktualisieren, um die Aktualisierungen zu sehen.
- Klicken Sie neben **zurücksetzen** auf die Schaltfläche **Aufrufen**, um die Statistik zurückzusetzen.
- Wenn Sie den Spectrum™ Technology Platform-Server beenden, wird die Leistungsüberwachung ausgeschaltet. Sie müssen Sie wieder einschalten, wenn Sie den Server erneut starten.

Überwachen der Statistik zum Caching von Datei-Handles über die JMX-Konsole

Bei der JMX-Konsole handelt es sich um ein browserbasiertes Tool, das die Leistung überwacht und Statistiken aufzeichnet. Dazu gehört die Statistik zum Caching von Datei-Handles für native TAB- und Shape-Dateien.

1. Öffnen Sie einen Webbrowser, und rufen Sie Folgendes auf:`http://server:port/jmx-console`

   Dabei gilt Folgendes:

   server ist die IP-Adresse oder der Hostname Ihres Spectrum™ Technology Platform-Servers.

   port ist der HTTP-Port, der von Spectrum™ Technology Platform verwendet wird. Der Standardwert ist 8080.

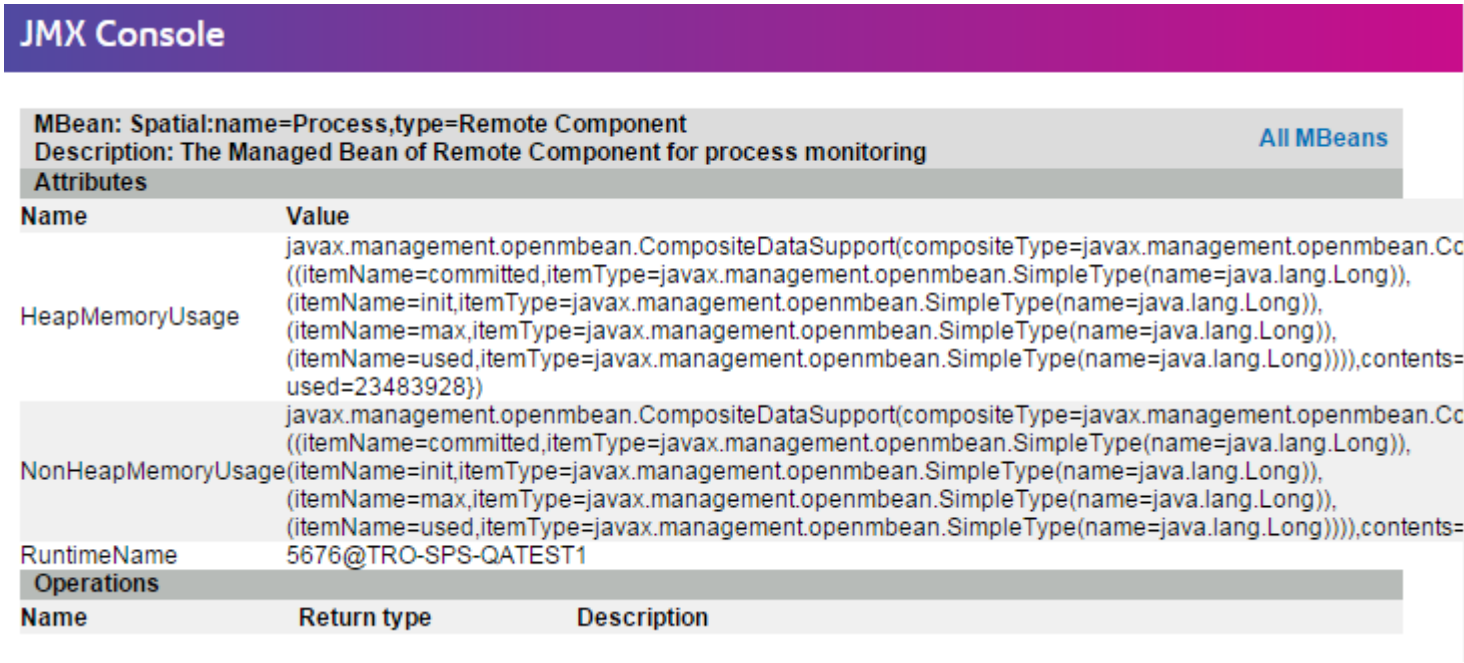
2. Melden Sie sich mit dem Administratorkonto an.
3. Klicken Sie unter „Domain: Spatial“ auf **Spatial:name=TABFileHandlePool,type=Remote Component** oder **Spatial:name=ShapeFileHandlePool,type=Remote Component**, um die Statistik zum Caching von Datei-Handles für TAB- oder Shape-Dateien anzuzeigen.

   Anmerkung: Sie können zudem den Cache für Datei-Handles auf dieser Seite deaktivieren oder löschen, ohne den Server neu starten zu müssen.

4. Klicken Sie auf **Alle MBeans**, um zum Hauptbereich der JMX-Konsole zurückzukehren.

Überwachen der Speichernutzung

Über die JMX-Konsole können Sie die JVM-Heapnutzung der Remote-Komponente für Geodaten überwachen.



Die Speichernutzung (HeapMemoryUsage und NonHeapMemoryUsage) basiert auf dem standardmäßigen MBean für JVM-Speicher. Es zeigt die Speichernutzung der JVM, in der die Remote-Komponente läuft. Es zeigt folgende Speichermengen an: anfänglich, maximal, übergeben, verwendet.

RuntimeName beinhaltet die Prozess-ID, die Sie verwenden können, um über das Betriebssystem an mehr Informationen zu gelangen (indem Sie beispielsweise den Windows Task-Manager verwenden) oder den Prozess sogar zu beenden.

Die Angaben in den Heapabschnitten `={committed=143130624, init=134217728, max=1908932608, used=23483928}` erfolgen in Byte.

„init“ ist die anfängliche Menge, die der JVM zugewiesen wurde (-Xms), „max“ ist die durch „–Xmx“ spezifizierte Menge. „used“ ist die Speichermenge, die von der JVM für Objekte verwendet wird. Die Beziehung stellt sich wie folgt dar: –Xms < committed < -Xmx und used < committed.

Sie können den Heapspeicher ändern, indem Sie die Option „-Xm“ in der Datei „java.vmargs“ im Ordner von Spatial (<Installed>\Pitney Bowes\Spectrum\server\modules\spatial\java.vmargs) ändern. Weitere Anweisungen finden Sie unter **Vergrößern des Heapspeichers**.

5 - Leistungsoptimierung

Dieser Abschnitt beschreibt Ansätze zur Verbesserung der Leistung durch Verwalten von Speicher und Threads. Darüber hinaus finden Sie Best Practices zur Optimierung der Leistung des Location Intelligence-Moduls. Zielgruppe sind erfahrene Administratoren.

Spectrum bietet diverse Optimierungsoptionen, um die Leistung des Servers zu steigern. Die optimale Auswahl der Einstellungen hängt von der Natur der Bereitstellung ab. Zum Erstellen einer gut optimierten Serverumgebung empfiehlt es sich, in der bereitgestellten Umgebung Leistungstests durchzuführen, um die optimalen Einstellungen zu ermitteln. Dieser Abschnitt enthält einige allgemeine Richtlinien zur Leistungsoptimierung.

In this section

Konfiguration von Remote-Komponenten

Alle Geodatendienste in der Spectrum™ Technology Platform werden in einer Remote-Komponente (JVM-Instanz) bereitgestellt, die separat von der Plattformlaufzeit ist. Dadurch wird sichergestellt, dass die Plattform unabhängig von den darin enthaltenen Modulen ist und dass die JVM-Konfiguration auf die Geodatendienste angewendet werden kann. Dies ermöglicht eine Flexibilität der Speicherzuordnung und eine Leistungsoptimierung basierend auf den Merkmalen dieser Dienste.

Die Remote-Komponente stellt Geodatenfunktionen für Geodatendienste (z. B. den Feature Service und den Mapping Service) und Schritte (z. B. Spatial Calculator und Query Spatial Data) bereit. Die Poolgröße einer Remote-Komponente umfasst die Anzahl der Anforderungen, die die Komponente gleichzeitig verarbeiten kann. Dies hat Auswirkungen auf den Durchsatz von Geodatendiensten und Geodatenschritten.

Um Berechtigungen für die Remote-Komponente für Geodaten zu verwalten, verwenden Sie die Management Console, wie Sie dies bei einem beliebigen anderen gesicherten Entitätstypen machen würden. Die Remote-Komponente für Geodaten wird unter der Gruppe **Datenbankressourcen** als gesicherter Entitätstyp vom Typ „Geodaten-Komponente“ aufgeführt. Sie können beim Erstellen oder Bearbeiten von Rollen oder über die Zugriffssteuerungseinstellungen Berechtigungen für die Remote-Komponente für Geodaten festlegen. Weitere Informationen finden Sie unter **Verwalten von Sicherheit** auf Seite 17.

Ändern der Poolgröße

Zusätzlich zur JVM-Optimierung können Sie die Poolgröße der Remote-Komponente für Geodaten anpassen. Die Poolgröße einer Remote-Komponente umfasst die Anzahl der Anforderungen, die die Komponente gleichzeitig verarbeiten kann. Diese Einstellung stellt die Anzahl der Threads auf den Komponenten dar, die Dienstanforderungen über die Spectrum™ Technology Platform abhören oder einen Schritt des Location Intelligence-Moduls ausführen (d. h. die maximale Anzahl verwalteter Verbindungen).

Jede Webdienstanforderung erreicht Spectrum über die Plattform und wird an die Komponente weitergegeben. Der Standardwert von 1 kann erhöht werden, um größeren Anforderungsmengen zu entsprechen. Es wird empfohlen, eine Poolgröße zu verwenden, die der Anzahl an CPU entspricht. Die maximale Einstellung sollte dem Doppelten der Anzahl der CPU-Kerne entsprechen. Auf einem Rechner mit 4 CPU sollte beispielsweise die Anzahl an Threads für alle Dienste insgesamt 8 nicht übersteigen. Es sollten Leistungstests mit unterschiedlichen Einstellungen ausgeführt werden, bis die optimale Leistung zur Verwendung erreicht wird.

Die haben die Möglichkeit, die Poolgröße für die Remote-Komponente für Geodaten in der Management Console anzupassen:

1. Öffnen Sie die Management Console.

2. Navigieren Sie zu **Ressourcen** > **Location Intelligence**.
3. Ändern Sie die Poolgröße für die Remote-Komponente mit den Pfeilen oder durch Eingabe eines Wertes. Der minimale Wert beträgt 1 und der maximale Wert 64.
4. Klicken Sie auf **Speichern**.
5. Starten Sie den Server neu, wenn Sie die Poolgröße verringert haben. Eine Erhöhung der Poolgröße wird sofort wirksam und macht keinen Neustart des Servers erforderlich.

Konfiguration von Datenquellen-Pooling

Sie können die Datei `pooling-datasource-factory.properties` unter `\server\modules\spatial` verwenden, um das Pooling von Verbindungen, die von JDBC-basierten Datenquellen (wie Oracle und SQL Server) verwendet werden, zu konfigurieren und die Leistung zu optimieren.

In den meisten Fällen empfehlen wir, die Klasse „Validator“ zu aktivieren. Dadurch können Objekte überprüft werden, bevor sie vom Pool ausgeliehen werden. Wenn die Überprüfung fehlschlägt, wird die Verbindung zum Pool getrennt und ein Ausleihen von einem anderen Pool versucht. Für Sonderfälle, wenn beispielsweise ein benutzerdefinierter Datenanbieter verwendet wird, ist eine Überprüfungsabfrage verfügbar. Wenn sowohl die Überprüfungsabfrage als auch die Klasse „Validator“ aktiviert sind, wird die Klasse „Validator“ verwendet.

Das Aktivieren der Überprüfung kann leichte negative Auswirkungen auf die Leistung nach sich ziehen. Allerdings erhält die Testabfrage die Integrität aller Verbindungen im Verbindungspool aufrecht, wohingegen die Kommunikation zwischen Spectrum Spatial und einer externen Datenbank nicht zuverlässig ist. Legen Sie ein Überprüfungsintervall fest, um die Auswirkungen der Überprüfung auf die Leistung zu mindern. Wenn die Überprüfung einer Verbindung ansteht, diese aber bereits zuvor in diesem Intervall überprüft wurde, wird die Überprüfung nicht durchgeführt.

Verbessern der Leistung für entfernungsbasierte Vorgänge

Eine PGD-Indexdatei ist eine ergänzende Datei zum TAB-Dateiset, die die Leistung für Native, Native Extended (NativeX) und Seamless TAB-Dateien steigern kann, sodass sie mit der von GSB-Dateien vergleichbar ist. Der PGD-Generator, ein Dienstprogramm der Eingabeaufforderung, ist verfügbar, um diese spezialisierten Indexdateien zu erstellen und die Leistung von bestimmten Entfernungsvorgängen für systemeigene Datasets, die Linien und Polygone enthalten, zu verbessern. Eine über den PGD-Generator erstellte Indexdatei ist nützlich, wenn die von Ihnen durchsuchten Daten auf Linien und Regionen basieren und Sie Folgendes verwenden:

- den „Point In Polygon“-Schritt, wenn Sie Entfernungen einschließen,

- den „Find Nearest“-Schritt, wenn die Eingabe ein Punkt ist (mit oder ohne Entfernungsberechnung),
- „SearchNearest“-Vorgänge im Feature-Dienst mit einem Eingabepunkt und einer Suchtabelle für Linien oder Polygone.

Der PGD-Generator kann im Bereich „Spectrum Spatial“ der Begrüßungsseite unter **PGD-Generator** auf der Registerkarte „Dienstprogramme“ heruntergeladen werden. Auf der Begrüßungsseite befindet sich zudem neben dem Download-Link für das Dienstprogramm ein Link zur Dokumentation von PGD-Generator.

> **Anmerkung:** Eine PGD-Datei ist fünf- bis sechsmal größer als die MAP-Datei für die TAB-Datei. Pro TAB-Datei wird eine PGD-Datei generiert, es sei denn, es handelt sich um eine Seamless TAB-Datei, bei der für jedes Unter-TAB eine PGD-Datei erstellt wird.
>
> Darüber hinaus wird eine PGD-Datei nicht mehr vom System verwendet, wenn sich die Daten in der TAB-Datei ändern (beispielsweise wenn Zeilen hinzugefügt oder gelöscht oder eine Geometrie im MAP-Teil der TAB-Datei geändert wurde). Wenn Warnungen aktiviert wurden (siehe **ProtoProtokollieren von Spatial** auf Seite 70), erscheint im `wrapper.log` oder falls zutreffend in der Protokolldatei, die für Spatial-Protokollierung konfiguriert wurde, eine Meldung zur veralteten PGD-Datei. Sie müssen die PGD-Datei erneut für die aktualisierte TAB-Datei generieren.

6 - Verwalten eines Clusters

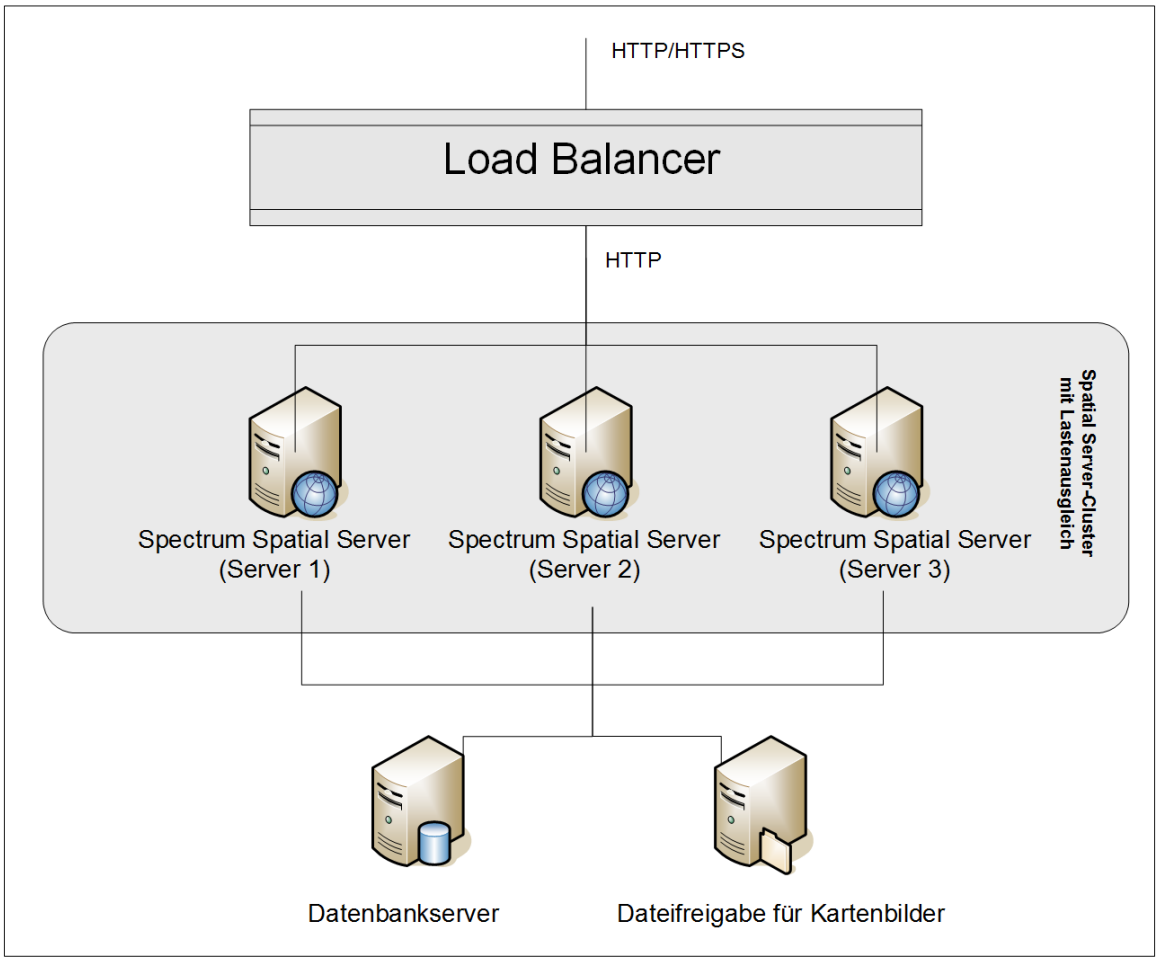
In this section

Clusterarchitektur für das Location Intelligence-Modul

In einer Cluster-Umgebung wird die Verarbeitung von mindestens zwei Serverinstanzen gemeinsam genutzt. In der folgenden Abbildung wird die Bereitstellungsarchitektur einer solchen Konfiguration dargestellt. Mithilfe eines Lastenausgleichs kann eine hohe Verfügbarkeit und Skalierung unterstützt werden. Die Bereitstellungsarchitektur umfasst einen Lastenausgleich, ein Spectrum Spatial-Cluster, eine Datenbank und eine Dateifreigabe. Mit diesem Ansatz können Sie eine horizontale und vertikale Skalierung durchführen. Sie können einen Cluster-Vorgang mit oder ohne Plattform-Clustering auf dem Location Intelligence-Modul ausführen.

Anmerkung: Die Einrichtung eines Spectrum™ Technology Platform-Clusters und eines Clusters für das Location Intelligence-Modul wird empfohlen und bietet mehrere Vorteile:

- Die Sicherheitssynchronisierung (ACL) erfolgt für benannte Ressourcen automatisch.
- Auf einem Knoten erstellte Datenflüsse, Benutzer und Rollen werden automatisch auf allen Knoten synchronisiert.
- Alle Demoseiten und Dienstprogramme (z. B. Spatial Manager) des Location Intelligence-Moduls können und sollten auf den Lastenausgleich verweisen.



Load Balancer

Der Lastenausgleich verteilt Anforderungen zwischen den Spectrum Spatial-Instanzen. Sie können einen beliebigen Lastenausgleich verwenden, der den Lastenausgleich von HTTP/HTTPS-Anforderungen unterstützt.

Spectrum Spatial-Cluster

Das Cluster ist eine Sammlung von Spectrum-Instanzen mit LIM-Freigabeverwaltung, benannten Ressourcen, geografischen Metadateninhalten und Konfigurationseinstellungen. Sie können zusätzliche Knoten zum Cluster hinzufügen, um die Zuverlässigkeit zu steigern und Unterstützung für größere Lasten zu gewährleisten. Darüber hinaus können Sie jeden Knoten vertikal über zusätzliche Hardwareressourcen und/oder zusätzliche Instanzen skalieren, wenn dies bei Hardware mit großen Ressourcenmengen erforderlich ist. Sie können Spectrum entsprechend konfigurieren, damit CPU in eingeschränkter Anzahl verwendet werden.

Datenbank

Spectrum speichert benannte Ressourcen (Karten, Layer, Tabellen und Stile), geografische Metadaten und Konfigurationen in einer Datenbank. In der standardmäßigen Installation eines

einzelnen Servers wird eine integrierte Datenbank verwendet, um diese Ressourcen auf dem lokalen Server zu speichern. Um eine robuste, skalierbare Lösung zu erstellen, sollten Sie diese eingebettete Datenbank durch eine stabile, unabhängige Datenbank ersetzen. Unterstützt werden die Datenbanken Oracle, PostGreSQL/PostGIS und Microsoft SQL-Server.

Bei der Lastenausgleichskonfiguration diese Ressourcen in einem lokalen Cache und Suchindex in jedem Knoten im Cluster von Spectrum-Knoten zwischengespeichert. Wenn ein Spectrum-Knoten eine Anforderung empfängt, sucht er Ressourcen anhand des lokalen Cache und Index. Sie können benannte Ressourcen über einen beliebigen Knoten im Cluster hinzufügen. Jeder Knoten stellt die Aktualität seines Cache sicher, indem er ihn auf Unterschiede zwischen seinem lokalen Cache und der Zentraldatenbank prüft. Standardmäßig erfolgt diese Überprüfung alle 2 Sekunden. Sie können die Zeitintervalle auch konfigurieren. Über diese Architektur wird sichergestellt, dass der Server Hochleistungstransaktionen liefert und die Last auf die Datenbank so gering wie möglich ausfällt. Wenn ein neuer Spectrum-Knoten zum Cluster hinzugefügt wird, werden der Cache und Index automatisch erstellt. Ein solches Szenario kann dazu dienen, einen Knotenfehler zu beheben oder die Leistungsfähigkeit der Bereitstellung zu steigern.

Dateifreigabe

Die Dateifreigabe stellt einen Ordner zur Verfügung, der von Spectrum generierte Kartenbilder enthält. Wenn Karten anhand der Webservices gerendert werden, unterstützt der Server Kartenbilder, die über URLs oder als Base-64-codiertes Bild zurückgegeben werden. Wenn eine URL zurückgegeben wird, wird das Kartenbild als Datei gespeichert und über eine Anforderung der URL bereitgestellt. Die Bilder werden über eine Dateifreigabe gespeichert, um sicherzustellen, dass jeder Spectrum-Knoten das Kartenbild zurückgeben kann.

Verwenden von Enterprise Designer mit einem Cluster

1. Starten Sie Enterprise Designer.
2. Geben Sie den Servernamen des Lastenausgleichs in das Feld **Servername** ein.
3. Geben Sie den Port, auf dem der Lastenausgleich gemäß Ihrer Konfiguration lauschen soll, im Feld **Port** ein.

   Anmerkung: Eingabedateien, Ausgabedateien und Datenbankressourcen müssen sich auf einem freigegebenen Laufwerk, einem Dateiserver oder einem allgemein zugänglichen Speicherort befinden. Andernfalls müssen alle Dateien auf jeden Server geladen werden, der einen Spectrum™ Technology Platform-Server hostet, und müssen sich auf demselben Pfad befinden.

Nach der Anmeldung können Sie Enterprise Designer wie gewohnt verwenden. Die durchgeführten Aktionen werden auf alle Instanzen von Spectrum™ Technology Platform im Cluster angewendet, auf dem Sie angemeldet sind.

Starten eines Clusters

Wenn alle Knoten in einem Cluster angehalten wurden, müssen Sie wie folgt vorgehen, um das Cluster sicher zu starten und den Verlust von Daten zu vermeiden.

1. Entfernen Sie die Seed-Knoten auf dem zuletzt beendeten Knoten, und starten Sie den Server.

   Warnung: Der zuletzt angehaltene Knoten muss zuerst gestartet werden und ein Seed-Knoten sein. Wenn Sie einen anderen Knoten zuerst starten, gehen Daten wie der Auftragsverlauf oder Konfigurationseinstellungen eventuell verloren. Wenn Sie nicht wissen, welcher Knoten zuletzt beendet wurde, überprüfen Sie im Wrapper-Protokoll eines jeden Knotens die Zeitmarke der Beendigungsmeldung. Sie finden das Wrapper-Protokoll unter: `*Spectrum Location*\server\app\repository\logs\wrapper.log`.

   a) Öffnen Sie die folgende Datei in einem Texteditor:

      `server/app/conf/spectrum-container.properties`

   b) Entfernen Sie in der Eigenschaft `spectrum.cluster.seeds` alle Hostnamen und IP-Adressen, mit Ausnahme der für diesen Server. Speichern Sie die Hostnamen und IP-Adressen, damit Sie sie zu einem späteren Zeitpunkt wieder hinzufügen können.
   c) Speichern Sie die Datei.
   d) Starten Sie den Server.
   e) Warten Sie, bis der Spectrum™ Technology Platform-Server *vollständig* gestartet wurde.

      Die Information, ob der Spectrum™ Technology Platform-Server vollständig gestartet wurde, erhalten Sie im Wrapper-Protokoll: `*Spectrum Location*\server\app\repository\logs\wrapper.log`. Die folgende Nachricht wird angezeigt, wenn der Server vollständig gestartet wurde:

      ```
      Pitney Bowes Spectrum(TM) Technology Platform (Version Version Number) Started.
      ```

   f) Fügen Sie in der Eigenschaftendatei `spectrum-container.properties` in der Eigenschaft `spectrum.cluster.seeds` die Hostnamen oder IP-Adressen hinzu, die Sie entfernt haben, und trennen Sie diese durch ein Komma voneinander.
   g) Speichern Sie die Datei und schließen Sie sie. Sie müssen den Server nicht neu starten.

2. Starten Sie die anderen Knoten im Cluster.

   Warnung: Warten Sie, bis der erste Knoten *vollständig* gestartet wurde, bevor Sie zusätzliche Knoten starten. Wenn Sie zusätzliche Knoten starten, bevor der erste gestartet wurde, gehen Daten eventuell verloren.

Beenden eines Clusters

So beenden Sie ein gesamtes Cluster:

1. Identifizieren Sie, bei welchen Knoten es sich um Seed-Knoten handelt. Öffnen Sie hierfür die Datei *SpectrumFolder*`/server/app/conf/spectrum-container.properties` und überprüfen Sie die Knoten, die in der Eigenschaft `spectrum.cluser.seeds` aufgeführt sind.
2. Fahren Sie jeden Spectrum™ Technology Platform-Server im Cluster herunter. Stellen Sie dabei sicher, dass der letzte beendete Knoten ein Seed-Knoten ist. Ändern Sie das Arbeitsverzeichnis in das Verzeichnis `bin` des Spectrum™ Technology Platform-Servers, führen Sie die Datei „setup“ aus und geben Sie anschließend den folgenden Befehl ein: `./server.stop`.

   Warnung: Bei dem letzten von Ihnen beendeten Knoten muss es sich um einen Seed-Knoten handeln, damit ein Datenverlust vermieden werden kann.

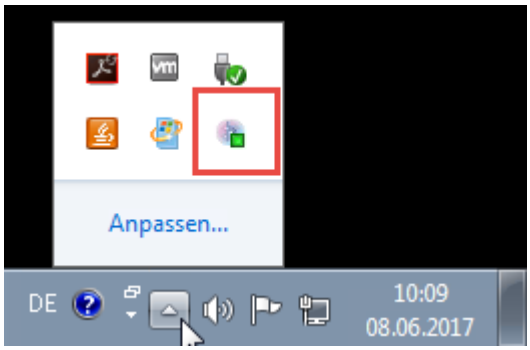
3. Notieren Sie sich, welchen Knoten Sie zuletzt beendet haben. Sie benötigen diese Informationen beim Hochfahren des Clusters. Klicken Sie mit der rechten Maustaste auf das Spectrum™ Technology Platform-Symbol in der Windows-Taskleiste, und wählen Sie **Spectrum ™stoppen** aus.

   Warnung: Bei dem ersten von Ihnen gestarteten Knoten muss es sich um den Knoten handeln, der zuletzt beendet wurde. Zudem muss dieser Knoten ein Seed-Knoten sein. Auf diese Weise kann ein Datenverlust verhindert werden.

Entfernen eines Knotens aus einem Cluster

Halten Sie den Spectrum™ Technology Platform-Server an, um einen Knoten aus einem Cluster zu entfernen.

1. Klicken Sie zum Beenden des Servers mit der rechten Maustaste auf das Spectrum™ Technology Platform-Symbol in der Windows-Taskleiste (nachfolgend dargestellt) und wählen Sie **Beenden Spectrum™** aus.



2. Beenden Sie den Knoten, den Sie entfernen möchten:

   Ändern Sie das Arbeitsverzeichnis in das Verzeichnis `bin` des Spectrum™ Technology Platform-Servers, „sourcen“ Sie die Datei setup (. ./setup) und geben Sie dann den folgenden Befehl ein: `./server.stop`.

   Klicken Sie unter Windows mit der rechten Maustaste auf das Symbol Spectrum™ Technology Platform auf der Taskleiste, und wählen Sie **Spectrum™ stoppen** aus.

3. Öffnen Sie die Datei `server/app/conf/spectrum-container.properties` in einem Texteditor und legen Sie `spectrum.cluster.enabled` auf `false` fest.
4. Öffnen Sie auf den einzelnen anderen Knoten im Cluster die Datei `spectrum-container.properties` und entfernen Sie den Knoten aus der Eigenschaft `spectrum.cluster.seeds`.

Für Benutzer des Location Intelligence-Moduls: Wenn der Knoten eigenständig bleiben und außerhalb des Clusters ausgeführt werden soll, kopieren Sie die ursprüngliche Datei `repository.xml` zurück und entfernen Sie für jede Instanz von Spectrum™ Technology Platform die folgenden Ordner aus dem Verzeichnis `/server/modules/spatial/jackrabbit`: Repository, Version, Arbeitsbereiche. Starten Sie den Server neu, und importieren Sie den Inhalt der Datenbank.

Cluster für das Location Intelligence-Modul verwalten

Einrichten einer allgemeinen Repository-Datenbank

Konfigurieren Sie das Location Intelligence-Modul, damit eine freigegebene Repository-Datenbank für das Cluster verwendet wird. Dadurch stellen Sie sicher, dass benannte Ressourcen, geografische Metadaten und Konfigurationseinstellungen im gesamten Cluster verwaltet werden.

Das Repository wird mit einer Reihe benannter Ressourcen, geografischen Metadaten und Konfigurationsdateien installiert. Für die Migration dieser Ressourcen in die freigegebene Repository-Datenbank müssen die Ressourcen aus der standardmäßigen internen

Repository-Datenbank exportiert und erneut in die neue freigegebene Repository-Datenbank importiert werden.

Verwenden Sie für`limrepo import` den Massenexport und -import von Repository-Inhalten die Befehle `limrepo export` und in der Administrationsumgebung. Anhand dieser Befehle können Sie Berechtigungen beibehalten (Anweisungen erhalten Sie im Abschnitt „Verwaltung“ im *Spectrum Spatial-Handbuch*).

In diesen Schritten wird beschrieben, wie Sie Ihr Repository auf einer allgemeinen Datenbank, entweder PostgreSQL, Oracle oder Microsoft SQL Server, einrichten:

1. Exportieren Sie alle Repository-Ressourcen in einen lokalen Ordner. Verwenden Sie dazu den Befehl `limrepo export` in der Administrationsumgebung (Anweisungen dazu finden Sie im Abschnitt „Administration“ im *Spectrum Spatial-Handbuch*).

   Die Inhalte des installierten Repositorys müssen exportiert werden. Sie müssen diesen Schritt nur einmal ausführen, da die Inhalte des Repositorys zu diesem Zeitpunkt für alle Instanzen von Spectrum™ Technology Platform dieselben sein sollten.

2. Halten Sie den Spectrum™ Technology Platform-Server auf allen Knoten an (Anweisungen dazu finden Sie unter **Beenden eines Clusters** auf Seite 87.)
3. Ändern Sie auf allen Knoten von Spectrum™ Technology Platform die Konfiguration, um die allgemeine Datenbank anzugeben.
   a) Kopieren Sie die Inhalte von `repository.<databaseType>.xml` nach `repository.xml` im Ordner `server/modules/spatial/jackrabbit`, wobei `<databaseType>` der entsprechende Typ Ihrer Datenbank ist (Postgres, Oracle oder MSSQL).
   b) In `repository.xml`:

      - Ändern Sie den Abschnitt „DataSource“ anhand des Hostnamens des Servers, des Ports, der Datenbank, des Benutzers und des Kennworts.
      - Ändern Sie den Abschnitt „Cluster“, um eine eindeutige Cluster-ID wie „Node1“ zuzuweisen. Vergewissern Sie sich, dass allen nachfolgenden Knoten im Cluster eindeutige IDs zugewiesen sind (z. B. Node2, Node3).
      - Speichern Sie die Änderungen in `repository.xml`.

   c) Entfernen Sie folgende Ordner aus dem Ordner `/server/modules/spatial/jackrabbit`: repository, version, workspaces.
4. Wenn Ihre Datenbank bereits Repository-Inhalte enthalten hat, müssen Sie die Tabellen entfernen, damit ein sauberes Repository erstellt werden kann.

   - default_binval
   - default_bundle
   - default_names
   - default_refs
   - rep_fsentry
   - rep_global_revision
   - rep_journal

- rep_local_revisions
- security_binval
- security_bundle
- security_names
- security_refs
- version_binval
- version_bundle
- version_names
- version_refs

Wenn Sie Oracle verwenden, löschen Sie außerdem `version_seq_names_id`, `security_seq_names_id` und `default_seq_names_id`.

5. Importieren Sie nur auf dem Seed-Knoten die gesicherten Repository-Inhalte.
   a) Starten Sie den Spectrum™ Technology Platform-Server (Anleitungen dazu finden Sie unter **Starten eines Clusters** auf Seite 86).
   b) Importieren Sie die Inhalte mithilfe des Befehls `limrepo import` mit dem Seed-Knoten als Ziel.
6. Starten Sie die restlichen Knoten im Cluster (Anleitungen dazu finden Sie unter **Starten eines Clusters** auf Seite 86).

Konfigurieren Ihres Systems

Sobald Sie Spectrum™ Technology Platform installiert und eine freigegebene Datenbank konfiguriert haben, müssen Sie Ihre Instanz konfigurieren, bevor Sie sie auf einem anderen virtuellen Computer replizieren können. Wenn Sie keine virtuelle Computerumgebung verwenden, müssen Sie diese Schritte bei jeder der Spectrum™ Technology Platform-Installationen durchführen.

Konfigurieren der Dateifreigabe von Karten

Sie benötigen zunächst ein freigegebenes Verzeichnis für Kartenbilder, um die Dateifreigabe für Karten (ein freigegebener Bildordner) für Spectrum™ Technology Platform zu konfigurieren.

> **Anmerkung:** Informationen zum Konfigurieren einer Dateifreigabe von Karten unter Unix/Linux finden Sie unter **Erstellen einer Dateifreigabe für Kartenbilder unter Unix/Linux** auf Seite 91.

> **Anmerkung:** Informationen zum Konfigurieren einer Dateifreigabe von Karten unter Windows finden Sie unter **Erstellen einer Dateifreigabe für Kartenbilder unter Windows** auf Seite 92.

Konfigurieren Sie die Dateifreigabe von Karten, nachdem Sie ein Verzeichnis für Kartenbilder erstellt haben:

1. Ändern Sie die Konfiguration des Mapping-Dienstes, indem Sie auf einen freigegebenen Bildordner und einen Server mit Lastenausgleich zeigen. Ändern Sie im ImageCache den Parameter „Directory“ in ein freigegebenes Bildverzeichnis, und ändern Sie den Parameter `AccessBaseURL` in die Bild-URL des Rechners mit Lastenausgleich.

   Wenn Sie eine virtuelle Rechnerumgebung verwenden, sollten Sie sich diese IP-Adresse merken, da Sie den virtuellen Rechner des Lastenausgleichs in diese IP-Adresse ändern müssen.

   Bei Unix/Linux-Installationen:

```
<ImageCache>
<Directory>/<spatial server
root>/server/modules/spatial/images</Directory>
<AccessBaseURL>http://<loadbalance_IP_address>/rest/Spatial/
MappingService/internal/imageCache</AccessBaseURL>
 <FileExpire>30</FileExpire>
 <ScanInterval>30</ScanInterval>
</ImageCache>
```

   Bei Windows-Installationen:

```
<ImageCache>
<Directory>\\server\Share\images</Directory>
<AccessBaseURL>http://<loadbalance_IP_address>/rest/Spatial/MappingService/
internal/imageCache
</AccessBaseURL>
 <FileExpire>30</FileExpire>
 <ScanInterval>30</ScanInterval>
</ImageCache>
```

2. Bei Unix/Linux-Installationen müssen Sie eine symbolische Verknüpfung einrichten, damit Kartenbilder in das freigegebene Dateisystem übertragen werden können.

   Erstellen Sie einen Unterordner `images` im bereitgestellten Freigabeordner, z. B. `/mnt/<linux mount>/images`.

```
cd /<spatial server root>/server/modules/spatial
rm -Rf images
ln -s /mnt/<linux mount>/images ./images
```

Erstellen einer Dateifreigabe für Kartenbilder unter Unix/Linux

Die Dateifreigabe stellt einen Order zur Verfügung, der von Spectrum Spatial generierte Kartenbilder enthält. Erstellen Sie einen freigegebenen Ordner, der von allen Spectrum-Knoten aus erreichbar ist. Die Dateifreigabe ist nicht erforderlich, wenn Karten vom Webservice als Base64-codierte Bilder zurückgegeben werden.

So erstellen Sie eine Dateifreigabe für Kartenbilder unter Unix/Linux:

1. Binden Sie auf jedem Betriebssystem, das Spectrum hostet, einen freigegebenen Ordner ein. Mit den folgenden Befehlen binden Sie ein Laufwerk auf einem Microsoft Windows Server oder ein Netzlaufwerk mit CIFS-Unterstützung ein.

```
mkdir /mnt/<linux mount>
mount -t cifs //<windows host>/<windows share> /mnt/<linux mount>-o
username=shareuser,password=sharepassword,domain=pbi
```

2. Legen Sie in `/etc/fstab` fest, dass die Freigabe für Bilder beim Start geladen wird.

```
//<windows ip address for share>/share /path_to/mount cifs
username=server_user,password=secret,_netdev 0 0
```

Erstellen einer Dateifreigabe für Kartenbilder unter Windows

Die Dateifreigabe stellt einen Order zur Verfügung, der von Spectrum Spatial generierte Kartenbilder enthält. Erstellen Sie einen freigegebenen Ordner, der von allen Spectrum-Knoten aus erreichbar ist. Die Dateifreigabe ist nicht erforderlich, wenn Karten vom Webservice als Base64-codierte Bilder zurückgegeben werden.

So erstellen Sie eine Dateifreigabe für Kartenbilder unter Windows:

1. Wählen Sie im Windows Explorer den Bildordner aus, den Sie freigeben möchten.
2. Klicken Sie mit der rechten Maustaste auf den Ordner und anschließend auf **Freigabe** oder **Freigeben für**.
3. Wählen Sie die Benutzer aus, die den Bildordner verwenden. Diese Benutzer müssen über Lese-/Schreibberechtigungen verfügen.

Ändern von OGC-Dienstkonfigurationen für das Clustering

Um die Funktionsweise von Clustering sicherzustellen, wenn Ihnen sowohl ein Spectrum™ Technology Platform-Cluster als auch ein Cluster für das Location Intelligence-Modul vorliegt, müssen Sie die OGC-Dienstkonfigurationsdateien (Open Geospatial Consortium) anhand von Spatial Manager ändern: Ändern Sie die URL der Online-Ressource (Service) in die IP-Adresse und den Port des Lastenausgleichs über die Einstellungsseiten des WFS, WMS und WMTS. Weitere Informationen finden Sie im *Spatial Manager-Handbuch* im Abschnitt „Dienstprogramme“ des *Spectrum Spatial-Handbuchs*.

Ändern der Java-Eigenschaftsdateien auf allen Knoten

Sie müssen die Java-Eigenschaftsdatei auf allen Knoten im Cluster ändern. So ändern Sie die Java-Eigenschaften für Spectrum™ Technology Platform:

1. Ändern Sie die Datei „java.properties“ in `<spectrum>/server/modules/spatial/java.properties`, sodass „repository.host“ auf „localhost“ verweist.

2. Ändern Sie „images.webapp.url“ sowie alle Hosts und Portnummern des Dienstes, sodass diese auf den Lastenausgleichserver verweisen.

Konfigurieren von Ports für mehrere Spectrum-Instanzen

Wenn Sie mehrere Instanzen von Spectrum™ Technology Platform auf einem einzelnen Rechner haben, müssen Sie die Portnummern für jede Instanz ändern. Ändern Sie alle Ports unter `<Spectrum root>/server/app/conf/spectrum-container.properties` in neue Portwerte, die nicht verwendet werden. Der HTTP-Port spiegelt die in das Installationsprogramm eingegebene Portnummer wider.

FreigegeFreigegebene lokale Daten von Spectrum

Wenn Sie im Dateisystem TAB-Dateidaten verwenden, müssen diese Daten sich an einem freigegebenen Speicherort befinden, auf den alle Instanzen von Spectrum in der Lastenausgleichumgebung zugreifen können. Außerdem ist es wichtig, zu beachten, dass alle benannten Ressourcen in der Datenbank, die auf Daten im Dateisystem zugreifen, auf diesen freigegebenen Speicherort verweisen.

Jede VM oder jeder Computer, die oder der Spectrum hostet, benötigt Zugriff auf das eingebundene Freigabelaufwerk.

> **Anmerkung:** Bei Verwendung von benannten Ressourcen, die auf Datenbanktabellen verweisen, ist kein Freigabelaufwerk erforderlich, da benannte Ressourcen in der Datenbank nicht über einen Dateipfad auf die Daten zugreifen. Sie verwenden stattdessen eine benannte Verbindung zu den Daten in der Datenbank.

7 - Verwenden der Administrationsumgebung

In this section

Erste Schritte in der Administrationsumgebung

Die Administrationsumgebung bietet über die Befehlszeile Zugriff auf administrative Funktionen. Sie können diese in einem Skript verwenden und so bestimmte administrative Aufgaben automatisieren. Sie können sie auch interaktiv verwenden. In der Administrationsumgebung stehen nicht alle administrativen Features zur Verfügung. Verwenden Sie Management Console, um auf die Features zuzugreifen, die nicht in der Administrationsumgebung verfügbar sind.

> **Anmerkung:** Für die Administrationsumgebung ist Java 8 oder höher erforderlich. Stellen Sie vor dem Ausführen der Administrationsumgebung sicher, dass Sie eine unterstützte Version von Java im Systempfad referenzieren.

1. Öffnen Sie einen Webbrowser und navigieren Sie zur Spectrum™ Technology Platform-Begrüßungsseite unter:

   http://<servername>:<port>

   Wenn Sie beispielsweise Spectrum™ Technology Platform auf einem Computer mit dem Namen „myspectrumplatform“ installiert haben und dieser den HTTP-Standardport 8080 verwendet, navigieren Sie zu:

   http://myspectrumplatform:8080

2. Klicken Sie auf **Platform-Clienttools**.
3. Klicken Sie auf **Befehlszeilen-Clients**.
4. Klicken Sie unter **Administrationsumgebung** auf **Herunterladen** und laden Sie die ZIP-Datei auf den Computer herunter, auf dem Sie die Administrationsumgebung verwenden möchten.
5. Extrahieren Sie den Inhalt der ZIP-Datei.
6. Starten Sie die Befehlszeilenschnittstelle über eine der folgenden Optionen:
   - Wenn der Server auf einem Unix- oder Linux-System läuft, führen Sie `cli.sh` aus.
   - Wenn der Server auf einem Windows-System läuft, führen Sie `cli.cmd` aus.

     > **Anmerkung:** Passen Sie bei Bedarf in der `.sh`- oder `.cmd`-Datei den Pfad zu Ihrer Java-Installation an.

7. Stellen Sie eine Verbindung zum Spectrum™ Technology Platform-Server her, indem Sie folgenden Befehl eingeben:

   `connect` --h *servername*:*port* --u *username* --p *password* --s *SSLTrueOrFalse*

   Beispiel:

   `connect` --h myserver:8080 --u admin --p myPassword1--s true

8. Sobald die Verbindung hergestellt ist, können Sie Befehle ausführen. Einige Tipps:

- Sie erhalten eine Liste der verfügbaren Befehle, indem Sie `help` eingeben oder die Tabulatortaste drücken.
- Wenn Sie die ersten Buchstaben eines Befehls eingeben und dann die Tabulatortaste drücken, wird der Befehl automatisch vervollständigt. Wenn Sie beispielsweise `us` eingeben und dann die Tabulatortaste drücken, wird Ihre Eingabe automatisch zum Befehl `user` vervollständigt. Wenn Sie die Tabulatortaste erneut drücken, wird eine Liste aller Befehle zu `user` angezeigt.
- Wenn Sie einen Optionswert angeben, der ein Leerzeichen enthält, schließen Sie den Wert in doppelten Anführungszeichen ein.

9. Wenn Sie fertig sind, geben Sie `exit` ein, um die Administrationsumgebung zu verlassen.

Verwenden eines Skripts in der Administrationsumgebung

In der Administrationsumgebung können mehrere Befehle über eine Skriptdatei ausgeführt werden. Das ist nützlich, wenn Sie administrative Aktionen automatisieren oder standardisieren möchten. Verwenden Sie in dem Fall ein Skript, anstatt die Befehle in der Administrationsumgebung oder über Management Console manuell auszuführen.

1. Verwenden Sie einen Texteditor, um eine Skriptdatei zu erstellen. Eine Skriptdatei enthält die Befehle, die Sie ausführen möchten.

   Um einen Befehl zu einer Skriptdatei hinzuzufügen, geben Sie den Befehl und die erforderlichen Parameter ein, als würden Sie den Befehl in der Eingabeaufforderung eingeben. Geben Sie einen Befehl pro Zeile ein.

   Verwendet Sie folgende Syntax, um in einer Skriptdatei Kommentare einzufügen:

`/*`	Dies zeigt den Start eines Kommentarblocks an.
`*/`	Dies zeigt das Ende eines Kommentarblocks an.
`//`	Dies zeigt einen Inline-Kommentar an. Verwenden Sie dies nur am Anfang einer Zeile.
`;`	Dies zeigt einen Inline-Kommentar an. Verwenden Sie dies nur am Anfang einer Zeile.

2. Speichern Sie das Skript entweder auf dem Computer, auf dem die Administrationsumgebung läuft, oder an einem Speicherort, auf den vom Computer, auf dem die Administrationsumgebung läuft, zugegriffen werden kann. Sie können einen beliebigen Dateinamen und eine beliebige Dateierweiterung verwenden. Die empfohlene Dateierweiterung lautet `.cli`.
3. Zum Ausführen des Skripts stehen Ihnen folgende Optionen zur Verfügung:

Option	Bezeichnung
Skript in der Befehlszeile ausführen	Geben Sie Folgendes in der Befehlszeile oder in einem Batch- oder Shell-Skript ein: `cli.cmd --cmdfile ScriptFile`
Skript in der Administrationsumgebung ausführen	Öffnen Sie die Administrationsumgebung und stellen Sie über den Befehl `connect` eine Verbindung zum Spectrum™ Technology Platform-Server her. Verwenden Sie dann den Befehl `script`, um das Skript auszuführen. Weitere Informationen zu diesem Befehl finden Sie unter **script**.

Beispiel: Datenflüsse vom Staging zur Produktion verschieben

In diesem Beispiel geht es um die drei Datenflüsse „Deduplication“, „AddressValidation“ und „DrivingDirections“. Auf dem Staging-Server werden Änderungen an diesen Datenflüssen vorgenommen und getestet. Die Datenflüsse werden dann in einer Produktionsumgebung zur Ausführung verfügbar gemacht. Um über eine konsistente und automatisierte Möglichkeit zu verfügen, diese Datenflüsse vom Staging-Server zum Produktionsserver zu verschieben, kann ein Skript in der Administrationsumgebung verwendet werden. Das Skript könnte wie folgt aussehen:

```
// Connect to the staging server
connect --h stagingserver:8080 --u allan12 --p something123

// Export from staging
dataflow export --d "Deduplication" --e true --o exported
dataflow export --d "AddressValidation" --e true --o exported
dataflow export --d "DrivingDirections" --e true --o exported

// Close connection to the staging server
close

// Connect to the production server
connect --h productionserver:8080 --u allan12 --p something123

// Import to production
dataflow import --f exported\Deduplication.df
dataflow import --f exported\AddressValidation.df
dataflow import --f exported\DrivingDirections.df

// Close the connection to the production server
close
```

Location Intelligence-Modul

limrepo export

> **Anmerkung:** Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `limrepo export` exportiert benannte Ressourcen (wie z. B. benannte Tabellen) aus dem Spectrum Spatial Repository in ein lokales Dateisystem. Zur Verwendung dieses Befehls muss das Location Intelligence-Modul installiert sein.

Die Ressourcen werden mit vollständigem Datenbankpfad in den Zielordner exportiert. Wenn Sie beispielsweise `limrepo export` --s /Samples/NamedTables --o C:\export ausführen, erstellt das Tool `C:\export\Samples\NamedTables\WorldTable` usw. für jede benannte Tabelle im Ordner oder Verzeichnis „NamedTables“.

> **Anmerkung:** Der Befehl `limrepo export` exportiert immer alle Ordner einschließlich leerer Ordner rekursiv.

Verwendung

`limrepo export --s`*Quelldatenbankpfad* `--o`*Ausgabedateipfad*

> **Anmerkung:** Geben Sie zur Anzeige einer Parameterliste `help limrepo export` ein.

Erforderlich	Argument	Beschreibung
Ja	`--s` *SourceRepositoryPath*	Gibt den Pfad zur Ressource oder zu einem Ordner an, der exportiert werden soll.
Ja	`--o` *OutputFilePath*	Gibt den Pfad zu einem Ordner im lokalen Dateisystem als Exportziel an. Dies kann ein neuer Ordner oder ein vorhandener Ordner sein, ein vorhandener Ordner muss dann jedoch leer sein, da der Export andernfalls fehlschlägt.
Nein	`--q` or `--quiet`	Dies deaktiviert die Anzeige der während des Exportierens kopierten Ressourcen. Dies ist der stille Modus. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.

Erforderlich	Argument	Beschreibung
Nein	`--f` or `--fullpaths`	Dies gibt die vollständigen Pfade für Quelle und Ausgabe aus. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.
Nein	`--r` or `--recursive`	Dies exportiert Unterordner (untergeordnete Elemente der angegebenen Quelle) rekursiv. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „wahr“.
Nein	`--c` or `--continueonerror`	Export wird fortgesetzt, wenn ein Fehler auftritt. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.
Nein	`--a` or `--acl`	Behält vorhandene Berechtigungen für exportierte Ressourcen im Exportordner auf dem lokalen Dateisystem bei. In einer Zugriffssteuerungsliste (ACL) sind alle Operationen für alle Benutzer oder Rollen aufgeführt, die mit einer benannten Ressource ausgeführt werden können wie Erstellen, Anzeigen, Bearbeiten oder Löschen. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.

Beispiel

In diesem Beispiel werden die benannten Ressourcen im Ordner „\Samples“ der Datenbank in Ihr lokales Dateisystem in den Ordner „C:\myrepository\samples“ exportiert.

```
limrepo export --s /Samples --o C:\myrepository\samples
```

limrepo import

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `limrepo import` importiert benannte Ressourcen (wie z. B. benannte Tabellen) aus einem lokalen Dateisystem in das Spectrum Spatial Repository. Zur Verwendung dieses Befehls muss das Location Intelligence-Modul installiert sein.

Beim Importieren müssen Sie denselben Ordner oder dasselbe Verzeichnis angeben, in den Sie vorher exportiert haben. Wenn Sie beispielsweise `limrepo export` --s /Samples/NamedTables --o C:\export ausführen, erstellt das Tool `C:\export\Samples\NamedTables\WorldTable` usw. für jede benannte Tabelle im Ordner oder Verzeichnis „NamedTables“. Die Ressourcen werden mit vollständigem Datenbankpfad in den Zielordner exportiert. Wenn Sie dann `limrepo import` --s C:\export ausführen, wird „WorldTable“ zurück in `/Samples/NamedTables/WorldTable` importiert.

> **Anmerkung:** Der Befehl `limrepo import` importiert immer alle Ordner einschließlich leerer Ordner rekursiv.

Nach dem Importieren müssen Sie in vielen Fällen die benannten Verbindungen über Spatial Manager anpassen, sodass sie auf ihren neuen Pfad verweisen. Wenn beispielsweise Ihre nativen TAB-Dateien in „C:\myfiles“ in Ihrer Testinstanz installiert waren und dieselben Dateien in „E:\ApplicationData\Spectrum\Spatial\Spring2016“ installiert sind, müssen Sie diese Verbindung nach dem Importieren mithilfe von Spatial Manager korrigieren. Im Abschnitt „Dienstprogramme“ im *Spectrum Spatial-Handbuch* finden Sie Anweisungen, wie Sie Spatial Manager verwenden können, um eine benannte Verbindung zu bearbeiten.

> **Anmerkung:** Wenn Sie `limrepo import` verwenden, um Dienstkonfigurationsdateien wiederherzustellen, die Sie aus einer Version vor Version 12.0 von Spectrum™ Technology Platform exportiert haben, werden die Dateien automatisch geändert, um mit Version 12.0 und höher konform zu sein. (Beispielsweise werden die Datenbank-URLs entfernt.)

Verwendung

`limrepo import --s`*Quelldateipfad*

> **Anmerkung:** Geben Sie zur Anzeige einer Parameterliste `help limrepo import` ein.

Erforderlich	Argument	Beschreibung
Ja	`--s` *SourceFilePath*	Gibt den Pfad zur Ressource oder zu einem Ordner im lokalen Dateisystem als Importquelle an. Es muss sich dabei um ein Stammverzeichnis eines vorherigen Exports im lokalen Dateisystem handeln.
Nein	`--q` or `--quiet`	Dies deaktiviert die Anzeige der während des Importierens kopierten Ressourcen. Dies ist der stille Modus. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.

Erforderlich	Argument	Beschreibung
Nein	`--u` or `--update`	Gibt an, ob vorhandene Ressourcen überschrieben werden sollen, wenn Ressourcen mit demselben Namen bereits auf dem Server vorhanden sind. **true** Wenn auf dem Server eine Ressource vorhanden ist, deren Name mit dem der Ressource identisch ist, die Sie gerade importieren, wird die Ressource auf dem Server überschrieben. Dies ist die Standardeinstellung, wenn die Kennzeichnung nicht oder ohne einen Wert angegeben wurde. **false** Wenn auf dem Server eine Ressource mit einem Namen vorhanden ist, der mit dem der Ressource identisch ist, die Sie gerade importieren, wird die Ressource nicht importiert.
Nein	`--f` or `--fullpaths`	Dies gibt die vollständigen Pfade für Quelle und Ausgabe aus. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.
Nein	`--c` or `--continueonerror`	Import wird fortgesetzt, wenn ein Fehler auftritt. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“.
Nein	`--a` or `--acl`	Behält beim Importieren von Ressourcen alle zuvor exportierten Berechtigungen bei und führt sie mit vorhandenen Berechtigungen zusammen. In einer Zugriffssteuerungsliste (ACL) sind alle Operationen für alle Benutzer oder Rollen aufgeführt, die mit einer benannten Ressource ausgeführt werden können wie Erstellen, Anzeigen, Ändern oder Löschen. Ein Benutzer verfügt beim Exportieren beispielsweise über Lese- und Schreibberechtigungen für eine Ressource. Wenn der Benutzer beim Importieren nur über die Leseberechtigung für die Ressource verfügt, wird die Schreibberechtigung nach erfolgreichem Abschluss des Imports wieder gewährt.

Erforderlich	Argument	Beschreibung
		Miteinander in Konflikt stehende Berechtigungen können nicht zusammengeführt werden und werden ignoriert. ACL-Einträge für Benutzer und Rollen, die nicht in der Zieldatenbank vorhanden sind, werden auch ignoriert. Wenn diese Kennzeichnung angegeben ist, ist der Standardwert „wahr“. Wenn diese Kennzeichnung nicht angegeben ist, ist der Standardwert „falsch“. **Tipp:** Wenn Sie diese Kennzeichnung verwenden, sollte der Benutzer auf dem Server, von dem Sie exportiert haben, auch auf dem Server vorhanden sein, in den Sie importieren. Wenn beispielsweise ein „Testbenutzer“ mit Zugriffssteuerungseinstellungen vorhanden ist und Sie die Ressourcen mit ACL von einem Server exportieren, dann diese benannte Ressource in einen anderen Server importieren, auf dem „Testbenutzer“ nicht vorhanden ist, wird die benannte Ressource, aber nicht die ACL hochgeladen.

Beispiel

In diesem Beispiel werden die benannten Ressourcen aus „C:\myrepository\samples“ in Ihr lokales Dateisystem importiert.

```
limrepo import --s C:\myrepository\samples
```

limrepo mwsimport

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Über den Befehl `limrepo mwsimport` in der Spectrum™ Technology Platform-Administrationsumgebung können Sie eine Karte aus einer MWS-Datei (MapInfo Workspace) bereitstellen, die entweder über MapInfo Pro oder MapXtreme Workspace Manager im Spectrum Spatial Repository erstellt wurde. Beim Importieren werden die benannte Karte und alle abhängigen Ressourcen (Layers, Tabellen und Verbindungen) erstellt. Der Verbindungsname wird durch Anhängen von „Connection“ an den Kartennamen erzeugt. Die benannten Tabellen und benannten Layer werden in Unterordnern (NamedTables bzw. NamedLayers) erstellt.

Zur Verwendung dieses Befehls muss das Location Intelligence-Modul installiert sein.

Verwendung

`limrepo mwsimport --s` *MWS-Dateipfad* `--o` *Ausgabe* `--p` *Serverpfad*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help limrepo mwsimport` ein.

Erforderlich	Argument	Beschreibung
Ja	`--s` *MWSFilePath*	Gibt den Pfad zu einer MWS-Datei im lokalen Dateisystem als Importquelle an.
Ja	`--o` *Output*	Gibt den Pfad zu einer benannten Karte in der Datenbank an. Alle Ressourcen werden im selben Ordner wie die benannte Karte erstellt.
Ja	`--p` *ServerPath*	Gibt den Dateipfad zum Speicherort der Daten auf dem Server an. Der Pfad wird verwendet, um eine benannte Verbindung zu erstellen, die dann von allen benannten Tabellen referenziert werden, die erstellt werden. Diese Tabellen verwenden relative Dateipfade zu dieser benannten Verbindung.
Nein	`--l` *LocalPath*	Gibt den Dateipfad zum Speicherort der Daten auf dem lokalen Dateisystem an, wenn der MWS Dateipfade enthält, die im Serverdateisystem nicht vorhanden sind. Alle Vorkommen des angegebenen Wertes in der MWS-Datei werden durch den angegebenen Serverpfad ersetzt. Wenn in der MWS-Datei Teilpfade vorhanden sind, ist dies nicht erforderlich. Das ist normalerweise bei allen von MapXtreme erstellten Ressourcen der Fall.

Beispiel

In diesem Beispiel wird eine MWS-Datei in das Laufwerk D: importiert (wobei sich die Daten auf dem Server unter „C:\mydata“ befinden). Die benannten Ressourcen werden dabei in der Datenbank unter „/Europe/Countries“ bereitgestellt.

```
limrepo mwsimport --s D:\europe.mws --o /Europe/Countries --p
C:\mydata
```

Ergebnis

Folgende benannte Ressourcen werden erstellt:

/Europe/Countries/Europe *(benannte Karte)*
/Europe/Countries/EuropeConnection *(benannte Verbindung)*
/Europe/Countries/NamedTables/austria *(benannte Tabelle)*
/Europe/Countries/NamedTables/belgium *(benannte Tabelle)*

.
/Europe/Countries/NamedLayers/austria *(benannter Layer)*
/Europe/Countries/NamedLayers/belgium *(benannter Layer)*
..

Enterprise Routing-Modul

ermdb list

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb list` ruft alle auf dem Server vorhandenen Routenführungs-Datenbankressourcen ab. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

```
ermdb list
```

Beispiel

In diesem Beispiel werden alle Datenbankressourcen des Servers zurückgegeben.

```
ermdb list
```

ermdb get

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb get` ermöglicht die Rückgabe von Informationen über die auf dem Server konfigurierte Routenführungs-Datenbanken. Die zurückgegebenen Informationen sind der Name der Datenbank, der Speicherort der Datenbank im Dateisystem (Pfad) und die für die Datenbank konfigurierte Poolgröße. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`ermdb get --name` *Datenbankname*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help ermdb get` ein.

Erforderlich	Argument	Beschreibung
Ja	`--name` or `--n` *database_name*	Gibt den Namen der Datenbankressource für die zurückzugebenden Informationen an. Der Name muss einzigartig auf dem Server sein. Eine Liste der vorhandenen Routenführungs-Datenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.

Beispiel

In diesem Beispiel werden die Informationen für die US-Datenbankressourcen vom Server zurückgegeben.

```
ermdb get --name US
```

ermdb add

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb add` erstellt eine neue Routenführungs-Datenbankressource auf dem Server. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: Der Befehl `ermdb add` erfordert einen einzigartigen Namen für jede der hinzugefügten Datenbanken.

Verwendung

`ermdb add --name` *Datenbankname* `--poolsize` *Poolgröße* `--path` *Datenbankpfad*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help ermdb add` ein.

Erforderlich	Argument	Beschreibung
Ja	`--name` or `--n` *database_name*	Gibt den Namen der hinzuzufügenden Datenbankressource an. Der Name muss einzigartig auf dem Server sein. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Nein	`--poolsize` or `--s` *pool_size*	Gibt die maximale Anzahl der gleichzeitigen Anforderungen an, die die Datenbank bearbeiten

Erforderlich	Argument	Beschreibung
		können muss. Der Standard ist 4, wenn kein anderer Wert angegeben wird. Der zulässige Bereich für gleichzeitige Anforderungen ist eine ganze Zahl zwischen 1 und 128.
JA	`--path` *database_path*	Gibt den Speicherort der Routenführungs-Datenbank auf dem Dateiserver an.

Beispiel

In diesem Beispiel werden die US-Datenbankressourcen von `E:/ERM-US/2014.09/driving/south` auf dem Server hinzugefügt.

```
ermdb add --name US --poolsize 10 --path
E:/ERM-US/2014.09/driving/south
```

ermdb delete

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb delete` entfernt eine vorhandene Routenführungs-Datenbankressource vom Server. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`ermdb delete --name` *Datenbankname*

Anmerkung: Geben Sie zur Auflistung der Parameter `help ermdb delete` ein.

Erforderlich	Argument	Beschreibung
Ja	`--name` or `--n` *database_name*	Gibt den Namen der zu löschenden Datenbankressource an. Eine Liste der vorhandenen Routenführungs-Datenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.

Beispiel

In diesem Beispiel werden die US-Datenbankressourcen vom Server entfernt.

```
ermdb delete --name US
```

ermdb modify

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb modify` ändert eine vorhandene Routenführungs-Datenbankressource auf dem Server. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`ermdb modify --name` *Datenbankname* `--poolsize` *Poolgröße* `--path` *Datenbankpfad*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help ermdb modify` ein.

Erforderlich	Argument	Beschreibung
Ja	`--name` or `--n` *database_name*	Gibt den Namen der zu ändernden Datenbankressource an. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Nein	`--poolsize` or `--s` *pool_size*	Gibt die maximale Anzahl der gleichzeitigen Anforderungen an, die die Datenbank bearbeiten können muss. Der zulässige Bereich für gleichzeitige Anforderungen ist eine ganze Zahl zwischen 1 und 128. Sie müssen entweder eine neue Poolgröße oder einen neuen Datenbankpfad angeben.
Nein	`--path` *database_path*	Gibt den neuen Speicherort der Routenführungs-Datenbank auf dem Dateiserver an. Sie müssen entweder eine neue Poolgröße oder einen neuen Datenbankpfad angeben.

Beispiel

In diesem Beispiel werden sowohl die Poolgröße als auch der Datenbankpfad für ein neues Jahr geändert.

```
ermdb modify --name US --poolsize 20 --path
E:/ERM-US/2015.03/driving/south
```

ermdb import

> **Anmerkung:** Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb import` ermöglicht den Import einer Datei mit Routenführungs-Datenbankkonfigurationen und erstellt die Datenbankressourcen auf dem Server. Sie können entweder die Importdatei erstellen oder die durch den Befehl `ermdb export` erstellte Datei verwenden. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Das Format der Importdatei lautet wie folgt:

```
[ { "product": "Spatial", "module": "routing", "name": "US", "maxActive": 4, "properties": {
"DatasetPaths": "E:/ERM-US/2014.09/driving/northeast" } } ]
```

Dabei muss für `product` und `module` die Option „spatial“ (räumlich) oder „routing“ (Routenführung) eingestellt sein. `Name` ist der Name der Datenbank, und `maxActive` ist die maximale Anzahl der gleichzeitigen Anforderungen, die diese Datenbank verarbeiten soll (oder Poolgröße). `DatasetPaths` ist der Pfad zu den Datensätzen für die Datenbankressource.

Sie können mehrere Datenbanken in einer Importdatei hinzufügen (obiges Beispiel duplizieren) und mehrere Datensätze für jede Datenbankressource hinzufügen, indem Sie sie durch Semikola voneinander trennen.

> **Anmerkung:** Wenn Sie UTF-8-Zeichen in der Importdatei verwenden möchten, müssen Sie die JVM-Parameterdateiverschlüsselung zum Wert „UTF-8“ in den Start der CLI-Eingabeaufforderung hinzufügen. Beispiel: -Dfile.encoding=UTF-8

Verwendung

`ermdb import --file` ***Dateiname***

> **Anmerkung:** Geben Sie zur Anzeige einer Parameterliste `help ermdb import` ein.

Erforderlich	Argument	Beschreibung
JA	`--file` or `--f` *file_name*	Gibt das Verzeichnis und den Namen der Importdatei an.

Beispiel

In diesem Beispiel werden die zwei Datenbanken US1 und US2 importiert, die beide mehrere Datensätze enthalten.

```
ermdb import --file E:/ERM-US/export/ermDbResource.txt
```

Die Eingabedatei wird wie folgt definiert:

```
[ { "product": "Spatial", "module": "routing", "name": "US1", "maxActive": 4, "properties":
{ "DatasetPaths":
"E:/ERM-US/2014.09/driving/northeast;E:/ERM-US/2014.09/driving/south" } }, {
"product": "Spatial", "module": "routing", "name": "US2", "maxActive": 4, "properties":
{ "DatasetPaths":
"E:/ERM-US/2014.09/driving/northeast;E:/ERM-US/2014.09/driving/central" } } ]
```

ermdb export

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `ermdb export` ermöglicht den Export von auf dem Server konfigurierten Routenführungs-Datenbanken in eine Datei. Diese Datei kann anschließend für den Import in eine andere Instanz mithilfe des Befehls `ermdb import` entweder als Sicherung oder für die Migration von einer Instanz zur anderen verwendet werden. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: Der Befehl `ermdb export` erstellt immer eine Exportdatei mit dem Namen `ermDbResource.txt`

Verwendung

`ermdb export --directory` *Verzeichnisname*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help ermdb export` ein.

Erforderlich	Argument	Beschreibung
Nein	`--directory` or `--o` *directory_name*	Gibt den Namen des Verzeichnisses im Dateisystem an, in das die Datenbankdatei exportiert werden soll. Der Exportbefehl erstellt immer eine Exportdatei mit dem Namen `ermDbResource.txt`. Falls dieser Parameter nicht angegeben ist, wird die Exportdatei in dem Verzeichnis erstellt, in dem der Exportbefehl ausgeführt wird.

Beispiel

In diesem Beispiel wird eine Datenbankexportdatei im Verzeichnis `E:/ERM-US/export` erstellt.

```
ermdb export --directory E:/ERM-US/export
```

erm getpointdata

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm getpointdata` gibt die Segmentinformationen für einen Punkt zurück. Die nächstgelegensten Segmente werden an den angegebenen Punkt zurückgegeben. Die zurückgegebenen Informationstypen sind: Segment-ID, Straßentyp, Länge, Geschwindigkeit, Richtung, Zeit, Straßenname usw. Sie müssen das Enterprise Routing-Modul installiert haben, um diesen Befehl nutzen zu können.

Verwendung

`erm getpointdata --datasource` *Datenbankressource* `--point` *„X,Y,Koordinatensys“*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm getpointdata` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource zur Rückgabe der Daten an. Eine Liste der vorhandenen Routenführungs-Datenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--point` *"x,y,coordsys"*	Gibt den Punkt an, um die Informationen des am nächstgelegenen Segments zurückzugeben. Der Punkt wird im Format *"X,X,Koordinatensys"* angegeben, wobei *Koordinatensys* das Koordinatensystem des Punktes ist.

Beispiel

In diesem Beispiel werden die nächstgelegensten Segmentdaten aus den auf dem Server konfigurierten US-NE-Datenbankressourcen zum angegebenen Punkt zurückgegeben.

```
erm getpointdata --datasource US_NE --point "-72,40,epsg:4326"
```

erm getsegmentdata

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm getsegmentdata` gibt die Segmentinformationen für eine gegebene Segment-ID zurück. Die zurückgegebenen Informationstypen sind: Segment-ID, Straßentyp, Länge, Geschwindigkeit, Richtung, Zeit, Straßenname usw. Sie müssen das Enterprise Routing-Modul installiert haben, um diesen Befehl nutzen zu können.

Verwendung

`erm getsegmentdata --datasource` *Datenbankressource* `--segmentid` *"Segment-ID"*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm getsegmentdata` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource zur Rückgabe der Daten an. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--segmentid` *"segment_id"*	Gibt das Segment zur Rückgabe von Informationen an. Das Segment wird in dem Format angegeben, das in den Daten festgelegt ist. Beispiel: *"7e3396fc:6e5251"*.

Beispiel

In diesem Beispiel werden die Daten für das angegebene Segment aus den auf dem Server konfigurierten US-NE-Datenbankressourcen zurückgegeben.

```
erm getsegmentdata --datasource US_NE --segmentid
"7e3396fc:6e5251"
```

erm createpointupdate

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm createpointupdate` setzt die Routenführungsdaten des am nächstgelegenen Segments für einen gegebenen Punkt außer Kraft. Mit diesem Befehl können Sie die Geschwindigkeit festlegen oder ändern oder einen Abschnitt der Route ausschließen. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: Der Typ des persistenten Updates gilt nur für die angegebene Datenressource und könnte nach einem Daten-Update nicht mehr gültig sein.

Verwendung

`erm createpointupdate --datasource` *Datenbankressource* `--point` *"X,Y,Koordinatensys"* `--exclude --velocity` *Geschwindigkeitswert* `--velocityunit` *Geschwindigkeitseinheit* `--velocityadjustment` *Wert der Geschwindigkeitsanpassung* `--velocitypercentage` *Wert des Geschwindigkeitsprozentsatzes*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm createpointupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, um die Daten außer Kraft zu setzen. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--point` *"x,y,coordsys"*	Gibt den Punkt an, um die Informationen des am nächstgelegenen Segments außer Kraft zu setzen. Der Punkt wird im Format *"X,X,Koordinatensys"* angegeben, wobei *Koordinatensys* das Koordinatensystem des Punktes ist.
Nein	`--exclude`	Schließt den angegebenen Punkt von allen Routenberechnungen aus, wenn `true` festgelegt ist. Dieser Parameter gibt im Befehl an, ob der Punkt ausgeschlossen werden soll. Um den Ausschluss zu vermeiden, fügen Sie nach --exclude `false` hinzu.
Nein	`--velocity` *velocity_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie die neue Geschwindigkeit des Punktes festlegen, indem Sie die neue Geschwindigkeit angeben. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.
Nein	`--velocityunit` *velocity_unit*	Definiert eine Geschwindigkeitseinheit für die Außerkraftsetzungen `velocity` und `velocityadjustment`. Der Standardwert ist mph (Meilen pro Stunde). Bei Geschwindigkeitsaktualisierungen kann die Geschwindigkeitseinheit einen der folgenden Werte aufweisen: kph (Kilometer pro Stunde), mps (Meter pro Sekunde) oder mph (Meilen pro Stunde).
Nein	`--velocityadjustment` *velocity_adjustment_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Änderung der Geschwindigkeit des

Erforderlich	Argument	Beschreibung
		Punktes festlegen, indem Sie die Änderung der Geschwindigkeit (Einheit und Wert) angeben. Geschwindigkeitswerte können erhöht (positiver Wert) und verringert (negativer Wert) werden. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.
Nein	`--velocitypercentage` *velocity_percentage_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Erhöhung der Geschwindigkeit des Punktes definieren, indem Sie einen Prozentsatz zur Erhöhung (positiver Wert) oder zur Verringerung (negativer Wert) der Geschwindigkeit angeben.

Beispiele

In diesem Beispiel wird die Geschwindigkeit des Punktes von 15 mph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createpointupdate --datasource US_NE --point
"-72,40,epsg:4326" --velocity 15 --velocityunit mph
```

In diesem Beispiel wird der angegebene Punkt aus den auf dem Server konfigurierten US-NE-Datenbankressourcen ausgeschlossen.

```
erm createpointupdate --datasource US_NE --point
"-72,40,epsg:4326" --exclude true
```

In diesem Beispiel wird die Geschwindigkeit des Punktes durch Erhöhung um 45 kph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createpointupdate --datasource US_NE --point
"-72,40,epsg:4326" --velocityadjustment 45 --velocityunit kph
```

In diesem Beispiel wird die Geschwindigkeit des Punktes durch Verringerung um 60 Prozent aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createpointupdate --datasource US_NE --point
"-72,40,epsg:4326" --velocitypercentage -60
```

erm resetpointupdate

> **Anmerkung:** Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm resetpointupdate` setzt mögliche Außerkraftsetzungen in den ursprünglichen Zustand der Daten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`erm resetpointupdate --datasource` *Datenbankressource* `--point` *„X,Y,Koordinatensys“* `--resettype` *Rücksetzungstyp*

> **Anmerkung:** Geben Sie zur Anzeige einer Parameterliste `help erm resetpointupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die die Außerkraftsetzungen enthält. Eine Liste der vorhandenen Routenführungs-Datenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--point` *"x,y,coordsys"*	Gibt den Punkt an, an dem sich die vorhandenen Außerkraftsetzungen befinden. Der Punkt wird im Format *"X,X,Koordinatensys"* angegeben, wobei *Koordinatensys* das Koordinatensystem des Punktes ist.
Ja	`--resettype` *reset_type*	Der Typ der zu entfernenden (rückgängig zu machenden) Außerkraftsetzung. **speed** Entfernt die Geschwindigkeitsaktualisierung. **exclude** Entfernt die Ausschlussaktualisierung.

Beispiel

In diesem Beispiel werden vorhandene Außerkraftsetzungen von Ausschlüssen für den angegebenen Punkt aus den US_NE-Datenbankressourcen zurückgegeben, die auf dem Server konfiguriert sind.

```
erm resetpointupdate --datasource US_NE --point
"-72,40,epsg:4326" --resettype exclude
```

erm createsegmentupdate

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm createsegmentupdate` setzt die Routenführungsdaten des angegebenen Segments außer Kraft. Mit diesem Befehl können Sie die Geschwindigkeit festlegen oder ändern, einen Abschnitt der Route ausschließen oder den Straßentyp ändern. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: Der Typ des persistenten Updates gilt nur für die angegebene Datenressource und könnte nach einem Daten-Update nicht mehr gültig sein.

Verwendung

`erm createsegmentupdate --datasource` *Datenbankressource* `--segmentid` *"Segment-ID"* `--exclude --velocity` *Geschwindigkeitswert* `--velocityunit` *Geschwindigkeitseinheit* `--velocityadjustment` *Wert der Geschwindigkeitsanpassung* `--velocitypercentage` *Wert des Geschwindigkeitsprozentsatzes* `--roadtype` *Straßentyp*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm createsegmentupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, um die Daten außer Kraft zu setzen. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--segmentid` *"segment_id"*	Gibt das außer Kraft zu setzende Segment an. Das Segment wird in dem Format angegeben, das in den Daten festgelegt ist. Beispiel: *"7e3396fc:6e5251"*.
Nein	`--exclude`	Schließt das angegebene Segment von allen Routenberechnungen aus, wenn `true` festgelegt ist. Dieser Parameter gibt im Befehl an, ob das Segment ausgeschlossen werden soll. Um den Ausschluss zu vermeiden, fügen Sie nach --exclude `false` hinzu.

Erforderlich	Argument	Beschreibung
Nein	`--velocity` *velocity_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie die neue Geschwindigkeit des Segments festlegen, indem Sie die neue Geschwindigkeit angeben. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.
Nein	`--velocityunit` *velocity_unit*	Definiert eine Geschwindigkeitseinheit für die Außerkraftsetzungen `velocity` und `velocityadjustment`. Der Standardwert ist mph (Meilen pro Stunde). Bei Geschwindigkeitsaktualisierungen kann die Geschwindigkeitseinheit einen der folgenden Werte aufweisen: kph (Kilometer pro Stunde), mps (Meter pro Sekunde) oder mph (Meilen pro Stunde).
Nein	`--velocityadjustment` *velocity_adjustment_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Änderung in der Geschwindigkeit des Segments festlegen, indem Sie die Änderung der Geschwindigkeit (Einheit und Wert) angeben. Geschwindigkeitswerte können erhöht (positiver Wert) und verringert (negativer Wert) werden. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.
Nein	`--velocitypercentage` *velocity_percentage_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Erhöhung der Geschwindigkeit des Segments definieren, indem Sie einen Prozentsatz zur Erhöhung (positiver Wert) oder zur Verringerung (negativer Wert) der Geschwindigkeit angeben.
Nein	`--roadtype` *road_type*	Definiert den neuen Straßentyp für das Segment.

Beispiele

In diesem Beispiel wird die Geschwindigkeit des Segments von 15 mph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createsegmentupdate --datasource US_NE --segmentid
"7e3396fc:6e5251" --velocity 15 --velocityunit mph
```

In diesem Beispiel wird das angegebene Segment aus den auf dem Server konfigurierten US-NE-Datenbankressourcen ausgeschlossen.

```
erm createsegmentupdate --datasource US_NE --segmentid
"7e3396fc:6e5251" --exclude true
```

In diesem Beispiel wird die Geschwindigkeit des Segments durch Erhöhung um 45 kph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createsegmentupdate --datasource US_NE --segmentid
"7e3396fc:6e5251" --velocityadjustment 45 --velocityunit kph
```

In diesem Beispiel wird die Geschwindigkeit des Segments durch Verringerung um 60 Prozent aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createsegmentupdate --datasource US_NE --segmentid
"7e3396fc:6e5251" --velocitypercentage -60
```

In diesem Beispiel wird der Straßentyp des Segments zur Fähre aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createsegmentupdate --datasource US_NE --segmentid
"7e3396fc:6e5251" --roadtype Fähre
```

erm resetsegmentupdate

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm resetsegmentupdate` setzt mögliche Außerkraftsetzungen in den ursprünglichen Zustand der Daten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`erm resetsegmentupdate --datasource` *Datenbankressource* `--segmentid` *"Segment-ID"* `--resettype` *Rücksetzungstyp*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm resetsegmentupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die die Änderungen enthält. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.

Erforderlich	Argument	Beschreibung
Ja	`--segment` *"segment_id"*	Gibt das Segment an, in dem sich die vorhandenen Außerkraftsetzungen befinden. Das Segment wird in dem Format angegeben, das in den Daten festgelegt ist. Beispiel: *"7e3396fc:6e5251"*.
Ja	`--resettype` *reset_type*	Der Typ der zu entfernenden (rückgängig zu machenden) Außerkraftsetzung. **speed** Entfernt die Geschwindigkeitsaktualisierung. **exclude** Entfernt die Ausschlussaktualisierung. **roadtype** Entfernt eine Straßentypaktualisierung.

Beispiel

In diesem Beispiel werden vorhandene Außerkraftsetzungen von Straßentypen für das angegebene Segment aus den US_NE-Datenbankressourcen zurückgegeben, die auf dem Server konfiguriert sind.

```
erm resetsegmentupdate --datasource US --segmentid
"7e3396fc:6e5251" --resettype roadtype
```

erm getsegmentupdates

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm getsegmentupdates` gibt für die angegebenen Segmente eine Liste von Änderungen in den Routingdaten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: `segmentids` ist ein optionaler Parameter. Wenn keine Segment-IDs angegeben werden, werden die Änderungen für alle verfügbaren Segmente zurückgegeben.

Usage

`erm getsegmentupdates --datasource` *Datenbankressource* `--segmentids` *"Segment-IDs"* `--velocityunit` *Geschwindigkeitseinheit*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm getsegmentupdates` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die Änderungen enthält. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Nein	`--segmentids` *"segment_ids"*	Eine durch Komma getrennte Liste der Segment-IDs, um Änderungensinformationen zurückzugeben. Segmente werden in dem Format angegeben, das in den Daten angegeben ist. Beispiel: *"7e3396fc:6e5251"*.
Nein	`--velocityunit` *velocityunit*	Gibt die Geschwindigkeitseinheiten für die Antwort an (mph – Meilen pro Stunde, kph – Kilometer pro Stunde, mtps – Meter pro Sekunde und mtpm – Meter pro Minute). Der Standardwert ist „mph“.

Beispiel

In diesem Beispiel werden alle Änderungen für ein Segment aus den US_NE-Datenbankressourcen zurückgegeben, die auf dem Server konfiguriert sind.

```
erm getsegmentupdates --datasource US_NE --segmentids
"7e3396fc:6e5251" --velocityunit kph
```

erm createroadtypeupdate

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm createroadtypeupdate` setzt die Routenführungsdaten des angegebenen Straßentyps außer Kraft. Mit diesem Befehl können Sie die Geschwindigkeit der Route für den jeweiligen Straßentyp festlegen oder ändern. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: Der Typ des persistenten Updates gilt nur für die angegebene Datenressource und könnte nach einem Daten-Update nicht mehr gültig sein.

Verwendung

`erm createroadtypeupdate --datasource` *Datenbankressource* `--roadtype` *"Straßentyp"* `--velocity` *Geschwindigkeitswert* `--velocityunit` *Geschwindigkeitseinheit* `--velocityadjustment` *Wert der Geschwindigkeitsanpassung* `--velocitypercentage` *Wert des Geschwindigkeitsprozentsatzes* `--roadtype` *Straßentyp*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm createroadtypeupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, um die Daten außer Kraft zu setzen. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--roadtype` *"road_type"*	Gibt den außer Kraft zu setzenden Straßentyp an. Der Straßentyp kann einer der folgenden sein: • Zugangsweg • Nebenstraße • Verbindungsstraße • Fähre • Fußweg • Zufahrtsbeschränkung, dicht, städtisch • Zufahrtsbeschränkung, ländlich • Zufahrtsbeschränkung, vorstädtisch • Zufahrtsbeschränkung, städtisch • Lokale Straße, dicht, städtisch • Lokale Straße, ländlich • Lokale Straße, vorstädtisch • Lokale Straße, städtisch • Lokale Hauptverkehrsstraße, dicht, städtisch • Lokale Hauptverkehrsstraße, ländlich • Lokale Hauptverkehrsstraße, vorstädtisch • Lokale Hauptverkehrsstraße, städtisch • Hauptverkehrsstraße, dicht, städtisch • Hauptverkehrsstraße, ländlich • Hauptverkehrsstraße, vorstädtisch • Hauptverkehrsstraße, städtisch • Lokale Nebenstraße, dicht, städtisch • Lokale Nebenstraße, ländlich • Lokale Nebenstraße, vorstädtisch • Lokale Nebenstraße, städtisch • Normale Straße, dicht, städtisch • Normale Straße, ländlich • Normale Straße, ländlich • Normale Straße, städtisch • Autobahn/Bundesstraße, dicht, städtisch

Erforderlich	Argument	Beschreibung
		• Autobahn/Bundesstraße, ländlich • Autobahn/Bundesstraße, vorstädtisch • Autobahn/Bundesstraße, städtisch • Auffahrt, dicht, städtisch • Auffahrt, Zufahrtsbeschränkung • Auffahrt Hauptverkehrsstraße • Auffahrt Autobahn/Bundesstraße • Auffahrt, ländlich • Auffahrt Landstraße • Auffahrt, städtisch • Auffahrt, vorstädtisch • Landstraße, dicht, städtisch • Landstraße, ländlich • Landstraße, vorstädtisch • Landstraße, städtisch
Nein	`--velocity` *velocity_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie die neue Geschwindigkeit des Straßentyps festlegen, indem Sie die neue Geschwindigkeit angeben. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.
Nein	`--velocityunit` *velocity_unit*	Definiert eine Geschwindigkeitseinheit für die Außerkraftsetzungen `velocity` und `velocityadjustment`. Der Standardwert ist mph (Meilen pro Stunde). Bei Geschwindigkeitsaktualisierungen kann die Geschwindigkeitseinheit einen der folgenden Werte aufweisen: kph (Kilometer pro Stunde), mps (Meter pro Sekunde) oder mph (Meilen pro Stunde).
Nein	`--velocityadjustment` *velocity_adjustment_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Änderung in der Geschwindigkeit des Straßentyps festlegen, indem Sie die Änderung der Geschwindigkeit (Einheit und Wert) angeben. Geschwindigkeitswerte können erhöht (positiver Wert) und verringert (negativer Wert) werden. Die Standardeinheit ist mph (Meilen pro Stunde), außer wenn Sie den Parameter `velocityunit` festlegen.

Erforderlich	Argument	Beschreibung
Nein	`--velocitypercentage` *velocity_percentage_value*	Definiert eine Geschwindigkeitsaktualisierung, bei der Sie eine Erhöhung der Geschwindigkeit des Straßentyps definieren, indem Sie einen Prozentsatz zur Erhöhung (positiver Wert) oder zur Verringerung (negativer Wert) der Geschwindigkeit angeben.

Beispiele

In diesem Beispiel wird die Geschwindigkeit des Straßentyps von 25 mph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createroadtypeupdate --datasource US_NE --roadtype "Normale
Straße, vorstädtisch" --velocity 25 --velocityunit kph
```

In diesem Beispiel wird die Geschwindigkeit des angegebenen Straßentyps von 50 mph aus den auf dem Server konfigurierten US-NE-Datenbankressourcen erhöht.

```
erm createroadtypeupdate --datasource US_NE --roadtype "Normale
Straße, vorstädtisch" --velocityadjustment 50 --velocityunit
mph
```

In diesem Beispiel wird die Geschwindigkeit des Straßentyps durch Verringerung um 65 Prozent aus den auf dem Server konfigurierten US-NE-Datenbankressourcen außer Kraft gesetzt.

```
erm createroadtypeupdate --datasource US_NE --roadtype "Normale
Straße, vorstädtisch" --velocitypercentage -65
```

erm resetroadtypeupdate

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm resetroadtypeupdate` setzt mögliche Außerkraftsetzungen in den ursprünglichen Zustand der Daten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`erm resetroadtypeupdate --datasource` *Datenbankressource* `--roadtype` *"Straßentyp"*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm resetroadtypeupdate` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die die Änderungen enthält. Eine Liste der vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Ja	`--roadtype` *"road_type"*	Gibt den Straßentyp an, der die vorhandenen Außerkraftsetzungen enthält. Eine Liste der Straßentypen finden Sie unter **erm createroadtypeupdate** auf Seite 119.

Beispiel

In diesem Beispiel wird die Außerkraftsetzung des Straßentyps „Normale Straße, städtisch“ aus den auf dem Server konfigurierten US_NE-Datenbankressourcen zurückgesetzt.

```
erm resetroadtypeupdate --datasource US_NE --roadtype "Normale
Straße, vorstädtisch"
```

erm getroadtypeupdates

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm getroadtypeupdates` gibt für die angegebenen Straßentypen eine Liste von Änderungen in den Routingdaten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Anmerkung: `roadtypes` ist ein optionaler Parameter. Wenn keine Straßentypen angegeben werden, werden die Änderungen für alle verfügbaren Straßentypen zurückgegeben.

Usage

`erm getroadtypeupdates --datasource` *Datenbankressource* `--roadtypes` *"Straßentypen"* `--velocityunit` *Geschwindigkeitseinheit*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm getroadtypeupdates` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die Änderungen enthält. Eine Liste der vorhandenen

Erforderlich	Argument	Beschreibung
		Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Nein	`--roadtypes` *"road_types"*	Eine durch Komma getrennte Liste der Straßentypen, um Änderungensinformationen zurückzugeben. Eine Liste der Straßentypen finden Sie unter **erm createroadtypeupdate** auf Seite 119.
Nein	`--velocityunit` *velocityunit*	Gibt die Geschwindigkeitseinheiten für die Antwort an (mph – Meilen pro Stunde, kph – Kilometer pro Stunde, mtps – Meter pro Sekunde und mtpm – Meter pro Minute). Der Standardwert ist „mph“.

Beispiel

In diesem Beispiel werden alle Änderungen für den Straßentyp „Normale Straße, städtisch“ aus den US_NE-Datenbankressourcen zurückgegeben, die auf dem Server konfiguriert sind.

```
erm getroadtypeupdates --datasource US_NE --roadtypes "Normale
Straße, städtisch" --velocityunit kph
```

erm getallupdates

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm getallupdates` gibt eine Liste aller Änderungen für eine bestimmte Routingdatenbankressource zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Usage

`erm getallupdates --datasource` *Datenbankressource „Segment-IDs“* `--velocityunit` *Geschwindigkeitseinheit*

Anmerkung: Geben Sie zur Anzeige einer Parameterliste `help erm getallupdates` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die die Änderungen enthält. Eine Liste der

Erforderlich	Argument	Beschreibung
		vorhandenen Routingddatenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.
Nein	`--velocityunit` *velocityunit*	Gibt die Geschwindigkeitseinheiten für die Antwort an (mph – Meilen pro Stunde, kph – Kilometer pro Stunde, mtps – Meter pro Sekunde und mtpm – Meter pro Minute). Der Standardwert ist „mph“.

Beispiel

In diesem Beispiel werden alle Änderungen aus den US_NE-Datenbankressourcen zurückgegeben, die auf dem Server konfiguriert sind.

```
erm getallupdates --datasource US_NE --velocityunit kph
```

erm resetallupdates

Anmerkung: Anweisungen zur Installation und Ausführung der Administrationsumgebung finden Sie unter **Erste Schritte in der Administrationsumgebung** auf Seite 95.

Der Befehl `erm resetallupdates` setzt alle Außerkraftsetzungen in den ursprünglichen Zustand der Daten zurück. Zur Verwendung dieses Befehls muss das Enterprise Routing-Modul installiert sein.

Verwendung

`erm resetallupdates --datasource` *Datenbankressource*

Anmerkung: Geben Sie zur Auflistung der Parameter `help erm resetallupdates` ein.

Erforderlich	Argument	Beschreibung
Ja	`--datasource` *db_resource*	Gibt den Namen der Datenbankressource an, die die Außerkraftsetzungen enthält. Eine Liste der vorhandenen Routenführungs-Datenbankressourcen erhalten Sie mithilfe des Befehls `ermdb list`.

Beispiel

In diesem Beispiel werden alle Außerkraftsetzungen aus den US_NE-Datenbankressourcen zurückgesetzt, die auf dem Server konfiguriert sind.

```
erm resetallupdates --datasource US_NE
```

8 - Enterprise Routing-Modul

In this section

Angeben von Standarddienst-/Standardschrittoptionen

Standarddienstoptionen steuern das Standardverhalten der einzelnen Dienste oder Schritte auf Ihrem System. Sie können für jede Option einen Standardwert angeben. Die Standardoption wird wirksam, wenn in einer Anforderung ein Wert für eine bestimmte Option nicht explizit definiert ist. Diese Standardoptionen sind auch die Einstellungen, die standardmäßig verwendet werden, wenn Sie unter Verwendung dieses Dienstes einen Datenfluss in Enterprise Designer erstellen.

Informationen zu den Optionen finden Sie im *Spectrum Spatial-Handbuch* in den Abschnitten „Schritte“, „Ressourcen“ und „Daten“, die für das Enterprise Routing-Modul gelten.

Anmerkung: Persistent Updates werden nicht mit der Management Console verwaltet. Verwenden Sie zum Durchführen von Persistent Updates die Befehlszeilenfunktion von Spectrum in der Administrationsumgebung.

Anmerkung: Der Get Route Data-Dienst in der Management Console legt keine Standardoptionen fest. Er bietet die Möglichkeit, Routing-Daten für Segmente interaktiv zurückzugeben. Informationen zu Get Route Data finden Sie unter **Abrufen von Routendaten mithilfe der Management Console** auf Seite 130.

1. Öffnen Sie die Management Console.
2. Klicken Sie auf **Dienste**.
3. Klicken Sie auf das gewünschte Modul (Enterprise Routing-Modul).
4. Klicken Sie in der Liste auf der linken Seite auf den Dienst, der konfiguriert werden soll.
5. Legen Sie die Optionen für den Dienst fest. Die meisten Dienste weisen verschiedene Optionstypen auf, die auf unterschiedlichen Registerkarten angezeigt werden.
6. Klicken Sie auf **Speichern**.

Anzeigen einer Vorschau für einen Dienst/einen Schritt

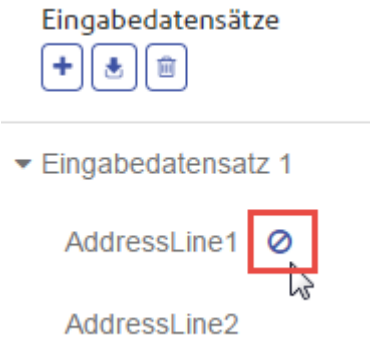
Sie können für die Ergebnisse eines Dienstes in der Management Console über die Registerkarte „Vorschau“ des Dienstes eine Vorschau anzeigen. Die Vorschau kann sich als nützliche Hilfe erweisen, wenn Sie entscheiden müssen, welche Optionen angegeben werden sollen, da Sie direkt sehen können, welche Auswirkungen die verschiedenen Optionen auf die von dem Dienst oder dem Schritt zurückgegebenen Daten haben.

1. Öffnen Sie die Management Console.
2. Öffnen Sie das Menü **Dienste**, und wählen Sie den Dienst aus, für den Sie eine Vorschau anzeigen möchten.

3. Klicken Sie auf die Registerkarte **Vorschau**.
4. Geben Sie die Testdaten in die einzelnen Felder ein.

   Im Folgenden finden Sie einige Tipps zur Verwendung der Vorschau:

   - Sie müssen nicht in jedes Feld Daten eingeben. Wenn Sie ein Feld leer lassen, wird in der Vorschau eine leere Zeichenfolge verwendet.
   - Klicken Sie neben dem Feld auf das Symbol „Deaktivieren“, um eine Vorschau für den Effekt anzuzeigen, wenn ein Nullwert in einem Feld übergeben wird:

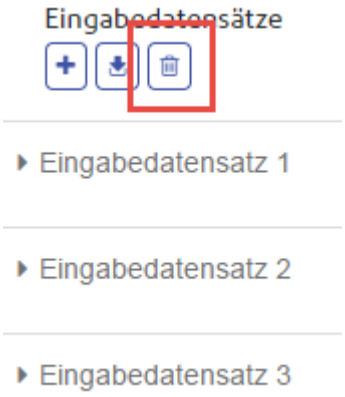


   - Sie können eine Vorschau für mehrere Datensätze gleichzeitig anzeigen lassen. Um einen Datensatz hinzuzufügen, klicken Sie auf die Schaltfläche „Hinzufügen“ .
   - Sie können Testdaten aus einer Datei importieren. Um Daten zu importieren, klicken Sie auf die Schaltfläche „I^mportieren“ . Wählen Sie **Dateiname** und **Feldtrennzeichen** aus. Beachten Sie Folgendes:

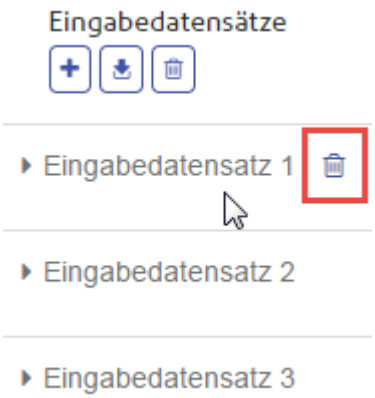
     - Die erste Zeile der Datei muss ein Header-Datensatz sein. Die Feldnamen im Header müssen mit den Feldnamen übereinstimmen, die der Dienst erfordert.
     - Es können maximal fünf Datensätze importiert werden.
     - Wenn in der Datei Leerzeichen als Feldtrennzeichen verwendet werden, müssen die Feldwerte in Anführungszeichen stehen. Im Folgenden finden Sie ein Beispiel einer Datei, in der ein Leerzeichen als Feldtrennzeichen verwendet wird:

```
AddressLine1 AddressLine2 City StateProvince PostalCode
"One Global View" "" "Troy" "NY" "12180"
"3001 Summer St" "" "Stamford" "CT" "06926"
"224 N Michigan Ave" "Suite 300" "Chicago" "IL" ""
```

   - Um alle Datensätze zu löschen, klicken Sie auf die Schaltfläche „Löschen“ im oberen Bereich der Vorschau:



- Um einen einzelnen Datensatz zu löschen, bewegen Sie den Mauszeiger über den Namen des Eingabedatensatzes (beispielsweise „Input Record 1“) und klicken Sie auf die Schaltfläche „Löschen“ neben dem Datensatznamen:



- Gehen Sie wie folgt vor, wenn der Dienst hierarchische Eingabedaten benötigt:
  - Um untergeordnete Datensätze hinzuzufügen, bewegen Sie den Mauszeiger über den übergeordneten Datensatz und klicken Sie auf die Schaltfläche „Hinzufügen“.
  - Um alle untergeordneten Datensätze eines übergeordneten Datensatzes zu löschen, bewegen Sie den Mauszeiger über den übergeordneten Datensatz und klicken Sie auf die Schaltfläche „Löschen“.
  - Um einzelne untergeordnete Datensätze zu löschen, bewegen Sie den Mauszeiger über den untergeordneten Datensatz und klicken Sie auf die Schaltfläche „Löschen“.

5. Klicken Sie auf **Vorschau ausführen**.

   Der Dienst verarbeitet die Eingabedatensätze und zeigt die Ergebnisse an

6. Überprüfen Sie Ihre Ausgabedaten und stellen Sie dabei sicher, dass die Ergebnisse dem entsprechen, was Sie von dem Dienst oder dem Schritt abrufen wollten. Bei Bedarf können Sie Änderungen an der Option vornehmen und erneut auf **Vorschau ausführen** klicken. (Sie müssen die Daten nicht erneut eingeben.)

Abrufen von Routendaten mithilfe der Management Console

Sie können mithilfe der Management Console eine Vorschau anzeigen und Segmentinformationen von einem nächstgelegenen Punkt oder einer Segment-ID speichern. Der GetRouteData-Dienst gibt Segmentinformationen für einen Punkt oder eine Segment-ID zurück. Wenn ein Punkt angegeben ist, werden die am nächsten liegenden Routensegmente zurückgegeben. Wenn eine Segment-ID angegeben ist, werden die Routendaten für dieses angegebene Routensegment zurückgegeben.

So zeigen Sie eine Vorschau an und/oder speichern Routendaten:

1. Öffnen Sie die Management Console.
2. Navigieren Sie zum Menü **Dienste** und wählen Sie Enterprise Routing-Modul aus.
3. Wählen Sie **Get Route Data** aus der Liste der Dienste aus.
4. Wählen Sie im Feld **Eingabetyp** den Eintrag „Punktdaten“ oder den Eintrag „Segmentdaten“ aus.
5. Wählen Sie im Feld **Datenbank** die Routing-Datenbankressource aus.

   Wenn Sie eine neue Routing-Datenbankressource hinzufügen müssen, finden Sie unter **Hinzufügen einer Routing-Datenbankressource** weitere Informationen.

6. Geben Sie die erforderlichen Informationen für den von Ihnen ausgewählten Eingabetyp ein.

   Geben Sie die Punktkoordinaten und das Koordinatensystem ein, wenn Sie „Punktdaten“ ausgewählt haben. Geben Sie die Segment-ID ein, wenn Sie „Segmentdaten“ ausgewählt haben.

7. Klicken Sie auf **Vorschau**.

   Die Routensegmentdaten werden im Abschnitt **Ausgabedaten** zurückgegeben. Wenn der Eingabe mehrere Segmente zugeordnet sind, werden mehrere Segmente mit „Segmentdetails 1“, „Segmentdetails 2“ etc. aufgelistet.

8. Klicken Sie auf die Schaltfläche **Speichern**, um die Ergebnisse der Routenführungsdaten als Textdatei zu speichern, oder klicken Sie auf die Schaltfläche **Löschen**, um die Ergebnisse aus den Ausgabedaten zu entfernen.

9 - Beheben von Fehlern in Ihrem System

In this section

Neuerstellen eines beschädigten Datenbankindex

Wenn der Server unvermittelt heruntergefahren oder der Java-Prozess erzwungen beendet wird (ob manuell oder durch einen Stromausfall), kann manchmal die Datenbank beschädigt werden. Als Ergebnis können Sie möglicherweise nicht mehr auf Ressourcen zugreifen, die vorher suchbar waren. Im Protokoll sind dabei keine Fehler oder Warnungen verzeichnet. Nachdem Sie überprüft haben, dass nicht Änderungen an den Berechtigungen der Grund sind, erstellen Sie den Index neu, um dieses Problem zu beheben:

1. Fahren Sie den Server herunter.
2. Löschen Sie das Indexverzeichnis an folgenden Speicherorten:
   - <Spectrum>\server\modules\spatial\jackrabbit\workspaces\default
   - <Spectrum>\server\modules\spatial\jackrabbit\workspaces\security
   - <Spectrum>\server\modules\spatial\jackrabbit\repository
3. Starten Sie den Server neu.
   Jackrabbit erstellt während des Startvorgangs den Index an den oben aufgeführten Speicherorten neu.

Nach der Neuerstellung des Index funktioniert die Suche wieder korrekt.

Überwachen der Speichernutzung auf einem nicht reagierenden Server

Wenn Ihr Spectrum-Server nicht mehr reagiert, können Sie den unten aufgeführten Schritten folgen, um seine Leistung und seinen Ressourcenverbrauch zu überwachen. Aus dieser Überwachung gewinnen Sie Informationen, die Sie verwenden können, um Speicher- und Thread-Nutzung anzupassen.

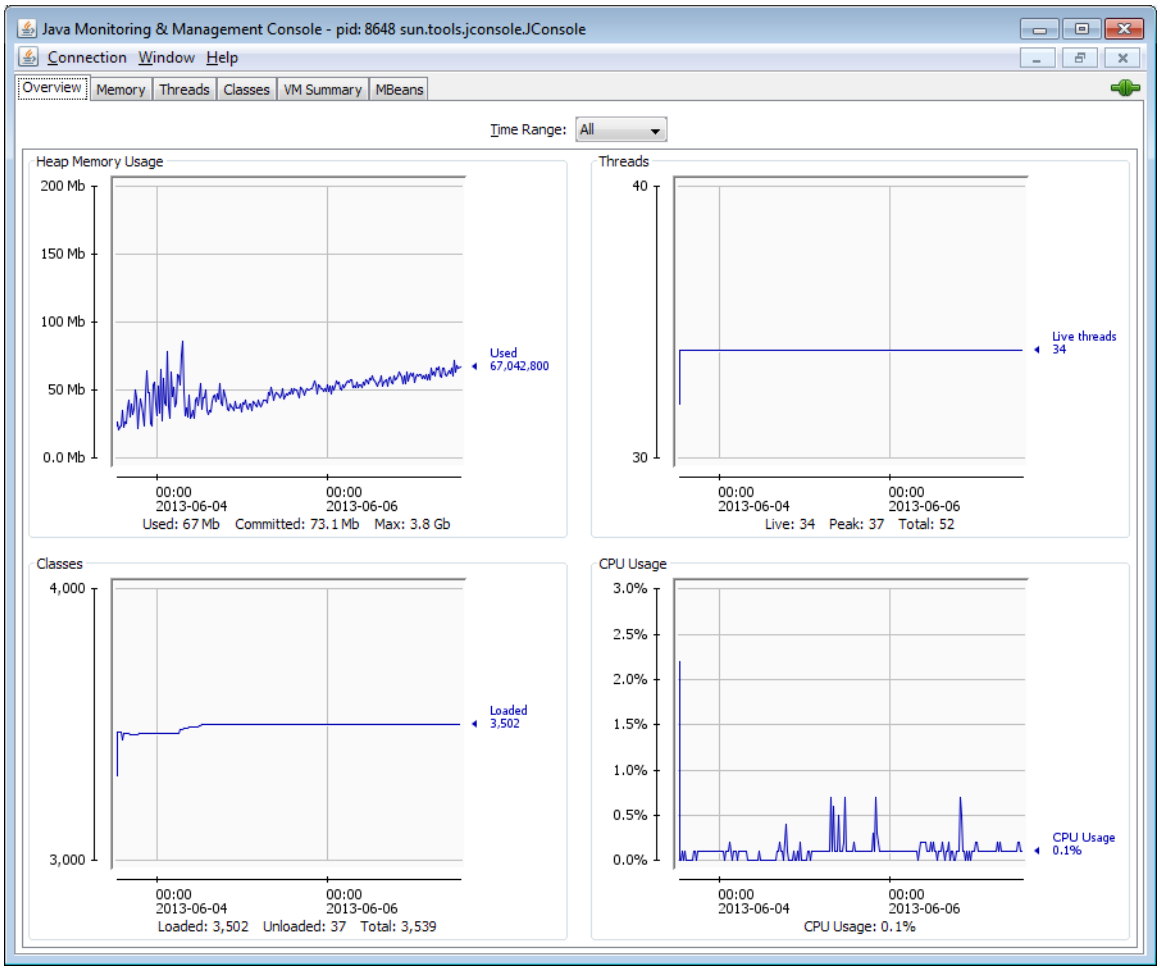
1. Überprüfen Sie, ab ein anderer Dienst außer dem Mapping-Dienst funktioniert. Starten Sie beispielsweise den Feature-Dienst auf der Demoseite: http://<servername>:<port>/Spatial/FeatureService//DemoPage.html. So stellen Sie fest, ob der gesamte Server nicht verfügbar ist oder nur der Mapping-Dienst.
2. Überprüfen Sie, ob genügend Festplattenspeicher zur Speicherung der Bilder von Mapping und Map Tiling zur Verfügung steht, indem Sie sich die Konfigurationsdateien ansehen:
   - **Mapping:**
     „http://<server>:<port>/RepositoryService/repository/default/Configuration/MappingConfiguration“

unter "<Directory> C:\Program Files\Pitney Bowes\Spectrum/server/modules/spatial/images </Directory>"

- **Map Tiling:**
  „http://<server>:<port>/RepositoryService/repository/default/Configuration/MapTilingConfiguration“ unter "<Property name="diskPath" value="C:/Program Files/Pitney Bowes/Spectrum/server/modules/spatial/TileCache"/>"

3. Halten Sie den Spectrum-Server an.
4. Öffnen Sie die Datei „java.vmargs“ in <Installed>\Pitney Bowes\Spectrum\server\modules\spatial\java.vmargs mithilfe eines Texteditors.
5. Ändern Sie die Standardeinstellung für „vmargs“ von 2GB (2048MB). Um beispielsweise den Speicher für die Remote-Komponente auf 4 GB zu erhöhen, ändern Sie „vmargs“ vom Standard von -Xmx2048m auf -Xmx4096m. Überschreiten Sie nicht den maximalen Speicher, der Ihrem Betriebssystem zur Verfügung steht, und lassen Sie genügend Speicherplatz übrig, damit das Betriebssystem ordnungsgemäß funktionieren kann.
6. Speichern Sie die Datei „java.vmargs“.
7. Starten Sie den Server-Wrapper:
   a) Öffnen Sie eine Eingabeaufforderung als Administrator.
   b) Navigieren Sie zum Verzeichnis <Installed>\Pitney Bowes\Spectrum\server\bin\wrapper, und geben Sie **wrapper.exe -c** ein.

   Dieser Spectrum-Server startet in wenigen Minuten.
8. Wenn der Server gestartet ist, führen Sie über die Demoseiten folgende Anforderungen aus:
   a) Öffnen Sie „http://<servername>:<port>/Spatial/MappingService/DemoPage.html“, und führen Sie die Anforderung „Benannte Karten auflisten“ aus.
   b) Öffnen Sie „http://<servername>:<port>/Spatial/FeatureService/DemoPage.html“, und führen Sie die Anforderung „Tabellennamen auflisten“ aus.
9. Navigieren Sie zu „<Installed>\Pitney Bowes\Spectrum\java64\bin“, und führen Sie „jconsole.exe“ aus.
10. Wählen Sie unter „Lokaler Prozess“ den Wrapper-Prozess aus.
11. Fügen Sie in Jconsole eine neue Sitzung hinzu, und wählen Sie den Prozess des Feature-Dienstes aus.
12. Fügen Sie in Jconsole eine neue Sitzung hinzu, und wählen Sie den Prozess des Mapping-Dienstes aus.
13. Lassen Sie Jconsole aktiv, um Speicher, CPU-Threads usw. für den Spectrum Platform-Wrapper des Feature- und Mapping-Dienstes zu überwachen.


Java Monitoring & Management Console - pid: 8648 sun.tools.jconsole.JConsole
Connection Window Help
Overview Memory Threads Classes VM Summary MBeans
Time Range: All
Heap Memory Usage
200 Mb
150 Mb
100 Mb
50 Mb
0.0 Mb
Used
67,042,800
00:00
2013-06-04
00:00
2013-06-06
Used: 67 Mb Committed: 73.1 Mb Max: 3.8 Gb
Threads
40
30
Live threads
34
00:00
2013-06-04
00:00
2013-06-06
Live: 34 Peak: 37 Total: 52
Classes
4,000
3,000
Loaded
3,502
00:00
2013-06-04
00:00
2013-06-06
Loaded: 3,502 Unloaded: 37 Total: 3,539
CPU Usage
3.0%
2.5%
2.0%
1.5%
1.0%
0.5%
0.0%
CPU Usage
0.1%
00:00
2013-06-04
00:00
2013-06-06
CPU Usage: 0.1%

Notices

USPS® Urheberrechtshinweise

Datenbereitstellung und Hinweise

Diese CD-ROM enthält Daten einer urheberrechtlich geschützten Datenerfassung der Canada Post Corporation.

Das Geocode Address World Dataset enthält lizenzierte Daten des GeoNames-Projekts (**www.geonames.org**), die unter den Bedingungen der Creative Commons Attribution License ("Attribution License") bereitgestellt werden. Die Attribution License können Sie unter **http://creativecommons.org/licenses/by/3.0/legalcode** einsehen. Ihre Nutzung der GeoNames-Daten (wie im Spectrum™ Technology Platform Nutzerhandbuch beschrieben) unterliegt den Bedingungen der Attribution License. Bei Konflikten zwischen Ihrer Vereinbarung mit Pitney Bowes Software, Inc. und der Attribution License hat die Attribution License lediglich bezüglich der Nutzung von GeoNames-Daten Vorrang.

3001 Summer Street
Stamford CT 06926-0700
USA

www.pitneybowes.com