IBM SPSS Collaboration and Deployment
Services Repository
Version 8 Release 2

Installation and Configuration Guide

IBM

Note

Before using this information and the product it supports, read the information in .

Contents

Chapter 1. Overview

IBM SPSS Collaboration and Deployment Services

IBM SPSS Collaboration and Deployment Services is an enterprise-level application that enables widespread use and deployment of predictive analytics.

IBM SPSS Collaboration and Deployment Services provides centralized, secure, and auditable storage of analytical assets and advanced capabilities for management and control of predictive analytic processes, as well as sophisticated mechanisms for delivering the results of analytical processing to users. The benefits of IBM SPSS Collaboration and Deployment Services include:

- Safeguarding the value of analytical assets
- Ensuring compliance with regulatory requirements
- Improving the productivity of analysts
- Minimizing the IT costs of managing analytics

IBM SPSS Collaboration and Deployment Services allows you to securely manage diverse analytical assets and fosters greater collaboration among those developing and using them. Furthermore, the deployment facilities ensure that people get the information they need to take timely, appropriate action.

Collaboration

Collaboration refers to the ability to share and reuse analytic assets efficiently, and is the key to developing and implementing analytics across an enterprise.

Analysts need a location in which to place files that should be made available to other analysts or business users. That location needs a version control implementation for the files to manage the evolution of the analysis. Security is required to control access to and modification of the files. Finally, a backup and restore mechanism is needed to protect the business from losing these crucial assets.

To address these needs, IBM SPSS Collaboration and Deployment Services provides a repository for storing assets using a folder hierarchy similar to most file systems. Files stored in the IBM SPSS Collaboration and Deployment Services Repository are available to users throughout the enterprise, provided those users have the appropriate permissions for access. To assist users in finding assets, the repository offers a search facility.

Analysts can work with files in the repository from client applications that leverage the service interface of IBM SPSS Collaboration and Deployment Services. Products such as IBM SPSS Statistics and IBM SPSS Modeler allow direct interaction with files in the repository. An analyst can store a version of a file in development, retrieve that version at a later time, and continue to modify it until it is finalized and ready to be moved into a production process. These files can include custom interfaces that run analytical processes allowing business users to take advantage of an analyst's work.

The use of the repository protects the business by providing a central location for analytical assets that can be easily backed-up and restored. In addition, permissions at the user, file, and version label levels control access to individual assets. Version control and object version labels ensure the correct versions of assets are being used in production processes. Finally, logging features provide the ability to track file and system modifications.

Deployment

To realize the full benefit of predictive analytics, the analytic assets need to provide input for business decisions. Deployment bridges the gap between analytics and action by delivering results to people and processes on a schedule or in real time.

In IBM SPSS Collaboration and Deployment Services, individual files stored in the repository can be included in processing **jobs**. Jobs define an execution sequence for analytical artifacts and can be created

with IBM SPSS Deployment Manager. The execution results can be stored in the repository, on a file system, or delivered to specified recipients. Results stored in the repository can be accessed by any user with sufficient permissions using the IBM SPSS Collaboration and Deployment Services Deployment Portal interface. The jobs themselves can be triggered according to a defined schedule or in response to system events.

In addition, the scoring service of IBM SPSS Collaboration and Deployment Services allows analytical results from deployed models to be delivered in real time when interacting with a customer. An analytical model configured for scoring can combine data collected from a current customer interaction with historical data to produce a score that determines the course of the interaction. The service itself can be leveraged by any client application, allowing the creation of custom interfaces for defining the process.

The deployment facilities of IBM SPSS Collaboration and Deployment Services are designed to easily integrate with your enterprise infrastructure. Single sign-on reduces the need to manually provide credentials at various stages of the process. Moreover, the system can be configured to be compliant with Federal Information Processing Standard Publication 140-2.

System architecture

In general, IBM SPSS Collaboration and Deployment Services consists of a single, centralized IBM SPSS Collaboration and Deployment Services Repository that serves a variety of clients, using execution servers to process analytical assets.
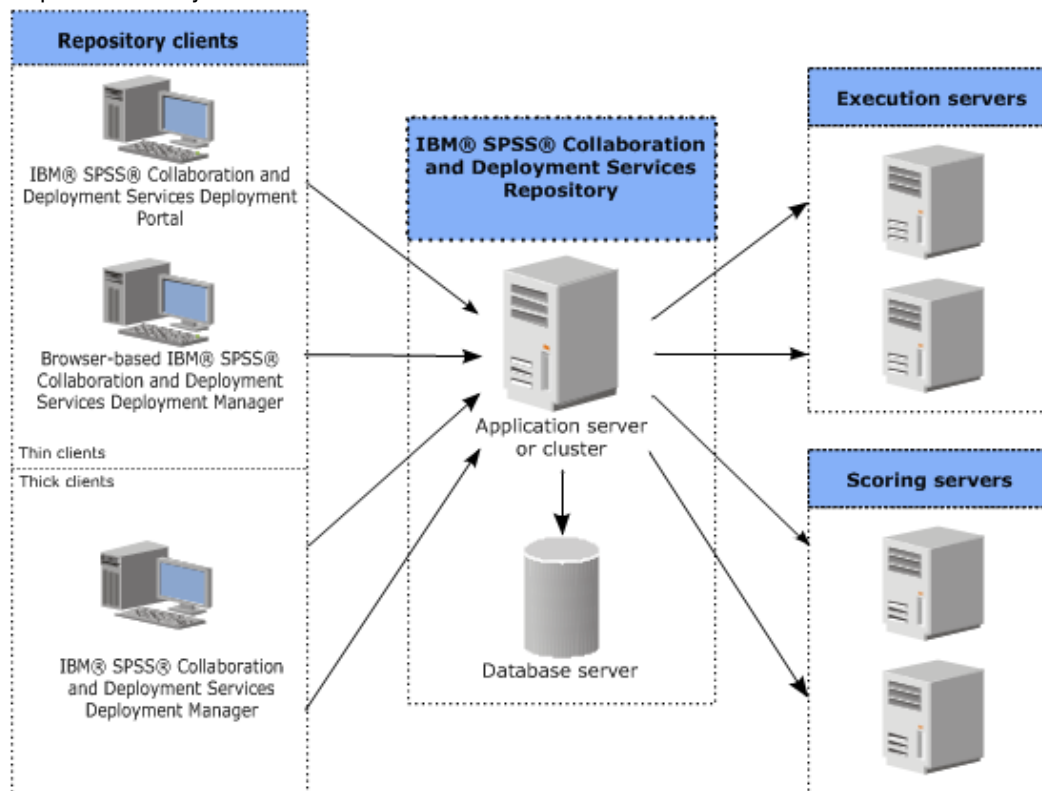
Figure 1. IBM SPSS Collaboration and Deployment Services Architecture

IBM SPSS Collaboration and Deployment Services consists of the following components:

- IBM SPSS Collaboration and Deployment Services Repository for analytical artifacts
- IBM SPSS Deployment Manager
- IBM SPSS Collaboration and Deployment Services Deployment Portal
- Browser-based IBM SPSS Deployment Manager

IBM SPSS Collaboration and Deployment Services Repository

The repository provides a centralized location for storing analytical assets, such as models and data. The repository requires an installation of a relational database, such as IBM Db2, Microsoft SQL Server, or Oracle.

The repository includes facilities for:

- Security
- Version control
- Searching
- Auditing

Configuration options for the repository are defined using the IBM SPSS Deployment Manager or the browser-based IBM SPSS Deployment Manager. The contents of the repository are managed with the Deployment Manager and accessed with the IBM SPSS Collaboration and Deployment Services Deployment Portal.

IBM SPSS Deployment Manager

IBM SPSS Deployment Manager is a client application for IBM SPSS Collaboration and Deployment Services Repository that enables users to schedule, automate, and execute analytical tasks, such as updating models or generating scores.

The client application allows a user to perform the following tasks:

- View any existing files within the system, including reports, SAS syntax files, and data files
- Import files into the repository
- Schedule jobs to be executed repeatedly using a specified recurrence pattern, such as quarterly or hourly
- Modify existing job properties
- Determine the status of a job
- Specify email notification of job status

In addition, the client application allows users to perform administrative tasks for IBM SPSS Collaboration and Deployment Services, including:

- Manage users
- Configure security providers
- Assign roles and actions

Browser-based IBM SPSS Deployment Manager

The browser-based IBM SPSS Deployment Manager is a thin-client interface for performing setup and system management tasks, including:

- Setting system configuration options
- Configuring security providers
- Managing MIME types

Non-administrative users can perform any of these tasks provided they have the appropriate actions associated with their login credentials. The actions are assigned by an administrator.

You typically access the browser-based IBM SPSS Deployment Manager at the following URL:

```
http://<host IP address>:<port>/security/login
```

Note: An IPv6 address must be enclosed in square brackets, such as [3ffe:2a00:100:7031::1].

If your environment is configured to use a custom context path for server connections, include that path in the URL.

```
http://<host IP address>:<port>/<context path>/security/login
```

IBM SPSS Collaboration and Deployment Services Deployment Portal

IBM SPSS Collaboration and Deployment Services Deployment Portal is a thin-client interface for accessing the repository. Unlike the browser-based IBM SPSS Deployment Manager, which is intended for administrators, IBM SPSS Collaboration and Deployment Services Deployment Portal is a web portal serving a variety of users.

The web portal includes the following functionality:

- Browsing the repository content by folder
- Opening published content
- Running jobs and reports
- Generating scores using models stored in the repository
- Searching repository content
- Viewing content properties
- Accessing individual user preferences, such as email address and password, general options, subscriptions, and options for output file formats

You typically access the home page at the following URL:

```
http://<host IP address>:<port>/peb
```

Note: An IPv6 address must be enclosed in square brackets, such as `[3ffe:2a00:100:7031::1]`.

If your environment is configured to use a custom context path for server connections, include that path in the URL.

```
http://<host IP address>:<port>/<context path>/peb
```

Execution servers

Execution servers provide the ability to execute resources stored within the repository. When a resource is included in a job for execution, the job step definition includes the specification of the execution server used for processing the step. The execution server type depends on the resource.

Execution servers currently supported by IBM SPSS Collaboration and Deployment Services include:

- **Remote Process**. A remote process execution server allows processes to be initiated and monitored on remote servers. When the process completes, it returns a success or failure message. Any machine acting as a remote process server must have the necessary infrastructure installed for communicating with the repository.

  Note: The IBM SPSS Collaboration and Deployment Services Remote Process Server has a default thread pool core size of 16, which allows a maximum of 16 concurrent jobs to be executed on a single remote process server. Any concurrent jobs in excess of 16 must wait in the queue until the available thread pool has free resources. To manually configure the IBM SPSS Collaboration and Deployment Services Remote Process Server thread pool core size, add the following JVM option (with a user defined value) to the remote process server's startup script: `prms.thread.pool.coresize=<user defined value>`

  For more information regarding the start-up script, see the "Starting and stopping the remote process server" section in the IBM SPSS Collaboration and Deployment Services Remote Process Server guide.

Execution servers that process other specific types of resources can be added to the system by installing the appropriate adapters. For information, consult the documentation for those resource types.

During job creation, assign an execution server to each step included in the job. When the job executes, the repository uses the specified execution servers to perform the corresponding analyses.

Scoring server

IBM SPSS Collaboration and Deployment Services Scoring Service is also available as a separately deployable application, the Scoring Server.

The Scoring Server improves deployment flexibility in several key areas:

- Scoring performance can be scaled independently from other services
- Scoring Server(s) can be independently configured to dedicate computing resources to one or any number IBM SPSS Collaboration and Deployment Services scoring configurations
- Scoring Server operating system and processor architecture does not need match the IBM SPSS Collaboration and Deployment Services Repository or other Scoring Servers
- Scoring Server application server does not need match the application server used for IBM SPSS Collaboration and Deployment Services Repository or other Scoring Servers

IBM Analytical Decision Management

IBM SPSS Collaboration and Deployment Services are a prerequisite for installing IBM Analytical Decision Management, a suite of applications for integrating predictive analytics with operational decision-making. IBM Analytical Decision Management uses high-speed scoring, master data management, and process automation facilities of IBM SPSS Collaboration and Deployment Services to optimize and automate high-volume decisions and produce improved outcomes in specific business situations.

License tracking

When you use IBM SPSS Collaboration and Deployment Services, license usage is tracked and logged at regular intervals. The license metrics that are logged are *AUTHORIZED_USER* and *CONCURRENT_USER*, and the type of metric that is logged depends on the type of license that you have for IBM SPSS Collaboration and Deployment Services.

The log files that are produced can be processed by the IBM License Metric Tool, from which you can generate license usage reports.

The license log files are created in the same directory where IBM SPSS Collaboration and Deployment Services log files are recorded (by default, `<UserProfile>\AppData\Roaming\SPSSInc \Deployment Manager`).

Chapter 2. What's new for installers

IBM SPSS Collaboration and Deployment Services Repository 8.2.2 delivers new capabilities that can help you simplify deployment of predictive analytics and manage costs.

Support for more platforms

IBM SPSS Collaboration and Deployment Services Repository 8.2.2 includes support for new versions of operating systems, including AIX 7.1 and Ubuntu 16.04 LTS s390x, application servers, databases, virtualization environments, and web browsers.

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

IBM SPSS Collaboration and Deployment Services Repository bundles the WebSphere Application Server Liberty Profile to simplify installation and deployment. You can either use this application server for a standalone or clustered installation, or provide your own application server instance.

Simplified and automated installation and configuration process for IBM SPSS Collaboration and Deployment Services Repository

A new installer offers a simplified installation and configuration process by leveraging the full functionality of IBM Installation Manager.

What's changed in this release

Oracle WebLogic Server is no longer supported.

Deprecated features

If you are migrating from an earlier release of IBM SPSS Collaboration and Deployment Services, you should be aware of the various features that have been deprecated since the last version.

If a feature is deprecated, IBM Corp. might remove this capability in a subsequent release of the product. Future investment will be focused on the strategic function listed under the recommended migration action. Typically, a feature is not deprecated unless an equivalent alternative is provided.

No features have been deprecated in this release. For reference purposes, the following table indicates features that were deprecated in recent previous versions of the product. Where possible, the table also indicates the recommended migration action.

Table 1. Features deprecated in previous versions	
Deprecation	**Recommended migration action**
Security Provider: Active Directory with local override, which supports extended groups and allowed users	Use the standard Active Directory security provider with any necessary groups added
IBM SPSS Collaboration and Deployment Services Enterprise View	Use the Analytic Data View feature
IBM SPSS Collaboration and Deployment Services Enterprise View Driver	Use the Analytic Data View feature

Table 1. Features deprecated in previous versions (continued)	
Deprecation	**Recommended migration action**
Scenario files	Scenario files (.scn) are no longer supported. Enterprise View source nodes cannot be modified in Deployment Manager. Old scenario files can be modified in IBM SPSS Modeler client and resaved as stream files. Also, scoring configurations that used a scenario file must be deleted and recreated based on a stream file.
Web Install for IBM SPSS Deployment Manager	Use the standalone installer
BIRT Report Designer for IBM SPSS	None
BIRT Report Designer for IBM SPSS viewer	None
IBM SPSS Collaboration and Deployment Services Portlet	Use the IBM SPSS Collaboration and Deployment Services Deployment Portal directly, or use the web services APIs
IBM SPSS Collaboration and Deployment Services Web Part	Use the IBM SPSS Collaboration and Deployment Services Deployment Portal directly, or use the web services APIs
Servizio di calcolo del punteggio V1 API	Servizio di calcolo del punteggio V2 API
Servizio pianificazione server	None
Servizio gestione report	None
Servizio di autenticazione `login` operation	Servizio di autenticazione `doLogin` operation
Servizio di ricerca `search` operation	Servizio di ricerca `search2.5` operation
SPSS AXIS/Castor web services client jar	Use the tools provided with the Java Runtime Environment, Integrated Development Environment, or Eclipse Web Tools Platform (WTP)
`clemrtl_setLogFile()` API function	None

Chapter 3. Installation

This chapter provides the information about installing IBM SPSS Collaboration and Deployment Services Repository. The process consists of a number of pre-installation, installation and configuration, and post-installation steps.

- **Pre-installation** steps for setting up the application environment include determining the system requirements based on the installation type and projected system use, provisioning the machine(s) to run the application server or server cluster, making sure the server(s) meet all hardware and software requirements, configuring the application server or cluster, and configuring the database. It may also be necessary to migrate the content from the previous installation to the new database using database copy tools.
- **Installation and configuration** steps include installing the application files on the host system using IBM Installation Manager and subsequent IBM SPSS Collaboration and Deployment Services Repository configuration to run with the designated application server or server cluster and the repository database.
- **Post-installation** steps include starting IBM SPSS Collaboration and Deployment Services Repository, verifying connectivity, configuring autostart, installing additional database drivers, optional components, and content adapters for other IBM SPSS products.

Note that in some environments IBM SPSS Collaboration and Deployment Services Repository deployment may also require a number of optional enterprise configuration steps related to the application security, access control, and notification capabilities.

- Email and RSS notifications. For more information, see the corresponding chapter of the administrator's guide.
- Secure repository connection. See the topic Chapter 9, "Utilizzo di SSL per proteggere il trasferimento di dati," on page 59 for more information.
- FIPS 140-2 security and secure repository database connection. See the topic Chapter 8, "FIPS 140–2 compliance," on page 57 for more information.
- Single sign-on. See the topic Chapter 6, "Single sign-on," on page 43 for more information.

Pre-installation

Before you install IBM SPSS Collaboration and Deployment Services, you must set up the resources in your environment so that the components can operate. For example, you must create a database for the content repository, and configure an application server.

Use the following checklist to guide you through the pre-installation process:

- Determine the installation type based on projected system use and the corresponding system requirements.
- Provision the machine(s) to run the application server or server cluster. Make sure the server(s) meet all hardware and software requirements.
- Verify installing user authority and host file system permissions.
- Configure the application server or cluster.
- Configure the database. If necessary, migrate the content from the previous installation to the new database using database copy tools. See the topic Chapter 4, "Migration," on page 37 for more information.

Planning your installation

Before installing IBM SPSS Collaboration and Deployment Services Repository, you must determine the installation type in order to be able to set up the application environment. IBM SPSS Collaboration and Deployment Services Repository is an enterprise-level system that requires integration with multiple IBM Corp. and third-party components and technologies. In its most basic configuration, it requires a preexisting installation of an application server to run the Web services that enable the application's functionality, and a relational database, such as IBM Db2 UDB, Oracle, or Microsoft SQL Server to store analytical artifacts and application settings.

Use the following guidelines when planning your installation:

- In operational environments, the repository must be installed on a server-grade system. See the topic "Host system requirements" on page 10 for more information. Running the repository database on a separate dedicated server may improve overall system performance.
- In enterprise environments with large processing loads (for example, producing real-time scores) and a greater number of users, scaling up with an application server cluster rather than a stand-alone application server is recommended.
- While the repository can be installed and run on a desktop workstation or a notebook for educational and demonstration purposes, it cannot be run on such systems in a production environment.

When planning your IBM SPSS Collaboration and Deployment Services Repository deployment, you must also consider the additional requirements of a production environment. For example, to enable the processing of analytical artifacts and scoring, it may be necessary to set up execution servers, such as IBM SPSS Statistics and IBM SPSS Modeler servers, which may also require dedicated hardware and network resources. To enable the email notifications functionality, an SMTP server must be available. It may also be necessary to configure repository authentication through an external directory system and single sign-on with a Kerberos server.

Host system requirements

Before installing IBM SPSS Collaboration and Deployment Services Repository, verify that the following hardware and software requirements have been met. If you are installing with an application server cluster, the requirements must be met on all nodes.

For current system requirements information, refer to the software product compatibility reports on the IBM Technical Support site at: http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html

Important: The specified amount of RAM is the minimum required to successfully install and start the repository. Depending on the types of analytical processing performed by IBM SPSS Collaboration and Deployment Services, runtime memory requirements may be significantly higher and use a large portion of RAM typically installed on a server-grade system. Note that installing repository adapters for other IBM SPSS products, such as IBM SPSS Modeler adapter, requires additional dedicated memory. It is recommended to consult the application server documentation when estimating for memory requirements for your selected application server.

If installing into WebSphere, the WebSphere profile used with IBM SPSS Collaboration and Deployment Services must be configured to run with Java 7 SDK or above. See "WebSphere" on page 12.

Requisiti aggiuntivi

IBM Installation Manager (per tutti i sistemi operativi)

IBM Installation Manager 1.9.1 o superiore deve essere installato e configurato per utilizzare un repository che contiene i file di installazione IBM SPSS Collaboration and Deployment Services

Se IBM Installation Manager non è già presente sul sistema, verrà automaticamente installato quando si avvia l'installazione di IBM SPSS Collaboration and Deployment Services. Se si dispone di una vecchia versione di IBM Installation Manager, verrà richiesto di aggiornarlo come parte dell'operazione di installazione.

Se IBM Installation Manager non viene automaticamente installato e non è presente sul sistema, scaricare ed installare IBM Installation Manager dal sito del supporto IBM Corp. (http://www.ibm.com/support). Per le informazioni sul percorso di download e sull'utente, consultare la documentazione IBM Installation Manager: http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

UNIX e Linux

• È richiesto il software X Window System Terminal per l'installazione IBM SPSS Collaboration and Deployment Services Repository basata su GUI. In alternativa, è possibile eseguire il server in modalità headless (opzione da riga di comando Java `-Djava.awt.headless=true`) oppure PJA (Pure Java AWT) Toolkit.

User and file system permissions

As a general rule, you should install and configure the repository with the same user permissions that were used to install and configure the application server. See seeing your application server vendor documentation for information about supporting installations as a non-root/non-administrator user.

The user installing the repository must have the following permissions on the host system:

• Write permissions to the installation directory and subdirectories.
• Write permissions to the deployment and configuration directories and read and execute permissions to other application server directories.
• When the repository is installed with an application server cluster, the repository installation directory on the machine hosting the management profile (WebSphere traditional profile or Liberty profile) must be shared to be available to all nodes of the cluster.

Note: When installing IBM SPSS content adapters, you must use the same user that was used for IBM SPSS Collaboration and Deployment Services Repository installation.

Important: If you install IBM SPSS Collaboration and Deployment Services Repository on Windows by using an administrator account, you will need to use the administrator privilege to run all accompanying utilities and scripts, such as the configuration utility.

Virtualization

IBM SPSS Collaboration and Deployment Services Repository or client components can be deployed into virtualized environments provided by third-party software. For example, in order to simplify deployment of a development or testing environment, a system administrator can configure a virtual server on which to install IBM SPSS Collaboration and Deployment Services. The virtual machines hosting IBM SPSS Collaboration and Deployment Services components must meet minimum system requirements. See the topic "Host system requirements" on page 10 for more information.

Assuming that the configured virtualized environment meets the minimum system requirements, no performance degradation of IBM SPSS Collaboration and Deployment Services Repository or client installations is expected. It is important to note, however, that virtualized systems might share available physical resources, and resource contention on systems with a heavy processing load can cause performance degradation of the hosted IBM SPSS Collaboration and Deployment Services installations.

Note that additional restrictions on deployment into virtualized environments may exist if the application server used to run the repository cannot be deployed into these environments.

Application server

Before you install IBM SPSS Collaboration and Deployment Services Repository, a supported application server or a server cluster must be installed and accessible.

You can use either the single-server, base IBM WebSphere Application Server included with IBM SPSS Collaboration and Deployment Services or any other supported application server. The included application server is licensed only for use with IBM SPSS Collaboration and Deployment Services Repository and cannot be used in a cluster environment. For more information about IBM WebSphere, see the product documentation in the IBM Knowledge Center

If the repository is reinstalled, re-create the application server, for example, by deploying a new WebSphere profile. Make sure that the latest versions of vendor patches are applied to application server installations. When you install the IBM SPSS Collaboration and Deployment Services Repository with an application server cluster, all cluster nodes must have the same version of the application server and run on the same operating system.

The application server must be set up with an appropriate JRE. Verify that you are running Java in 64-bit mode and that your application server is working properly in 64-bit mode before you attempt to install IBM SPSS Collaboration and Deployment Services Repository. For example, if you are using JBoss and have both a 32-bit and a 64-bit JDK installed, configure the JVM to run in 64-bit mode by specifying the -d64 option for the Java command. For deployment to WebSphere Liberty profile, the IBM JRE is bundled with IBM SPSS Collaboration and Deployment Services. For more information, see the application server vendor documentation.

Important: To support connections from web browsers that have disabled cookies, you must enable URL rewriting for your application server. In WebSphere, for example, this setting is available in the administration console at **Application servers** > *server1* > **Web container** > **Session management** > **Enable URL rewriting**. For more information, see your application server documentation.

Restriction: URL rewriting is not supported by features that were deprecated in past releases. Those features might require that cookies be enabled.

WebSphere
IBM SPSS Collaboration and Deployment Services Repository can be run with a stand-alone WebSphere server, a managed server, or a cluster.

Before installing with a stand-alone WebSphere server

- Create a new profile for every installation using the default application profile template.

Before installing with a managed WebSphere server

- Create the deployment management profile.
- Start management profile.
- Create the managed profile.
- Add a managed node to the management profile.
- Using WebSphere console, create the managed server based on the managed node.

Before installing with a WebSphere cluster

- Create the cluster and make sure it is accessible through the load balancer.

Before installing with a WebSphere Application Server Network Deployment topology

Increase the default memory configuration for the WebSphere Deployment Manager (**dmgr**) process and the WebSphere Nodeagent processes. The actual memory requirements depend on your system. For example, a minimum memory configuration would be to increase the memory as follows:

- For the WebSphere Deployment Manager process, increase the minimum heap size to 512 and the maximum heap size to 1024
- For the WebSphere Nodeagent processes, increase the minimum heap size to 256 and the maximum heap size to 512

Note: IBM SPSS Collaboration and Deployment Services must be configured to run with Java 7 SDK or later. The latest WebSphere 8.5.5 and WebSphere 9 fix packs already bundle the Java 8 SDK, and the Java 8 SDK is the only supported version of WebSphere 9. So no extra configuration is needed for Java SDK when these versions of WebSphere are used.

Configuring your profile to run with Java

Note: Since the latest fix packs of WebSphere 8.5.5 already bundle the Java SDK 8, this section only applies to WebSphere 8.5.5.8 or prior fix levels.

Before installing IBM SPSS Collaboration and Deployment Services into WebSphere, the WebSphere profile used with IBM SPSS Collaboration and Deployment Services must be configured to run with Java 7 SDK or later as follows.

1. Download and install **IBM WebSphere SDK Java Technology Edition Version 7.0** into the WebSphere 8.5.x installation. See http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/ com.ibm.websphere.installation.base.doc/ae/tins_installation_jdk7.html.

2. Once installed, configure the WebSphere profile for IBM SPSS Collaboration and Deployment Services to use the Java 7 SDK. See http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/ com.ibm.websphere.nd.multiplatform.doc/ae/rxml_managesdk.html.

3. WebSphere allows the SDK to be configured globally (all profiles) or per-profile. To set Java 7 SDK for a specific WebSphere profile:

   From the `<app_server_root>/bin` directory:

   a. Step 1: (optional) View a list of available SDK names for the product installation (confirm Java 7 SDK is present). For example:

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

   b. Step 2: Set the profile used for IBM SPSS Collaboration and Deployment Services to the Version 7.0 SDK. For example:

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

   Or to set Java 7 SDK for all WebSphere profiles (and any subsequent profiles created):

   The following example demonstrates the sequence of commands to use for listing available SDKs, changing the default SDK to a Version 7.0 SDK and, if profiles exist already, enabling the profiles to use the Version 7.0 SDK.

   a. Step 1: (optional) View a list of available SDK names for the product installation (confirm Java 7 SDK is present):

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

   b. Step 2: Set the command default to the Version 7.0 SDK:

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

   c. Step 3: Set the new profile default to the Version 7.0 SDK:

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

   d. Step 4: If profiles already exist, enable the profiles to use the Version 7.0 SDK:

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

To change federated profiles in a Network Deployment installation, the deployment manager must be running. The `managesdk` command updates the master configuration repository. After the command runs, a synchronization operation must occur before the new SDK can be used for the federated profiles.

JBoss
IBM SPSS Collaboration and Deployment Services Repository can be run only with a stand-alone JBoss server.

Before installing with JBoss

• Create a new server for every repository installation.

Note:

• It is recommended that only one instance of the server be run. If multiple instances of the repository must be set up on a single machine using JBoss, consult the JBoss documentation.
• To avoid errors at repository startup, it is recommended that JBoss application server installation path not contain any spaces, for example, as in `c:\jboss-eap-7.1`.
• If you are running JBoss in an IPv6 environment, some additional application server configuration is needed. For more information, see the Red Hat JBoss documentation.

Liberty
IBM SPSS Collaboration and Deployment Services Repository can be run only with a IBM WebSphere Liberty stand-alone server or a cluster.

Before installing with a Liberty cluster

1. Create a WebSphere Liberty cluster and make sure it's accessible through the load balancer.
2. Configure the file transfer so it writes white list entries by adding the following entries to `server.xml` for each Collective Member in the cluster:

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

3. For WebSphere Liberty cluster on Windows, set up RXA for Liberty collective operations. For more information about how to do this, see the WebSphere Liberty documentation.

Database

Before installing IBM SPSS Collaboration and Deployment Services Repository, a database must be running and accessible. A connection to the database is required in order to establish the necessary control tables and infrastructure.

The database and the IBM SPSS Collaboration and Deployment Services Repository do not need to be installed on the same server, but some configuration information is necessary to ensure connectivity. During the installation, you will be prompted for the database server name, port number, user name and password, and the name of the database to use for information storage and retrieval.

Important: You must manually create the database before installation. Any valid database name can be used, but if a previously created database does not exist, the installation will not continue.

Database permissions

The following table identifies the general database permissions that are required for a user to install, apply fixes to, update, and run IBM SPSS Collaboration and Deployment Services Repository:

Table 2. User permissions for repository maintenance tasks		
Permission	**Installation, Fix Pack Application, Migration**	**Run Time**
Alter any schema	Required	Optional
Create function	Required	Optional
Create procedure	Required	Optional
Create table	Required	Optional
Create view	Required	Optional
Create XML schema collection	Required	Optional
Connect	Required	Required
Delete	Required	Required
Execute	Required	Required
Insert	Required	Required
References	Required	Required
Select	Required	Required
Update	Required	Required

For example, when you install the repository, you need all of the permissions in the table. After installation, many of the permissions can be removed before you start and run the repository. To apply a fix pack, those permissions need to be reinstated.

The exact names of these permissions vary depending on the database, and other permissions might be needed. The following examples illustrate the permissions for specific database systems.

Example: Db2 11.1 for Linux, Windows, and UNIX

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

Note: DBADM provides explicit create schema privilege that is needed for configuring IBM SPSS Collaboration and Deployment Services Repository.

Example: Microsoft SQL Server 2016

- ALTER ANY SCHEMA
- CONNECT
- CREATE FUNCTION
- CREATE PROCEDURE

- CREATE TABLE
- CREATE VIEW
- CREATE XML SCHEMA COLLECTION
- DELETE
- EXECUTE
- INSERT
- REFERENCES
- SELECT
- UPDATE

Example: Oracle 12cR1

The following permissions are required for configuring IBM SPSS Collaboration and Deployment Services Repository with Oracle 12cR1 database:

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

The following permissions are required for starting IBM SPSS Collaboration and Deployment Services Repository with Oracle 12c database:

- CREATE SESSION
- ALTER SESSION
- SESSIONS_PER USER - must be set to value equal to, or greater than, 100.

Db2

Db2 for Linux, UNIX, and Windows

When using Db2 for Linux, UNIX, and Windows database, the default database creation parameters are not sufficient. The following additional parameters must be specified:

- UTF-8 code set
- 8 KB page sized buffer pool (in the sample script *CDS8K*) for the tables that are wider than 4 KB
- 8 KB table space using the 8 KB buffer pool
- 32 KB buffer pool (*CDSTEMP* in the sample script)
- 32 KB temporary table space for any wide result sets using the 32 KB buffer pool

An example script for creating a database named *SPSSCDS* follows. If you copy and paste the script, make sure it matches exactly the SQL as shown. Note that the script references a UNIX-style database file path which must be modified if the script is to be run on Windows. In the software downloads, the script is included as part of the documentation package.

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

Db2 on z/OS

- When using Db2 z/OS database, you must ensure that Db2 zOS subsystem is enabled for Java, Stored Procedure, Function and XML.
- To enable XQuery support, PTF UK73139 or later must be applied.

JMS message store table configuration

When IBM SPSS Collaboration and Deployment Services Repository is installed with a WebSphere Application Server, the default WebSphere JMS provider, Service Integration Bus (SIB), is configured to use the repository database as the JMS message store. When the repository is started, it will automatically create the required JMS tables in the database if they do not already exist.

When using WebSphere on z/OS with Db2, you must manually create the JMS message store tables. To create WebSphere JMS message store tables on z/OS with Db2, use WebSphere *sibDDLGenerator* command to generate the DDL and then apply the DDL to the database to create the tables. For more information about *sibDDLGenerator*, see WebSphere documentation.

Additional considerations

When running Db2 on dedicated hardware, it is recommended that Db2 Configuration Advisor be used for database Performance Management. Increasing the values of the following parameters may improve performance:

- **IBMDEFAULTBP**. The buffer pool size should be set according to the available memory and with regard to other applications running on the system.
- **NUM_IOCLEANERS**. The number of asynchronous page cleaners must at least equal the number of processors on the system.
- **NUM_IOSERVERS**. Increasing the number of I/O servers optimizes prefetching.
- **LOCKLIST**. Increasing the amount of storage for the lock list helps avoid timeouts and deadlocks during write operations.
- **MAXLOCKS**. The percentage of the *LOCKLIST* that must be filled before the database manager performs an escalation.

If Db2 is run on a shared system, changing these values must be done with consideration of available system resources, and Db2 self-tuning functionality should be considered as an alternative for managing the database performance.

Microsoft SQL Server

When using Microsoft SQL Server database:

- The *DBO* schema must be used.
- A SQL Server user is required for configuring database access. Windows-based authentication is not supported.
- IP addresses must be enabled for the Internet Protocol network protocol.
- Appropriate options must be used for processing non-Latin character sets. For example, it is recommended to use the Kana-sensitive (_KS) option to distinguish between Hiragana and Katakana Japanese characters. For more information about database collation, refer to Microsoft SQL Server documentation.
- The selected database collation must be case-insensitive (_CI).
- Snapshot isolation must be enabled for Microsoft SQL Server database. The following is a example of statements to activate snapshot isolation:

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

Oracle

Initialization parameters

When you use an Oracle database with IBM SPSS Collaboration and Deployment Services, the following parameters and configurations must be followed. Changes are made to the `init.ora` and `spfile.ora` parameter files.

Table 3. Oracle database Parameters	
Parameter	**Setting**
OPEN_CURSORS	300
NLS_CHARACTERSET	AL32UTF8
NLS_NCHAR_CHARACTERSET	AL16UTF16
SESSIONS_PER USER	Equal to, or greater than, 100

Note: Set both NLS_CHARACTERSET and NLS_NCHAR_CHARACTERSET when you create the Oracle instance.

Tip: To address case sensitivity of user login values, use parameters such as NLS_LANG, NLS_COMP, or NLS_SORT for your Oracle instance. See the Oracle documentation to determine which parameter best addresses your needs.

Oracle XDB

For an Oracle database, Oracle XDB (XML database feature) must be installed. You can verify that by querying for schema (user account) **XDB** (SELECT * FROM ALL_USERS), or by verifying that **RESOURCE_VIEW** exists (DESCRIBE RESOURCE_VIEW). The Oracle principal that is used with IBM SPSS Collaboration and Deployment Services Repository must be granted the **XDBADMIN** role.

Errori durante la migrazione da 12c a 19c

Quando si passa da dalla versione 12c alla 19c, considerare che i seguenti nove nomi di ruolo dell'utente presenti in 12c non esistono più in 19c:

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

Se si utilizzano queste regole in 12c, verranno visualizzati i seguenti errori quando si importano i dati in 19c:

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

Poiché alcuni nomi ruolo sono stati modificati in 19c, l'amministratore del database dovrebbe accertarsi che siano concesse manualmente le autorizzazioni del nuovo ruolo corrispondente prima di eseguire l'importazione. Facendo ciò, si eviterà che questi errori influenzino l'installazione e l'utilizzo di IBM SPSS Collaboration and Deployment Services.

Repository database maintenance

It is strongly recommended that IBM SPSS Collaboration and Deployment Services Repository database maintenance tasks be performed at regular intervals.

Task	Recommended schedule
Table 4. Repository database maintenance schedule	
Task	**Recommended schedule**
Backup	Daily
Update statistics	Daily
Consistency check	Weekly
Reorganize	Weekly
Rebuild	Monthly

Enabling custom JDBC URL settings

1. Create a new properties file on your local machine and add your user-defined JDBC URL to it. For example, create the file `C:\temp\db.properties` and add the following URL setting to it:

```
db2_url=spss:jdbc:spssoem:db2://${host}:${port};DatabaseName=$
{name};LobStreamingProtocol=materialize;DynamicSections=400;CreateDefaultPackage=TRUE;Authent
icationMethod=encryptedUIDPassword;ReplacePackage=TRUE%{;EncryptionMethod=SSL}
```

Notes:

- One line is allowed in the properties file (since you only have one database as your installation target).

- For the property name, you must use one of the following: `sqlserver_url`, `oracle_sid_url`, `oracle_service_url`, `db2_url`, or `db2zos_url`.

- For the property value, you must use a JDBC connection URL based on the IBM SPSS Collaboration and Deployment Services default setting (refer to the following bullet), and must include one of the following items: `url.contains("%{;EncryptionMethod=SSL}") && url.contains("$ {host}") && url.contains("${port}") && url.contains("${name}")`.

- The default JDBC URL for IBM SPSS Collaboration and Deployment Services is:

```
sqlserver_url=spss:jdbc:spssoem:sqlserver://${host}:${port};DatabaseName=$
{name};SelectMethod=cursor;MaxPooledStatements=250;allowPortWithNamedInstance=true%
{;EncryptionMethod=SSL}
db2_url=spss:jdbc:spssoem:db2://${host}:${port};DatabaseName=$
{name};LobStreamingProtocol=materialize;DynamicSections=400;BatchPerformanceWorkaround=TRUE
%{;EncryptionMethod=SSL}
oracle_sid_url=spss:jdbc:spssoem:oracle://${host}:${port};SID=${name}%
{;EncryptionMethod=SSL}
oracle_service_url=spss:jdbc:spssoem:oracle://${host}:${port};ServiceName=${name}%
{;EncryptionMethod=SSL}
db2zos_url=spss:jdbc:spssoem:db2://${host}:${port};LocationName=$
{name};LobStreamingProtocol=materialize;QueryBlockSize=1;ConcurrentAccessResolution=useCurr
entlyCommitted;AddToCreateTable=CCSID UNICODE;BatchPerformanceWorkaround=TRUE%
{;EncryptionMethod=SSL}
```

2. Before launching Installation Manager, edit the `IBMIM.ini` file in the directory `[Install Manager Install Dir]/eclipse`. Add a new line that points to the properties file you created in step 1:

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

3. Now when you launch Installation Manager and start the IBM SPSS Collaboration and Deployment Services installation, the installation process will leverage your user-defined JDBC URL settings.

Installation and configuration

Use the following checklist to guide you through installation with a stand-alone application server:

- Install the application files on the host system using IBM Installation Manager.
- Also in Installation Manager, enter the preconfigured application server and database information, then configure IBM SPSS Collaboration and Deployment Services Repository to be used with the application server and the database.

While the steps described for stand-alone server are also applicable to clustered installation, installing on a cluster topology requires additional steps. See the topic for more information.

Installazione e configurazione

I file dell'applicazione IBM SPSS Collaboration and Deployment Services Repository vengono installati sul sistema host con IBM Installation Manager. I file di installazione possono essere scaricati da IBM Passport Advantage.

Il programma di utilità di configurazione IBM SPSS Collaboration and Deployment Services Repository esegue le seguenti attività:

- Crea gli oggetti del database per il repository di contenuto
- Crea le risorse del server delle applicazioni, ad esempio, le code JMS e distribuisce i programmi Java nel server delle applicazioni
- Configura la crittografia e la sicurezza

La configurazione con un server delle applicazioni autonomo è l'ultima fase di installazione richiesta, mentre in un ambiente cluster sono necessarie fasi aggiuntive. Per ulteriori informazioni, consultare la sezione .

Prima dell'installazione e configurazione

1. Verificare che il server delle applicazioni sia installato e in esecuzione. Se si esegue una configurazione automatica, ovvero una configurazione che crea risorse distribuendole sul server delle applicazioni, è necessario che il server delle applicazioni sia nel seguente stato:

   - **WebSphere autonomo:** il server deve essere arrestato.
   - **WebSphere gestito:** interrompere il server gestito, lasciare che il server di Deployment Manager resti in esecuzione.
   - **WebSphere in cluster:** interrompere i membri del cluster, lasciare che il server di Deployment Manager resti in esecuzione.
   - **JBoss:** interrompere.
   - **Liberty autonomo:** Non è necessaria alcuna azione.
   - **Cluster Liberty:** Entrambi il controller collettivo e i membri del cluster devono essere arrestati. Le funzioni richieste dal server del repository devono essere installate su entrambi il server controller e il server dei membri.

     ```
     appSecurity-2.0
     blueprint-1.0
     concurrent-1.0
     ejb-3.2
     ejbLite-3.2
     jaxrs-2.0
     jaxws-2.2
     jca-1.7
     jdbc-4.2
     jms-2.0
     jndi-1.0
     json-1.0
     jsp-2.3
     mdb-3.2
     servlet-3.1
     ssl-1.0
     wab-1.0
     websocket-1.1
     wasJmsClient-2.0
     wasJmsSecurity-1.0
     ```

```
wasJmsServer-1.0
transportSecurity-1.0
javaMail-1.5
localConnector-1.0
ejbPersistentTimer-3.2
jaxb-2.2
restConnector-2.0
```

2. Verificare che il database sia accessibile.
3. Se si riutilizza un database del repository con WebSphere preesistente, eliminare il SIB (tabelle dell'archivio messaggi JMS).

Passi di installazione e configurazione

1. Accedere al sistema operativo come utente con il livello di autorizzazione appropriato. Per ulteriori informazioni, consultare la sezione "User and file system permissions" a pagina 11.
2. Avviare IBM Installation Manager:

   Modalità GUI:

   ```
   <IBM Installation Manager installation directory>/eclipse/IBMIM
   ```

   Modalità riga di comando:

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

3. Se non è configurato il repository di installazione, specificare il percorso del repository, ad esempio, come un percorso nel file system host, una rete o un indirizzo HTTP.

   Nota: To successfully access an installation repository, the repository location path must not contain an ampersand (&).

4. Selezionare IBM SPSS Collaboration and Deployment Services come package da installare.

   Nota: È possibile anche selezionare gli adattatori o i componenti da installare con il server IBM SPSS Collaboration and Deployment Services, ad esempio IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML, premesso che quegli adattatori o componenti siano disponibili nei repository di installazione.

5. Leggere il contratto di licenza e accettarne i termini.
6. Specificare il gruppo di package e la directory di installazione.

   • Per installare IBM SPSS Collaboration and Deployment Services Repository è necessario un nuovo gruppo di package.
   • Specificare la directory di installazione delle risorse condivise. La directory delle risorse condivise può essere specificata solo durante la prima installazione del package.

7. Selezionare la **Destinazione di distribuzione** selezionando uno dei seguenti tipi di server delle applicazioni:

   • Profilo WebSphere Tradizionale
   • Profilo WebSphere Liberty
   • JBoss EAP

8. Specificare le impostazioni del server delle applicazioni:

   • WebSphere

     – **Root profilo WebSphere Profile.** Il percorso della directory del profilo server WebSphere. Considerare che per un server o cluster gestito, è il percorso del profilo Deployment Manager.
     – **Root di installazione WebSphere** Il percorso della directory in cui è installato il server WebSphere.
     – **Topologia server** La topologia del profilo WebSphere: autonomo, gestito o cluster. Se il profilo del gestore distribuzione contiene sia server gestiti che cluster, è necessario selezionare una topologia.

- **Prefisso URL.** Per l'installazione in cluster , l'URL del programma di bilanciamento del carico o il server proxy per instradare le richieste generate dal server .
- **Server o cluster WebSphere** Il nome server o cluster WebSphere.
- **Nodo WebSphere** Per un server gestito WebSphere, il nome del nodo in cui è presente il server di destinazione. Per un cluster WebSphere, questo è il nome nodo del nodo dmgr.
- **JVM.** Percorso della directory di WebSphere JVM utilizzato dal profilo di destinazione.
- **Nome utente e password WebSphere** Solo se è abilitata la sicurezza amministrativa.

- JBoss

  - **Percorso directory server** Il percorso della directory in cui è installato JBoss.
  - **Server JBoss** Nome server JBoss. Specificare il valore `standalone`.
  - **JVM.** Percorso della directory della JVM JBoss.
  - **Prefisso URL.** L'URL per instadare le richieste generate dal server . Il prefisso URL predefinito per JBoss è *http://127.0.0.1:8080*, tranne se proprietà del server, quali indirizzo del bind o porta, hanno subito modifiche. Si precisa che *localhost* non è consentita nell'ambito del prefisso URL. Il valore del prefisso si deve poter risolvere esternamente se i client esterni si connetteranno a IBM SPSS Collaboration and Deployment Services Repository.

- Liberty

  - **Autonomo.** Il profilo WebSphere Liberty è collegato al server IBM SPSS Collaboration and Deployment Services Repository. Selezionare questa opzione se si desidera installare un nuovo profilo Liberty con il server del repository.
  - **Cluster.** Selezionare questa opzione se si desidera installare il server IBM SPSS Collaboration and Deployment Services Repository in un cluster Liberty esistente.

    Le seguenti opzioni di configurazione sono disponibili solo quando viene selezionato **Cluster**.

    - Host controller collettivo (Nome host o IP). Il nome host o l'indirizzo IP in cui è configurato il controller collettivo.
    - Porta controller collettivo. La porta HTTPS sicura del controller collettivo che è definito nel file `server.xml`.
    - Nome utente amministrativo controller collettivo. Il nome utente per l'account amministrativo del controller collettivo.
    - Password amministrativa controller collettivo. La password per l'account amministrativo del controller collettivo.
    - File truststore controller collettivo. L'ubicazione file del file truststore del controller collettivo, denominato `collectiveTrust.p12`. Questo file può essere presente nel filesystem locale oppure copiato da un altro filesystem. In Liberty 19.0.0.3 il tipo predefinito di keystore è stato cambiato da JKS a PKCS12. Se il server Liberty ha una configurazione presente che utilizza un file JKS, è necessario modificarlo nel formato PKCS12. Per informazioni sulla conversione del file keystore, vedere https://www.ibm.com/support/knowledgecenter/SS7K4U_liberty/com.ibm.websphere.wlp.zseries.doc/ae/rwlp_liberty_keystore_default.html.
    - Password truststore controller collettivo. La password per il file truststore del controller collettivo.
    - Prefisso URL. Questo è l'URL per l'instradamento delle richieste avviate dal server. Nella maggior parte dei casi, è la porta di bilanciamento del carico per la configurazione del cluster.
    - Rileva cluster. Una volta immesse tutte le informazioni del controller collettivo Liberty, fare clic su **Rileva cluster**. Verranno elencati tutti i cluster disponibili che sono preconfigurati sul server del controller collettivo. È possibile quindi selezionare il cluster in cui si prevede di installare IBM SPSS Collaboration and Deployment Services Repository Server.

9. Specificare le informazioni sulla connessione al database:

- **Tipo di database.** IBM Db2, SQL Server o Oracle.
- **Host.** Il nome host o l'indirizzo del server di database.

- **Porta.** La porta di accesso per il server di database.
- **Nome database.** Il nome del database da utilizzare per il repository di contenuti.
- **Nome servizio/SID.** Per Oracle, SID o nome servizio
- **Esegui come servizio.** Per Oracle, indica che la connessione avviene ad un servizio di database piuttosto che da un SID.
- **Nome utente.** Nome utente di database.
- **Password.** Password utente di database.

10. Se si riutilizza un database di una installazione precedente, specificare se i dati presenti devono essere conservati o eliminati.

11. Specificare le opzioni per il keystore della crittografia. Il keystore è un file crittografato che contiene la chiave per decrittografare le password utilizzate dal repository, quali la password di amministrazione del repository, la password di accesso al database e così via.

   - Per riutilizzare un keystore di una previa installazione del repository, specificarne il percorso e la password. La chiave del keystore precedente verrà estratta e utilizzata nel nuovo keystore. Si precisa che il JRE utilizzato per eseguire il server delle applicazioni deve essere compatibile con il JRE utilizzato per creare le chiavi di crittografia.
   - Se non si sta riutilizzando un keystore preesistente, specificare e confermare la password per il nuovo keystore. Il keystore verrà creato in *<repository installation directory>/keystore*.

   Importante: Se il file keystore viene perduto, l'applicazione non sarà in grado di decrittografare alcuna password diventando inutilizzabile. Sarà pertanto necessario reinstallarla. Si consiglia, pertanto, di eseguire copie di backup del file del keystore.

12. Specificare il valore della password da utilizzare per l'account utente dell'amministratore del repository integrato (*admin*). Tale password verrà utilizzata per l'accesso iniziale al repository.

13. Selezionare la modalità di distribuzione (automatica o manuale):

   - La distribuzione automatica crea le risorse del server delle applicazioni distribuendo i file dell'applicazione.
   - La distribuzione manuale genererà il file dell'applicazione e gli script di installazione nella directory di output *toDeploy/<timestamp>*. Tali risorse possono essere utilizzate in un momento successivo per la distribuzione manuale del repository. La procedura di configurazione manuale è destinata agli utenti avanzati nel caso si richieda un maggiore controllo dell'ambiente del server delle applicazioni.

14. Esaminare il riepilogo delle informazioni e procedere con l'installazione. Nel menu principale, selezionare **Installa**. I file dell'applicazione verranno installati nella directory specificata.

- Se l'applicazione è stata configurata correttamente, si può procedere con le fasi di post-installazione, quali l'avvio del repository e l a verifica della connettività. Per ulteriori informazioni, consultare la sezione "Post-installation" a pagina 27.

- Se si sceglie la modalità di distribuzione manuale, procedere con le fasi manuali.

- Se il repository viene installato con un cluster di server delle applicazioni, procedere con la configurazione dei nodi del cluster. Per ulteriori informazioni, consultare la sezione "Cluster configuration" a pagina 24.

Nota: Per completare l'operazione di configurazione potrebbero essere necessari almeno 15-30 minuti o un intervallo di tempo maggiore, in base all'hardware, alla velocità della rete, alla complessità della topologia del server delle applicazioni e così via. Se il processo di configurazione sembra non rispondere o se viene notificato un errore, esaminare i file di log in *<directory di installazione di IBM SPSS Collaboration and Deployment Services Repository/log*.

Configurazione non presidiata

La configurazione IBM SPSS Collaboration and Deployment Services Repository può essere automatizzata eseguendo IBM Installation Manager in modalità non presidiata con input proveniente da un file di risposta IBM Installation Manager. Il modello del file di risposta è simile al seguente. Considerare che

questo modello è un esempio di un'installazione per un profilo WebSphere Liberty e un database di repository DB2.

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared'/>
  </variables>
  <server>
    <repository location=xxxx'/>
    <repository location='xxxx'/>
  </server>
  <profile id='IBM SPSS Collaboration and Deployment Services 8.2.2' installLocation='/opt/IBM/
SPSS/Deployment/8.2.2/Server'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.LibertyTopologyUserData,com.ibm.spss.cds.server.v8.2.2.offering'
value='single'/>
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.2.2.offering' value='50000'/>
    <data key='user.DBName,com.ibm.spss.cds.server.v8.2.2.offering' value='cadsdb'/>
    <data key='user.DBHost,com.ibm.spss.cds.server.v8.2.2.offering' value='x.x.x.x'/>
    <data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='db2'/>
    <data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.DBPassword,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.2.2.offering'
value='false'/>
    <data key='user.DBUsername,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.DeployOptionUserData,com.ibm.spss.cds.server.v8.2.2.offering'
value='automatic deployment'/>

  </profile>
  <install>
    <!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.cds.server.v8.2.2.offering' features='deploy.liberty'/>
    <!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.modeler.adapter.18.2.2' features='main.feature,text.analytics'/>
    <!-- IBM SPSS PMML Scoring Adapter 8.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.pmml.scoring.adapter.v8.2.2' features='main.feature'/>
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='$
{sharedLocation}'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='true'/>
</agent-input>
```

Per eseguire l'installazione in modalità non presidiata:

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

Cluster configuration

IBM SPSS Collaboration and Deployment Services Repository can be deployed into an environment of clustered application servers. Each application server in the cluster should have the identical configuration for the hosted application components and the repository is accessed through a hardware or software-based load balancer. This architecture allows processing to be distributed among multiple application servers and it also provides redundancy in case of a single server failure.
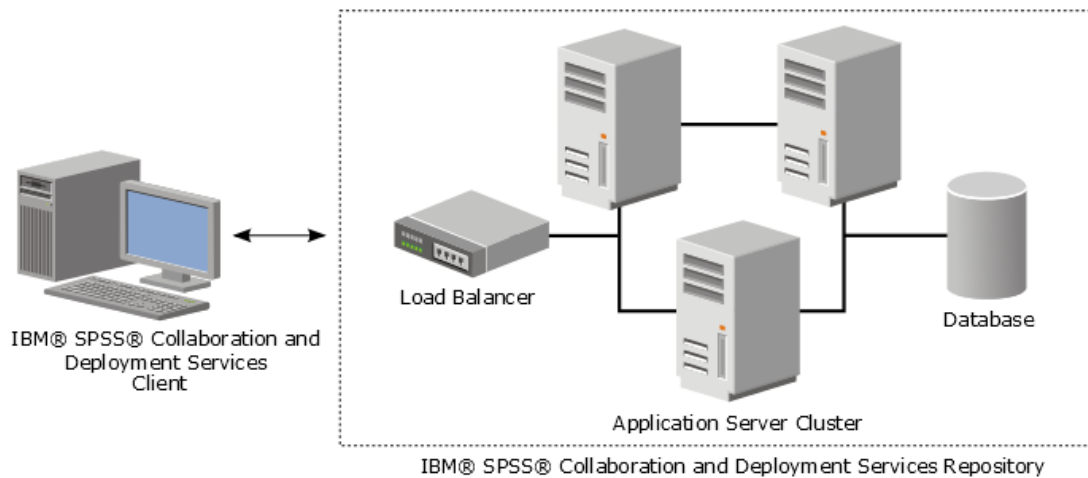
Figure 2. Clustered deployment architecture

The process of installing the repository into a cluster includes the following steps:

- Initial installation and configuration of application components on the management node of the cluster.
- Subsequent configuration of cluster nodes.

IBM SPSS Collaboration and Deployment Services Repository currently supports clustering WebSphere traditional application servers and WebSphere Liberty profiles. Follow the application server-specific instructions to complete the deployment.

Installation prerequisites

- Host system requirements must be met on all nodes of the cluster.
- All members of IBM SPSS Collaboration and Deployment Services Repository cluster must run on the same operating system as the main (management) node.
- The repository database must already exist and be accessible
- The application server topology must already exist before installing IBM SPSS Collaboration and Deployment Services Repository. It is recommended that you verify that the cluster is accessible and running properly at the load balancer address.
- The IBM SPSS Collaboration and Deployment Services Repository installation directory must be shared across all nodes in the cluster.

WebSphere cluster

1. Make sure all prerequisites have been met.
2. Perform the installation and configuration. You can choose to deploy the application either automatically or manually. See the topic "Installation and configuration" on page 19 for more information.
3. Configure the installation directory to be shared so that it is accessible to all members of the cluster.
4. Set the value of the **CDS_HOME** variable for each node.
   - Open the administrative console
   - Open the **Environment** > **WebSphere variables** section.
   - For each node in the cluster, there will be a **CDS_HOME** variable defined. Verify that the value contains the appropriate path to the shared installation directory.
5. Set the value of the **log4j.configuration** Java system property for each cluster member. This property identifies the location at which the logging system can access the logging configuration file. Typically, this property has a value of: `file://${CDS_HOME}\platform\log4j.properties`.
   - Open the administrative console

- For each server in the cluster, review the **log4j.configuration** value. This value is available at **Application servers** > *server-name* > **Process definition** > **Java Virtual Machine** > **Custom properties**, where *server-name* corresponds to the particular server.
- On the Windows operating system, if the **CDS_HOME** variable from step "4" on page 25 contains a drive letter, add a forward slash ("/") escape character to the **log4j.configuration** value. For example, the new value would be `file:///${CDS_HOME}\platform\log4j.properties`.

6. Save and synchronize your changes.
7. Make sure the IBM SPSS Collaboration and Deployment Services Repository URL Prefix configuration property value is set correctly to the URL of the load balancer. See the topic "Load balancer configuration" on page 26 for more information.
8. Start the Liberty cluster.

Load balancer configuration
A software or hardware-based load balancer must be configured for accessing the repository in a clustered environment.

WebSphere application servers provide built-in software-based load-balancer utilities(for example, IBM HTTP Server).

Important: Session affinity must be enabled for any load balancer used with IBM SPSS Collaboration and Deployment Services cluster. For more information, see load balancer vendor documentation.

Setting the URL prefix property

In a cluster environment, *URL_Prefix* repository configuration property value, used for routing server-initiated HTTP requests, must be set to the URL of the load balancer. Note that this property can be initially set when the IBM SPSS Collaboration and Deployment Services Repository configuration utility is run. See "Installazione e configurazione" on page 20 for more information.

To set/update the value of URL prefix property after repository configuration:

- Start a single cluster member.
- Open the browser-based IBM SPSS Deployment Manager by navigating to *http://<repository host>:<port number>/security/login*.
- Update the *URL_Prefix* configuration property with the URL of the load balancer for the cluster and save your changes.
- Stop the running cluster member.
- Start the cluster.

Expanding the cluster
In enterprise environments with large processing loads, it may be necessary to expand the cluster running IBM SPSS Collaboration and Deployment Services Repository by adding nodes after the initial installation.

WebSphere

1. Create additional WebSphere managed profiles and federate them to the cell. Create servers and add them to the cluster using the WebSphere console.
2. Execute the *CrtCDSresources.py* script in the */toDeploy/* directory to update the new node(s) that have been defined for the cell.

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

3. Set the value of the *CDS_HOME* variable for each node. See the topic "WebSphere cluster" on page 25 for more information.
4. Restart the cluster.

Post-installation

Use the following checklist to guide you through post-installation steps:

- Start the server and verify the connectivity. If necessary, configure server autostart.
- Install any content adapter for using IBM SPSS Collaboration and Deployment Services Repository with other IBM SPSS products such as IBM SPSS Statistics and IBM SPSS Modeler.
- If necessary, install IBM SPSS Collaboration and Deployment Services Remote Process Server and IBM SPSS Collaboration and Deployment Services - Essentials for Python. For more information, see *IBM SPSS Collaboration and Deployment Services Remote Process Server 8.2.2 Installation Instructions* and *IBM SPSS Collaboration and Deployment Services - Essentials for Python 8.2.2 Installation Instructions*.
- If necessary, change the master database password.
- If necessary, install additional JDBC drivers.
- Install IBM SPSS Collaboration and Deployment Services clients and IBM SPSS Deployment Manager. For more information, see client application installation instructions.
- Using Deployment Manager, create repository users and group and assign application permissions through roles. For more information, see *IBM SPSS Collaboration and Deployment Services 8.2.2 Administrator's Guide*.

If problems occur during post-installation steps, see *IBM SPSS Collaboration and Deployment Services 8.2.2 Troubleshooting Guide*.

Starting the repository server

The repository server can run either on a console or in the background.

Running on a console allows viewing of processing messages and can be useful for diagnosing unexpected behavior. However, the repository server typically runs in the background, handling requests from clients such as IBM SPSS Modeler or the IBM SPSS Deployment Manager.

Note: Running other applications simultaneously may reduce system performance and startup speed.

On the Windows platform, running on a console corresponds to running in a command window. Running in the background corresponds to running as a Windows service. In contrast, on a UNIX platform, running on a console corresponds to running in a shell, and running in the background corresponds to running as a daemon.

Important: To avoid permissions conflicts, the repository server must always be started under the same credentials, preferably a user with sudo (UNIX) or administrator-level (Windows) privileges.

The repository server is started by starting the application server. This can be accomplished with the scripts provided with the repository server installation or native application server administration tools. For more information, see the application server vendor documentation.

WebSphere

Use WebSphere administration tools. For more information, see WebSphere documentation.

WebSphere Liberty stand-alone

By default, the bundled Liberty profile uses 9080 for the HTTP endpoint and 9443 for the HTTPS endpoint. If you want to change these port numbers, update the `server.xml` file in the following directory:

```
<repository installation directory>/wlp/usr/servers/cdsServer
```

If you use the default port numbers, make sure the port number isn't already being used by other applications before you start the server. Use the following scripts with the repository installation:

```
<repository installation directory>/bin/startserver.bat
```

```
<repository installation directory>/bin/startserver.sh
```

During the WebSphere Liberty start up process, the Liberty profile will start first and then the application will be deployed. To check repository server status, see the `cds.log` file in `<repository installation directory>/wlp/usr/servers/cdsServer/`.

WebSphere Liberty cluster

Before starting the repository server that was deployed to your WebSphere Liberty cluster, deploy related configuration files. These files are required by Liberty for collective members in the cluster, and they include the configuration files in `server.xml` in each collective member. Before deploying the configuration files:

1. Configure the installation directory to be shared and make sure it's accessible to all members of the cluster.
2. Ensure `{wlp.usr.dir}` and `{server.config.dir}` are added to the write white list for each collective member in the cluster. You need to do this in `server.xml` for the collective controller. See your WebSphere Liberty documentation for details.
3. For WebSphere Liberty on Windows, make sure RXA is set up correctly.
4. Start the collective controller and all collective members in the cluster.

Use the following scripts with the repository server installation:

```
<repository installation directory>/bin/deployUtility.bat -cads_home ${CDS_HOME}
```

```
<repository installation directory>/bin/deployUtility.sh -cads_home ${CDS_HOME}
```

where `${CDS_HOME}` is the shared location of IBM SPSS Collaboration and Deployment Services system files. This location must be accessible to all the collective members by using file sharing on Windows or NFS on Linux/UNIX.

Then restart all collective members in the cluster to load the newly deployed configuration files.

JBoss

Use the following scripts with the repository server installation:

```
<repository installation directory>/bin/startserver.bat
```

```
<repository installation directory>/bin/startserver.sh
```

Alternatively, you can also use JBoss administration tools to start the server. For more information, see JBoss documentation.

Verifying connectivity

You can verify that IBM SPSS Collaboration and Deployment Services Repository is running by accessing browser-based IBM SPSS Deployment Manager using one of the following supported Web browsers:

- Internet Explorer 10 or above
- Firefox 48 ESR or above
- Safari 5 or above

To access browser-based IBM SPSS Deployment Manager

1. Navigate to the login page at *http://<repository host>:<port number>/security/login*.
2. Specify the administrator login credentials. The credentials are established during repository configuration.

Managing the database password

The database password provided during IBM SPSS Collaboration and Deployment Services Repository configuration is stored as part of the data source definition in the application server settings. Additional steps may be required to ensure the database password security.

Testing the database connection

The IBM SPSS Collaboration and Deployment Services Repository database connection can be tested using the data source management facilities in the application server administrative console.

Application server	Data source object name
WebSphere Traditional	CDS_DataSource
WebSphere Liberty	CDS_DataSource
JBoss	jdbc/spss/PlatformDS

JAAS object security

The credentials for IBM SPSS Collaboration and Deployment Services data source created in the application server are persisted as a JAAS object.

Important: When the repository is configured on WebSphere application server using either automatic deployment (with IBM Installation Manager) or with scripts generated by the configuration utility, the password is passed to the application server as clear text and then persisted according to the application server settings. Although the default WebSphere settings provide for storing passwords in encrypted form, it may be necessary to verify that the password is not stored as clear text. See application server documentation for additional information about password security.

Changing the database password

For security reasons, it may be necessary to change the database password following IBM SPSS Collaboration and Deployment Services Repository installation. In such cases, the stored database password can be changed by using IBM SPSS Collaboration and Deployment Services Password Utility.

To run the password utility:

1. Shut down the application server that hosts IBM SPSS Collaboration and Deployment Services.
2. Execute

   Windows:

   ```
   <repository installation directory>/bin/cliUpdateDBPassword.bat
   ```

   UNIX:

   ```
   <repository installation directory>/bin/cliUpdateDBPassword.sh
   ```

   System i:

   ```
   <repository installation directory>/bin/cliUpdateDBPassword.qsh
   ```

3. Start the application server that hosts IBM SPSS Collaboration and Deployment Services.
4. Specify and confirm the new password using the command prompt.

The password can also be changed by modifying the application server settings. Note that the password is stored in encrypted form, therefore the new password can be converted to an encrypted string by running `cliEncrypt.bat/cliEncrypt.sh` with the password as command line argument.

JDBC drivers

Adding driver support to IBM SPSS Collaboration and Deployment Services Repository

IBM SPSS Collaboration and Deployment Services includes a set of IBM Corp. JDBC drivers for all major database systems: IBM Db2, Microsoft SQL Server, and Oracle. These JDBC drivers are installed by default with the repository.

If IBM SPSS Collaboration and Deployment Services does not include a driver for a needed database, you can update your environment to include a third-party driver for the database. Third party drivers can be used by augmenting your repository installation with the driver files.

Depending on the application server, the directory location of the JDBC drivers is as follows:

• WebSphere: `<WebSphere installation directory>/lib/ext`

For JBoss, you need to install the JDBC driver as a JBoss core module and register the module as global. For details, see the JBoss documentation.

Note that for Netezza, the version 5.0 driver should be used to access both version 4.5 and 5.0 databases.

Adding driver support to client applications

To add a JDBC driver to the IBM SPSS Deployment Manager:

1. Close the client application if it is running.
2. Create a folder named JDBC at the root level of the client installation directory.
3. Place the driver files in the JDBC folder

After adding the driver files to your environment, the driver can be used in a data source definition. In the JDBC Name and URL dialog box, type the name and URL for the driver. Consult the vendor documentation for the driver to obtain the correct class name and URL format.

IBM SPSS products compatibility

IBM SPSS Collaboration and Deployment Services Repository functionality can be extended to support other IBM SPSS applications by installing additional content adapter packages.

For current compatibility information, refer to the software product compatibility reports on the IBM Technical Support site at: http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html

Note:

• For some products, patches may need to be applied. Check with IBM Corp. support to determine that correct patch level.

• You must verify that the installation and runtime requirements for IBM SPSS applications (for example, application servers and databases) are compatible with the requirements for IBM SPSS Collaboration and Deployment Services Repository. For detailed information, consult Software product compatibility reports and the documentation for individual IBM SPSS products.

IBM SPSS Statistics client and IBM SPSS Modeler client are not required for use of IBM SPSS Collaboration and Deployment Services. However, these applications offer interfaces for using the IBM SPSS Collaboration and Deployment Services Repository to store and retrieve objects. The server versions of these products are required for jobs containing IBM SPSS Statistics or IBM SPSS Modeler objects to be executed.

By default, the repository is installed without adapters for other IBM SPSS products and users must install the adapter packages corresponding to their versions of products. The packages are included on the products' distribution media.

Note that you should avoid storing IBM SPSS product objects in the repository until you first install the required adapter packages. If you do so, the object will not be a recognized type even after installing the adapter packages and you will need to delete the objects and add them to the repository again. For

example, if an IBM SPSS Modeler stream is stored in the repository before the IBM SPSS Modeler adapter is installed, the MIME type will not be known and will instead be set to a generic type, resulting in an unusable stream file.

Dockerized installation

A dockerized Repository Server installation is available for easier deployment. You can load the predefined IBM SPSS Collaboration and Deployment Services image. In a future release, a fully functioned docker based cluster support will be added, which will give you high availability, load balancing, etc.

The dockerized IBM SPSS Collaboration and Deployment Servicesdelivery package can run in various docker environments, and provides the full Repository Server functional via a container method.

Prerequisites

If you want to run the deodorized Repository Server, ensure you meet the following prerequisites.

- The docker engine must be properly installed and configured on the target operating system. Refer to the docker vendor documentation. Supported operating systems are Windows x64, RedHat x64, and Ubuntu x64.
- The docker daemon must be in a running state.
- For the docker engine hosted on Windows x64, the docker daemon must be running in *Linux container* mode.
- Make sure there is at least 20GB free disk space to load the docker image for the Repository Server.
- Make sure you have a prepared IBM SPSS Collaboration and Deployment Services Database, either initialized from a new database or migrated from a previous release, or from another instance of a working IBM SPSS Collaboration and Deployment Services Database. For information about Repository database initialization and migration, see **Dockerized preparation** later in this section.

Typical use case

1. Run the IBM SPSS Collaboration and Deployment Services Dockerize Preparation Toolkit to initialize a fresh new database or perform a migration from a 8.1.1 Repository database. See the following section **Dockerize preparation** for details.
2. Download the IBM SPSS Collaboration and Deployment Services docker package (.zip file) from Passport Advantage and extract it to the local file system.
3. Make a copy of the keystore folder, which is generated or reused in step 1, in the unzipped folder from step 2.
4. Edit the file cads_db.env with your Repository database information. The contents of this file is as follows:

```
#CaDS Repository Database configuration file. Enter your database information.
#Examples:
#DB_TYPE=db2
#DB_HOST=8.8.8.8
#DB_PORT=50000
#DB_NAME=cadsdb
#DB_USERNAME=dbuser
#Additional Notes:
#DB_TYPE can be db2, sqlserver, oracle_sid, db2zos, or oracle_service
DB_TYPE=
DB_HOST=
DB_PORT=
DB_NAME=
DB_USERNAME=
```

5. Depending on your OS, run `cdsServer.sh` or `cdsServer.bat` to conduct operations such as checking the environment and loading the image and startup container. Detailed usage is as follows:

```
./cdsServer.sh

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

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

check
    check the availability of docker engine

load
    load CaDS docker image tarball to local

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

list
    list all the containers of CaDS

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

remove
    remove all the stopped CaDS containers

help
    print all the command usage
```

Dockerized preparation

The IBM SPSS Collaboration and Deployment Services Dockerize Preparation Toolkit helps you initialize or migrate a prepared Repository database for use with the dockerized Repository Server.

1. Run the toolkit in GUI mode:

```
<IBM Installation Manager installation directory>/eclipse/IBMIM
```

Or run the toolkit in Console mode:

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

2. If the installation repository is not configured, specify the repository path (for example, as a location on the host file system, the network, or an HTTP address).
3. Select IBM SPSS Collaboration and Deployment Services as the package to be installed. You can also select adapters or components to be installed with the server, such as the IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML, provided those adapters or components are available in the installation repositories.
4. Read the license agreement and accept its terms.
5. Specify the package group and the installation directory. A new package group is required for this installation.
6. Specify the installation directory for shared resources. You can specify the shared resources directory only the first time that you install a package.
7. Select **Dockerize Preparation** as the Deployment Target.
8. Specify database connection information:

   - **Database type.** IBM DB2, SQL Server, or Oracle.
   - **Host.** The host name or address of the database server.
   - **Port.** The access port for the database server.
   - **Database name.** The name of the database to use for the Repository.

- **SID/Service Name.** For Oracle, the SID or service name.
- **User name.** Database user name.
- **Password.** Database user password.
- If reusing a database from a prior installation, specify whether existing data should be preserved or discarded.

9. Specify options for the encryption keystore. The keystore is an encrypted file that contains the key for decrypting the passwords used by the Repository, such as the Repository administration password and the database access password.

- To reuse a keystore from an existing Repository installation, specify the path and password to the keystore. The key from the old keystore will be extracted and used in the new keystore. Note that the JRE used to run the application server must be compatible with the JRE that was used to create the encryption keys.
- If you are not reusing an existing keystore, specify and confirm the password to the new keystore. The keystore will be created in `<repository installation directory>/keystore`.

10. Specify the password to use for the built-in Repository administrator user account (admin). This password is used when logging on to the Repository for the first time.

11. Click **Install**.

Running the toolkit in silent mode

You can automate the toolkit by running IBM Installation Manager in silent mode with input from an IBM Installation Manager response file. The template for the response file is similar to the following:

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared'/>
  </variables>
  <server>
    <repository location=xxxx'/>
    <repository location='xxxx'/>
  </server>
  <profile id='IBM SPSS Collaboration and Deployment Services 8.2.2' installLocation='/opt/IBM/
SPSS/Deployment/8.2.2/Server'>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.2.2.offering' value='50000'/>
    <data key='user.DBName,com.ibm.spss.cds.server.v8.2.2.offering' value='cadsdb'/>
    <data key='user.DBHost,com.ibm.spss.cds.server.v8.2.2.offering' value='x.x.x.x'/>
    <data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='db2'/>
    <data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.DBPassword,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
    <data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.2.2.offering' value='false'/>
    <data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.2.2.offering'
value='false'/>
    <data key='user.DBUsername,com.ibm.spss.cds.server.v8.2.2.offering' value='xxxx'/>
  </profile>
  <install>
    <!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.cds.server.v8.2.2.offering' features='deploy.docker'/>
    <!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.modeler.adapter.18.2.2' features='main.feature,text.analytics'/>
    <!-- IBM SPSS PMML Scoring Adapter 8.2.2.0 -->
    <offering profile='IBM SPSS Collaboration and Deployment Services 8.2.2'
id='com.ibm.spss.pmml.scoring.adapter.v8.2.2' features='main.feature'/>
  </install>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='$
{sharedLocation}'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='true'/>
</agent-input>
```

To run the installation in silent mode:

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

Important: Back up the keystore file. If you lose the keystore file, the Repository Server will not be able to decrypt any passwords and will be come unusable. This requires reinstallation.

Additional migration considerations

IBM SPSS Collaboration and Deployment Services Repository migration preserves the contents and configuration settings of an existing Repository.

For the dockerized Repository, the following migration scenario is supported.

- Migration from an earlier version of the Repository database. For IBM SPSS Collaboration and Deployment Services 8.2.2, migration from version 8.2.1 is supported.
- Migration from a different host, application server, or database server. Dockerized IBM SPSS Collaboration and Deployment Services Repository Server can connect to an existing 8.2.2 Repository database.

Important: Due to the usage of a keystore, the JRE before and after the migration must be the same IBM JRE.

Notes

- The `url_prefix` setting is the URL for routing server-initiated requests. The prefix value must be externally resolvable if external clients will connect to the Repository. Due to the complex configuration scenario of docker networking, sometimes this setting needs to be manually configured.
  - For a single container instance of the Repository, set `url_prefix` to the host name where the docker daemon is hosted and the port that the container exposes.
  - For clustering container instances (Swam, Kubernetes, etc.), set `url_prefix` to the reverse proxy server address (Ngnix, for example).
- The dockerized 8.2.2 Repository Server already has the 18.2.2 Modeler Adapter installed and configured. No extra configuration is needed for the adapter.
- The timezone for each container may differ from the docker daemon. This is a limitation of docker itself. You can update the timezone settings by manually changing `docker run` in the file `cdsServer.bat/cdsServer.sh`. For example: `docker run -e TZ=Europe/Amsterdam`
- Known issues:
  - For clustering mode, the scoring configuration may not be synchronized among containers properly. If you encounter this issue, restart the container. Then synchronization should be invoked during startup.
  - SSL is not enabled by default. To use SSL, you may need to import and configure the SSL certificate to the container manually

Uninstalling

In the event that an installation is no longer required, the current version can be uninstalled.

To uninstall the repository:

1. Stop the repository.
2. If the Manual option was used when configuring the repository, undeploy the repository resources from the application server:
   - WebSphere stand-alone server

     ```
     <WAS profile root>/bin/wsadmin -lang jython -connType none -f
     <repository installation directory>/toDeploy/<time stamp>/delCDS.py
     ```

- WebSphere managed server or cluster

```
<WAS profile root>/bin/wsadmin -lang jython -f
<repository installation directory>/toDeploy/<time stamp>/delCDS.py
```

- JBoss

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

3. To delete all data in the repository database, open *<repository installation directory>/uninstall/uninstall.properties* configuration file and set the `cds.uninstall.remove.user.data property` to `true`. Note that some data may still remain in the database after IBM Installation Manager uninstall is run, and it must be deleted manually.

   Important: Do not perform this step if you plan on using the repository again for new installs, or need to preserve the audit or logging data. You should also consider using the database vendor tools to create a database backup before using this option.

4. Run IBM Installation Manager (GUI or command line), select the option to uninstall IBM SPSS Collaboration and Deployment Services, and follow the prompts. IBM Installation Manager can also be run in the silent mode. For more information, see the IBM Installation Manager documentation: http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome.

5. Manually delete the root installation directory for the repository.

   Important: If you intend to reuse repository data, it is recommended to save the keystore file, which can be found in *<repository installation directory>/keystore*.

Chapter 4. Migration

IBM SPSS Collaboration and Deployment Services Repository migration preserves the contents configuration settings of an existing repository including the following:

- Repository files and folder structure
- Scheduling and notification components
- Notification templates
- Local users
- Locally defined overrides of remote directory user lists and groups
- Role definitions and membership
- User preferences
- Icons

The following migration scenarios are supported:

- Migration from an earlier version of the repository.
- Migration to a different host, application server, or database server.

The following paths can be used for migration:

- Installation with a copy of the repository database. This is the recommended way to migrate.
- Installation of the repository with an existing repository database.

Before selecting a migration path, review this entire chapter, including the information on additional migration considerations.

Regardless of the selected migration path, you must follow these guidelines:

- IBM SPSS Collaboration and Deployment Services Repository application files must be installed in a different location from the original installation. Do not overwrite the files in the original location.
- A new application server instance must be created. Do not reuse the profile (WebSphere) or server (JBoss) already used to run the old instance of the repository.
- Migration process does not preserve repository package configuration, so any additional packages for IBM SPSS products such as IBM SPSS Modeler and IBM SPSS Statistics must be reinstalled. the packages in the target instance must be at the same level or higher than the packages in the source repository; and they should reference the DB table for that. The packages must be at a level that is compatible with the given target version of IBM SPSS Collaboration and Deployment Services. See the topic " IBM SPSS products compatibility" on page 30 for more information.

  Note: The packages in the target instance must be at the same version level or higher than the packages in the source instance. The information about installed packages and their versions can be found in the SPSSSETUP_PLUGINS table of the source instance database.

For IBM SPSS Collaboration and Deployment Services 8.2, migration from version 8.1.1 is supported.

Installing with a copy of the repository database

Using a copy of an existing repository database allows the existing instance to remain online until the new installation is ready to go live.

This procedure is for migration with a copy of the repository database where the source and target databases are the same, for example, Db2 to Db2. For information about switching database systems, see "Migrating to a different database" on page 38

- Make a copy of the existing repository database. The database copy can be performed using the database vendor or third-party tools.
- Run IBM SPSS Collaboration and Deployment Services configuration utility and point it to the new copy of the repository database. Make sure that the Preserve Existing Data option is selected to retain all existing data.
- Reinstall additional packages.

Installing with an existing repository database

You can also upgrade to IBM SPSS Collaboration and Deployment Services Repository by installing the system with an existing repository database.

- Stop the repository.
- Backup the existing repository database.
- Install IBM SPSS Collaboration and Deployment Services and run the configuration utility. Make sure that the Preserve Existing Data option is selected to retain all existing data.
- Reinstall additional packages.

Migrating to a different database

Migrating to a different database can include moving to a different database vendor (for example, SQL Server to IBM Db2 or Oracle to Db2), or migrating to a database on a different operating system (for example from Db2 for i to Db2 for Linux, UNIX, and Windows).

Transferring repository objects to a different vendor's database can be accomplished by creating a copy of the old database in the new database.

- Create the target database following the instructions provided with the release of IBM SPSS Collaboration and Deployment Services you are migrating from.
- Use the database vendor tools to move the data from the source repository database to the target repository database. The database should already be configured, so it is only necessary to move the data in the IBM SPSS Collaboration and Deployment Services tables. See the database vendor documentation for more information.
- Make a copy of the keystore file that is used by the source repository database.
- Install IBM SPSS Collaboration and Deployment Services and run the configuration utility.
  - Specify the target database as the repository database
  - Make sure the Preserve Existing Data option is selected to retain all existing data
  - When prompted for the keystore, select the copy of the keystore file to be used for the new instance.
- Reinstall any additional packages.

Note that because of differences between database environments and vendor copy tools, such as Db2 backup, MS-SQL Server backup, or Oracle RMAN, you must verify during migration that the following database features are supported by the tool you have selected:

- XML tables (*SPSSDMRESPONSE_LOG* and *SPSSSCORE_LOG*)
- Binary data/BLOB, CLOB
- Special date formats

For example, Oracle 12cR1 Data Pump does not support XML tables. Therefore, it can be used for restoring all repository tables except the two XML tables. The XML tables can be migrated using Oracle Export. Review all database vendor requirements, like XML schema registration in MS SQL Server and Oracle. We recommend consulting your database administrator before migrating your database.

Errori durante la migrazione da 12c a 19c

Quando si passa da dalla versione 12c alla 19c, considerare che i seguenti nove nomi di ruolo dell'utente presenti in 12c non esistono più in 19c:

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

Se si utilizzano queste regole in 12c, verranno visualizzati i seguenti errori quando si importano i dati in 19c:

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

Poiché alcuni nomi ruolo sono stati modificati in 19c, l'amministratore del database dovrebbe accertarsi che siano concesse manualmente le autorizzazioni del nuovo ruolo corrispondente prima di eseguire l'importazione. Facendo ciò, si eviterà che questi errori influenzino l'installazione e l'utilizzo di IBM SPSS Collaboration and Deployment Services.

Additional migration considerations

Depending on your setup, additional tasks may be required for a successful migration of the following:

- Passwords
- JMS data store
- Notification templates

When planning the migration, note that some of these tasks may need to be performed before the configuration utility is run with an existing database or a database copy.

Migrating passwords

When migrating to a new IBM SPSS Collaboration and Deployment Services instance, it is best to use a Java environment from the same vendor and with the same bit size (32-bit or 64-bit) as the original installation. This is because the passwords that are stored in the repository are encrypted based on a keystore key that is provided by the Java runtime. A different Java bit size or vendor implementation will have a different keystore key which will not be able to decrypt the passwords correctly. In some cases, it is necessary to change Java vendors or bit size (for example, when moving from JBoss to WebSphere).

If Java encryption used while installing the repository over an existing database is different from the encryption used by the original instance (for example, IBM Java encryption versus Sun Java encryption), credentials passwords will not be migrated and the configuration utility will report failure. However, the repository can be still started, and you can use IBM SPSS Deployment Manager to manually change credentials passwords. The export/import utility will migrate passwords, but when reusing an existing database, the export must be performed from the source installation before importing the credential resources to the target installation.

If you need to use a different Java environment, you can replace the passwords in credential resource definitions and IBM SPSS Modeler job steps after IBM SPSS Collaboration and Deployment Services Repository configuration:

• Export the jobs and credential resource definitions from the source repository instance and import them into the target repository using IBM SPSS Deployment Manager.

or

• Manually update each password in job steps and each credential in the target repository using IBM SPSS Deployment Manager.

JMS store migration on WebSphere

When IBM SPSS Collaboration and Deployment Services Repository is installed with a WebSphere Application Server, the default WebSphere JMS provider, Service Integration Bus (SIB), is configured to use the repository database as the JMS message store. When the repository is started, it will automatically create the required JMS tables in the database if they do not already exist. Note that when using WebSphere on z/OS with Db2, you must manually create the JMS message store tables.

When using database copy to migrate the content of a repository to a new instance running on WebSphere, you must delete the JMS message store tables (the tables with the names starting with SIB*) from the database before you start IBM SPSS Collaboration and Deployment Services. The tables will then be automatically created, with the exception of WebSphere on z/OS.

To manually create WebSphere JMS message store tables on z/OS with DB2, use the WebSphere *sibDDLGenerator* command to generate the DDL and then apply the DDL to the database to create the tables. For more information about *sibDDLGenerator*, see WebSphere documentation.

Migrating notification templates

To preserve the customizations made to notifications templates in an existing repository, you must copy the templates from *<repository installation directory>/components/notification/templates* to the same directory of the new installation, after the new installation has been initially configured. For more information about notifications templates, see *IBM SPSS Collaboration and Deployment Services Repository 8.2.2 Administrator's Guide.*

Chapter 5. Package management

Updates, optional components, and content adaptors for IBM SPSS products are installed into the IBM SPSS Collaboration and Deployment Services Repository server as packages with IBM Installation Manager.

For details, see the installation instructions for individual components.

You can also use IBM SPSS Collaboration and Deployment Services Package Manager utility for troubleshooting IBM SPSS Collaboration and Deployment Services package configuration and installing additional components, for example, custom content adapters and security providers.

Installing packages

IBM SPSS Collaboration and Deployment Services Package Manager is a command line application. It can also be called in batch mode by other applications to install their package files into the repository.

If IBM SPSS Collaboration and Deployment Services Repository was initially deployed automatically, during package installation the application server must be in the following state:

- JBoss: Stopped
- Liberty: Stopped

The user must have administrator-level privileges to be able to install packages.

To prevent the newer version of a package from being overwritten by an older version, package manager performs a version check. Package manager also checks for prerequisite components to ensure that they are installed and their versions are equal to or newer than the required version. It is possible to override the checks, for example, to install an older version of the package.

Note: Dependency checks cannot be overridden if package manager is called in batch mode.

To install a package

1. Navigate to *<repository installation directory>/bin/*.
2. Depending on the operating system, execute *cliPackageManager.bat* on Windows or *cliPackageManager.sh* on UNIX.
3. When prompted, enter the user name and password.
4. Type the install command and press `Enter`. The command must include the `install` option and the path of the package in quotes, as in the following example:

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

   To install multiple packages at the same time, enter multiple package names separated by a space, for example:

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

   An alternative way to install multiple packages is to use the `-dir` or `-d` parameter with the path of a directory containing the packages to install

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

   In the case of failed dependencies or version checks, you will be brought back to the main package manager prompt. To install ignoring non-fatal failures, rerun the install command using the `-ignore` or `-i` parameter.
5. When the installation is completed, use `exit` command to exit package manager.

To display more command line install options, type `help` and press `Enter` key. The options include:

- `info "<package path>"`: Display information for a specified package file.
- `install "<package path>"`: Install the specified package files into the repository.
- `tree`: Display installed package tree information.

Silent mode

To automate package installation, IBM SPSS Collaboration and Deployment Services Package Manager can be run in silent mode:

```
<repository installation directory>/bin/cliPackageManager[.sh]
-user <administrator> -pass <administrator password>
install <package path> [<additional_package_path>]
```

Logging

IBM SPSS Collaboration and Deployment Services Package Manager logs (main and Ant log) can be found in *<repository installation directory>/log*.

Chapter 6. Single sign-on

IBM SPSS Collaboration and Deployment Services provides single sign-on capability by initially authenticating users through an external directory service based on the *Kerberos* security protocol, and subsequently using the credentials in all IBM SPSS Collaboration and Deployment Services applications (for example, IBM SPSS Deployment Manager, IBM SPSS Collaboration and Deployment Services Deployment Portal, or a portal server) without additional authentication.

Note: Single sign-on is not allowed for browser-based IBM SPSS Deployment Manager.
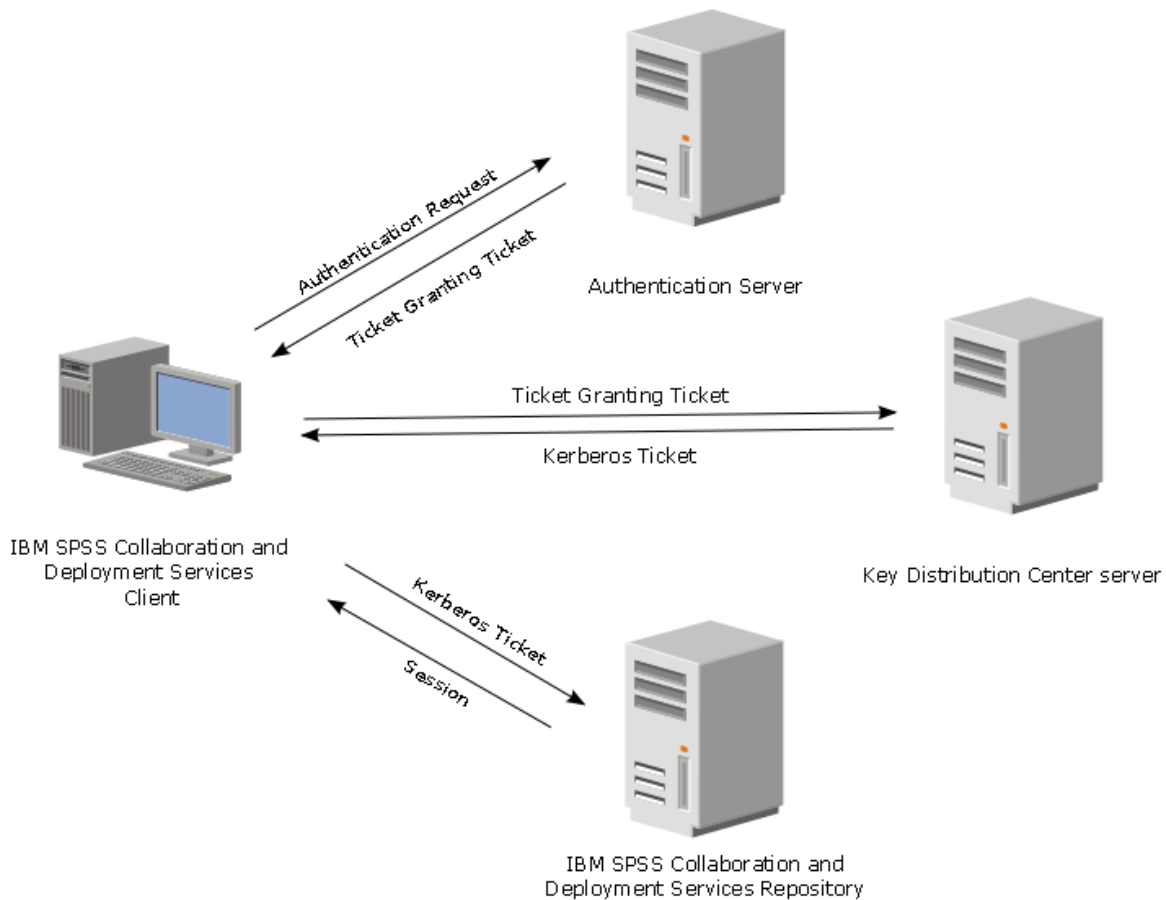
Figure 3. IBM SPSS Collaboration and Deployment Services SSO architecture

For example, when IBM SPSS Collaboration and Deployment Services is used in conjunction with Windows Active directory, you must configure the *Kerberos Key Distribution Center (KDC)* service to enable single sign-on. The service will supply session tickets and temporary session keys to users and computers within an Active Directory domain. The KDC must run on each domain controller as part of Active Directory Domain Services (AD DS). When single sign-on is enabled, IBM SPSS Collaboration and Deployment Services applications log into a Kerberos domain and use Kerberos tokens for web services authentication. If single sign-on is enabled, it is strongly recommended that SSL communication be configured for the repository.

Desktop client applications, such as Deployment Manager, create a Java subject and then establishes a GSS session with the repository using the subject context. The repository returns a Kerberos service ticket to the client when the GSS context is established. Thin client applications, such as Deployment Portal, also obtains a Kerberos service ticket from the repository. However, thin clients first perform HTTP-based cross-platform authentication via the Negotiate Protocol. Both desktop and thin client

applications require that you first log on to a Kerberos domain, for example, to your Microsoft Active Direcory/Windows domain.

Single sign-on configuration in IBM SPSS Collaboration and Deployment Services includes the following steps:

- Directory system setup.
- Configuring the directory system as an IBM SPSS Collaboration and Deployment Services *security provider* using the Server Administration tab of IBM SPSS Deployment Manager. For more information, see IBM SPSS Collaboration and Deployment Services administrator documentation.
- Kerberos Key Distribution Center server configuration. Credential delegation must be enabled for the Kerberos Service Principal on the Kerberos Key Distribution Center server. The procedure for enabling credential delegation will be different depending on your directory server and Kerberos environment.
- Configuring Kerberos Key Distribution Center server as an IBM SPSS Collaboration and Deployment Services single sign-on provider using the Server Administration tab of IBM SPSS Deployment Manager. For more information, see IBM SPSS Collaboration and Deployment Services administrator documentation.
- Configuring the application server for single sign-on.
- For Windows client systems, the registry must be updated for Kerberos LSA access.
- Depending on the application server used with the repository, it may be necessary to update the application server configuration.
- Windows client systems must have `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\` registry value updated. See the topic "Updating Windows registry for single sign-on" on page 48 for more information.
- For thin-client access to the repository (for example, with IBM SPSS Collaboration and Deployment Services Deployment Portal), the Web browser must have Simple and Protected GSS-API Negotiation (SPNEGO) enabled.

Additional configuration step are also required to enable the repository Server Process Credential. See the topic "Server Process Credential configuration" on page 49 for more information.

Directory configuration for single sign-on

IBM SPSS Collaboration and Deployment Services single sign-on requires an external directory to be set up. Directory authentication for IBM SPSS Collaboration and Deployment Services single sign-on can be based on the following directory systems:

- OpenLDAP directory
- Microsoft Active Directory

OpenLDAP

The overall configuration includes the following steps:

- Configuring OpenLDAP security provider. For more information, see *IBM SPSS Collaboration and Deployment Services 8.2.2 Administrator's Guide*.
- Kerberos server-specific changes to OpenLDAP configuration depending on the Kerberos server being used.

OpenLDAP with Windows Kerberos Server

If OpenLDAP directory is used with Windows Kerberos server, where OpenLDAP is the IBM SPSS Collaboration and Deployment Services security provider and Windows Kerberos server is the single sign-on provider, you must make sure that your OpenLDAP schema matches your Active Directory schema. If the schema does not match, you must change the user mapping on the OpenLDAP server.

MIT Kerberos Server

If MIT Kerberos Server is used with OpenLDAP, it may be necessary to set up SSL on the OpenLDAP server and client to ensure secure communication when the KDC service and LDAP server are on different host. Consult release-specific MIT Kerberos Server documentation for updated information.

Active Directory

The following instructions are for Windows Server 2003 domain controller. The steps will be similar for Windows Server 2012 systems.

1. Create a user profile that will be used as Kerberos service principal
2. Map this user profile to the IBM SPSS Collaboration and Deployment Services host system
3. Configure the encryption type and Kerberos credential delegation
4. Create a Kerberos keytab file and place it on IBM SPSS Collaboration and Deployment Services host system

After these steps have been completed, you can use Deployment Manager to configure Active Directory as a security provider, and then configure a Kerberos single sign-on provider.

To create a user profile for Kerberos principal

1. Using the Active Directory users and computers management console, create a domain user for the selected domain (for example, user `krb5.principal` in domain `spss`). This user corresponds to the Kerberos service principal.
2. Specify a surname parameter for this user. It is required by some application servers.
3. Select the option for password to never expire.

To map the user profile to the IBM SPSS Collaboration and Deployment Services host system

Associate the user profile with a Service Principal Name (SPN) by using the **setspn** tool. An SPN is a name that is used by a Kerberos client to identify a service on a Kerberos server. The client references the SPN instead of a specific domain user.

The **setspn** tool accesses, updates, and removes the SPN property for a user. To add an SPN, use the following command syntax:

```
setspn -A <spn> <user>
```

The `-A` option adds an arbitrary SPN to the domain account. The other arguments have the following definitions:

<spn>
  The SPN that is added to the user, having a format of *<service_class>/<host>*. The *<service_class>* value denotes the class of the service. The *<host>* value corresponds to the host name, either fully qualified or simplified.

<user>
  The user profile to associate with the SPN.

To map the user profile, perform the following steps. Add both the fully qualified host name and the simplified, shortened host name as a client may reference either name.

1. If you do not have the **setspn** tool, download and install an appropriate version of Windows Support Tools.
2. Run **setspn** with the IBM SPSS Collaboration and Deployment Services server fully qualified host name as the argument, as in the following example:

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

3. Run **setspn** with the IBM SPSS Collaboration and Deployment Services server host name as the argument, as in the following example:

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

For more information on the **setspn** tool, see http://technet.microsoft.com/en-us/library/cc731241.aspx.

To configure encryption type and credential delegation

1. On the Account tab of the user properties dialog, select the option to use AES encryption.
2. On the Delegation tab of the user properties dialog, select the option to trust the user with for delegation to any service.

To create a Kerberos keytab file

A keytab file contains Kerberos principals with their corresponding encrypted keys and is used for principal authentication. To create a keytab file, use the **ktpass** tool. For information on the **ktpass** tool, see http://technet.microsoft.com/en-us/library/cc753771.aspx.

1. Run the **ktpass** tool as in the following example:

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

- The value for the **princ** option must have the following format: *<service_provider_name>*@*<domain>*.
- The value for the **mapUser** option must have the following format: *<Kerberos_service_principal>*@*<domain>*.
- Any form of strong encryption, as defined by the **crypto** option, requires the JCE extension for strong encryption from Oracle.

2. Place the generated keytab file (in the example, *c:\temp\krb5.prin.keytab*) on the file system of your IBM SPSS Collaboration and Deployment Services host.

If the service password changes, the keytab file must also be updated.

Kerberos server configuration

In Microsoft Windows environment, using the Active Directory Server with Windows (integrated) Kerberos Server is recommended. You must update all client machines' registry for Kerberos LSA access. You must also make specific changes to the browsers to use Kerberos. For non-Microsoft-Windows Kerberos servers, you may need to install additional software both on your repository host machine as well as on each client machines. In all cases, Kerberos service principal must be set to delegate credential. You must also make specific changes to each client machines for credential delegation.

Application server configuration for single sign-on

Depending on the application server used with the repository, it may be necessary to update the application server settings.

WebSphere

IBM SPSS Collaboration and Deployment Services configuration for single sign-on in WebSphere 7 and 8 includes the following steps:

- Defining Kerberos keytab.
- Defining JAAS-JGSS policy.

Defining Kerberos keytab

1. In the administrative console, choose:

   Servers > **Application Servers** > **<Server Name>** > **Server Infrastructure** > **Process Definition** > **Java Virtual Machine** > **Custom Properties**

2. Add custom property *KRB5_KTNAME* with the value of the keytab file path.

Defining JAAS-JGSS policy

1. In the administrative console, choose:

   Security > **Secure Administration, application and infrastructure** > **Java Authentication and Authorization Service** > **Applications logins**

2. Define a property *JGSSServer*.

3. In Additional Properties for *JGSSServer*, define the module class *com.ibm.security.auth.module.Krb5LoginModule* with authentication strategy REQUIRED.

4. Define the following custom properties for *com.ibm.security.auth.module.Krb5LoginModule*.

Property name	Value
credsType	both
principal	<principal name>, for example, *HTTP/ cdsserver.spss.com@SPSS.COM*
useDefaultKeytab	true

JBoss

For JBoss application server, at least one JAAS (Java Authentication and Authorization Service) configuration for JGSSServer and CaDSMiddleTier must be provided. The template for single sign-on application policy can be found in the JGSSServer element of `<JBoss installation directory>/ standalone/configuration/cds_server.xml`. It may be necessary to change the Kerberos login module name to correspond to the application server JRE.

At a minimum, at least one JAAS configuration for JGSSServer must be provided with the following parameters:

- **JGSSServer** is required
- **CaDSMiddleTier** is required
- **KerberosLocalUser** is optional
- **JDBC_DRIVER_01** is optional

1. For Sun JRE, the following default JGSSServer configuration is created:

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

2. Optional `KerberosLocalUser` configuration is used to allow NTLM bypass. This configuration allows users to create a Kerberos credential when the client browser sends an NTLM token (instead of a Kerberos token) during the negotiation challenge. Note that on Windows systems, with browser on the same machine, where IBM SPSS Collaboration and Deployment Services server is installed, it will always send an NTLM token. All NTLM requests to IBM SPSS Collaboration and Deployment Services may be disabled by omitting this configuration from their JAAS configuration file.

   For IBM JRE:

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

For Sun JRE:

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

3. Optional `JDBC_DRIVER_01` configuration is used for Kerberos authentication to database servers.

   For IBM JRE:

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

   For Sun JRE:

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

4. For Sun JRE, the following default CaDSMiddleTier configuration is created:

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

5. It's also possible to specify appropriate login module class name, requirement type, and other options that the login module requires for each JAAS configuration. The login module class must be in class path. For more information, see JRE and application server vendor documentation.

Updating Windows registry for single sign-on

For SSO to function properly, the Kerberos Ticket-Granting Ticket (TGT) must include the session key. To enable this inclusion, the Windows registry must be updated. For more information, see http://support.microsoft.com/kb/308339.

IBM SPSS Collaboration and Deployment Services installation media include registry update files for configuring Windows XP SP2, Windows Vista, and Windows 2003 systems for Kerberos-based single sign-on. The files can be found in the `/Documentation/Utility_Files/Windows/registry` directory of the documentation package (downloaded from IBM Passport Advantage). The files are as follows:

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

For Windows Vista and later systems, use the `Win2003_Kerberos.reg` file.

The registry files allow the system administrator to push registry changes to all systems on the network that must have single sign-on access to the repository.

Configuring one-way trust relationships

You can configure your environment for cross-realm authentication to control user access.

For example, suppose you have two domains, `AppDomain` and `UserDomain`. The two domains have a one-way trust relationship, with `AppDomain` configured for outgoing trust and `UserDomain` configured

for incoming trust. You install the IBM SPSS Collaboration and Deployment Services server in the `AppDomain` domain and install IBM SPSS Deployment Manager in the `UserDomain` domain.

To configure IBM SPSS Collaboration and Deployment Services for one-way trust, you need to modify both the IBM SPSS Collaboration and Deployment Services server and IBM SPSS Deployment Manager.

Configuring the IBM SPSS Collaboration and Deployment Services server

1. Stop the IBM SPSS Collaboration and Deployment Services server.
2. Create a valid `krb5.conf` Kerberos configuration file on the server file system. The file should have content similar to the following lines, with the domains replaced with values corresponding to your system:

```
[libdefaults]
default_realm = APPDOMAIN.COM

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

3. Set the Java system property `java.security.krb5.conf` to the location of the `krb5.conf` file. For example:

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

See your application server documentation for instructions on setting Java system properties.
4. Start the IBM SPSS Collaboration and Deployment Services server.

Configuring IBM SPSS Deployment Manager

1. Close IBM SPSS Deployment Manager.
2. Create a valid `krb5.ini` Kerberos configuration file in the windows installation folder, such as `c:\windows\krb5.ini`. The file should have content valid for cross-realm authentication similar to the following lines, with the domains replaced with values corresponding to your system:

```
[libdefaults]
default_realm = USERDOMAIN.COM

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

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

3. Start IBM SPSS Deployment Manager.

Server Process Credential configuration

Server Process Credential is the built-in credentials definition of the user profile under which the repository server is run. In Active Directory or OpenLDAP-based single sign-on environment, Server Process Credential can be used instead of regular repository user credentials to:

• Run reporting job steps and schedule time-based jobs

- Query a security provider for a list of user and group profiles

For more information on using the Server Process Credential, see IBM SPSS Deployment Manager documentation.

After the repository has been configured for single sign-on, the following additional steps are required for enabling the Server Process Credential:

- Configure the middle tier user login configuration for the application server.
- Create the Kerberos ticket cache on the repository host.

To use the server process credential with reporting job steps:

- Add the data source database server to the domain/realm.
- Configure the data source database server to accept single sign-on connections from the domain/realm.
- Configure the data source database to provide the appropriate permissions to the Server Process Credential.

To configure the middle tier user login on WebSphere

1. Using administrative console, open

   Security > **Global security** > **JAAS - Application logins**
2. Define login configuration *CaDSMiddleTier*.
3. For *CaDSMiddleTier*, define a JAAS module with class name *com.ibm.security.auth.module.Krb5LoginModule*.
4. For *com.ibm.security.auth.module.Krb5LoginModule*, define the following custom properties:
   - `useDefaultCache` true
   - `renewTGT` true
   - `debug` false

To configure the middle tier user login on JBoss

Add the following application policy to *<JBoss installation directory>/server/<Server Name>/conf/login-config.xml*:

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

To create the Kerberos ticket cache

The Kerberos ticket cache will be used to store the Kerberos ticket used to authenticate the Server Process Credential. To create the ticket cache perform the following steps:

1. Update the Kerberos configuration file on the repository host server, for example *c:\windows\krb5.ini*. This file identifies the default realm/domain, default encoding types, renewable ticket, and KDC address, and will be used by the **kinit** application to generate our ticket cache. The following is an example of the Kerberos configuration file:

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

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

2. Login to the repository host using the domain credentials that will used for the Server Process Credential. Make sure that this credentials have appropriate permissions on the host.

3. Run **kinit** from directory of the JRE used by the repository application server with the options to create a renewable ticket and a ticket cache.

   Note: On the Windows operating system, **kinit** may not create a renewable ticket. To overcome this problem, add the following registry setting:

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

   For more information, see the Kerberos documentation for your operating system.

4. Enter the password for the user for the Server Process Credential.

Configuring browsers for single sign-on

To enable single sign-on for IBM SPSS Collaboration and Deployment Services Deployment Portal and other thin clients of IBM SPSS Collaboration and Deployment Services, you must configure your web browser to support Simple and Protected GSS-API Negotiation (SPNEGO) protocol.

Microsoft Internet Explorer

For information on configuring Microsoft Internet Explorer to support SPNEGO, see http://msdn.microsoft.com/en-us/library/ms995329.aspx.

Mozilla Firefox

SPNEGO support for Firefox is turned off by default. To enable it:

1. Go to the *about:config* URL (Firefox configuration file editor).

2. Change the following preference values:

   - **network.negotiate-auth.allow-non-fqdn** = false
   - **network.negotiate-auth.allow-proxies** = true
   - **network.negotiate-auth.delegation-uris** = Include the local intranet domain name, such as .your-domain.com, where the leading period represents a wildcard character
   - **network.negotiate-auth.trusted-uris** = Include the local intranet domain name, such as .your-domain.com, where the leading period represents a wildcard character
   - **network.negotiate-auth.using-native-gsslib** = true

Google Chrome

SPNEGO support for Chrome is disabled by default. To enable it, you need to include theIBM SPSS Collaboration and Deployment Services server name in an allowlist:

- For Windows, define the AuthNegotiateDelegateWhitelist group policy. For more information, see the Chrome Policy List, Issue 472145, and Issue 469171.

As a member of the allowlist, the IBM SPSS Collaboration and Deployment Services server is treated as a trusted destination for Kerberos ticket forwarding.

Safari

Single sign-on is not supported for Safari.

Forwardable tickets and IBM SPSS Deployment Manager

Although not necessary, you could use the **kinit.exe** tool of your JDK to obtain and cache Kerberos ticket-granting tickets. For example, from the `jre\bin` directory of your IBM SPSS Deployment Manager installation, you could issue the following command:

```
kinit.exe -f
```

The `-f` option creates a forwardable ticket. This command creates a cache file in the Windows `user` directory where the JVM automatically searches for a cache.

If you have issued this command by using an IBM JDK 7 older than 170_SR8, you may need to modify your `krb5.ini` file to access this cache successfully.

1. Open the `krb5.ini` file in a text editor. This file is often located in the `C:\Windows` directory.
2. In the **[libdefaults]:** section, add the following setting:

```
forwardable = true
```

3. Save the updated file.

This change is only needed for the client. No corresponding change is needed for the IBM SPSS Collaboration and Deployment Services Repository server.

Chapter 7. Application context roots

The context root for an application defines the location at which the module can be accessed. The context root is part of the URL you use to connect to the application.

A URL reference to an IBM SPSS Collaboration and Deployment Services application includes the following elements:

URL prefix
Consists of the protocol, the server name or IP address, and the port number

Context root
Determines the location at which the application is accessed. By default, the context root is the server root itself, denoted as a single forward slash.

Application root
Specifies the root of the application itself

For example, the IBM SPSS Collaboration and Deployment Services Deployment Portal has the following URL when the repository server is running locally on port 8080:

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

The URL prefix is `http://localhost:8080` and the context root is the application server root. The application root is peb.

There is nothing in the URL that identifies the web module as being part of IBM SPSS Collaboration and Deployment Services. If you add other applications to your server, managing the many modules available at the server root becomes increasingly difficult.

If you configure the repository server to use a context root, you can isolate the IBM SPSS Collaboration and Deployment Services components from other applications. For example, you can define a context root of `ibm/spss` for the IBM SPSS Collaboration and Deployment Services modules. In this case, the URL for the IBM SPSS Collaboration and Deployment Services Deployment Portal interface is:

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

Important: If you use a context root for your repository server, all client applications must include the same context root when they connect to the server. The URL for any application running within the IBM SPSS Collaboration and Deployment Services environment, such as IBM Analytical Decision Management, must be updated accordingly.

Related tasks
Adding a context root to the URL Prefix
If your system uses a custom URL prefix for accessing the IBM SPSS Collaboration and Deployment Services Repository, add the context root to the URL prefix specification.

Updating context roots for WebSphere
Modify the location at which applications deployed on WebSphere are accessed by using the administrative console.

Updating context roots for JBoss

Modify the location at which applications deployed on JBoss are accessed by updating the ear file that contains the location definitions.

Configuring application context roots

You must update the system URL prefix and modify the individual context root specifications to configure context roots.

Procedure

1. If the use of a URL prefix is enabled, add the context root to the URL prefix.
2. Update the context root for each application.

    The steps depend on the application server.

    - "Updating context roots for WebSphere" on page 55
    - "Updating context roots for JBoss" on page 55

Results

You can access the browser-based IBM SPSS Deployment Manager and the IBM SPSS Collaboration and Deployment Services Deployment Portal by using URL values that include your context root.

What to do next

Update any references to the repository server, such as those defined using IBM SPSS Deployment Manager, to include the context root in the server URL.

Adding a context root to the URL Prefix

If your system uses a custom URL prefix for accessing the IBM SPSS Collaboration and Deployment Services Repository, add the context root to the URL prefix specification.

Before you begin

- Your login credentials must be associated with the Configuration action.
- Use of the URL Prefix setting must be enabled by using the browser-based IBM SPSS Deployment Manager.

Procedure

1. Log in to the browser-based IBM SPSS Deployment Manager.
2. On the **Configuration** panel, click the **URL Prefix** option in the **Setup** group.
3. Add the context root to the **URL Prefix** definition.
    For example, if your URL prefix is `http://myserver:8080` and you want to use a context root of `ibm/spss`, the new value is `http://myserver:8080/ibm/spss`.

    Restriction: Do not end the URL specification with a slash. For example, specify a value of `http://myserver:8080/myroot` instead of `http://myserver:8080/myroot/`.
4. Restart the application server.

What to do next

Update the context root for each application. The steps depend on the application server.

Related concepts
Application context roots

The context root for an application defines the location at which the module can be accessed. The context root is part of the URL you use to connect to the application.

Related tasks
Updating context roots for WebSphere
Modify the location at which applications deployed on WebSphere are accessed by using the administrative console.

Updating context roots for JBoss
Modify the location at which applications deployed on JBoss are accessed by updating the ear file that contains the location definitions.

Updating context roots for WebSphere

Modify the location at which applications deployed on WebSphere are accessed by using the administrative console.

Before you begin
"Adding a context root to the URL Prefix" on page 54

Procedure

1. Log in to the WebSphere console.
2. Access the IBM SPSS Collaboration and Deployment Services application.
3. Update the **Context Root For Web Modules** settings to include your root value.

   If the URL prefix is enabled for your system, the root value for each module must be the same as the value you added to the URL Prefix. The application root must be unchanged.

   For example: /IBM/SPSS/CDS/admin
4. Restart the WebSphere nodes where IBM SPSS Collaboration and Deployment Services is deployed

Related concepts
Application context roots
The context root for an application defines the location at which the module can be accessed. The context root is part of the URL you use to connect to the application.

Related tasks
Adding a context root to the URL Prefix
If your system uses a custom URL prefix for accessing the IBM SPSS Collaboration and Deployment Services Repository, add the context root to the URL prefix specification.

Updating context roots for JBoss
Modify the location at which applications deployed on JBoss are accessed by updating the ear file that contains the location definitions.

Updating context roots for JBoss

Modify the location at which applications deployed on JBoss are accessed by updating the ear file that contains the location definitions.

Before you begin
"Adding a context root to the URL Prefix" on page 54

Procedure

1. Make a backup copy of the `cds80.ear` file in the `toDeploy/timestamp` directory of your JBoss installation.
2. Use an archive utility to modify the `META-INF/application.xml` file in the original ear file.

   Prefix the application root value for each `context-root` element with the new context root. You must add the same value to each `context-root` element.

3. Copy the ear file that contains the updated `application.xml` file to the `deploy` directory of the application server.
4. Restart the application server.

Example

Suppose the `application.xml` file contains the following specifications:

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

To add a context root of `ibm/spss`, update the `context-root` definitions with the following values:

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

Related concepts

Application context roots
The context root for an application defines the location at which the module can be accessed. The context root is part of the URL you use to connect to the application.

Related tasks

Adding a context root to the URL Prefix
If your system uses a custom URL prefix for accessing the IBM SPSS Collaboration and Deployment Services Repository, add the context root to the URL prefix specification.

Updating context roots for WebSphere
Modify the location at which applications deployed on WebSphere are accessed by using the administrative console.

Chapter 8. FIPS 140–2 compliance

The Federal Information Processing Standard (FIPS) Publication 140-2, FIPS PUB 140-2, is a US government computer security standard used to accredit cryptographic modules. The document specifies the requirements for cryptography modules which include both hardware and software components, corresponding to four different levels of security that are mandated for organization that do business with the US government. IBM SPSS Collaboration and Deployment Services can be configured to provide Security Level 1 as specified by FIPS 140-2.

Security configuration for FIPS 140-2-compliance must follow these guidelines:

- Communications between the repository and client applications must use SSL for transport layer security of general data transfers. Additional AES encryption is provided for credential passwords using a shared key stored in the application code. See the topic Chapter 9, "Utilizzo di SSL per proteggere il trasferimento di dati," on page 59 for more information.
- The repository server uses AES algorithm with the key stored in a keystore on the server file system to encrypt passwords in the configuration files, application server configuration files, security provider configuration files, etc.
- Communications between the repository server and the database server can optionally use SSL for transport layer security for general data transfer. AES encryption is provided for credential passwords, configuration passwords, user preference passwords, etc. using a shared key stored in a keystore on the database server file system.
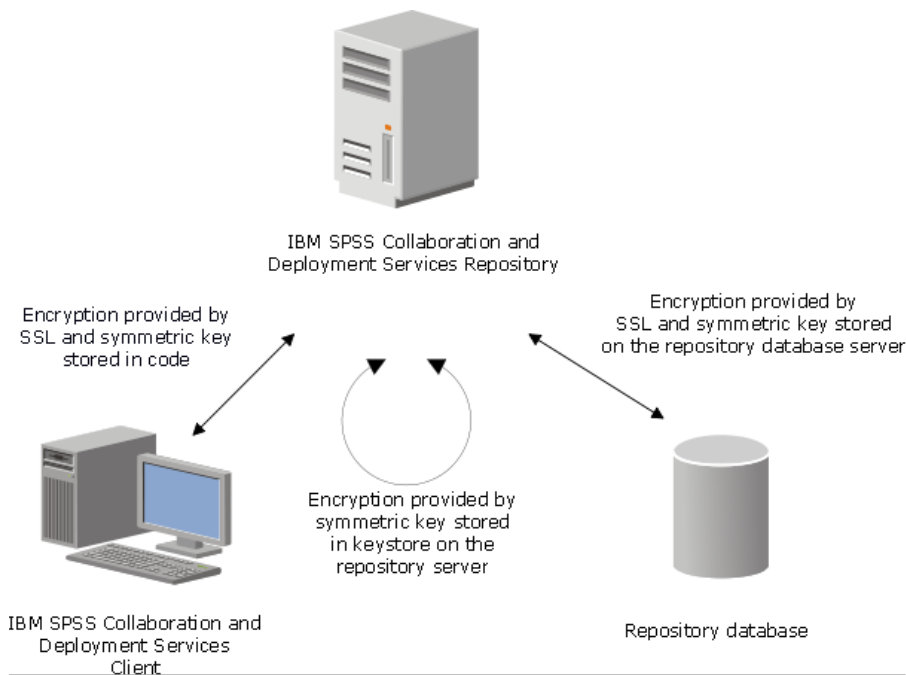
Figure 4. IBM SPSS Collaboration and Deployment Services FIPS 140-2-compliant security setup

Repository configuration

The repository configuration for FIPS 140-2-compliance must follow these guidelines:

- The database must be set up to accept SSL communications; the JCE encryption module must also be configured.
- If the repository is installed on UNIX, the default JRE must be set up with a JCE module.
- The application server JRE must also be set up with a JCE module.

- The application server must be configured to accept SSL communications; a JCE module must also be configured.
- If the repository is installed on Windows, you must exit the installation at setup screen, configure a JCE module, then restart the setup and select to run in FIPS 140-2-compliant mode on the appropriate screen.
- If the repository is deployed into a clustered environment, keystore must be replicated to all nodes in the cluster.
- The JREs that are being used by IBM Corp. server applications interacting with IBM SPSS Collaboration and Deployment Services, such as IBM SPSS Statistics Server and IBM SPSS Modeler Server, must have SSL certificates installed.

Desktop client configuration

For IBM SPSS Collaboration and Deployment Services desktop client applications, such as IBM SPSS Deployment Manager, JCE encryption module must be enabled for the JRE used to run the applications. The JRE must have SSL certificates installed.

Browser configuration

- Mozilla Firefox can be configured to run in FIPS 140-2 compliant mode by modifying the application options. For more information, see http://support.mozilla.com/en-US/kb/Configuring+Firefox+for+FIPS +140-2.
- Internet Explorer configuration requires enabling Windows cryptography and modifying the browser settings. For more information, see http://support.microsoft.com/kb/811833.
- Apple Safari cannot be used in FIPS 140-2 compliant mode.

Capitolo 9. Utilizzo di SSL per proteggere il trasferimento di dati

SSL (Secure Sockets Layer) è un protocollo per crittografare i dati trasferiti tra due computer. SSL garantisce che la comunicazione tra i computer sia sicura. SSL è in grado di crittografare l'autenticazione del binomio nome utente/password e il contenuto di uno scambio tra server e client.

Procedere come segue per utilizzare SSL con un server delle applicazioni supportato:

1. importare il certificato SSL nel JRE di IBM Installation Manager.
2. Durante l'installazione, selezionare l'opzione **SSL abilitato** per abilitare la connessione SSL al database.
3. Dopo l'installazione, prima di avviare il server, importare il certificato nel JRE che è collegato in IBM SPSS Collaboration and Deployment Services.

Per ulteriori istruzioni specifiche per il server delle applicazioni, vedere "Configurazione di SSL per i server delle applicazioni" a pagina 62.

How SSL works

SSL relies on the server's public and private keys, in addition to a public key certificate that binds the server's identity to its public key.

1. When a client connects to a server, the client authenticates the server with the public key certificate.
2. The client then generates a random number, encrypts the number with the server's public key, and sends the encrypted message back to the server.
3. The server decrypts the random number with its private key.
4. From the random number, both the server and client create the session keys used for encrypting and decrypting subsequent information.

The public key certificate is typically signed by a certificate authority. Certificate authorities, such as VeriSign and Thawte, are organizations that issue, authenticate, and manage security credentials contained in the public key certificates. Essentially, the certificate authority confirms the identity of the server. The certificate authority usually charges a monetary fee for a certificate, but self-signed certificates can also be generated.

IBM SPSS Statistics Server supports both OpenSSL and GSKit. If both are configured, GSKit is used by default.

Securing client/server and server-server communications with SSL

The main steps in securing client/server and server-server communications with SSL are:

1. Obtain and install the SSL certificate and keys.
2. If using encryption certificates with a strength greater than 2048 bits, install unlimited strength encryption on the Deployment Manager client computers. For more information, see "Installing unlimited strength encryption" on page 60
3. Add the certificate to the client keystore.
4. Instruct users to enable SSL when connecting to the server.

Note: Occasionally a server product acts as a client. An example is IBM SPSS Statistics Server connecting to the IBM SPSS Collaboration and Deployment Services Repository. In this case, IBM SPSS Statistics Server is the *client*.

Installing unlimited strength encryption

The Java Runtime Environment shipped with the product has US export-strength encryption enabled. For enhanced security of your data, upgrading to unlimited-strength encryption is recommended.

IBM J9

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for your version of the SDK from the IBM.com website.

2. Extract the unlimited jurisdiction policy files that are packaged in the compressed file. The compressed file contains a `US_export_policy.jar` file and a `local_policy.jar` file. In your WebSphere Application Server installation, go to the `$JAVA_HOME/jre/lib/security` directory and back up your `US_export_policy.jar` and `local_policy.jar` files.

3. Replace the existing copies of *US_export_policy.jar* and *local_policy.jar* files with the two files that you downloaded and extracted.

    Note: You need to also install the `*.jar` files to your `<DeploymentManager_Client_Install>/jre/lib/security` folder.

4. Enable security in the WebSphere Application Server administration console. Make sure that all node agents within the cell are active beforehand. For more information, see WebSphere documentation. Note that you must select an available realm definition from the list in **Security > Secure administration, applications, and infrastructure**, and then click **Set as current** so that security is enabled upon a server restart.

5. Log off the administrative console.

6. Stop the server.

7. Restart the server.

Sun Java

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for your version of the SDK from Sun Java website.

2. Extract the downloaded file.

3. Copy the two *.jar* files *local_policy.jar* and *US_export_policy.jar* into *<installation folder>/jre/lib/security*, where *<installation folder>* is the folder in which you installed the product.

Adding the certificate to client keystore (for connections to the repository)

Note: Skip this step if you are using a certificate that is signed by a certificate authority.

If you are using SSL to connect to an IBM SPSS Collaboration and Deployment Services repository and you are using self-signed certificates, you need to add the certificate to the client's Java keystore. The following steps are completed on the *client* computer.

1. Open a command prompt and change directories to the following location, where *<product install dir>* is the directory in which you installed the product:

    ```
    <product install dir>/jre/bin
    ```

2. Enter the following command:

    ```
    keytool -import -alias <alias name> -file <path to cert> -keystore <path
    to keystore>
    ```

    where *<alias name>* is an arbitrary alias for the certificate, *<path to cert>* is the full path to the certificate, and *<path to keystore>* is the full path to the Java keystore, which may be *<product install dir>/lib/security/jssecacerts* or *<product install dir>/lib/security/cacerts*.

3. When prompted, enter the keystore password, which is `changeit` by default.

4. When prompted about trusting the certificate, enter `yes`.

Importing the certificate file for browser-based client connections

When you connect to IBM SPSS Collaboration and Deployment Services Repository through SSL with a browser-based client, for example, IBM SPSS Collaboration and Deployment Services Deployment Portal, the browser either prompts you to accept the unsigned, untrusted certificate, or displays a message that the site is unsafe and provides a link to import the certificate into the browser truststore. This process is different for different browsers, and it might be different depending on the browser configuration. You can also manually install the certificate into the browser truststore.

Instructing users to enable SSL

When users connect to the server through a client product, they need to enable SSL in the dialog box for connecting to the server. Be sure to tell your users to select the appropriate check box.

Configuring the URL prefix

If IBM SPSS Collaboration and Deployment Services Repository is set up for SSL access, the value of the URL Prefix configuration setting must be modified as follows:

1. Log in to the repository using browser-based console.
2. Open *URL Prefix* configuration option.

   Configuration > **Setup** > **URL Prefix**

3. Set the value of the prefix to `https` instead of `http` and set the port value to the SSL port number. For example:

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

Securing LDAP with SSL

Lightweight Directory Access Protocol (LDAP) is an Internet Engineering Task Force (IETF) standard for exchanging information between network directories and databases containing any level of information. For systems requiring additional security, LDAP providers, such as Microsoft's Active Directory, can operate over Secure Socket Layer (SSL), provided that the Web or application server supports LDAP over SSL. Using SSL in conjunction with LDAP can ensure that login passwords, application information, and other sensitive data are not hijacked, compromised, or stolen.

The following example illustrates how to enable LDAPS using Microsoft's Active Directory as a security provider. For more specific information on any of the steps or to find details that address a particular release of the security provider, see the original vendor documentation.

1. Verify that Active Directory and the Enterprise Certificate Authority are installed and functioning.
2. Use the certificate authority to generate a certificate, and import the certificate into the certificate store of the IBM SPSS Deployment Manager installation. This allows the LDAPS connection to be established between the IBM SPSS Collaboration and Deployment Services Repository and an Active Directory server.

   To configure IBM SPSS Deployment Manager for secure Active Directory connections, verify that a connection exists to the repository.

3. Launch the IBM SPSS Deployment Manager.
4. From the **Tools** menu, choose **Server Administration**.
5. Log in to a previously defined administered server.
6. Double-click the **Configuration** icon for the server to expand the hierarchy.
7. Double-click the **Security Providers** icon to expand the hierarchy.

8. Double-click the Active Directory security provider.

9. Enter configuration values for the instance of Active Directory with security certificates installed.

10. Select the **Use SSL** check box.

11. Note the name in the Domain User field. Subsequent logins using Active Directory are authenticated using SSL.

For additional information about installing, configuring, and implementing LDAPS on a particular application server, see the original vendor's documentation.

Configurazione di SSL per i server delle applicazioni

È possibile installare il server IBM SPSS Collaboration and Deployment Services Repository su un database avbilitato a SSL. Per il server delle applicazioni procedere come segue:

JBoss

Fare riferimento alla documentazione JBoss EAP 7.x per istruzioni sull'abilitazione di SSL/TLS. SSL viene abilitato per impostazione predefinita in JBoss EAP 7.x. Procedere come segue alle personalizzazioni:

1. Creare un file delle chiavi con il formato keystore di Java. Ad esempio:

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

Verificare che il CN (Common Name) sia l'FQDN (fully qualified domain name) del sistema in cui IBM SPSS Collaboration and Deployment Services Repository è installato. L'`ip` è l'indirizzo IP del server IBM SPSS Collaboration and Deployment Services Repository.

Se il file delle chiavi è in un formato diverso dal keystore, trasformarlo innanzitutto nel formato keystore di Java.

2. Aggiornare le impostazioni SSL settings nel file `cds_server.xml` in `JBOSS_HOME\standalone\configuration`:

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

Dove il valore `alias` è lo stesso nome utilizzato per la creazione del file delle chiavi.

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

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

3. Facoltativo: È possibile apportare modifiche alla configurazione della porta. Per esempio, modificare la porta HTTPS JBoss predefinita da 8443 a 443 in `<socket-binding-group>` nel file `cds_server.xml`:

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

Liberty

Fare riferimento alla documentazione JBoss EAP 7.x per istruzioni sull'abilitazione di SSL/TLS. SSL viene abilitato per impostazione predefinita in JBoss EAP 7.x. Procedere come segue alle personalizzazioni:

1. Creare un file delle chiavi con il formato keystore di Java. Ad esempio:

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

Verificare che il CN (Common Name) sia l'FQDN (fully qualified domain name) del sistema in cui IBM SPSS Collaboration and Deployment Services Repository è installato. L'ip è l'indirizzo IP del server IBM SPSS Collaboration and Deployment Services Repository.

Se il file delle chiavi è in un formato diverso dal keystore, trasformarlo innanzitutto nel formato keystore di Java.

2. Aggiornare il file server.xml in CADS_HOME\wlp\usr\servers\cdsServer con le nuove informazioni del file keystore:

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

WebSphere

Fare riferimento alla documentazione WebSphere per istruzioni sull'abilitazione di SSL/TLS.

Chapter 10. Logging

Logging is essential when troubleshooting application problems as well as when planning preventive maintenance activities. As system and application events are generated, administrative personnel can be alerted when warning thresholds are reached or critical system events occur. Additionally, verbose information output can be stored in a text file for analysis at a later time.

The IBM SPSS Collaboration and Deployment Services Repository uses the log4j package for handling runtime log information. Log4j is Apache Software Foundation's logging solution for Java applications. The log4j approach permits logging control using a configuration file; the application binary does not have to be modified. For a comprehensive discussion of log4j, see the log4j website .

Logging configuration file

The location of the IBM SPSS Collaboration and Deployment Services Repository logging configuration file varies depending on the host application server:

- **WebSphere:** `<repository installation directory>/platform/log4j.properties`
- **Liberty:** `<repository installation directory>/platform/log4j.properties`
- **JBoss:** `<JBoss server directory>/standalone/configuration/cds_server.xml`

This file controls both the destination and the amount of log output. Configuration of log4j is handled by modifying this file to define appenders for log destinations and to route logger output to those appenders.

The following default loggers are defined:

Table 5. Loggers	
Logger	**Description**
log4j.rootCategory	Root logger
log4j.logger.com.spss	All IBM SPSS Collaboration and Deployment Services events
log4j.com.spss.cmor, log4j.com.spss.cmor.internal.MetaObjectImportEngine	Repository events
log4j.com.spss.security	Security events
log4j.com.spss.process	Job scheduling events
log4j.com.spss.reporting , log4j.com.spss.reportservice	Reporting events
log4j.com.spss.notification	Notification events
log4j.logger.org.springframework.jdbc.core.JdbcTemplate	Spring framework JDBC events
log4j.logger.com.spss.repository.internal.transfer	Export-import events

The following appenders are defined:

- Console
- Main log (*cds.log*)
- Export-import transactions log (*cds_transfer.log*)

The default location of the log files varies depending on the host application server:

- **WebSphere:** *<WebSphere profile directory>/logs/*
- **JBoss:** *<JBoss server directory>/log/*

Capitolo 11. Esempio: Installazione e configurazione cluster Websphere

Questa sezione fornisce un esempio end-to-end di installazione e configurazione di IBM SPSS Collaboration and Deployment Services Repository con un server di cluster IBM WebSphere

Questo esempio contiene le seguenti informazioni

- **Pre-installazione** procedure per determinare i requisiti di sistema in base al tipo di installazione e all'utilizzo del sistema, l'acquisizione delle macchine per eseguire il cluster di server delle applicazioni e per assicurare che i server soddisfino tutti i requisiti hardware e software.
- **Server di cluster WebSphere** procedure per installare WebSphere utilizzando IBM Installation Manager e per configurare un server di cluster.
- **Database** procedure per inizializzare il database.
- **Installazione e configurazione** procedure per installare i file dell'applicazione sul sistema host utilizzando IBM Installation Manager e per configurare il IBM SPSS Collaboration and Deployment Services Repository da eseguire con il cluster di server delle applicazioni e il database di repository progettati.
- **Post-installazione** procedure per avviare il IBM SPSS Collaboration and Deployment Services Repository e verificare la connettività.

Preinstallazione

Prima dell'installazione di IBM SPSS Collaboration and Deployment Services con un server di cluster WebSphere, verificare che l'ambiente soddisfi tutti i requisiti hardware e software su tutti i nodi del cluster. Consultare i report di compatibilità del prodotto software IBM all'indirizzo:https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html

Quando si distribuisce il server IBM SPSS Collaboration and Deployment Services Repository in un ambiente server di cluster, ogni server delle applicazioni nel cluster deve essere configurato in modo identico ai componenti dell'applicazione ospitata e al repository si deve poter accedere attraverso un hardware o un sistema di bilanciamento del carico basato sul software. Questa architettura consente di distribuire l'elaborazione tra più server delle applicazioni e fornisce anche ridondanza in caso di malfunzionamento di un singolo server.
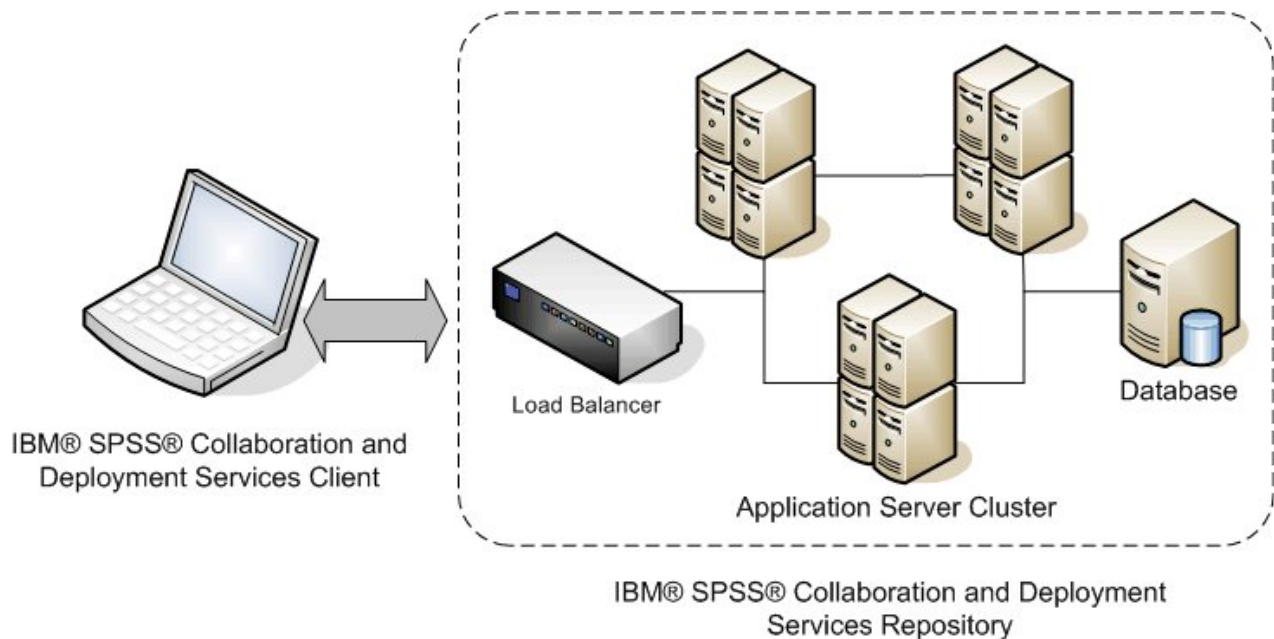
Figura 5. Architettura cluster

Il processo di installazione del server del repository in un cluster include le seguenti procedure:

- Installazione iniziale e configurazione dei componenti dell'applicazione sul nodo di gestione del cluster.
- Successiva configurazione dei nodi del cluster

Requisiti di installazione

- I requisiti del sistema host devono essere soddisfatti su tutti i nodi del cluster.
- Tutti i membri del cluster devono essere eseguiti sullo stesso sistema operativo del nodo (di gestione) principale
- Il database IBM SPSS Collaboration and Deployment Services Repository deve già esistere e essere accessibile prima dell'installazione del repository.
- La topologia del server delle applicazioni deve già esistere prima dell'installazione del repository. Si consiglia di verificare che sia possibile accedere al cluster e che sia in esecuzione correttamente all'indirizzo del sistema di bilanciamento del carico.
- La directory di installazione del repository deve essere condivisa tra tutti i nodi nel cluster.

Installazione server di cluster WebSphere

Prima di installare IBM WebSphere, deve essere installato IBM Installation Manager 1.9.1 o successivo. Per ulteriori informazioni relative all'installazione IBM Installation Manager, consultare https://jazz.net/ wiki/bin/view/Deployment/InstallingUpdatingScriptingWithInstallationManager.

A seconda del sistema operativo, WebSphere può essere installato utilizzando l'interfaccia Installation Manager, la riga comandi, un file di risposta o la modalità console. Consultare https://www.ibm.com/ support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.installation.base.doc/ae/tins_install.html per ulteriori informazioni.

Installazione WebSphere con IBM Installation Manager

1. Avvia Installation Manager
   - Modalità GUI: `<IBM Installation Manager installation directory>/eclipse/IBMIM`
   - Modalità riga comandi: `<IBM Installation Manager installation directory>/ eclipse/tools/imcl -c`

2. Configurare Installation Manager per utilizzare un repository che contenga i file di installazione di WebSphere Application Server.

3. Fare clic su **Installa**.

4. Selezionare le seguenti offerte di prodotto da installare e fare clic su **Avanti**.

   - IBM WebSphere Application Server Network Deployment

   - IBM SDK, Java Technology Edition, Versione 8

5. Accettare i termini degli accordi di licenza e fare clic su **Avanti**.

6. Selezionare la directory di risorse condivise che più package di installazione possono condividere e fare clic su **Avanti**.

7. Selezionare le lingue per installare il contenuto tradotto e fare clic su **Avanti**.

8. Selezionare le funzioni che si desidera installare e fare clic su **Avanti**.

9. Esaminare le informazioni di riepilogo e fare clic su **Installa**.

Importante: WebSphere Application Server deve essere installato su tutti i nodi nella topologia di cluster WebSphere progettata. Ripetere i passi precedenti su tutti i nodi nel cluster.

Configurazione server di cluster

Prima di configurare un server di cluster, confermare che il profilo WebSphere utilizzato con IBM SPSS Collaboration and Deployment Services sia configurato per essere eseguito con Java 7 SDK o successivo. Il seguente esempio dimostra la sequenza di comandi per elencare gli SDK disponibili e per impostare gli SDK predefiniti.

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

Importante: Accertarsi che la versione di Java SDK su tutti i nodi nel cluster sia 7 o successiva.

Generalmente una topologia di cluster contiene un nodo di gestione e pochi nodi gestiti. WebSphere fornisce un programma di utilità di gestione del profilo che può essere utilizzato per creare i profili. Ad esempio:

1. Creare il profilo *gestione distribuzione* sulla macchina di *gestione*:

   - Accedere al nodo di *gestione* ed eseguire il programma di utilità di gestione del profilo. Ad esempio:

     - Windows:

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

     - Linux/UNIX:

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

2. Creare il profilo *gestione distribuzione* sulla macchina *gestita*:

   - Accedere al nodo *gestito* ed eseguire il programma di utilità di gestione del profilo. Ad esempio:

     - Windows:

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

– Linux/UNIX:

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

Importante: Se sono presenti due o più nodi gestiti nella topologia del cluster, eseguire questo comando più volte per creare profili gestiti su ogni macchina gestita.

Una volta che tutti i profili sono pronti, è necessario creare la relazione tra il profilo di *gestione* e i profili *gestiti*. Se il profilo gestito è presente su una macchina diversa dalla macchina del profilo di gestione, garantire la connettività di rete adatta tra la macchina di gestione e la macchina gestita.

1. Avviare il profilo di *gestione* sul nodo di *gestione* :

   • Accedere alla macchina di *gestione* ed eseguire il seguente comando:

     – Windows:

       ```
       <WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startManager.bat
       ```

     – Linux/UNIX:

       ```
       <WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startManager.sh
       ```

2. Aggiungere i nodi *gestiti* al profilo di *gestione*:

   • Accedere alla macchina *gestita* ed eseguire il seguente comando:

     – Windows:

       ```
       <WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>addNode.bat
       <Management_Host>
       ```

     – Linux/UNIX:

       ```
       <WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>addNode.sh
       <Management_Host> Port
       ```

     Dove `<Management_Host>` è il nome host della macchina di gestione. `Port` è la porta del connettore SOAP di gestione del profilo di gestione, che è possibile trovare nel file `AboutThisProfile.txt`. Se esistono due o più nodi gestiti nella topologia cluster, eseguire questo comando più volte rispetto ad ogni profilo gestito.

3. Accedere alla console di gestione WebSphere e creare una definizione cluster in base ai nodi gestiti:

   • Accedere alla console di gestione WebSphere del profilo di gestione (`https://hostname:port/ibm/console/logon.jsp`, in cui `hostname` è il nome host della macchina di gestione e `port` è il numero della porta della console di gestione.

   • Passare a **Server** > **Cluster** > **Cluster WebSphere Application Server** e fare clic su **Nuovo** per creare una definizione cluster.

   • Specificare un nome cluster e fare clic su **Avanti**.

   • Specificare un nome membro per il primo membro del cluster e selezionare uno dei nodi disponibili. Fare clic su **Successiva**.

   • Creare altri membri del cluster aggiungendo altri nodi disponibili.

Database

Il database e IBM SPSS Collaboration and Deployment Services Repository non devono essere necessariamente installati sullo stesso server, ma è necessaria una configurazione per garantire la connettività. Durante l'installazione, verranno richiesti il nome, il numero porta, il nome utente e la

password del server di database, nonché il nome del database da utilizzare per l'archiviazione e il recupero dati.

Importante: È necessario creare il database manualmente prima dell'installazione, utilizzando un qualsiasi nome di database valido. Tuttavia, senza un database creato preventivamente, l'installazione si arresta.

Segue un esempio di script SQL per creare un databasde DB2 denominato SPSSCDS:

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

Installazione

Quando si distribuisce il server IBM SPSS Collaboration and Deployment Services Repository in un server di cluster WebSphere, è necessario accertarsi che il server del repository sia installato sulla stessa macchina del profilo di gestione WebSphere.

1. Accedere al sistema operativo come utente con appropriato livello di autorizzazioni.

2. Aprire IBM Installation Manager utilizzando uno dei seguenti metodi:

    • Modalità GUI: `<IBM Installation Manager installation directory>/eclipse/IBMIM`

    • Modalità riga comandi: `<IBM Installation Manager installation directory>/eclipse/tools/imcl -c`

3. Se il repository di installazione non è configurato, specificare il percorso del repository (ad esempio come ubicazione sul file system host, la rete o un indirizzo HTTP).

    Nota: Per accedere correttamente ad un repository di installazione, il percorso del repository non deve contenere una E commerciale &).

4. Nel menu principale, selezionare **Installa**.

5. Selezionare IBM SPSS Collaboration and Deployment Services come package da installare. Ad esempio:

    • IBM SPSS Collaboration and Deployment Services - Servizi di repository

    • IBM SPSS Collaboration and Deployment Services Scoring Adapter for PMML

    • IBM SPSS Modeler Adapter for Collaboration and Deployment Services

6. Leggere il contratto di licenza e accettarne i termini.

7. Specificare il gruppo di package e la directory di installazione

    • È necessario un nuovo gruppo di package per l'installazione IBM SPSS Collaboration and Deployment Services Repository.

    • Specificare la directory di installazione delle risorse condivise. È possibile specificare la directory di risorse condivise solo la prima volta che si installa un package.

8. Esaminare il riepilogo delle informazioni e procedere con l'installazione. I file dell'applicazione verranno installati nella directory specificata dopo aver fatto clic su **Installa**.

9. Configurare la directory di installazione da condividere in modo che sia accessibile da tutti i membri del cluster (ad esempio, utilizzare la condivisione file su Windows o NFS su Linux/UniX).

    Se si verificano dei problemi durante l'installazione, è possibile utilizzare i log IBM Installation Manager per la risoluzione dei problemi. Accedere ai file di log dal menu principale in IBM Installation Manager.

Configurazione

Una volta seguiti i precedenti passi di installazione, ora si dovrebbe avere:

- tutti i membri nel cluster WebSphere in esecuzione sullo stesso sistema operativo del nodo (di gestione) principale
- Il database del repository pronto ed accessibile
- La directory di installazione IBM SPSS Collaboration and Deployment Services Repository condivisa da tutti i nodi nel cluster WebSphere

Distribuire il server del repository nel cluster

1. Avviare il programma di utilità di configurazione utilizzando uno dei seguenti metodi:

    - Modalità GUI:

        – Windows: `<repository installation directory>\bin\configTool.bat`

        – Linux/UNIX: `<repository installation directory>/bin/configTool.sh`

    - Modalità riga di comando:

        – Windows: `<repository installation directory>\bin\cliConfigTool.bat`

        – Linux/UNIX: `<repository installation directory>/bin/cliConfigTool.sh`

2. Specificare il tipo di server delle applicazioni. Per un cluster WebSphere, si seleziona **IBM WebSphere**.

3. Specificare le impostazioni del server delle applicazioni come segue:

    - **Directory profilo WebSphere** Il percorso alla directory del profilo server WebSphere. Per un cluster WebSphere questo è il percorso del profilo di gestione. Altre impostazioni WebSphere, come ad esempio la root di installazione WebSphere, la topologia del profilo e il nodo verranno inserite automaticamente in base alle informazioni del profilo. Se non è possibile inserire qualche valore automaticamente, sarà necessario specificarli manualmente.

    - **Prefisso URL.** L'URL utilizzato per l'accesso al server di repository (ad esempio, `http://<machine>:<port>`). In un ambiente cluster, la porta è generalmente il numero della porta del sistema di bilanciamento del carico.

4. Specificare le informazioni di connessione al database come segue:

    - **Tipo di database.** IBM DB2, SQL Server o Oracle.

    - **Host.** Il nome host o l'indirizzo IP del server di database.

    - **Porta.** La porta di accesso per il server di database.

    - **Nome database.** Il nome del database da utilizzare per il repository

    - **Nome SID/Servizio.** Per Oracle, SID o nome servizio.

    - **Eseguire come un servizio** Per Oracle, indica che la connessione avviene ad un servizio di database piuttosto che da un SID.

    - **Nome utente.** Nome utente di database.

    - **Password.** Password utente di database.

5. Se si riutilizza un database di una installazione precedente, specificare se i dati presenti devono essere conservati o eliminati.

6. Specificare le opzioni per il keystore di codifica. Il keystore è un file codificato che contiene la chiave per decodificare le password utilizzate dal repository come ad esempio la password di amministrazione del repository, la password di accesso al database, ecc.

    - Per riutilizzare un keystore di una precedente installazione del repository, specificare il percorso e la password per il keystore. La chiave del keystore precedente verrà estratta e utilizzata nel nuovo keystore. Si precisa che il JRE utilizzato per eseguire il server delle applicazioni deve essere compatibile con il JRE utilizzato per creare le chiavi di crittografia.

    - Se non si riutilizza un keystore esistente, specificare e confermare la password per il nuovo keystore. Il keystore verrà creato in `<repository installation directory>/keystore`.

Importante: Se si perde il file keystore, l'applicazione non sarà in grado di decodificare le password e non sarà utilizzabile. Sarà necessario reinstallarla. Si consiglia di salvare le copie di backup del file Keystore.

7. Specificare il valore password da utilizzare per l'account utente amministratore del repository. (admin). Questa password viene utilizzata quando ci si collega al repository per la prima volta.

8. Selezionare la modalità di distribuzione (automatica o manuale) In questo esempio, selezioneremo **automatic**.

9. Esaminare il riepilogo delle informazioni e procedere con la configurazione.

Configurare il cluster

Quando il server IBM SPSS Collaboration and Deployment Services Repository viene distribuito sul cluster WebSphere correttamente, sono necessari alcune passi di configurazione esterni per essere sicuri che ogni nodo nel cluster possa accedere al server o sul sistema di bilanciamento del carico.

1. Impostare CDS_HOME per ogni nodo:

   • Accedere alla console di gestione WebSphere

   • Passare a **Ambiente** > **Variabili WebSphere**

   • Verificare il valore della variabile **CDS_HOME** per ogni nodo. Se un nodo WebSphere si trova su un server diverso rispetto al server Repository, aggiornare il valore di CDS_HOME in modo da puntare alla directory di installazione condivisa (ad esempio, \\<Management_Host>\SPSS\Deployment \8.2\Server, dove <Management_Host> è il nome host della macchina su cui è installato il server Repository.

2. Impostare Log4j Properties per ogni nodo:

   • Accedere alla console di gestione WebSphere

   • Individuare la proprietà log4j.cnfiguration in **Server** > **Server delle applicazioni WebSphere** > **[nome server]** > **Java e gestione processo** > **Definizione processo** > **JVM (Java Virtual Machine)** > **Proprietà personalizzate**. Questa proprietà identifica l'ubicazione in cui il sistema di registrazione può accedere al file di configurazione di registrazione. Generalmente, questa proprietà ha un valore di file://${CDS_HOME}\platform\log4j.properties. In Windows, se la variabile CDS_HOME contiene una lettera di unità, aggiungere una barra, (/) un carattere di escape al valore log4j.configuration (ad esempio file:///${CDS_HOME}\platform\log4j.properties).

   • Salvare e sincronizzare le modifiche.

Sistema di bilanciamento del carico

È necessario configurare un sistema di bilanciamento del carico basato su software o hardware per accedere al repository in un ambiente cluster. I server delle applicazioni WebSphere forniscono programmi di utilità di bilanciamento del carico basati su software integrato (ad esmpio, IBM HTTP Server). I seguenti passi descrivono l'installazione e configurazione di IBM HTTP Server.

Installazione IBM HTTP Server

1. Avviare IBM Installation Manager

2. Configurare Installation Manager per utilizzare un repository che contenga i file di installazione IBM HTTP Server.

3. Fare clic su **Installa**.

4. Selezionare le seguenti offerte di prodotto da installare e fare clic su **Avanti**.

   • IBM HTTP Server for WebSphere Application Server

   • Plug-in Server web per IBM WebSphere Application Server

5. Accettare i termini degli accordi di licenza e fare clic su **Avanti**.

6. Specificare la directory di installazione e fare clic su **Avanti**.

7. Selezionare le funzioni da installare e fare clic su **Avanti**.

8. Configurare i dettagli per IBM HTTP Server.

9. Esaminare le informazioni di riepilogo e fare clic su **Installa**.

Creare una definizione server web nel cluster WebSphere

1. Accedere alla console di gestione WebSphere per il profilo di gestione all'indirizzo `https://hostname:port/ibm/console/logon.jsp`, in cui `hostname` è il nome host della macchina di gestione e `port` è la porta della console di gestione.

2. Passare a **Tipi di server** > **Server web** e fare clic su **Nuovo** per creare una nuova definizione server web.

3. Specificare il nome server e selezionare il nodo che corrisponde al server web che si desidera aggiungere. Generalmente, il nodo dovrebbe essere sullo stesso server in cui è installato HTTP. Per il tipo, selezionare **IBM HTTP Server** e fare clic su **Avanti**.

4. Selezionare il modello che corrisponde al server che si desidera creare e fare clic su **Avanti**. In questo esempio si utilizzerà l'impostazione predefinita.

5. Specificare le proprietà per il nuovo server web.

6. Esaminare il riepilogo della nuova definizione server web e fare clic su **Fine**.

7. Salvare le modifiche.

Configurare il server web

1. Accedere alla console di gestione WebSphere per il profilo di gestione.

2. Trovare il file `conf.httpd` in **Server** > **Tipi di server** > **Server web** > **[nome server]**. Aggiungere il seguente script al file:

```
LoadModule was_ap22_module "<Plug-ins directory>\bin\32bits\mod_was_ap22_http.dll"
WebSpherePluginConfig "<Plug-ins directory>\config\<web server name>\plugin-cfg.xml"
```

Dove `<Plug-in directory>` è la directory di installazione dei plug-in del server Web e `<Web server name>` è il nome del server Web.

3. Passare a **Server** > **Tipi di server** > **Server web**, selezionare il server web e fare clic su **Genera plug-in**.

4. Fare clic su **Propaga plug-in** per trasmettere il plug-in.

5. Passare a **Server** > **Tipi di server** > **Server Web** > **[nome server]** e visualizzare `plugin-cfg.xml` per confermare che tutti gli URI per IBM SPSS Collaboration and Deployment Services siano stati generati (ad esempio, `<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/admin/*"/>`.

Impostare la proprietà del prefisso URL

In un ambiente cluster, la proprietà di configurazione del repository **URL_Prefix** viene utilizzata per instradare le richieste HTTP avviate dal server. La proprietà deve essere impostata sull'URL del sistema di bilanciamento del carico. Considerare che è possibile impostare questa proprietà quando si esegue inizialmente il programma di utilità della configurazione IBM SPSS Collaboration and Deployment Services Repository.

Per impostare o aggiornare il valore della proprietà del prefisso URL dopo la configurazione del repository:

1. Avviare un singolo membro del cluster.

2. Aprire IBM SPSS Deployment Manager basato sul browser passando a `http://<repository host>:<port number>/security/login` ed effettuando l'accesso con l'account admin creato durante la configurazione del repository.

3. Aggiornare la proprietà di configurazione **URL_Prefix** con l'URL del sistema di bilanciamento del carico per il cluster. Salvare le modifiche.

4. Interrompere il membro del cluster in esecuzione. Avviare il cluster.

Post-installazione

La seguente checklist guida l'utente nei passi di post-installazione:

1. Avviare il server e verificare la connettività (istruzioni fornite dopo questa sezione).

2. Installare gli adattatori di contenuto necessari per utilizzare IBM SPSS Collaboration and Deployment Services Repository con altri prodotti SPSS come ad esempio IBM SPSS Modeler o IBM SPSS Statistics.

3. Se necessario, installare IBM SPSS Collaboration and Deployment Services Remote Process Server e IBM SPSS Collaboration and Deployment Services - Essentials for Python. Per ulteriori informazioni, fare riferimento ale istruzioni di installazione per tali componenti.

4. Installare i client IBM SPSS Collaboration and Deployment Services incluso IBM SPSS Deployment Manager. Per ulteriori informazioni, consultare le istruzioni di installazione dell'applicazione client.

5. Utilizzando IBM SPSS Deployment Manager, creare gli utenti e gruppi del repository ed assegnare loro le autorizzazioni all'applicazione mediante i ruoli. Per ulteriori informazioni, consultare *IBM SPSS Collaboration and Deployment ServicesAdministrator's Guide*.

Se si rilevano problemi durante i passi di post-installazione, consultare *IBM SPSS Collaboration and Deployment ServicesTroubleshooting Guide*.

Avviare il server del reposotory

Per i server di cluster WebSphere, il server del repository si avvia automaticamente quando si avvia il server delle applicazioni. Avviare il server delle applicazioni utilizzando gli script forniti con gli strumenti di gestione WebSphere

1. Accedere alla macchina di gestione e avviare il nodo di gestione:

   - Windows: `<WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startManager.bat`
   - Linux/UNIX: `<WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startManager.sh`

2. Accedere ad ogni macchina e avviare ogni agent del nodo gestito:

   - Windows: `<WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startNode.bat`
   - Linux/UNIX: `<WebSphere Installation Directory>\profiles\<PROFILE_NAME>\bin>startNode.sh`

3. Accedere alla console di gestione WebSphere per il nodo di gestione (`http://hostname:port/ibm/console`). Passare a **Server** > **Tipi di server** > **Server delle applicazioni WebSphere**, selezionare ogni nodo e fare clic su **Avvia**.

4. Passare a **Server** > **Tipi di server** > **Server web** e fare clic su **Avvia**.

Importante: Per evitare conflitti di autorizzazione, il server del repository deve sempre essere avviato utilizzando le stesse credenziali, preferibilmente un utente con privilegi sudo (UNIX) o a livello di amministratore (Windows).

Verificare la connettività

È possibile verificare che il server IBM SPSS Collaboration and Deployment Services Repository sia in esecuzione accedendo a IBM SPSS Deployment Manager basato sul browser in un browser Web supportato all'indirizzo `http://<repository host>:<port number>/security/login`. Se lo strumento non si avvia, il server probabilmente non è in esecuzione. Fare riferimento ai report sulla compatibilità del prodotto software IBM all'indirizzo https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html per ulteriori informazioni relative ai browser web supportati.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Index

scoring 5
scoring servers 5
Secure Sockets Layer 59
securing
    LDAP 61
security events
    logging 65
server clustering 24–26
server updates 41
session affinity 26
SIB 40
sicurezza
    SSL 59
silent
    IBM Installation Manager 34
    package installation 41
    unistalling 34
single sign-on
    Active Directory 45
    application server configuration 46
    Google Chrome 51
    JBoss 47
    Microsoft Internet Explorer 51
    MIT Kerberos 44
    Mozilla Firefox 51
    one-way trust 48
    OpenLDAP 44
    registry update files 48
    WebSphere 46
    Windows Kerberos Server 44
SPNEGO 51
SSL
    certificates 57
    overview 59
    securing communications 59
SSL per JBoss 62
SSL per Liberty 62
SSL per WebSphere 62
supported applications 30
symmetric encryption 57
System Integration Bus 16

U

UNC 25
unistalling 34
URL prefix 26, 54, 61
user preferences 4
user privileges 11

V

version check 41
versions
    IBM SPSS Modeler 30
    IBM SPSS Statistics 30
virtualization 11
VMWare 11

W

WebLogic 24
WebLogic Apache Plugin 24, 26

WebSphere
    automatic deployment 25
    cluster 25
    manual deployment 25
    single sign-on 46
Windows share 25
Windows Terminal Services 11