

IBM SPSS Collaboration and Deployment Services
Repository
Version 8 Release 2

Installation and Configuration Guide



Note

Before using this information and the product it supports, read the information in "Notices" on page 69.

Informazioni sul prodotto

Questa edizione si applica alla versione 8, release 2, livello di modifica 0 di IBM SPSS Collaboration and Deployment Services e a tutte le successive release e modifiche a meno che non diversamente indicato nelle nuove edizioni.

© Copyright IBM Corporation 2000, 2018.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Overview 1

IBM SPSS Collaboration and Deployment Services	1
Collaboration	1
Deployment	2
System architecture	2
IBM SPSS Collaboration and Deployment Services	
Repository	3
IBM SPSS Deployment Manager	4
IBM SPSS Collaboration and Deployment Services	
Deployment Portal	4
Server di esecuzione	5
Scoring server	5
IBM Analytical Decision Management	6
License tracking	6

Chapter 2. Novità per gli addetti all'installazione 7

Modifiche in questa release	7
Funzionalità obsolete	7

Chapter 3. Installation 9

Pre-installation	9
Planning your installation	10
Requisiti del sistema host	10
Server delle applicazioni	12
Database	14
Installazione e configurazione	19
Installazione e configurazione	19
Configurazione del cluster	23
Post-installation	25
Avvio del server di repository	26
Verifica della connettività	27
Gestione della password del database	27
Driver JDBC	29
IBM SPSS products compatibility	29
Disinstallazione	30

Chapter 4. Migrazione 31

Installing with a copy of the repository database	31
Installing with an existing repository database	32
Migrazione su un database diverso	32
Ulteriori considerazioni sulla migrazione	33
Migrazione della password	33
JMS store migration on WebSphere	33
Migrating notification templates	34

Chapter 5. Package management 35

Installazione dei package	35
-------------------------------------	----

Chapter 6. Single sign-on 37

Directory configuration for single sign-on	38
--	----

OpenLDAP	38
Active Directory	39
Kerberos server configuration	40
Application server configuration for single sign-on	40
WebSphere	40
JBoss	41
Updating Windows registry for single sign-on	42
Configuring one-way trust relationships	42
Configurazione di Server Process Credential	43
Configuring browsers for single sign-on	45
Forwardable tickets and IBM SPSS Deployment Manager	45

Chapter 7. Application context roots . . . 47

Configurazione delle root di contesto delle applicazioni	47
Adding a context root to the URL Prefix	48
Updating context roots for WebSphere	48
Updating context roots for JBoss	49

Chapter 8. FIPS 140–2 compliance . . . 51

Repository configuration	51
Desktop client configuration	52
Browser configuration	52

Chapter 9. Using SSL to secure data transfer 53

How SSL works	53
Securing client/server and server-server communications with SSL	53
Installing unlimited strength encryption	53
Adding the certificate to client keystore (for connections to the repository)	54
Importing the certificate file for browser-based client connections	54
Instructing users to enable SSL	55
URL prefix configuration	55
Securing LDAP with SSL	55

Chapter 10. Registrazione 57

Chapter 11. Esempio: Installazione e configurazione cluster Websphere . . . 59

Notices 69

Privacy policy considerations	70
Trademarks	71

Index 73

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.

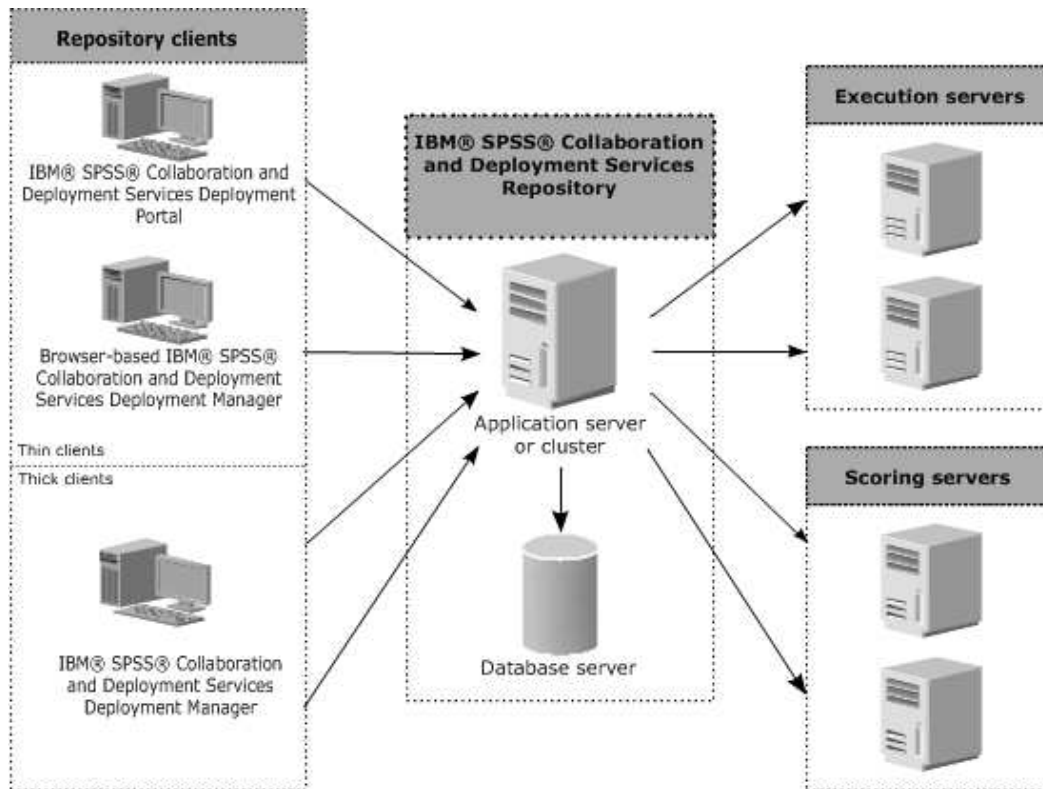


Figure 1. IBM SPSS Collaboration and Deployment Services Architecture

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`

Server di esecuzione

I server di esecuzione consentono di eseguire le risorse archiviate nel repository. Inserendo una risorsa in un lavoro per essere eseguita, nel definire la fase di lavoro viene specificato il server di esecuzione destinato alla sua elaborazione. Il tipo di server di esecuzione dipende dalla risorsa.

I server di esecuzione attualmente supportati da IBM SPSS Collaboration and Deployment Services sono:

- **Processo remoto.** Un server di esecuzione per processi remoti consente l'inizializzazione e il monitoraggio dei processi su server remoti. A processo ultimato, restituisce un messaggio di operazione riuscita o non riuscita. Qualsiasi computer che funge da remote process server deve essere dotato dell'opportuna infrastruttura di comunicazione con il repository.

Note: IBM SPSS Collaboration and Deployment Services Remote Process Server dispone di una dimensione core del pool di thread di 16 che consente l'esecuzione di un massimo di 16 lavori simultanei su un singolo remote process server. Qualsiasi lavoro simultaneo oltre i 16 deve attendere nella coda finché il pool di thread disponibile non liberi risorse. Per configurare manualmente la dimensione core del pool di thread di IBM SPSS Collaboration and Deployment Services Remote Process Server aggiungere la seguente opzione JVM (con un valore definito dall'utente) allo script di avvio di remote process server `prms.thread.pool.coresize=<user defined value>`

Per ulteriori informazioni relative allo script di avvio, consultare la sezione "Avvio e arresto remote process server" nella guida IBM SPSS Collaboration and Deployment Services Remote Process Server.

I server di esecuzione che elaborano altri tipi specifici di risorse possono essere aggiunti al sistema installando gli opportuni adattatori. Per informazioni, consultare la documentazione delle risorse in questione.

Nel definire il lavoro, assegnare a ciascuna fase un server di esecuzione. Quando viene eseguito il lavoro, il repository utilizza i server di esecuzione specificati per effettuare le relative analisi.

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. Novità per gli addetti all'installazione

IBM SPSS Collaboration and Deployment Services Repository 8.2 offre nuove capacità che aiutano a semplificare la distribuzione delle funzionalità di analisi predittiva e gestire i costi.

Supporto per più piattaforme

IBM SPSS Collaboration and Deployment Services Repository 8.2 include il supporto per le nuove versioni di sistemi operativi, incluso AIX 7.1 e Ubuntu 16.04 LTS s390x, server delle applicazioni, database, ambienti di virtualizzazione e browser web.

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

IBM SPSS Collaboration and Deployment Services Repository combina WebSphere Application Server Liberty Profile per semplificare l'installazione e la distribuzione. È possibile utilizzare questo server delle applicazioni per un'installazione standalone o cluster, o per fornire una propria istanza del server delle applicazioni.

Processo di installazione e configurazione semplificato e automatizzato per IBM SPSS Collaboration and Deployment Services Repository

Il nuovo programma di installazione offre un processo di installazione e configurazione semplificato sfruttando la piena funzionalità di IBM Installation Manager.

Modifiche in questa release

Oracle WebLogic Server non è più supportato.

Funzionalità obsolete

Se si sta eseguendo la migrazione da una release precedente di IBM SPSS Collaboration and Deployment Services, è necessario essere a conoscenza delle diverse funzioni che sono state rese obsolete dall'ultima versione.

Se una funzione è obsoleta, IBM Corp. potrebbe rimuovere questa funzionalità in una release successiva del prodotto. Gli investimenti futuri saranno attivati sulla funzione strategica elencata sotto Azione di migrazione consigliata. Solitamente una funzione non viene resa obsoleta finché non ne viene fornita una alternativa equivalente.

Nessuna funzione è obsoleta in questa release. A scopo di riferimento, la seguente tabella indica le funzioni obsolete nelle recenti versioni precedenti del prodotto. Ove possibile la tabella indica anche le azioni di migrazione consigliate.

Table 1. Funzioni obsolete nelle versioni precedenti

Funzione obsoleta	Azione di migrazione consigliata
Provider di sicurezza: Active Directory con sostituzione locale, che supporta gruppi estesi ed utenti consentiti	Utilizzare il provider di sicurezza Active Directory con tutti i gruppi necessari aggiunti
IBM SPSS Collaboration and Deployment Services Enterprise View	Utilizzare la funzione Vista dati analitici
IBM SPSS Collaboration and Deployment Services Enterprise View Driver	Utilizzare la funzione Vista dati analitici

Table 1. Funzioni obsolete nelle versioni precedenti (continued)

Funzione obsoleta	Azione di migrazione consigliata
File Scenario	I file scenario (.scn) non sono più supportati. I nodi di origine Enterprise View non possono essere modificati in Deployment Manager. I file scenario precedenti possono essere modificati nel client IBM SPSS Modeler e salvati nuovamente come file di flusso. Sarà inoltre necessario eliminare le configurazioni di calcolo del punteggio che utilizzavano un file scenario e salvarle nuovamente sulla base di un file di flusso.
Installazione Web per IBM SPSS Deployment Manager	Utilizzare il programma di installazione autonomo
BIRT Report Designer for IBM SPSS	Nessuna
Visualizzatore BIRT Report Designer for IBM SPSS	Nessuna
IBM SPSS Collaboration and Deployment Services Portlet	Utilizzare direttamente IBM SPSS Collaboration and Deployment Services Deployment Portal oppure utilizzare le API dei servizi Web
IBM SPSS Collaboration and Deployment Services Web Part	Utilizzare direttamente IBM SPSS Collaboration and Deployment Services Deployment Portal oppure utilizzare le API dei servizi Web
API Servizio di calcolo del punteggio V1	API Servizio di calcolo del punteggio V2
Servizio pianificazione server	Nessuna
Servizio gestione report	Nessuna
Operazione login di Servizio di autenticazione	Operazione doLogin Servizio di autenticazione
Operazione search di Servizio di ricerca	Operazione search2.5 di Servizio di ricerca
Jar del client dei servizi Web SPSS AXIS/Castor	Utilizzare gli strumenti forniti con JRE (Java Runtime Environment), IDE (Integrated Development Environment) o Eclipse WTP (Web Tools Platform)
Funzione API clemrt1_setLogFile()	Nessuna

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, "Using SSL to secure data transfer," on page 53 for more information.
- FIPS 140-2 security and secure repository database connection. See the topic Chapter 8, "FIPS 140-2 compliance," on page 51 for more information.
- Single sign-on. See the topic Chapter 6, "Single sign-on," on page 37 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, "Migrazione," on page 31 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 “Requisiti del sistema host” 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.

Requisiti del sistema host

Prima di installare IBM SPSS Collaboration and Deployment Services Repository, verificare che i seguenti requisiti hardware e software siano stati soddisfatti. Se l'installazione viene eseguita utilizzando un cluster di server delle applicazioni, è necessario che i requisiti siano soddisfatti su tutti i nodi.

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>

Importante: La quantità di RAM specificata costituisce il requisito minimo per installare e avviare il repository. In funzione del tipo di elaborazione analitica eseguita da IBM SPSS Collaboration and Deployment Services, il fabbisogno di memoria runtime potranno essere sostanzialmente superiore e utilizzare un'ampia parte della RAM tipicamente presente sui sistemi a livello di server. Si precisa che l'installazione degli adattatori per il repository di altri prodotti IBM SPSS, quali gli adattatori IBM SPSS Modeler, richiede la designazione di memoria aggiuntiva. Nel valutare i requisiti di memoria, si consiglia di consultare la documentazione del server delle applicazioni prescelto.

Se l'installazione avviene in WebSphere, il profilo WebSphere utilizzato con IBM SPSS Collaboration and Deployment Services deve essere configurato per essere eseguito con Java 7 SDK o successivo. Consultare “WebSphere” on page 12.

Requisiti aggiuntivi IBM Installation Manager (per tutti i sistemi operativi)

IBM Installation Manager 1.8.9 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.

Autorizzazioni utente e file system

Come regola generale, è necessario installare e configurare il repository con le stesse autorizzazioni utente utilizzate per installare e configurare il server delle applicazioni. Consultare la documentazione del produttore del server delle applicazioni per informazioni su come supportare le installazioni senza essere un utente root/amministratore.

L'utente autore dell'installazione deve essere dotato delle seguenti autorizzazioni sul sistema host:

- Autorizzazioni di scrittura nella directory di installazione e relative sottodirectory.
- Autorizzazioni di scrittura per le directory di distribuzione e configurazione, e autorizzazioni di lettura ed esecuzione per le altre directory del server delle applicazioni.
- Quando il repository è installato con un cluster di server delle applicazioni, la directory di installazione del repository sulla macchina che ospita il profilo di gestione (profilo WebSphere tradizionale o profilo Liberty) deve poter essere condivisa da tutti i nodi disponibili del cluster.

Note: nell'installare gli adattatori di contenuto di IBM SPSS, è necessario che l'utente sia lo stesso utilizzato per l'installazione di IBM SPSS Collaboration and Deployment Services Repository.

Importante: Se si installa IBM SPSS Collaboration and Deployment Services Repository su Windows utilizzando un account dell'amministratore, sarà necessario utilizzare le autorizzazioni di amministratore per eseguire tutti i programmi di utilità e gli script correlati, come il programma di utilità per la configurazione.

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 "Requisiti del sistema host" 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.

Server delle applicazioni

Prima di installare IBM SPSS Collaboration and Deployment Services Repository, è necessario che sia installato ed accessibile un server delle applicazioni o un cluster di server supportato.

È possibile utilizzare un singolo server, IBM WebSphere Application Server di base incluso con IBM SPSS Collaboration and Deployment Services o qualsiasi altro server delle applicazioni supportato. Il server delle applicazioni incluso è concesso in licenza solo per l'utilizzo con IBM SPSS Collaboration and Deployment Services Repository e non è possibile utilizzarlo in un ambiente cluster. Per ulteriori informazioni relative a IBM WebSphere, consultare la documentazione del prodotto in IBM Knowledge Center

Se il repository viene reinstallato, ricreare il server delle applicazioni, ad esempio, mediante la distribuzione di un nuovo profilo WebSphere. Accertarsi che alle installazioni del server delle applicazioni siano applicate le versioni di patch del fornitore più recenti. Quando si installa IBM SPSS Collaboration and Deployment Services Repository con un cluster di server delle applicazioni, tutti i nodi cluster devono essere alla stessa versione del server delle applicazioni ed essere eseguiti sullo stesso sistema operativo.

Il server delle applicazioni deve essere configurato con un JRE appropriato. Verificare che Java sia in esecuzione in modalità in 64 bit e che il server delle applicazioni funzioni correttamente in modalità 64 bit prima di provare ad installare IBM SPSS Collaboration and Deployment Services Repository. Ad esempio, se si utilizza JBoss e si dispone di entrambe le versioni di JDK a 32 bit e a 64 bit installate, configurare la JVM in modalità a 64 bit specificando l'opzione `-d64` per il comando Java. Per la distribuzione per il profilo WebSphere Liberty, IBM JRE è fornito con IBM SPSS Collaboration and Deployment Services. Per ulteriori informazioni, consultare la documentazione del produttore del server delle applicazioni.

Importante: Per supportare le connessioni dai browser web che hanno i cookie disabilitati, è necessario abilitare la riscrittura URL per il proprio server delle applicazioni. In WebSphere, ad esempio, questa impostazione è disponibile nella console di gestione in **Server delle applicazioni > server1 > Contenitore Web > Gestione sessioni > Abilita riscrittura URL**. Per ulteriori informazioni, consultare la documentazione del server delle applicazioni.

Limitazione: La riscrittura URL non è supportata dalle funzioni che sono state rese obsolete nelle release precedenti. Tali funzioni possono richiedere l'abilitazione dei cookie.

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-6.1.
- 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 può essere eseguito solo con un server autonomo IBM WebSphere Liberty o un cluster.

Prima di eseguire l'installazione con un cluster Liberty

Creare un cluster WebSphere Liberty ed accertarsi che sia accessibile attraverso il sistema di bilanciamento del carico.

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.

Autorizzazioni del database

La seguente tabella identifica le autorizzazioni generali del database che non necessari ad un utente per installare, applicare delle correzioni, aggiornare ed eseguire IBM SPSS Collaboration and Deployment Services Repository:

Table 2. Autorizzazioni dell'utente per l'attività di manutenzione del repository

Autorizzazione	Installazione, Applicazione Fix Pack, Migrazione	Tempo di esecuzione
Modifica qualsiasi schema	Richiesto	Facoltativo
Crea funzione	Richiesto	Facoltativo
Crea procedura	Richiesto	Facoltativo
Crea tabella	Richiesto	Facoltativo
Crea vista	Richiesto	Facoltativo
Crea raccolte di schemi XML	Richiesto	Facoltativo
Connetti	Richiesto	Richiesto
Elimina	Richiesto	Richiesto
Esegui	Richiesto	Richiesto
Inserisci	Richiesto	Richiesto
Riferimenti	Richiesto	Richiesto
Seleziona	Richiesto	Richiesto
Aggiorna	Richiesto	Richiesto

Ad esempio, quando si installa il repository, è necessario che ci siano tutte le autorizzazioni nella tabella. Dopo l'installazione, molte delle autorizzazioni possono essere rimosse prima di iniziare ed eseguire il repository. Per applicare un fix pack, queste autorizzazioni è necessario che siano reintegrate.

L'esatta denominazione di tali autorizzazioni varia in funzione del database, mentre altre autorizzazioni potrebbero essere necessarie. I seguenti esempi illustrano le autorizzazioni per specifici sistemi di database.

Esempio: 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 fornisce il privilegio create schema esplicito richiesto per la configurazione di IBM SPSS Collaboration and Deployment Services Repository.

Esempio: 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

Esempio: Oracle 12cR1

Sono richieste le seguenti autorizzazioni per configurare IBM SPSS Collaboration and Deployment Services Repository con il database Oracle 12cR1

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

Sono necessarie le seguenti autorizzazioni per avviare IBM SPSS Collaboration and Deployment Services Repository con il database Oracle 12c:

- CREATE SESSION
- ALTER SESSION
- SESSIONS_PER_USER - deve essere impostato con un valore uguale o maggiore a 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 z/OS 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.

Repository database maintenance

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

Table 4. Repository database maintenance schedule

Task	Recommended schedule
Backup	Daily
Update statistics	Daily
Consistency check	Weekly
Reorganize	Weekly
Rebuild	Monthly

Installazione e configurazione

Utilizzare il seguente elenco di controllo come guida per l'installazione di un server delle applicazioni autonomo:

- Installare i file dell'applicazione sul sistema host usando IBM Installation Manager.
- Inoltre in Installation Manager, immettere le informazioni del server delle applicazioni preconfigurato e del database, quindi configurare IBM SPSS Collaboration and Deployment Services Repository da utilizzare con il server delle applicazioni e il database.

Mentre le operazioni descritte per il server autonomo sono anche applicabili in un'installazione di cluster, l'installazione su una topologia cluster richiede dei passi aggiuntivi. Per ulteriori informazioni, consultare la sezione "Configurazione del cluster" on page 23.

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 "Configurazione del cluster" on page 23.

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 "Autorizzazioni utente e file system" on page 11.
2. Avviare IBM Installation Manager:

Modalità GUI:

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

Modalità riga di comando:

```
<directory installazione IBM Installation Manager>/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.

Note: 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.

Note: 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 standardone.
 - **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 conetteranno a IBM SPSS Collaboration and Deployment Services Repository.
 - Liberty
 - **Autonomo.** Il profilo WebSphere Liberty è fornito 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.
 - **Prefisso URL.** Visibile solo quando si seleziona **Cluster**. Questo è l'URL per l'instradamento delle richieste avviate dal server. Generalmente è la porta del sistema di bilanciamento del carico per la configurazione del cluster.
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 *<directory installazione repository>/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 genera 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 la verifica della connettività. Per ulteriori informazioni, consultare la sezione "Post-installation" on page 25.
 - Se si sceglie la modalità di distribuzione manuale, procedere con le fasi manuali. Per ulteriori informazioni, consultare la sezione Distribuzione manuale.
 - 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 "Configurazione del cluster" on page 23.

Note: Il completamento dell'operazione di configurazione può richiedere 15-30 minuti o più a seconda dell'hardware, della velocità di rete, della complessità della topologia del server delle applicazioni ecc. Se sembra che il processo di configurazione non risponde o se viene segnalato un errore, esaminare i file di log nella directory di installazione *<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' installLocation='/opt/IBM/SPSS/Deployment/8.2/Server'>
    <data key='cic.selector.arch' value='x86_64' />
    <data key='user.LibertyTopologyUserData,com.ibm.spss.cds.server.v8.2.offering' value='single' />
    <data key='user.KeyPassUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
    <data key='user.ReuseKeyUserData,com.ibm.spss.cds.server.v8.2.offering' value='false' />
    <data key='user.KeyPwdUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
    <data key='user.AdminPassUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
    <data key='user.AdminPwdUserData,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
    <data key='user.DBPort,com.ibm.spss.cds.server.v8.2.offering' value='50000' />
  </profile>
</agent-input>
```

```

<data key='user.DBName,com.ibm.spss.cds.server.v8.2.offering' value='cadsdb' />
<data key='user.DBHost,com.ibm.spss.cds.server.v8.2.offering' value='x.x.x.x' />
<data key='user.DBTypeUserData,com.ibm.spss.cds.server.v8.2.offering' value='db2' />
<data key='user.DataEraseUserData,com.ibm.spss.cds.server.v8.2.offering' value='false' />
<data key='user.DBPassword,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
<data key='user.SSLServiceUserData,com.ibm.spss.cds.server.v8.2.offering' value='false' />
<data key='user.OracleServiceUserData,com.ibm.spss.cds.server.v8.2.offering' value='false' />
<data key='user.DBUsername,com.ibm.spss.cds.server.v8.2.offering' value='xxxx' />
</profile>
<install>
<!-- IBM SPSS Collaboration and Deployment Services - Repository Server 8.2.0.0 -->
<offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.cds.server.v8.2.offering' fe
<!-- IBM SPSS Modeler Adapters for Collaboration and Deployment Services 18.2.0.0 -->
<offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.modeler.adapter.18.2.0' fea
<!-- IBM SPSS PMML Scoring Adapter 8.2.0.0 -->
<offering profile='IBM SPSS Collaboration and Deployment Services 8.2' id='com.ibm.spss.pmml.scoring.adapter.v8.2' f
</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:

```

<Directory di installazione IBM Installation Manager>/eclipse/tools/imcl input
responseFile -acceptLicense -showProgress

```

Configurazione del cluster

IBM SPSS Collaboration and Deployment Services Repository può essere distribuito in ambienti di server delle applicazioni in cluster. Tuttavia, la configurazione di ciascun server delle applicazioni nel cluster deve essere identica a quella dei componenti dell'applicazione ospitata e l'accesso al repository deve avvenire attraverso un software di bilanciamento del carico. Questa architettura consente che l'elaborazione sia distribuita tra più server delle applicazioni e consente anche la ridondanza nel caso di errore di un singolo server.

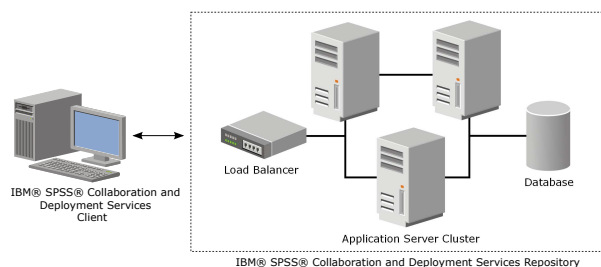


Figure 2. Architettura di distribuzione in cluster

Il processo di installazione del repository su un cluster prevede le seguenti fasi:

- Installazione e configurazione iniziali dei componenti dell'applicazione su un nodo di gestione del cluster.
- Successiva configurazione dei nodi del cluster.

IBM SPSS Collaboration and Deployment Services Repository attualmente supporta il clustering di profili WebSphere Application Server tradizionale e Liberty. Attenersi alle istruzioni specifiche per i server delle applicazioni per completare la distribuzione.

Requisiti di installazione

- I requisiti del sistema host devono essere soddisfatti su tutti i nodi del cluster.
- Tutti i membri del cluster IBM SPSS Collaboration and Deployment Services Repository devono essere eseguiti nello stesso ambiente operativo del nodo principale (di gestione).
- Il database del repository deve essere già stato definito ed essere accessibile
- Prima di installare IBM SPSS Collaboration and Deployment Services Repository, è necessario che la topologia del server delle applicazioni sia stata già definita. Si consiglia di verificare che il cluster sia accessibile e funzionale presso l'indirizzo di bilanciamento del carico.
- La directory di installazione di IBM SPSS Collaboration and Deployment Services Repository deve essere condivisa tra tutti i nodi del cluster.

Cluster WebSphere

1. Verificare che tutti i requisiti siano stati soddisfatti.
2. Eseguire l'installazione e la configurazione. È possibile scegliere di distribuire l'applicazione automaticamente o manualmente. Per ulteriori informazioni, consultare la sezione "Installazione e configurazione" on page 19.
3. Configurare la condivisione della directory di installazione per consentire l'accesso a tutti i membri del cluster.
4. Impostare il valore della variabile **CDS_HOME** per ogni nodo.
 - Aprire la console di gestione
 - Aprire la sezione **Ambiente > Variabili WebSphere**.
 - Per ciascun nodo nel cluster, sarà definita una variabile **CDS_HOME**. Verificare che il valore contenga il percorso appropriato per la directory di installazione condivisa.
5. Impostare il valore della proprietà di sistema Java **log4j.configuration** per ogni membro cluster. Questa proprietà identifica la posizione 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`.
 - Aprire la console di gestione
 - Per ogni server nel cluster, esaminare il valore **log4j.configuration**. Questo valore è disponibile in **Server delle applicazioni > nome-server > Definizione processo > Java Virtual Machine > Proprietà personalizzate**, in cui *nome-server* corrisponde ad un particolare server.
 - Sul sistema operativo Windows, se la variabile **CDS_HOME** dalla procedura 4 contiene una lettera di unità, aggiungere una barra ("/") carattere escape al valore **log4j.configuration**. Ad esempio, il nuovo valore dovrebbe essere `file:///CDS_HOME/platform/log4j.properties`.
6. Salvare e sincronizzare le modifiche.
7. Verificare che il valore della proprietà di configurazione Prefisso URL di IBM SPSS Collaboration and Deployment Services Repository viene impostato correttamente sull'URL del bilanciamento del carico. Per ulteriori informazioni, consultare la sezione "Configurazione del bilanciamento del carico."
8. Avviare il cluster Liberty.

Configurazione del bilanciamento del carico

È necessario configurare un bilanciamento del carico basato su software o hardware per accedere al repository in un ambiente cluster.

I server delle applicazioni forniscono programmi di utilità di bilanciamento del carico basati sul software integrato (ad esempio IBM HTTP Server).

Importante: Abilitare l'affinità di sessione per qualsiasi servizio di bilanciamento del carico utilizzato con cluster di IBM SPSS Collaboration and Deployment Services. Per ulteriori informazioni, consultare la documentazione del produttore del servizio di bilanciamento del carico.

Impostazione della proprietà Prefisso URL

In un ambiente cluster, il valore della proprietà di configurazione del repository *URL_Prefix*, utilizzato per instradare le richieste HTTP avviate dal server, deve essere impostato sull'URL del sistema di bilanciamento del carico. Si precisa che tale proprietà può essere impostata inizialmente durante l'esecuzione del programma di utilità per la configurazione di IBM SPSS Collaboration and Deployment Services Repository. Per ulteriori informazioni, consultare la sezione Configuration.

Per impostare/aggiornare il valore della proprietà prefisso URL a configurazione del repository avvenuta:

- Avviare un singolo membro del cluster.
- Aprire IBM SPSS Deployment Manager basato su browser passando a *http://<host repository>:<numero porta>/security/login*.
- Aggiornare la proprietà di configurazione *URL_Prefix* con l'URL di bilanciamento del carico associato al cluster e salvare le modifiche.
- Interrompere il membro del cluster in esecuzione.
- Avviare il cluster.

Espansione del cluster

Negli ambienti enterprise sottoposti a ampi carichi di elaborazione, potrebbe essere necessario espandere il cluster che esegue IBM SPSS Collaboration and Deployment Services Repository aggiungendo nodi dopo l'installazione iniziale.

WebSphere

1. Creare ulteriori profili gestiti WebSphere e unirli alla cella. Creare server e aggiungerli al cluster utilizzando la console WebSphere.
2. Eseguire lo script *CrtCDSresources.py* nella directory */toDeploy/* per aggiornare i nuovi nodi definiti per la cella.

```
/bin/wsadmin -lang jython -f CrtCDSresources.py -update
```
3. Impostare il valore della variabile *CDS_HOME* per ogni nodo. Per ulteriori informazioni, consultare la sezione "Cluster WebSphere" on page 24.
4. Riavviare il 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 Installation Instructions* and *IBM SPSS Collaboration and Deployment Services - Essentials for Python 8.2 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 Administrator's Guide*.

If problems occur during post-installation steps, see *IBM SPSS Collaboration and Deployment Services 8.2 Troubleshooting Guide*.

Avvio del server di repository

Il server di repository può essere eseguito su console o in background.

L'esecuzione su console permette la visualizzazione dei messaggi relativi all'elaborazione e può risultare utile per la diagnosi di comportamenti imprevisti. Tuttavia, di norma, il server di repository viene eseguito in background, gestendo richieste da client, quali IBM SPSS Modeler o IBM SPSS Deployment Manager.

Note: L'esecuzione simultanea di altre applicazioni può ridurre le prestazioni del sistema e la velocità di avvio.

Su piattaforme Windows, l'esecuzione su console corrisponde all'esecuzione in una finestra di comando. L'esecuzione in background corrisponde all'esecuzione come servizio Windows. Al contrario, su una piattaforma UNIX, l'esecuzione su console corrisponde all'esecuzione in una shell e l'esecuzione in background corrisponde all'esecuzione come daemon.

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

Il server di repository viene avviato inizializzando il server delle applicazioni. Questa operazione può essere eseguita con gli script forniti con l'installazione del server di repository o gli strumenti di amministrazione nativi del server delle applicazioni. Per ulteriori informazioni, consultare la documentazione del produttore del server delle applicazioni.

WebSphere

Utilizzare gli strumenti di amministrazione di WebSphere. Per ulteriori informazioni, consultare la documentazione WebSphere.

WebSphere Liberty autonomo

Per impostazione predefinita, il profilo Liberty fornito utilizza 9080 per l'endpoint HTTP e 9443 per l'endpoint HTTPS. Se si desidera modificare questi numeri della porta, aggiornare il file `server.xml` nella seguente directory:

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

Se si utilizzano i numeri della porta predefiniti, accertarsi che il numero della porta non sia già utilizzato da altre applicazioni prima di avviare il server. Utilizzare i seguenti script con l'installazione del repository:

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

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

Durante il processo di avvio di WebSphere Liberty, si avvierà prima il profilo Liberty e poi verrà distribuita l'applicazione. Per verificare lo stato del server, esaminare il file `cds.log` in `<directory di installazione del repository >/wlp/usr/servers/cdsServer/`.

Cluster WebSphere Liberty

Prima di avviare il server del repository che è stato distribuito sul cluster WebSphere Liberty, generare i file di configurazione correlati. Questi file sono richiesti da Liberty per i membri collettivi nel cluster e includono i file di configurazione in `server.xml` in ogni membro collettivo.

Utilizzare i seguenti script con l'installazione del server di repository:

```
<repository installation directory>/bin/configUtility.bat  
<repository installation directory>/bin/configUtility.sh
```

Specificare i valori per:

- **Home CDS.** L'ubicazione dei file di sistema IBM SPSS Collaboration and Deployment Services. Accertarsi che questa ubicazione sia accessibile da tutti i membri collettivi utilizzando la condivisione file in Windows o NFS su Linux/UNIX.
- **Percorso server dei membri controller** La directory locale del server dei membri (ad esempio, `C:\wlp\usr\servers\myController`).
- **Percorso di output del file di configurazione generato** Un'ubicazione valida sul file system locale.

Copiare tutti i file di configurazione generati nella directory in cui è presente il file `server.xml` in ogni membro del cluster. Per ogni membro, aggiungere la seguente riga al file `server.xml` per ogni file `cads.server.xml`:

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

Quindi avviare tutti i membri nel cluster.

JBoss

Utilizzare i seguenti script con l'installazione del server di repository:

```
<directory installazione repository>/bin/startserver.bat  
<directory installazione repository>/bin/startserver.sh
```

In alternativa, è altresì possibile avviare il server utilizzando gli strumenti di amministrazione di JBoss. Per ulteriori informazioni, consultare la documentazione JBoss.

Verifica della connettività

Per verificare che IBM SPSS Collaboration and Deployment Services Repository sia in esecuzione, accedere IBM SPSS Deployment Manager basato su browser utilizzando uno dei seguenti browser Web supportati:

- Internet Explorer 10 o superiore
- Firefox 48 ESR o superiore
- Safari 5 o superiore

Accesso a IBM SPSS Deployment Manager basato su browser

1. Passare alla pagina di accesso all'indirizzo `http://<host repository>:<numero porta>/security/login`.
2. Specificare le credenziali di accesso dell'amministratore. Le credenziali vengono definite durante la configurazione del repository.

Gestione della password del database

La password del database fornita durante la configurazione di IBM SPSS Collaboration and Deployment Services Repository è memorizzata come parte della definizione dell'origine dati nelle impostazioni del server delle applicazioni. Potrebbero essere richieste ulteriori operazioni per garantire la sicurezza password del database.

Verifica della connessione al database

La connessione al database IBM SPSS Collaboration and Deployment Services Repository può essere verificata utilizzando le funzioni di gestione dell'origine dati nella console di gestione del server delle applicazioni.

Server delle applicazioni	Nome oggetto dell'origine dati
WebSphere Tradizionale	CDS_DataSource
WebSphere Liberty	CDS_DataSource
JBoss	jdbc/spss/PlatformDS

Sicurezza oggetti JAAS

Le credenziali per l'origine dati IBM SPSS Collaboration and Deployment Services creata nel server delle applicazioni sono mantenute come oggetto JAAS.

Importante: Quando il repository è configurato su un WebSphere application server utilizzando la distribuzione automatica (con IBM Installation Manager) o con script generati dal programma di utilità di configurazione, la password viene trasferita al server delle applicazioni come testo in chiaro e quindi diviene persistente a seconda delle impostazioni del server delle applicazioni. Sebbene le impostazioni WebSphere predefinite prevedono la memorizzazione delle password in formato codificato, può essere necessario verificare che la password non sia memorizzata come testo in chiaro. Per ulteriori informazioni sulla sicurezza della password, consultare la documentazione del server delle applicazioni.

Modifica della password del database

Per motivi di sicurezza, dopo l'installazione di IBM SPSS Collaboration and Deployment Services Repository, potrebbe essere necessario modificare la password del database. In alcuni casi, la password di database memorizzata può essere modificata utilizzando IBM SPSS Collaboration and Deployment Services Password Utility.

Per eseguire il programma di utilità delle password:

1. Chiudere il server delle applicazioni su cui si trova IBM SPSS Collaboration and Deployment Services.
2. Eseguire in
Windows:
`<directory installazione repository>/bin/cliUpdateDBPassword.bat`
UNIX:
`<directory installazione repository>/bin/cliUpdateDBPassword.sh`
Sistema i:
`<directory installazione repository>/bin/cliUpdateDBPassword.qsh`
3. Avviare il server delle applicazioni su cui si trova IBM SPSS Collaboration and Deployment Services.
4. Specificare e confermare la nuova password utilizzando il prompt dei comandi.

La password può essere modificata anche alterando le impostazioni del server delle applicazioni. Si precisa che la password viene memorizzata in formato crittografato, pertanto la nuova password può essere convertita in una stringa crittografata eseguendo `cliEncrypt.bat/cliEncrypt.sh` e inserendola come argomento della riga di comando.

Driver JDBC

Aggiunta del supporto driver a IBM SPSS Collaboration and Deployment Services Repository

IBM SPSS Collaboration and Deployment Services include una serie di driver JDBC IBM Corp. per tutti i principali sistemi di database: IBM Db2, Microsoft SQL Server, and Oracle. Questi driver JDBC vengono installati per impostazione predefinita con il repository.

Se IBM SPSS Collaboration and Deployment Services non contiene il driver di un database necessario, aggiornare l'ambiente integrando il relativo driver di terze parti. I driver di terze parti possono essere utilizzati potenziando l'installazione del repository con i file del driver.

In base al server delle applicazioni, il percorso dei driver JDBC è il seguente:

- WebSphere: <directory installazione WebSphere>/lib/ext

Per JBoss, è necessario installare il driver JDBC come modulo principale JBoss e registrare il modulo come globale. Per i dettagli, consultare la documentazione JBoss.

Si precisa che per Netezza, è necessario utilizzare la versione 5.0 del driver per accedere ai database versione 4.5 e 5.0.

Aggiunta del supporto driver alle applicazioni client

Per aggiungere un driver JDBC a IBM SPSS Deployment Manager:

1. Chiudere l'applicazione client, se in esecuzione.
2. Creare una cartella denominata JDBC al livello root della directory di installazione del client.
3. Archiviare i file del driver nella cartella JDBC

Una volta aggiunti i file del driver nell'ambiente, è possibile utilizzare il driver in una definizione dell'origine dati. Nella finestra di dialogo Specifica URL e nome JDBC, digitare il nome e l'URL del driver. Consultare la documentazione del driver per rilevare il formato corretto del nome classe e dell'URL.

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.

Disinstallazione

Nel caso in cui un'installazione non fosse più necessario, è possibile disinstallare la versione corrente.

Per disinstallare il repository:

1. Interrompere il repository.
2. Se la configurazione del repository è stata eseguita utilizzando l'opzione Manuale, rimuovere la distribuzione delle risorse del repository dal server delle applicazioni:
 - Server autonomo WebSphere

```
<root profilo WAS>/bin/wsadmin -lang jython -connType none -f
<directory installazione repository>/toDeploy/<time stamp>/delCDS.py
```
 - Server gestito o cluster WebSphere

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

```
<directory installazione repository>/setup/ant/bin/ant -lib "<directory installazione repository>/setup/lib"
-Dinstall.dir="<directory installazione repository>" -Doutput.dir="."
-f <directory installazione repository>/setup/resources/scripts/JBoss/delete-resources.xml
```
3. Per eliminare tutti i dati dal database del repository, aprire il file di configurazione *<directory installazione repository>/uninstall/uninstall.properties* e impostare `cds.uninstall.remove.user.data` property su `true`. Si precisa che alcuni dati potrebbero comunque persistere nel database dopo la disinstallazione con IBM Installation Manager e dovranno essere eliminati manualmente.

Importante: Non eseguire questa fase se si prevede di riutilizzare il repository per nuove installazioni o è necessario conservare i dati di verifica o accesso. Si consiglia di valutare l'utilizzo degli strumenti del produttore del database per creare una copia di backup prima di utilizzare questa opzione.

4. Eseguire IBM Installation Manager (GUI o riga di comando), selezionare l'opzione per disinstallare IBM SPSS Collaboration and Deployment Services e seguire le istruzioni su schermo. IBM Installation Manager può essere eseguito anche in modalità non presidiata. Per ulteriori informazioni, consultare la documentazione IBM Installation Manager <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.
5. Eliminare la directory root di installazione del repository.

Importante: Se si ha intenzione di riutilizzare i dati del repository, si consiglia di salvare il file del keystore, contenuto in *<directory installazione repository>/keystore*.

Chapter 4. Migrazione

La procedura di migrazione di IBM SPSS Collaboration and Deployment Services Repository conserva il contenuto delle impostazioni di configurazione di un repository preesistente compreso quanto segue:

- Struttura di file e cartelle del repository
- Componenti di pianificazione e notifica
- Modelli di notifica
- Utenti locali
- Sovrascritture di elenchi e gruppi di utenti della directory remota definiti a livello locale
- Definizioni dei ruoli e appartenenza
- Preferenze utente
- Icone

Sono supportati i seguenti scenari di migrazione:

- Migrazione da una versione precedente del repository.
- Migrazione su un host, un server delle applicazioni o un server di database diverso.

È possibile utilizzare i seguenti percorsi di migrazione:

- Installazione con una copia del database di repository. Metodo di migrazione consigliato.
- Installazione del repository con un database di repository preesistente.

Prima di selezionare un percorso di migrazione, esaminare nuovamente l'intero capitolo, ivi compresa la sezione Ulteriori considerazioni sulla migrazione.

Indipendentemente dal percorso di migrazione selezionato, è necessario attenersi alle seguenti indicazioni:

- Installare i file dell'applicazione IBM SPSS Collaboration and Deployment Services Repository in un percorso diverso da quello dell'installazione originale. Non sovrascrivere i file nel percorso originale.
- È necessario creare una nuova istanza del server delle applicazioni. Non riutilizzare il profilo (WebSphere) o il server (JBoss) già utilizzati per eseguire la precedente istanza del repository.
- La procedura di migrazione non conserva la configurazione del package del repository, pertanto è necessario reinstallare tutti gli eventuali package aggiuntivi di prodotti IBM SPSS, quali IBM SPSS Modeler e IBM SPSS Statistics. I package nell'istanza di destinazione devono trovarsi allo stesso livello o a un livello più alto rispetto ai package nel repository di origine e devono fare riferimento alla tabella DB per tale motivo. I package devono essere a un livello che sia compatibile con la versione di destinazione di IBM SPSS Collaboration and Deployment Services in questione. Per ulteriori informazioni, consultare la sezione "IBM SPSS products compatibility" on page 29.

Note: I package nell'istanza di destinazione devono trovarsi allo stesso livello o a un livello più alto rispetto ai package nell'istanza di origine. Le informazioni relative ai package installati e alle rispettive versioni sono presenti nella tabella SPSSSETUP_PLUGINS del database dell'istanza di origine.

Per IBM SPSS Collaboration and Deployment Services 8.2, è supportata la migrazione dalla versione 8.1.1.

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 “Migrazione su un database diverso”

- 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.

Migrazione su un database diverso

La migrazione ad un differente database può includere il passaggio ad un differente fornitore di database (ad esempio da SQL Server a IBM Db2 o da Oracle a Db2) o la migrazione su un differente sistema operativo (ad esempio da Db2 for i a Db2 for Linux, UNIX e Windows).

Il trasferimento degli oggetti del repository del database di un altro produttore può essere realizzato creando una copia del precedente database nel nuovo database.

- Creare un database di destinazione seguendo le istruzioni fornite con la versione di IBM SPSS Collaboration and Deployment Services da cui si sta migrando.
- Utilizzare gli strumenti del produttore del database per trasferire i dati dal repository del database di origine a quello di destinazione. Il database deve essere già stato configurato, in modo che sia necessario solo il trasferimento dei dati nelle tabelle di IBM SPSS Collaboration and Deployment Services . Per ulteriori informazioni, consultare la documentazione del fornitore di database.
- Effettuare una copia del file keystore utilizzato dal database di repository dell'origine.
- Installare IBM SPSS Collaboration and Deployment Services ed eseguire il programma di utilità per la configurazione.
 - Specificare il database di destinazione come database di repository
 - Verificare che l'opzione Mantieni i dati esistenti sia stata selezionata per non perdere tutti i dati esistenti.
 - Quando viene richiesto il keystore, selezionare la copia del file keystore da utilizzare per la nuova istanza.
- Reinstallare eventuali package aggiuntivi.

Notare che a causa delle differenze tra gli ambienti di database e gli strumenti di copia del fornitore, come ad esempio il backup Db2, il backup MS-SQL Server o Oracle RMAN, è necessario verificare durante la migrazione che lo strumento selezionato supporti le seguenti funzioni di database.

- Tabelle XML (*SPSSDMRESPONSE_LOG* e *SPSSSCORE_LOG*)
- Dati binari/BLOB, CLOB
- Date dal formato speciale

Ad esempio, Oracle 12cR1 Data Pump non supporta le tabelle XML. Pertanto, può essere utilizzato per il ripristino tutte le tabelle del repository ad eccezione delle due tabelle XML. Le tabelle XML possono essere migrate utilizzando Oracle Esporta. Riesaminare tutti i requisiti del produttore del database, come la registrazione dello schema XML in MS SQL Server e Oracle. Si consiglia di consultare l'amministratore del database prima di migrare il database.

Ulteriori considerazioni sulla migrazione

A seconda della configurazione, possono essere richieste ulteriori attività per una corretta migrazione:

- Password
- Archivio dati JMS
- Modelli di notifica

Nel pianificare la migrazione, si precisa che potrebbe essere necessario eseguire alcune delle attività succitate prima del programma di utilità per la configurazione del database preesistente o della copia di un database.

Migrazione della password

Quando si migra a una nuova istanza di IBM SPSS Collaboration and Deployment Services, si consiglia di utilizzare un ambiente Java con produttore e dimensioni in bit (32 bit o 64 bit) equivalenti all'installazione originale. Ciò lo si deve alle password memorizzate nel repository che sono crittografate in base a una chiave del keystore fornita dal runtime Java. Una implementazione Java con dimensione in bit o produttore diverso sarà dotata di un'altra chiave del keystore, che non è in grado di decrittografare le password correttamente. In alcuni casi, è necessario modificare i fornitori Java o la dimensione bit (ad esempio quando si passa da JBoss a WebSphere).

Se la crittografia Java utilizzata per l'installazione del repository su un database preesistente è diversa dalla crittografia utilizzata dall'istanza originale (a esempio, crittografia IBM Java e non crittografia Sun Java), le password delle credenziali non verranno migrate e il programma di utilità di configurazione riporterà errori. Tuttavia, potendo ancora avviare il repository, utilizzare IBM SPSS Deployment Manager per modificare le password delle credenziali manualmente. Il programma di utilità di esportazione/importazione eseguirà la migrazione delle password, ma quando si riutilizza un database preesistente, prima di potere importare le risorse con credenziali sull'installazione di destinazione, è necessario eseguire l'esportazione dall'installazione di origine.

Se è necessario utilizzare ambienti Java diversi, sostituire le password nelle definizioni delle risorse con credenziale e e nelle fasi di lavoro di IBM SPSS Modeler dopo la configurazione di IBM SPSS Collaboration and Deployment Services Repository:

- Esportare i lavori e le definizioni delle risorse con credenziale dall'istanza del repository di origine e importarli nel repository di destinazione utilizzando IBM SPSS Deployment Manager.

oppure

- aggiornare manualmente ciascuna password nelle singole fasi di lavoro e in ciascuna credenziale del repository di destinazione, utilizzando 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 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.

Installazione dei package

IBM SPSS Collaboration and Deployment Services Package Manager è un'applicazione a riga di comando. Può essere chiamato in modalità batch da altre applicazioni per installare i relativi file dei package nel repository.

Se IBM SPSS Collaboration and Deployment Services Repository è stato inizialmente distribuito automaticamente, è necessario che, durante l'installazione del package, il server delle applicazioni sia nel seguente stato:

- JBoss: Arrestato
- Liberty: Arrestato

L'utente deve essere dotato di privilegi a livello di amministratore per installare i package.

Per evitare che una nuova versione del package venga sovrascritta da una precedente, il gestore package esegue il controllo di versione, verificando inoltre che i componenti richiesti siano stati installati e i numeri di versione siano pari o superiori alla versione richiesta. Questi controlli possono essere evitati nel caso, ad esempio, sia necessario installare una versione precedente del package.

Note: i controlli di dipendenza non possono essere evitati se il gestore package è stato chiamato in modalità batch.

Procedura di installazione di un package

1. Passare a *<directory installazione repository>/bin/*.
2. A seconda del sistema operativo, eseguire *cliPackageManager.bat* su Windows o *cliPackageManager.sh* su UNIX.
3. Quando richiesto, immettere il nome utente e la password.
4. Digitare il comando `install` e premere Invio. Il comando deve includere l'opzione `install` seguito dal percorso del package racchiuso tra virgolette, secondo il seguente esempio:

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

Per installare più package contemporaneamente, immettere tutti i nomi dei package separati da uno spazio, ad esempio:

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

In alternativa, per installare più package, utilizzare il parametro `-dir` o `-d` seguito dal percorso contenente i package da installare

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

Qualora il controllo di dipendenza o versione non dovesse completarsi correttamente, si tornerà al prompt principale del gestore package. Per installare ignorando errori non irreversibili, eseguire nuovamente il comando `install` utilizzando il parametro `-ignore` o `-i`.

5. A installazione ultimata, utilizzare il comando `exit` per uscire dal gestore package.

Per visualizzare ulteriori opzioni di installazione con riga comandi, digitare `help` e premere il tasto Invio. Le opzioni sono:

- `info "<percorso package>":` visualizza le informazioni del file del package specificato.
- `install "<percorso package>":` installa i file del package specificato nel repository.
- `tree:` visualizza le informazioni sulla struttura ad albero del package installato.

Modalità non presidiata

Per automatizzare l'installazione del package, IBM SPSS Collaboration and Deployment Services Package Manager può essere eseguito in modalità non presidiata:

```
<directory di installazione repository>/bin/cliPackageManager[.sh]  
-user <amministratore> -pass <password amministratore>  
- install <percorso package> [<percorso_package_aggiuntivo>]
```

Registrazione

I log di IBM SPSS Collaboration and Deployment Services Package Manager (log principale e log Ant) sono reperibili in `<directory installazione repository>/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.

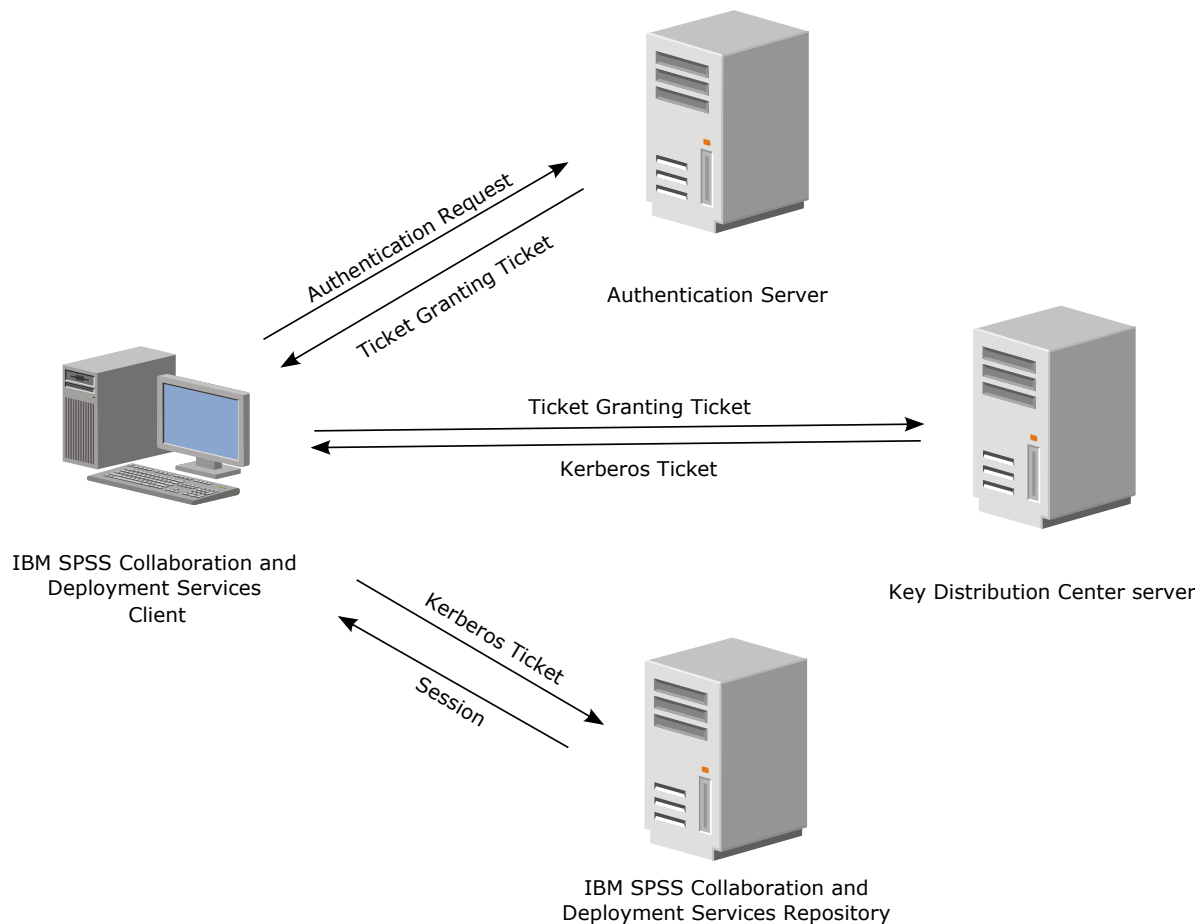


Figure 3. IBM SPSS Collaboration and Deployment Services SSO architecture

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 Directory/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 42 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 steps are also required to enable the repository Server Process Credential. See the topic “Configurazione di Server Process Credential” on page 43 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 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

Le seguenti istruzioni si riferiscono al controller di dominio di Windows Server 2003. I passi saranno simili per i sistemi Windows Server 2012.

1. Creare il profilo utente che il servizio Kerberos utilizzerà come principal
2. Mappare questo profilo utente al sistema host IBM SPSS Collaboration and Deployment Services
3. Configurare il tipo di crittografia e la delega delle credenziali Kerberos
4. Creare un file di tabella delle chiavi e posizionarlo sul sistema host IBM SPSS Collaboration and Deployment Services

Completate queste fasi, utilizzare Deployment Manager per configurare Active Directory come provider di sicurezza e un provider di single sign-on Kerberos.

Creazione di un profilo utente per il principal Kerberos

1. Utilizzando gli utenti e la console di gestione dei computer Active Directory creare un utente del dominio per il dominio selezionato (ad esempio l'utente `krb5.principal` nel dominio `spss`). Questo utente corrisponde al principal service Kerberos
2. Specificare un parametro surname per questo utente. È richiesto da alcuni server delle applicazioni.
3. Selezionare l'opzione che non fissa alcuna scadenza per la password.

Per mappare il profilo utente al sistema host IBM SPSS Collaboration and Deployment Services

associare il profilo utente ad un SPN (Service Principal Name) utilizzando lo strumento **setspn**. Un SPN è un nome che viene utilizzato dal client Kerberos per identificare un servizio su un server Kerberos. Il client fa riferimento a SPN invece che ad uno specifico utente del dominio.

Lo strumento **setspn** accede, aggiorna e rimuove la proprietà SPN property per un utente. Per aggiungere un SPN, utilizzare la seguente sintassi del comando:

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

L'opzione **-A** aggiunge un SPN arbitrario all'account del dominio. Gli altri argomenti hanno le seguenti definizioni:

<spn> SPN aggiunto all'utente avente il formato `<service_class>/<host>`. Il valore `<service_class>` indica la classe del servizio. Il valore `<host>` corrisponde al nome host sia completo che semplificato.

<utente>

Il profilo utente da associare all'SPN.

Per mappare il profilo utente, eseguire le seguenti procedure. Aggiungere sia il nome completo che semplificato, il nome host abbreviato poiché il client può fare riferimento ad entrambi i nomi.

1. Se non si dispone dello strumento **setspn** scaricare e installare una versione appropriata di Windows Support Tools.
2. Eseguire **setspn** con il nome host completo del server IBM SPSS Collaboration and Deployment Services come argomento, come illustrato nel seguente esempio:

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

3. Eseguire **setspn** con il nome host del server IBM SPSS Collaboration and Deployment Services come argomento, come illustrato nel seguente esempio:

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

Per ulteriori informazioni sullo strumento **setspn**, consultare <http://technet.microsoft.com/en-us/library/cc731241.aspx>.

Configurazione del tipo di crittografia e delega delle credenziali

1. Nella scheda Account della finestra di dialogo Proprietà utente, selezionare l'opzione per utilizzare la crittografia AES.
2. Nella scheda Delega della finestra di dialogo Proprietà utente, selezionare l'opzione per considerare l'utente attendibile e assegnargli la delega a qualsiasi servizio.

Creazione di un file di tabella delle chiavi Kerberos

Un file di tabella delle chiavi contiene i principal Kerberos con le corrispondenti chiavi crittografate e viene utilizzato per l'autenticazione dei principal. Per creare un file di tabella delle chiavi, utilizzare lo strumento **ktpass**. Per le informazioni relative allo strumento **ktpass** consultare <http://technet.microsoft.com/en-us/library/cc753771.aspx>.

1. Eseguire lo strumento **ktpass** come descritto nel seguente esempio:

```
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
```

- Il valore dell'opzione **princ** deve avere il seguente formato: *<service_provider_name>@<domain>*.
 - Il valore dell'opzione **mapUser** deve avere il seguente formato: *<Kerberos_service_principal>@<domain>*.
 - Qualsiasi modulo di crittografia potente, come definito dall'opzione **crypto** richiede l'estensione JCE per la crittografia potente da Oracle.
2. Archiviare il file di tabella delle chiavi così generato (nell'esempio, *c:\temp\krb5.prin.keytab*) nel file system dell'host di IBM SPSS Collaboration and Deployment Services.

Se si modifica la password del servizio, anche il file di tabella delle chiavi deve essere aggiornato.

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, <i>HTTP/cdsserver.spss.com@SPSS.COM</i>
useDefaultKeytab	true

JBoss

For JBoss application server, at least one JAAS (Java Authentication and Authorization Service) configuration for JGSSServer must be provided. The template for single sign-on application policy can be found in the JGSSServer element of <JBoss installation directory>/standalone/configuration/standalone.xml or cds_server.xml. It may be necessary to change 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** required
- **KerberosLocalUser** optional
- **JDBC_DRIVER_01** 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 the user to create a Kerberos credential when client browser sends a NTLM token (instead of a Kerberos token) during the negotiation challenge. Note that on Windows system, browsers on the same machine, where IBM SPSS Collaboration and Deployment Services server is installed, will always send 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;
};
```

- 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;
};
```

- It is 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

- 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.

Configurazione di Server Process Credential

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

Per ulteriori informazioni su come utilizzare Server Process Credential, consultare la documentazione di IBM SPSS Deployment Manager.

Una volta configurato il repository per il single sign-on, è necessario eseguire le seguenti fasi aggiuntive per abilitare Server Process Credential:

- Configurare l'accesso utente di livello intermedio per il server delle applicazioni.

- Creare la cache dei ticket Kerberos sull'host del repository.

Per utilizzare Server Process Credential con le fasi del lavoro report:

- Aggiungere il server di database dell'origine dati al dominio/area di autenticazione.
- Configurare il server di database dell'origine dati in modo che accetti le connessioni single sign-on del dominio/area di autenticazione.
- Configurare il database dell'origine dati in modo che fornisca le opportune autorizzazioni a Process Server Credential.

Configurazione dell'accesso utente di livello intermedio su WebSphere

1. Utilizzando la console di gestione, aprire **Sicurezza > Sicurezza globale > JAAS - Accessi applicazione**
2. Definire la configurazione di accesso *CaDSMiddleTier*.
3. Per *CaDSMiddleTier*, definire un modulo JAAS con nome classe *com.ibm.security.auth.module.Krb5LoginModule*.
4. Per *com.ibm.security.auth.module.Krb5LoginModule*, definire le seguenti proprietà personalizzate:
 - useDefaultCache true
 - renewTGT true
 - debug false

Configurazione dell'accesso utente di livello intermedio su JBoss

Aggiungere la seguente politica dell'applicazione a *<directory installazione JBoss>/server/<Nome server>/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">##DOMAINNAME##</module-option>
      <module-option name="kdc">##KDC#SERVER#HOST##</module-option>
      <module-option name="renewTGT">true</module-option>
    </login-module>
  </authentication>
</application-policy>
```

Creazione della cache dei ticket Kerberos

La cache dei ticket Kerberos verrà utilizzata per memorizzare i ticket Kerberos per l'autenticazione di Server Process Credential. Per creare la cache dei ticket, attenersi alle seguenti fasi:

1. Aggiornare il file di configurazione Kerberos sul server dell'host del repository, ad esempio *c:\windows\krb5.ini*. Questo file identifica area di autenticazione/dominio, tipi di codifica predefiniti, ticket rinnovabili e indirizzo KDC e verrà utilizzato dall'applicazione **kinit** per generare la cache dei ticket. Il seguente è un esempio del file di configurazione Kerberos:

```
[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. Accedere all'host del repository con le credenziali di dominio che verranno utilizzate per Server Process Credential. Appurare che tali credenziali siano dotate delle opportune autorizzazioni sull'host.
3. Eseguire **kinit** dalla directory del JRE utilizzato dal server delle applicazioni del repository con le opzioni per creare un ticket rinnovabile e una cache dei ticket.

Note: Sul sistema operativo Windows, **kinit** potrebbe non creare un ticket rinnovabile. Per risolvere questo problema, aggiungere la seguente impostazione di registro:

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

Per ulteriori informazioni, consultare la documentazione Kerberos per il proprio sistema operativo.

4. Inserire la password dell'utente di 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 the IBM SPSS Collaboration and Deployment Services server name in a whitelist:

- 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 whitelist, 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.

Configurazione delle root di contesto delle applicazioni

Per configurare le root di contesto, è necessario aggiornarne il prefisso URL del sistema e modificarne le specifiche di ciascuna di esse.

Procedura

1. Se è stato abilitato l'utilizzo di un prefisso URL, aggiungere la root di contesto al prefisso URL.
2. Aggiornare la root di contesto di ciascuna applicazione. La procedura dipende dal server delle applicazioni.
 - “Updating context roots for WebSphere” on page 48
 - “Updating context roots for JBoss” on page 49

Risultati

È possibile accedere al IBM SPSS Deployment Manager basato su browser e a IBM SPSS Collaboration and Deployment Services Deployment Portal utilizzando i valori URL che includono la root di contesto.

Operazioni successive

Aggiornare tutti i riferimenti al server del repository, come ad esempio quelli definiti utilizzando IBM SPSS Deployment Manager, includendo la root di contesto nell'URL del server.

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.

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”

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

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 48

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>
```

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, “Using SSL to secure data transfer,” on page 53 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.

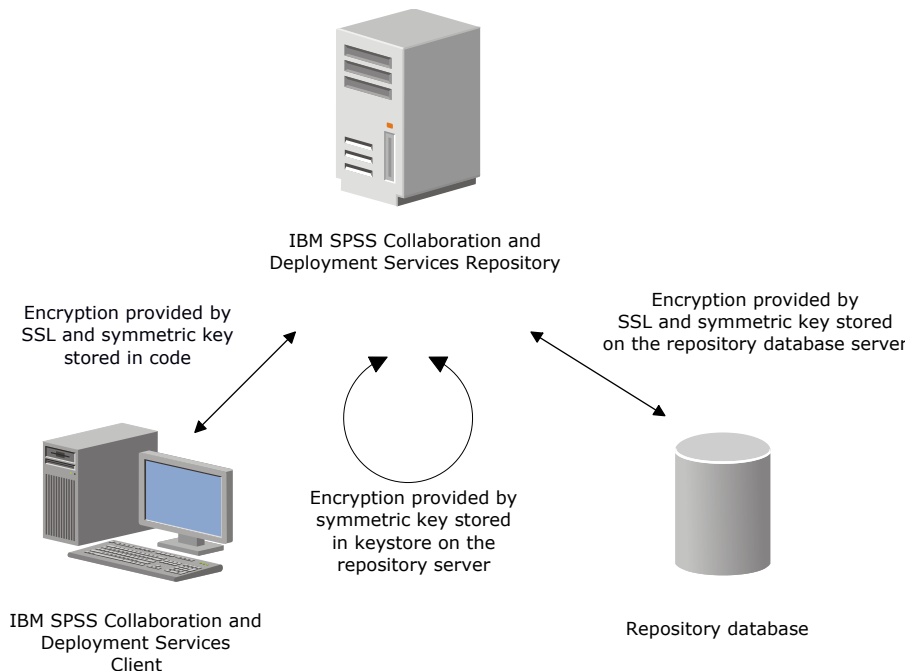


Figure 4. IBM SPSS Collaboration and Deployment Services FIPS 140-2-compliant security setup

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 .
- Internet Explorer configuration requires enabling Windows cryptography and modifying the browser settings. For more information, see .
- Apple Safari cannot be used in FIPS 140-2 compliant mode.

Chapter 9. Using SSL to secure data transfer

Secure Sockets Layer (SSL) is a protocol for encrypting data transferred between two computers. SSL ensures that communication between the computers is secure. SSL can encrypt the authentication of a username/password and the contents of an exchange between a server and client.

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"
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.

URL prefix configuration

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.

Chapter 10. Registrazione

La registrazione è un elemento essenziale della risoluzione dei problemi applicativi, così come della pianificazione delle attività di manutenzione preventiva. Al generarsi di eventi su sistemi e applicazioni, il personale amministrativo può essere avvisato non appena si raggiunge una soglia di avvertenza oppure si verifica un evento critico del sistema. Inoltre, l'output di informazioni dettagliate può essere memorizzato in un file di testo per consentirne l'analisi successiva.

Il IBM SPSS Collaboration and Deployment Services Repository utilizza il package log4j per gestire le informazioni del log in fase di runtime. Log4j è una soluzione di registrazione della Apache Software Foundation per applicazioni Java. L'approccio log4j consente il controllo della registrazione mediante un file di configurazione; non è necessario modificare l'applicazione binaria. Per una disamina completa di log4j, consultare il sito web di log4j.

File di configurazione della registrazione

Il percorso del file di configurazione di registrazione IBM SPSS Collaboration and Deployment Services Repository varia a seconda del server delle applicazioni host:

- **WebSphere:** <directory di installazione repository>/platform/log4j.properties
- **Liberty:** <directory di installazione repository>/platform/log4j.properties
- **JBoss:** <directory server JBoss>/deploy/jboss-logging.xml

Questo file controlla sia la destinazione che la quantità di output del log. La configurazione di log4j viene gestita modificando questo file per definire gli appender delle destinazioni dei log e per instradare l'uscita del logger verso tali appender.

Vengono definiti i seguenti logger predefiniti:

Table 5. Logger.

Logger	Descrizione
<i>log4j.rootCategory</i>	Logger root
<i>log4j.logger.com.spss</i>	Tutti gli eventi di IBM SPSS Collaboration and Deployment Services
<i>log4j.com.spss.cmor</i> , <i>log4j.com.spss.cmor.internal.MetaObjectImportEngine</i>	Eventi del repository
<i>log4j.com.spss.security</i>	Eventi di sicurezza
<i>log4j.com.spss.process</i>	Eventi di pianificazione lavori
<i>log4j.com.spss.reporting</i> , <i>log4j.com.spss.reportservice</i>	Eventi di gestione report
<i>log4j.com.spss.notification</i>	Eventi di notifica
<i>log4j.logger.org.springframework.jdbc.core.JdbcTemplate</i>	Eventi Spring Framework JDBC
<i>log4j.logger.com.spss.repository.internal.transfer</i>	Eventi di importazione/esportazione

Vengono definiti i seguenti appender:

- Console
- Log principale (*cds.log*)
- Log delle transazioni di esportazione/importazione (*cds_transfer.log*)

Il percorso predefinito dei file di log varia in funzione del server delle applicazioni host:

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

Chapter 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.

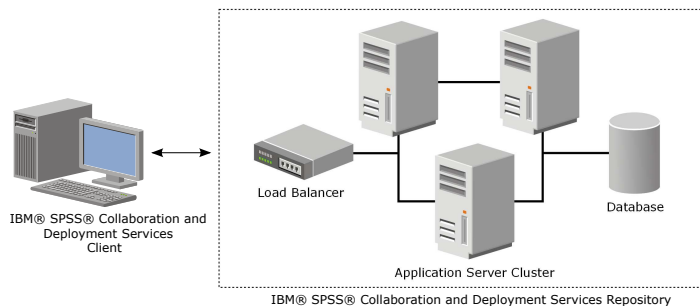


Figure 5. Architettura cluster

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 1.8.9 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: <Directory di installazione IBM Installation Manager >/eclipse/IBMIM

- Modalità riga comandi <Directory di installazione IBM Installation Manager >/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 esistono due o più nodi gestiti nella topologia cluster, eseguire questo comando più volte per creare i nodi 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
```

In cui <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 database DB2 denominato SPSSCDS:

```
CREATE DATABASE SPSSCDS ON c:\ USING CODESET UTF-8 TERRITORY US COLLATE USING SYSTEM;  
CONNECT TO SPSSCDS;  
CREATE Bufferpool SPSSBK IMMEDIATE SIZE 250 AUTOMATIC PAGESIZE 8 K ;  
CREATE REGULAR TABLESPACE SPSSBK PAGESIZE 8 K MANAGED BY AUTOMATIC STORAGE EXTENTSIZ 8 OVERHEAD 10.5 PREFETCHSIZE 8 TRANSFERRATE 0.14 BUFFERPOOL SPSSBK DROPPED TABLE RECOVERY ON;  
COMMENT ON TABLESPACE SPSSBK 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 CADSDUSER;
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: <Directory di installazione IBM Installation Manager >/eclipse/IBMIM
 - Modalità riga comandi <Directory di installazione IBM Installation Manager >/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).

Note: 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: <directory di installazione del repository >\bin\configTool.bat
 - Linux/UNIX: <directory di installazione del repository >/bin/configTool.sh
 - Modalità riga di comando:
 - Windows: <directory di installazione del repository >\bin\cliConfigTool.bat
 - Linux/UNIX: <directory di installazione del repository >/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 accedere al server del 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.
 - **Eeguire 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 <directory installazione repository>/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 è su un server differente rispetto al server del repository, aggiornare il valore di CDS_HOME per puntare ad una directory di installazione condivisa (ad esempio, \\<Management_Host>\SPSS\Deployment\8.2\Server, in cui <Management_Host> è il nome host della macchina in cui è installato il server del 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 esempio, 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 negli 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 proprie 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"
```

In cui `<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 sono 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` e accedere utilizzando l'account admin che è stato 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 proprie 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 alle 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 Services Administrator's Guide*.

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

Avviare il server del repository

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: <Directory di installazione WebSphere >\profiles\<PROFILE_NAME>\bin>startManager.bat
 - Linux/UNIX: <Directory di installazione WebSphere >\profiles\<PROFILE_NAME>\bin>startManager.sh
2. Accedere ad ogni macchina e avviare ogni agent del nodo gestito:
 - Windows: <Directory di installazione WebSphere >\profiles\<PROFILE_NAME>\bin>startNode.bat
 - Linux/UNIX: <Directory di installazione WebSphere >\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 su browser in un browser web supportato <http://<repository host>:<port number>/security/login>. Se lo strumento non sia via, 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-IBM products. 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](http://www.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

A

- accesso utente di livello intermedio 43
- Active Directory 37, 39
- AES 51
- affinità di sessione 24
- aggiunta di nodi al cluster 25
- applications
 - supported versions 29
- authentication 37
- autorizzazioni 11, 15
- autorizzazioni del database 15

B

- bilanciamento del carico
 - basato su hardware 23, 24
 - basato su software 23, 24
- browser 54
- browser trust store 54
- browsers
 - single sign-on 45

C

- cache dei ticket Kerberos 43
- case insensitive collation 17
- certificate
 - importing 54
- certificates 51
- Chrome
 - single sign-on 45
- Citrix Presentation Server 11
- client updates 35
- clipackagemanager.bat 35
- clipackagemanager.sh 35
- cluster
 - espansione 25
 - WebLogic 25
 - WebSphere 25
- clustering 23, 24
- clustering di server 23, 24
- clustering di server delle applicazioni 23, 24
- collaboration 1
- condivisione su Windows 24
- configuring
 - Db2 16
 - MS SQL Server 17
 - Oracle databases 18
- connettività del database 28
- context roots
 - in JBoss 49
 - in WebSphere 48
 - URL prefix 48
- credentials 32
- credenziali 32, 33
- crittografia 32, 33

D

- database maintenance 18
- databases
 - requirements 14
- Db2
 - configuration 16
- Db2 for Linux, UNIX e Windows 15
- Db2 UDB 14
- dependency check 35
- deployment 2
- disinstallazione 30

E

- encrypt.bat 28
- encrypt.sh 28
- encryption 32, 51, 52
 - SSL 53
- Esempio di installazione cluster
 - WebSphere 59
- espansione del cluster 25
- eventi del repository
 - registrazione 57
- eventi di gestione report
 - registrazione 57
- eventi di importazione/esportazione
 - registrazione 57
- eventi di lavoro
 - registrazione 57
- eventi di notifica
 - registrazione 57
- eventi di sicurezza
 - registrazione 57
- execution servers
 - remote process 2
 - SAS 2

F

- failover 23, 24
- FIPS 140-2 51
- funzioni
 - rimosso 7

G

- Google Chrome
 - single sign-on 45

I

- IBM HTTP Server 24
- IBM Installation Manager 19, 30
- IBM SPSS Collaboration and Deployment Services Deployment Manager 2, 4
- IBM SPSS Collaboration and Deployment Services Deployment Portal 2, 4
- IBM SPSS Collaboration and Deployment Services Package Manager 35

- IBM SPSS Collaboration and Deployment Services Password Utility 28
- IBM SPSS Collaboration and Deployment Services Repository 2, 3
- IBM SPSS Modeler Decision Management 6
- IBM SPSS Modeler version 29
- IBM SPSS Statistics version 29
- importing
 - certificate 54
- installazione 10, 19
 - package 35
- installing
 - packages 35

J

- Java 12
- JBoss 12, 43
 - single sign-on 41
- JCE module 51, 52
- JMS 33
- JMS message store 16
- JRE (64 bit) 12
- Jython 24

K

- Kerberos 42
 - domain 37
 - Key Distribution Center Service Ticket 37
- Kerberos server 40

L

- LDAP 55
 - securing 55
- log 57
- log4j 57
 - configurazione 57
- logging in 45

M

- manuale 12
- Microsoft Internet Explorer
 - single sign-on 45
- Microsoft SQL Server 14, 15
 - configuration 17
- migration
 - notification templates 34
 - with a copy of repository database 32
 - with existing repository database 32
- migrazione
 - password 33
 - su un altro database 32
 - su un server diverso 31

migrazione (*continued*)
 su una versione successiva del
 repository 31
migrazione della password 32, 33
MIT Kerberos 38
modulo JCE 24
Mozilla Firefox
 single sign-on 45

N

Netezza 29
non presidiata
 disinstallazione 30
 IBM Installation Manager 19, 30
 installazione 19
notification templates migration 34

O

one-way trust
 configuration 42
OpenLDAP 38
optional components 35
Oracle 10g 14
Oracle Database 15
Oracle databases
 configuration 18
Oracle WebLogic 12

P

package
 installazione 35
packages
 installing
 in command line mode 35
 silent 35
password
 crittografare 28
 modifica 28
performance degradation 11
prefisso URL 24
privilegi utente 11
processo remoto
 server di esecuzione 5
programma di utilità per password 28

R

registry update files 42
remote process
 execution servers 2
remotely-deployed scoring servers 5
repository database maintenance 18
repository updates 35
requirements
 application 29
 databases 14
requisiti 11
 server delle applicazioni 12
ridondanza 23, 24
riga di comando 35
root di contesto 47

S

Safari 45
SAS
 execution server 2
 server di esecuzione 5
scenario di installazione di esempio 59
scoring 6
scoring servers 5
Secure Sockets Layer 53
securing
 LDAP 55
security
 SSL 53
server delle applicazioni
 requisiti 12
server di esecuzione 5
 processo remoto 5
 SAS 5
server updates 35
SIB 33
silent
 package installation 35
single sign-on 37, 40
 Active Directory 39
 application server configuration 40
 Google Chrome 45
 JBoss 41
 Microsoft Internet Explorer 45
 MIT Kerberos 38
 Mozilla Firefox 45
 one-way trust 42
 OpenLDAP 38
 registry update files 42
 WebSphere 40
 Windows Kerberos Server 38
SPNEGO 45
SSL 51, 53
 certificates 51
 overview 53
 securing communications 53
strumenti di registrazione 57
supported applications 29
symmetric encryption 51
System Integration Bus 16

U

UNC 24
URL prefix 48, 55
user preferences 4

V

version check 35
versions
 IBM SPSS Modeler 29
 IBM SPSS Statistics 29
virtualization 11
VMWare 11

W

WebLogic 23
WebLogic Apache Plugin 23, 24
WebSphere 12, 23, 24, 33, 43

WebSphere (*continued*)
 cluster 24
 distribuzione automatica 24
 distribuzione manuale 24
 single sign-on 40
Windows Terminal Services 11



Printed in USA