

IBM SPSS Collaboration and Deployment Services
Repository
Versione 8 Release 1

*Manuale di installazione e
configurazione*

IBM

Nota

Prima di utilizzare queste informazioni ed il prodotto supportato, leggere le informazioni contenute in "Informazioni particolari" a pagina 65.

Informazioni sul prodotto

Questa edizione si applica alla versione 8, release 1, livello di modifica 0 di IBM SPSS Collaboration and Deployment Services e a tutte le successive release e modifiche a meno che non sia diversamente indicato nelle nuove edizioni.

© Copyright IBM Corporation 2000, 2017.

Indice

Capitolo 1. Panoramica 1

IBM SPSS Collaboration and Deployment Services	1
Collaborazione	1
Distribuzione	2
Architettura del sistema	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
Server di calcolo del punteggio	5
IBM Analytical Decision Management	6

Capitolo 2. Novità per gli addetti all'installazione 7

Novità in questa versione	7
Funzionalità obsolete	7

Capitolo 3. Installazione 9

Preinstallazione	9
Pianificazione dell'installazione	10
Requisiti del sistema host	10
Server delle applicazioni	12
Database	14
Installazione e configurazione	19
Installazione	19
Configurazione	20
Distribuzione manuale	23
Configurazione del cluster	25
Post-installazione	29
Avvio del server di repository	29
Verifica della connettività	30
Gestione della password del database	31
Driver JDBC	32
Compatibilità con i prodotti IBM SPSS	33
Disinstallazione	33

Capitolo 4. Migrazione 35

Installazione utilizzando una copia del database del repository	35
Installazione utilizzando un database del repository preesistente	36
Migrazione su un database diverso	36
Ulteriori considerazioni sulla migrazione	37
Migrazione della password	37
Migrazione dell'archivio JMS su WebSphere	37
Migrazione dell'archivio JMS su WebLogic	38
Migrazione dei modelli di notifica	38

Capitolo 5. Gestione dei package 39

Installazione dei package	39
-------------------------------------	----

Capitolo 6. Single sign-on 41

Configurazione della directory per il single sign-on	42
OpenLDAP	42
Active Directory	43
Configurazione del server Kerberos	44
Configurazione del server delle applicazioni per il single sign-on	44
WebSphere	45
JBoss	45
WebLogic	46
Aggiornamento del registro di sistema Windows con il single sign-on	47
Configurazione di relazioni attendibili undirezionali	47
Configurazione di Server Process Credential	48
Configurazione dei browser per il single sign-on	50
Ticket che è possibile inoltrare e IBM SPSS Deployment Manager	50

Capitolo 7. Root di contesto dell'applicazione 53

Configurazione delle root di contesto delle applicazioni	53
Aggiunta di una root di contesto al prefisso URL	54
Aggiornamento delle root di contesto di WebSphere	54
Aggiornamento delle root di contesto di JBoss	55
Aggiornamento delle root di contesto di WebLogic	55

Capitolo 8. Conformità FIPS 140-2 57

Configurazione del repository	58
Configurazione del client desktop	58
Configurazione del browser	58

Capitolo 9. Utilizzo di SSL per proteggere il trasferimento di dati 59

Come funziona il protocollo SSL	59
Protezione delle comunicazioni client-server e server-server con SSL	59
Installazione della crittografia "Unlimited Strength"	59
Aggiunta del certificato al keystore sul client (per le connessioni al repository di)	60
Importazione del file certificato per connessioni client basate su browser	60
Istruzione agli utenti per l'abilitazione di SSL	61
Configurazione del prefisso URL	61
Protezione di LDAP mediante SSL	61

Capitolo 10. Registrazione 63

Informazioni particolari 65

Considerazioni sulla politica della privacy	66
Marchi	67

Indice analitico 69

Capitolo 1. Panoramica

IBM SPSS Collaboration and Deployment Services

IBM® SPSS Collaboration and Deployment Services è un'applicazione di livello enterprise che consente l'utilizzo e la distribuzione diffusi dell'analisi predittiva.

IBM SPSS Collaboration and Deployment Services propone archiviazione centralizzata, protetta e verificabile delle risorse analitiche e capacità avanzate di gestione e controllo dei processi di analisi predittiva, così come meccanismi evoluti per la distribuzione agli utenti dei risultati dell'elaborazione analitica. Tra i vantaggi di IBM SPSS Collaboration and Deployment Services si annoverano:

- Tutela del valore delle risorse analitiche
- Garanzia di conformità con gli obblighi normativi
- Miglioramento della produttività degli analisti
- Riduzione al minimo dei costi IT di gestione delle analisi

IBM SPSS Collaboration and Deployment Services consente di gestire in regime di sicurezza diverse risorse analitiche, promuovendo una maggiore collaborazione tra sviluppatori e utenti. Inoltre, le funzioni di distribuzione fanno in modo che i destinatari ricevano le informazioni necessarie per intraprendere le opportune azioni in modo tempestivo.

Collaborazione

Collaborazione si riferisce alla capacità di condividere e riutilizzare le risorse analitiche con efficienza ed è la chiave per lo sviluppo e la distribuzione di analisi in ambito aziendale.

Gli analisti hanno bisogno di un percorso in cui salvare i file per renderli disponibili ad altri analisti o utenti aziendali. È necessario implementare nel percorso il controllo di versione dei file per gestire l'evoluzione dell'analisi. La sicurezza è necessaria per controllare l'accesso ai file e relativa modifica. Infine, è opportuno adottare un meccanismo di backup e ripristino per proteggere l'azienda dalla perdita di risorse essenziali.

Per soddisfare queste esigenze, IBM SPSS Collaboration and Deployment Services fornisce un repository per l'archiviazione delle risorse utilizzando una gerarchia di cartelle analoga alla maggior parte dei file system. I file archiviati in IBM SPSS Collaboration and Deployment Services Repository sono messi a disposizione degli utenti dell'intera azienda, purché dotati delle opportune autorizzazioni di accesso. Per assistere utenti nel rilevamento delle risorse, il repository propone una funzione di ricerca.

Gli analisti possono gestire i file nel repository utilizzando le applicazioni client che sfruttano l'interfaccia di servizio di IBM SPSS Collaboration and Deployment Services. Prodotti, quali IBM SPSS Statistics e IBM SPSS Modeler, consentono l'interazione diretta con i file nel repository. Un analista può archiviare una versione di un file in fase di sviluppo, recuperarla in un momento successivo e continuare a modificarla finché non è stata completata ed è pronta per essere introdotta nel processo produttivo. Questi file possono contenere interfacce in grado di eseguire processi analitici, consentendo agli utenti aziendali di avvalersi del lavoro svolto dall'analista.

L'utilizzo di un repository protegge l'azienda dotandola di un archivio centrale in cui eseguire facilmente il backup e il ripristino delle risorse analitiche. Inoltre, le autorizzazioni a livello di utente, file ed etichetta di versione, controllano l'accesso alle singole risorse. Il controllo versione e le etichette di versione degli oggetti fanno sì che le versioni delle risorse utilizzate nei processi produttivi siano sempre quelle corrette. Infine, funzioni di accesso consentono di monitorare le modifiche apportate a file e sistemi.

Distribuzione

Per usufruire appieno dei vantaggi dell'analisi predittiva, è necessario che le risorse analitiche contribuiscano alle decisioni aziendali. La distribuzione colma le lacune tra l'analisi e l'azione diramando i risultati alle parti e ai processi interessati secondo un piano prestabilito o in tempo reale.

In IBM SPSS Collaboration and Deployment Services, i singoli file archiviati nel repository possono essere inclusi nell'elaborazione dei **lavori**. I lavori definiscono una sequenza di esecuzione delle risorse analitiche e possono essere creati con IBM SPSS Deployment Manager. I risultati dell'esecuzione possono essere archiviati nel repository, in un file system o diramati a destinatari specifici. I risultati archiviati nel repository sono accessibili da qualsiasi utente, purché dotato delle autorizzazioni necessarie, utilizzando l'interfaccia di IBM SPSS Collaboration and Deployment Services Deployment Portal. I lavori in sé possono essere attivati secondo un piano prestabilito o come reazione a un evento di sistema.

Inoltre, il servizio di calcolo del punteggio di IBM SPSS Collaboration and Deployment Services consente di diramare i risultati analitici, generati dai modelli distribuiti, in tempo reale in fase di interazione con il cliente. Un modello analitico configurato per il calcolo del punteggio può combinare i dati raccolti dall'interazione in atto con il cliente con i dati storici producendo un punteggio in grado di determinare l'andamento dell'interazione stessa. Il servizio in sé può essere sfruttato da qualsiasi applicazione client, agevolando la creazione di interfacce personalizzate per la definizione del processo.

Le funzioni di distribuzione di IBM SPSS Collaboration and Deployment Services sono studiate per integrarsi facilmente nell'infrastruttura aziendale. L'implementazione del protocollo single sign-on riduce l'esigenza di fornire credenziali manuali durante i vari stadi del processo. Per di più, il sistema può essere configurato in modo che sia conforme alla FIPS 140-2 (Federal Information Processing Standard Publication 140-2).

Architettura del sistema

In generale, IBM SPSS Collaboration and Deployment Services è costituito da un unico IBM SPSS Collaboration and Deployment Services Repository centralizzato, accessibile da vari client, che utilizza server di esecuzione per elaborare le risorse analitiche.

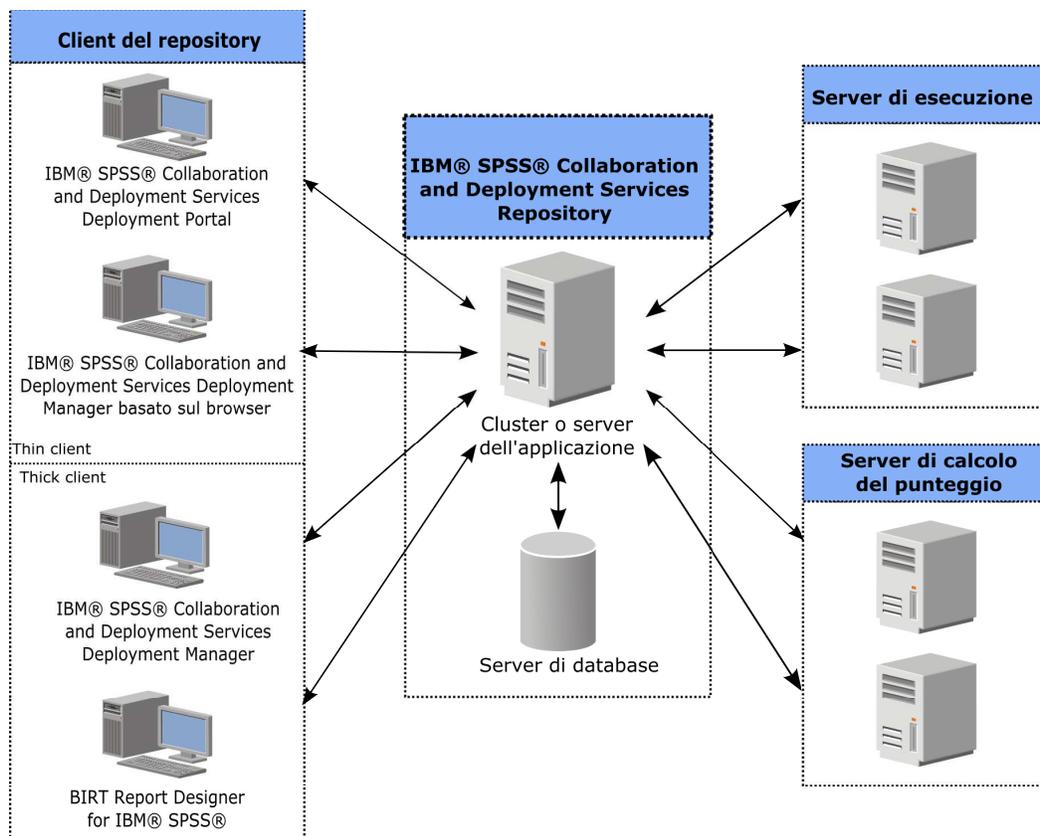


Figura 1. Architettura di IBM SPSS Collaboration and Deployment Services

IBM SPSS Collaboration and Deployment Services è costituito dai seguenti componenti:

- IBM SPSS Collaboration and Deployment Services Repository per risorse analitiche
- IBM SPSS Deployment Manager
- IBM SPSS Collaboration and Deployment Services Deployment Portal
- IBM SPSS Deployment Manager

IBM SPSS Collaboration and Deployment Services Repository

Il repository costituisce un archivio centralizzato per le risorse analitiche, quali modelli e dati, che richiede l'installazione di un database relazionale, come IBM DB2, Microsoft SQL Server o Oracle.

Il repository include funzioni di:

- Sicurezza
- Controllo versione
- Ricerca
- Verifica

Le opzioni di configurazione del repository vengono definite mediante IBM SPSS Deployment Manager oppure IBM SPSS Deployment Manager basato su browser. Il contenuto del repository viene gestito con Deployment Manager e aperto con IBM SPSS Collaboration and Deployment Services Deployment Portal.

IBM SPSS Deployment Manager

IBM SPSS Deployment Manager è un'applicazione client per IBM SPSS Collaboration and Deployment Services Repository che consente agli utenti di pianificare, automatizzare ed eseguire attività analitiche, quali aggiornamento di modelli e calcolo di punteggi.

Con l'applicazione client gli utenti possono:

- Visualizzare tutti i file presenti nel sistema, inclusi report , file di sintassi SAS, file di sintassi di file di dati
- Importare file nel repository
- Pianificare l'esecuzione ciclica di lavori utilizzando un modello di ricorrenza specificato, ad esempio, con cadenza trimestrale oppure oraria
- Modificare le proprietà di lavori preesistenti
- Determinare lo stato di un lavoro
- Specificare le notifiche e-mail dello stato lavori

Inoltre, l'applicazione client consente agli utenti di eseguire attività amministrative per IBM SPSS Collaboration and Deployment Services, tra cui:

- Gestire utenti
- Configurare provider di sicurezza
- Assegnare ruoli e azioni

IBM SPSS Deployment Manager basato su browser

IBM SPSS Deployment Manager basato su browser è un'interfaccia per thin client dedicata all'esecuzione di attività di impostazione e gestione del sistema, tra cui:

- Impostazione delle opzioni di configurazione del sistema
- Configurazione dei provider di sicurezza
- Gestione dei tipi MIME

Tutte queste attività possono essere eseguite da utenti non amministratori, purché abbiano le azioni appropriate siano state associate alle loro credenziali di accesso. Le azioni sono assegnate da un amministratore.

Di norma, si accede a IBM SPSS Deployment Manager basato su browser dal seguente indirizzo:

`http://<indirizzo IP host>:<porta>/security/login`

Nota: L'indirizzo IPv6 deve essere racchiuso tra parentesi quadre, ad esempio `[3ffe:2a00:100:7031::1]`.

Se l'ambiente è configurato per l'utilizzo di un percorso di contesto personalizzato per le connessioni server, includerlo nell'URL.

`http://<indirizzo IP host>:<porta>/<percorso contesto>/security/login`

IBM SPSS Collaboration and Deployment Services Deployment Portal

IBM SPSS Collaboration and Deployment Services Deployment Portal è un'interfaccia thin client per l'accesso al repository. A differenza di IBM SPSS Deployment Manager basato su browser, studiato per gli amministratori, IBM SPSS Collaboration and Deployment Services Deployment Portal è un portale Web che serve utenti diversi.

Il portale Web propone le seguenti funzionalità:

- Visualizzazione strutturata del contenuto del repository
- Apertura del contenuto pubblicato

- Esecuzione di lavori e di report
- Creazione di punteggi servendosi dei modelli archiviati nel repository
- Ricerca di contenuto nel repository
- Visualizzazione delle proprietà del contenuto
- Accesso alle preferenze del singolo utente, quali indirizzo e-mail e password, opzioni generali, sottoscrizioni e scelta dei formati di output dei file

Di norma, si accede alla home page dal seguente indirizzo:

`http://<indirizzo IP host>:<porta>/peb`

Nota: L'indirizzo IPv6 deve essere racchiuso tra parentesi quadre, ad esempio `[3ffe:2a00:100:7031::1]`.

Se l'ambiente è configurato per l'utilizzo di un percorso di contesto personalizzato per le connessioni server, includerlo nell'URL.

`http://<indirizzo IP host>:<porta>/<percorso contesto>/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:

- **SAS.** Il server di esecuzione SAS corrisponde all'eseguibile di SAS, *sas.exe*, incluso nel software Base SAS®. Utilizzare questo server di esecuzione per elaborare i file di sintassi SAS.
- **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.

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.

Server di calcolo del punteggio

IBM SPSS Collaboration and Deployment Services Scoring Service è anche disponibile quale applicazione distribuibile indipendentemente, nota come Scoring Server.

Lo Scoring Server rende più flessibile la distribuzione in numerose aree chiave:

- Le prestazioni di calcolo possono essere scalate indipendentemente da altri servizi
- Gli Scoring Server possono essere configurati indipendentemente, riservando risorse informatiche a qualsiasi altra configurazione di calcolo del punteggio di IBM SPSS Collaboration and Deployment Services
- Il sistema operativo e l'architettura del processore del Scoring Server non devono eguagliare quelli di IBM SPSS Collaboration and Deployment Services Repository o ad altri Scoring Server
- Il server delle applicazioni con lo Scoring Server non deve essere lo stesso utilizzato per IBM SPSS Collaboration and Deployment Services Repository o altri Scoring Server

IBM Analytical Decision Management

IBM SPSS Collaboration and Deployment Services è un requisito per l'installazione di IBM Analytical Decision Management, una suite di applicazioni per l'integrazione dell'analisi predittiva nel processo decisionale operativo. IBM Analytical Decision Management si serve delle funzioni ad alta velocità per il calcolo del punteggio, la gestione dei dati master e l'automazione dei processi di IBM SPSS Collaboration and Deployment Services per ottimizzare e automatizzare un elevato numero di decisioni e produrre risultati migliori in specifiche situazioni aziendali.

Capitolo 2. Novità per gli addetti all'installazione

IBM SPSS Collaboration and Deployment Services Repository 8.1 propone nuove capacità volte a semplificare la distribuzione dell'analisi predittiva e la gestione dei costi.

Supporto di ulteriori piattaforme operative

IBM SPSS Collaboration and Deployment Services Repository 8.1 include il supporto per le nuove versioni dei sistemi operativi, server delle applicazioni, database, ambienti di virtualizzazione e browser web.

IBM WebSphere Application Server per IBM SPSS Collaboration and Deployment Services Repository

IBM SPSS Collaboration and Deployment Services include il server singolo, IBM WebSphere Application Server di base per l'utilizzo con IBM SPSS Collaboration and Deployment Services Repository. È possibile utilizzare questo server delle applicazioni o fornire un server delle applicazioni supportato alternativo.

IBM WebSphere Application Server Liberty Profile per IBM SPSS Collaboration and Deployment Services Scoring Server

IBM SPSS Collaboration and Deployment Services Scoring Server include WebSphere Application Server Liberty Profile per rendere semplice l'installazione e la distribuzione. È possibile utilizzare il server delle applicazioni o fornirne un altro.

SSL per IBM SPSS Collaboration and Deployment Services Remote Process Server

È possibile configurare IBM SPSS Collaboration and Deployment Services Remote Process Server per utilizzare SSL.

Novità in questa versione

Le seguenti funzioni non sono più supportate:

- IBM iSeries
- IBM WebSphere Application Server 7.x
- Oracle WebLogic Server 11gR1 PS5 (10.3.6)
- Red Hat JBoss EAP 6.1.0 Alpha
- IBM DB2 9.5
- IBM DB2 for i5/OS
- Teradata Enterprise Data Warehouse 13.1 (solo origine dati)
- Solaris

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 dichiarate obsolete dall'ultima versione.

Se una funzione è obsoleta, IBM Corp. potrebbe rimuovere tale funzionalità in una successiva release del prodotto. Gli investimenti futuri saranno concentrati sulla funzione strategica elencata nelle azioni di migrazione consigliate. Generalmente, una funzione non è obsoleta fino a quando non viene fornita un'alternativa equivalente.

La seguente tabella indica le funzione obsolete. Quando possibile, la tabella indica anche l'azione di migrazione consigliata.

Tabella 1. Funzioni obsolete nella versione precedente

Funzione obsoleta	Azione di migrazione consigliata
Provider di sicurezza: Active Directory con sostituzione locale, che supporta i gruppi estesi e gli utenti autorizzati.	Utilizzare il provider di sicurezza standard Active Directory con l'aggiunta di ogni gruppo necessario
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
File scenario	I file scenario (.scn) non sono più supportati. I nodi origine Enterprise View non possono essere modificati in Deployment Manager. I vecchi file scenario possono essere modificati sul client IBM SPSS Modeler ed essere nuovamente salvati come file di flusso. Inoltre, le configurazioni di calcolo del punteggio che hanno utilizzato i file scenario devono essere eliminate e devono essere ricreate in base al file di flusso.
Installazione Web per IBM SPSS Deployment Manager	Utilizzare il programma di installazione autonomo
BIRT Report Designer for IBM SPSS	Nessuna
BIRT Report Designer for IBM SPSS visualizzatore	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
Servizio di autenticazione login operazione	Servizio di autenticazione doLogin operazione
Servizio di ricerca ricerca operazione	Servizio di ricerca ricerca2.5 operazione
SPSS AXIS/Castor web services client jar	Utilizzare gli strumenti forniti con Java Runtime Environment, Integrated Development Environment, o Eclipse Web Tools Platform (WTP)

Per aggiornare informazioni su funzioni obsolete, consultare IBM Knowledge Center.

Capitolo 3. Installazione

Questo capitolo fornisce informazioni sull'installazione di IBM SPSS Collaboration and Deployment Services Repository. Il processo è costituito dal susseguirsi delle fasi di preinstallazione, installazione e configurazione, e post-installazione.

- Le fasi di **preinstallazione** impostano l'ambiente dell'applicazione e prevedono la definizione dei requisiti di sistema in funzione del tipo di installazione e del sistema previsto per l'utilizzo, l'approvvigionamento dei computer per l'esecuzione del server delle applicazioni o del cluster di server, la verifica che i server soddisfano tutti i requisiti hardware e software, la configurazione del server delle applicazioni o del cluster e la configurazione del database. Potrebbe inoltre essere necessario migrare il contenuto dall'installazione precedente a un nuovo database, utilizzando gli strumenti di copia database.
- Le fasi di **installazione e configurazione** prevedono l'installazione dei file dell'applicazione sul sistema host utilizzando IBM Installation Manager e successiva configurazione di IBM SPSS Collaboration and Deployment Services Repository da eseguirsi con il server delle applicazioni o il cluster di server designato e il database del repository.
- Le fasi di **post-installazione** prevedono l'avvio di IBM SPSS Collaboration and Deployment Services Repository, la verifica della connettività, la configurazione dell'avvio automatico, nonché l'installazione di driver di database aggiuntivi, componenti opzionali e altri adattatori per altri prodotti IBM SPSS.

Si precisa che in alcuni ambienti IBM SPSS Collaboration and Deployment Services Repository, la distribuzione potrebbe richiedere una serie di fasi di configurazione enterprise opzionali legate alla sicurezza dell'applicazione, il controllo dell'accesso e le capacità di notifica.

- Notifiche e-mail e RSS. Per informazioni, consultare il relativo capitolo del manuale dell'amministratore.
- Connessione sicura al repository. Per ulteriori informazioni, consultare la sezione Capitolo 9, "Utilizzo di SSL per proteggere il trasferimento di dati", a pagina 59.
- Protezione FIPS 140-2 e connessione sicura al repository. Per ulteriori informazioni, consultare la sezione Capitolo 8, "Conformità FIPS 140-2", a pagina 57.
- Single sign-on. Per ulteriori informazioni, consultare la sezione Capitolo 6, "Single sign-on", a pagina 41.

Preinstallazione

Prima di installare IBM SPSS Collaboration and Deployment Services, è necessario impostare le risorse nell'ambiente in modo che i componenti siano in grado di operare. Ad esempio, è necessario creare un database per il repository di contenuto e configurare un server delle applicazioni.

Lasciarsi guidare dal seguente elenco di controllo nel corso del processo di preinstallazione:

- Determinare il tipo di installazione in funzione dell'utilizzo previsto per il sistema e i relativi requisiti.
- Fornire i computer su cui eseguire il server o il cluster di server. Verificare che i server soddisfino tutti i requisiti hardware e software.
- Verificare le autorizzazioni del file system dell'host e dell'utente che esegue l'installazione.
- Configurare il cluster o il server delle applicazioni.
- Configurare il database. Se necessario, migrare il contenuto dall'installazione precedente a un nuovo database, utilizzando gli strumenti di copia database. Per ulteriori informazioni, consultare la sezione Capitolo 4, "Migrazione", a pagina 35.

Pianificazione dell'installazione

Prima di installare IBM SPSS Collaboration and Deployment Services Repository, è necessario determinare il tipo di installazione per essere in grado di impostare l'ambiente applicativo. IBM SPSS Collaboration and Deployment Services Repository è un sistema di livello enterprise che richiede l'integrazione con una molteplicità di componenti e tecnologie IBM Corp. e di terze parti. Nella configurazione di base, esso richiede la presenza di un server delle applicazioni, per eseguire i servizi Web che abilitano le funzionalità dell'applicazione e di un database relazionale, come IBM DB2 UDB, Oracle o Microsoft SQL Server, per memorizzare risorse analitiche e le impostazioni dell'applicazione.

Nel pianificare l'installazione, utilizzare le seguenti indicazioni:

- In ambienti operativi, il repository deve essere installato su un sistema a livello di server. Per ulteriori informazioni, consultare la sezione “Requisiti del sistema host”. L'esecuzione del repository del database su un server dedicato a se stante, può migliorare le prestazioni complessive del sistema.
- In ambienti aziendali con intensi carichi elaborativi (ad esempio, produzione di punteggi in tempo reale) e un numero maggiore di utenti, si consiglia di potenziare l'installazione con un cluster di server delle applicazioni piuttosto che un server delle applicazioni autonomo.
- Sebbene a scopi istruttivi e dimostrativi il repository possa essere installato ed eseguito su postazioni di lavoro portatili o desktop, non può tuttavia essere eseguito su tali sistemi in ambienti di produzione.

Nel pianificare la distribuzione di IBM SPSS Collaboration and Deployment Services Repository, è necessario valutare anche i requisiti dell'ambiente di produzione. Ad esempio, per abilitare l'elaborazione delle risorse analitiche e di calcolo del punteggio, potrebbe essere necessario impostare i server di esecuzione, come IBM SPSS Statistics e IBM SPSS Modeler, cui potrebbe essere anche necessario designare risorse hardware e di rete. Per abilitare la funzionalità di notifica e-mail, è necessario disporre di un server SMTP. Potrebbe anche essere necessario configurare l'autenticazione al repository tramite un sistema di directory esterna e di single sign-on con server Kerberos.

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.

Per le informazioni aggiornate relative ai requisiti di sistema, fare riferimento ai report di compatibilità dei prodotti software sul sito IBM Technical Support all'indirizzo: <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 l'esecuzione con Java 7 SDK. Consultare “WebSphere” a pagina 12.

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

IBM Installation Manager 1.8.0 o successivo (1.8.3 è consigliato) 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.
- Una volta installato il repository con un cluster di server delle applicazioni, è necessario condividere la directory di installazione del repository sul computer host del profilo di gestione (WebSphere) o dell'adminServer (WebLogic) per renderla accessibile da tutti i nodi del cluster.

Nota: 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.

Virtualizzazione

I componenti di IBM SPSS Collaboration and Deployment Services Repository o del client possono essere distribuiti in ambienti virtualizzati con software di terze parti. Ad esempio, per semplificare la distribuzione di un ambiente di sviluppo o verifica, un amministratore di sistema potrebbe configurare un server virtuale su cui installare IBM SPSS Collaboration and Deployment Services. Le macchine virtuali che ospitano i componenti di IBM SPSS Collaboration and Deployment Services devono soddisfare i requisiti minimi del sistema. Per ulteriori informazioni, consultare la sezione "Requisiti del sistema host" a pagina 10.

Presupponendo che l'ambiente virtualizzato configurato soddisfi i requisiti minimi di sistema, non si prevede alcun peggioramento delle prestazioni delle installazioni di IBM SPSS Collaboration and Deployment Services Repository o del client. Tuttavia, è importante precisare che i sistemi virtualizzati potrebbero condividere risorse fisiche ed eventuali conflitti di risorse su sistemi con intensi carichi elaborativi possono provocare un peggioramento delle prestazioni sulle installazioni IBM SPSS Collaboration and Deployment Services ospitate.

Si precisa che ulteriori limiti sulla distribuzione in ambienti virtualizzati potrebbe sussistere qualora non sia possibile distribuirvi i server delle applicazioni utilizzati per eseguire il repository.

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 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 può essere eseguito con un server WebSphere autonomo, gestito o un cluster.

Prima dell'installazione con un server WebSphere autonomo

- Creare un nuovo profilo per ogni installazione utilizzando il modello predefinito del profilo applicazione.

Prima dell'installazione con un server WebSphere gestito

- Creare un profilo di gestione distribuzione.
- Avviare il profilo di gestione.
- Creare un profilo gestito.
- Aggiungere un nodo gestito al profilo di gestione.
- Utilizzando la console WebSphere, creare un server gestito basato sul nodo gestito.

Prima dell'installazione con un cluster WebSphere

- Creare il cluster e appurare che sia accessibile tramite il bilanciamento del carico.

Prima di eseguire l'installazione con una topologia WebSphere Application Server Network Deployment

Incrementare la configurazione della memoria predefinita per il processo WebSphere Deployment Manager (**dmgr**) e i processi WebSphere Nodeagent. I requisiti di memoria effettivi dipendono dal sistema. Ad esempio, una configurazione di memoria minima dovrebbe incrementare la memoria nel seguente modo:

- Per il processo WebSphere Deployment Manager, incrementare la dimensione heap minimo a 512 e la dimensione heap massima a 1024.
- Per i processi WebSphere Nodeagent, incrementare la dimensione minima heap a 256 e la dimensione heap massima a 512.

Configurazione del profilo per l'esecuzione con Java 7

Prima di installare IBM SPSS Collaboration and Deployment Services in WebSphere, il profilo WebSphere utilizzato con IBM SPSS Collaboration and Deployment Services deve essere configurato per l'esecuzione con Java 7 SDK come illustrato di seguito:

1. Scaricare e installare **IBM WebSphere SDK Java Technology Edition Versione 7.0** nell'installazione WebSphere 8.5.x. Consultare http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.installation.base.doc/ae/tins_installation_jdk7.html.
2. Una volta installato, configurare il profilo WebSphere per IBM SPSS Collaboration and Deployment Services per utilizzare Java 7 SDK. Consultare http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_managesdk.html.
3. WebSphere consente che SDK sia configurato in modo globale (tutti i profili) o per-profilo. Per impostare Java 7 SDK per un profilo WebSphere specifico:

Dalla directory `<app_server_root>/bin`:

- a. Passo 1: (facoltativo) visualizzare un elenco dei nomi SDK disponibili per l'installazione del prodotto (confermare che Java 7 SDK è presente). Ad esempio:

```
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. Passo 2: impostare il profilo utilizzato per IBM SPSS Collaboration and Deployment Services alla versione 7.0 SDK. Ad esempio:

```
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.
```

Oppure impostare Java 7 SDK per tutti i profili WebSphere (e i successivi profili creati):

L'esempio che segue mostra la sequenza di comandi da utilizzare per elencare gli SDK disponibili, per modificare l'SDK predefinito nella versione 7.0 e, se i profili già esistono, per abilitare i profili ad utilizzare la versione SDK 7.0.

- a. Passo 1: (facoltativo) visualizzare un elenco dei nomi SDK disponibili per l'installazione del prodotto (confermare Java che 7 SDK è presente):

```
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. Passo 2: impostare il comando predefinito alla versione SDK 7.0:

```
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. Passo 3: impostare il nuovo profilo predefinito alla versione SDK 7.0:

```
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. Passo 4: se i profili già esistono, consentire ai profili di utilizzare SDK Versione 7.0:

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

Per modificare i profili federati in un'installazione di Network Deployment, Deployment Manager deve essere in esecuzione. Il comando `managesdk` aggiorna il repository della configurazione master. Una volta eseguito il comando, deve essere eseguita un'operazione di sincronizzazione prima di poter utilizzare il nuovo SDK per i profili federati.

JBoss

IBM SPSS Collaboration and Deployment Services Repository può essere eseguito solo con un server JBoss.

Prima dell'installazione con JBoss

- Creare un nuovo server per ogni installazione del repository.

Nota:

- Si consiglia l'esecuzione di un'unica istanza del server. Se è necessario impostare più istanze del repository su una sola macchina utilizzando JBoss, consultare la documentazione JBoss.
- Per evitare errori all'avvio del repository, si consiglia che il percorso di installazione del server delle applicazioni JBoss non contenga spazi, come nel seguente esempio `c:\jboss-eap-6.1`.
- Se JBoss è in esecuzione in un ambiente IPv6, sono necessarie ulteriori configurazioni del server delle applicazioni. Per ulteriori informazioni, consultare la documentazione Red Hat JBoss.

WebLogic

IBM SPSS Collaboration and Deployment Services Repository può essere eseguito con un server WebLogic autonomo o un cluster.

Prima dell'installazione con un server WebLogic autonomo

- Creare un nuovo server per ogni installazione del repository.

Prima dell'installazione con un server WebLogic gestito

- Creare un nuovo server gestito per ogni installazione del repository.

Prima dell'installazione con un cluster WebLogic

- Creare il cluster e appurare che sia accessibile tramite il bilanciamento del carico.

Nota:

- Se WebLogic è utilizzato con JRockit JRE su un sistema Linux, copiare il contenuto della directory `<WEBLOGIC_HOME>/endorsed` in `<JAVA_HOME>/jre/lib/endorsed`. Per ulteriori informazioni sulla configurazione WebLogic JRE, consultare la documentazione Oracle.
- Se si utilizza WebLogic con JRockit JRE, è necessario avviare il server utilizzando il parametro `-XstrictFP` (per abilitare l'utilizzo rigoroso a livello globale dell'aritmetica in virgola mobile in tutti i metodi di tutte le classi).

Database

Prima di installare IBM SPSS Collaboration and Deployment Services Repository, installare un database e abilitarne l'accesso. La connessione al database è richiesta per definire le necessarie tabelle di controllo e l'infrastruttura.

Il database e IBM SPSS Collaboration and Deployment Services Repository non devono essere installati su uno stesso server, alcuni dati di configurazione sono tuttavia necessari 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.

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:

Tabella 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 9.7 for Linux, Windows e UNIX

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

- DBADM

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

Esempio: Microsoft SQL Server 2008

- ALTER ANY SCHEMA
- CONNECT
- CREATE FUNCTION
- CREATE PROCEDURE
- CREATE TABLE
- CREATE VIEW
- CREATE XML SCHEMA COLLECTION
- DELETE
- EXECUTE
- INSERT
- REFERENCES
- SELECT
- UPDATE

Esempio: Oracle 11gR2

Le seguenti autorizzazioni sono necessarie per la configurazione di IBM SPSS Collaboration and Deployment Services Repository con il database Oracle 11gR2:

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

Le seguenti autorizzazioni sono necessarie per l'avvio di IBM SPSS Collaboration and Deployment Services Repository con il database Oracle 11gR2:

- CREATE SESSION
- ALTER SESSION
- SESSIONS_PER_USER - deve essere impostato con un valore uguale o maggiore a 100.

DB2

DB2 for Linux, UNIX e Windows

Quando si utilizzano i database DB2 for Linux, UNIX e Windows, i parametri di creazione del database predefiniti non sono sufficienti. È necessario specificare i seguenti parametri aggiuntivi:

- Insieme di codici UTF-8
- Pool di buffer con pagina da 8 KB (nello script campione *CDS8K*) per le tabelle superiori a 4 KB
- Spazio tabella da 8 KB utilizzando un pool di buffer da 8 KB
- Pool di buffer da 32 KB (*CDSTEMP* nello script campione)
- Spazio tabella temporaneo da 32 KB per eventuali insiemi di risultati ampi ottenuti con il pool di buffer da 32 KB

Segue uno script campione per la creazione di un database denominato *SPSSCDS*. Se lo si compia e incolla, appurare che corrisponda esattamente con l'SQL illustrato. Si precisa che lo script fa riferimento a un percorso file in stile UNIX ed è pertanto necessario modificarlo qualora lo si esegua su Windows. Nei download del software lo script è incluso come parte del package della documentazione.

```
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 su z/OS

- Quando si utilizza un database DB2 z/OS, è necessario verificare che il sottosistema DB2 zOS sia abilitato per Java, procedura memorizzata, funzione e XML.
- Per abilitare il supporto XQuery, è necessario applicare PTF UK73139 o versione superiore.

Configurazione della tabella dell'archivio messaggi JMS

Quando si installa IBM SPSS Collaboration and Deployment Services Repository con WebSphere Application Server, il provider JMS predefinito di WebSphere, SIB (Service Integration Bus), viene configurato in modo da utilizzare il database del repository come archivio dei messaggi JMS. All'avvio, il repository crea automaticamente nel database le opportune tabelle JMS, se non sono già presenti.

Quando si utilizza WebSphere su z/OS con DB2, le tabelle dell'archivio messaggi JMS devono essere create manualmente. Per creare le tabelle dell'archivio messaggi JMS di WebSphere su z/OS con DB2, utilizzare il comando WebSphere *sibDDLGenerator* per generare il DDL e applicarlo al database per creare le tabelle. Per ulteriori informazioni su *sibDDLGenerator*, consultare la documentazione WebSphere.

Ulteriori considerazioni

Quando si esegue DB2 su hardware designato, si consiglia di utilizzare DB2 Configuration Advisor per la gestione delle prestazioni del database. L'incremento dei valori dei seguenti parametri può comportare un miglioramento delle prestazioni:

- **IBMDEFAULTBP.** La dimensione del pool di buffer deve essere impostata in base alla memoria disponibile e prendendo in considerazione le altre applicazioni in esecuzione sul sistema.
- **NUM_IOCLEANERS.** Il numero di programmi di eliminazione pagine asincroni deve essere almeno pari al numero di processori sul sistema.
- **NUM_IOSERVERS.** L'aumento del numero di server I/O ottimizza la prelettura.
- **LOCKLIST.** L'aumento della quantità della memoria per l'elenco dei blocchi contribuisce a evitare timeout e deadlock durante le operazioni di scrittura.
- **MAXLOCKS.** Percentuale della *LOCKLIST* residua prima che il database manager la riassegni.

Se DB2 viene eseguito su un sistema condiviso, modificare tali valori valutando le risorse di sistema disponibili e, in alternativa, prendere in considerazione l'utilizzo della funzionalità di autoregolazione di DB2 per gestire le prestazioni del database.

Microsoft SQL Server

Quando si utilizza il database di Microsoft SQL Server:

- È necessario utilizzare lo schema *DBO*.
- La configurazione dell'accesso al database richiede un utente di SQL Server. L'autenticazione Windows non è supportata.
- Gli indirizzi IP devono essere abilitati per il protocollo di rete IP (Internet Protocol).

- Utilizzare le opportune opzioni per l'elaborazione del set di caratteri non latini. Ad esempio, si consiglia di utilizzare l'opzione Distinzione Kana (_KS) per distinguere tra i caratteri giapponesi Hiragana e Katakana. Per ulteriori informazioni sul confronto nel database, consultare la documentazione di Microsoft SQL Server.
- Il confronto database selezionato non deve essere sensibile alle minuscole/maiuscole (_CI).
- Nel database di Microsoft SQL Server abilitare l'isolamento dello snapshot. Di seguito si riporta un esempio delle istruzioni per l'attivazione di tale modalità:

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

Oracle Parametri di inizializzazione

Quando si utilizza un database Oracle con IBM SPSS Collaboration and Deployment Services, è necessario attenersi ai seguenti parametri e configurazioni. Le modifiche devono essere apportate ai file di parametro `init.ora` e `spfile.ora`.

Tabella 3. Parametri del database Oracle.

Parametro	Impostazione
OPEN_CURSORS	300
NLS_CHARACTERSET	AL32UTF8
NLS_NCHAR_CHARACTERSET	AL16UTF16
SESSIONS_PER_USER	Uguale a, o maggiore di 100

Nota: Impostare sia `NLS_CHARACTERSET` che `NLS_NCHAR_CHARACTERSET` quando si crea un'istanza Oracle.

Suggerimento: Per far sì che i valori di accesso utente siano sensibili al maiuscolo/minuscolo utilizzare i parametri come `NLS_LANG`, `NLS_COMP`, o `NLS_SORT` per l'istanza Oracle. Fare riferimento alla documentazione Oracle per determinare quale parametro meglio soddisfa le proprie esigenze.

Oracle XDB

Per un database Oracle, deve essere installato Oracle XDB (funzione del database XML). Verificabile eseguendo una query dello schema (account utente) `XDB` (`SELECT * FROM ALL_USERS`) oppure appurando la presenza di `RESOURCE_VIEW` (`DESCRIBE RESOURCE_VIEW`). Il principal Oracle che viene utilizzato con IBM SPSS Collaboration and Deployment Services Repository deve essere concesso al ruolo `XDBADMIN`.

Manutenzione del database del repository

Si consiglia vivamente di eseguire le attività di manutenzione del database di IBM SPSS Collaboration and Deployment Services Repository a intervalli regolari.

Tabella 4. Pianificazione della manutenzione del database repository

Attività	Pianificazione consigliata
Backup	Giornaliero
Aggiornamento statistiche	Giornaliero
Verifica coerenza	Settimanale
Riorganizzazione	Settimanale
Ricostruzione	Mensile

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.
- Configurare il IBM SPSS Collaboration and Deployment Services Repository da utilizzarsi 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" a pagina 25.

Installazione

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.

1. Accedere al sistema operativo come utente con il livello di autorizzazione appropriato. Per ulteriori informazioni, consultare la sezione "Autorizzazioni utente e file system" a pagina 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.

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

4. Nel menu principale, selezionare **Installa**.
5. Selezionare IBM SPSS Collaboration and Deployment Services come package da installare.

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

6. Leggere il contratto di licenza e accettarne i termini.
7. 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.
8. Selezionare le funzioni da installare.
9. Esaminare il riepilogo delle informazioni e procedere con l'installazione. I file dell'applicazione verranno installati nella directory specificata. È necessario procedere ulteriormente con la configurazione. Per ulteriori informazioni, consultare la sezione "Configurazione" a pagina 20. Se si sta eseguendo IBM Installation Manager in modalità GUI, l'opzione per avviare il programma di utilità di configurazione verrà presentato sull'ultimo pannello.

Nel caso di problemi durante l'installazione, è possibile risolverli utilizzando i log di IBM Installation Manager. I file di log sono accessibili dal menu principale di IBM Installation Manager.

Per automatizzare l'installazione di IBM SPSS Collaboration and Deployment Services, è possibile eseguire IBM Installation Manager in modalità non presidiata. Per ulteriori informazioni, consultare la documentazione IBM Installation Manager: <http://www-01.ibm.com/support/knowledgecenter/SSDV2W/welcome>.

Configurazione

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

- 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" a pagina 25.

Prima della 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.
 - **WebLogic autonomo:** il server deve essere arrestato.
 - **WebLogic gestito:** interrompere il server gestito, lasciare che il server di amministrazione di WebLogic resti in esecuzione.
 - **WebLogic in cluster:** interrompere i membri del cluster, lasciare che il server di amministrazione di WebLogic resti in esecuzione.
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).

Esecuzione del programma di utilità di configurazione

1. Accedere al sistema operativo con le medesime credenziali utente utilizzate per installare IBM SPSS Collaboration and Deployment Services Repository.
2. Avviare il programma di utilità di configurazione:
 - Modalità GUI - Windows
`<directory installazione repository>\bin\configTool.bat`
 - Modalità GUI - UNIX e Linux
`<directory installazione repository>/bin/configTool.sh`
 - Modalità riga di comando - Windows
`<directory installazione repository>\bin\cliConfigTool.bat`
 - Modalità riga di comando - UNIX e Linux
`<directory installazione repository>/bin/cliConfigTool.sh`

Nota: il programma di utilità può essere avviato automaticamente o come opzione alla fine della fase di installazione. Per ulteriori informazioni, consultare la sezione "Installazione" a pagina 19.

3. Selezionare il tipo di server delle applicazioni.
4. Specificare le impostazioni del server delle applicazioni:
 - **WebSphere**
 - **Root del profilo WebSphere** Percorso della directory del profilo del server di WebSphere. Si precisa che nel caso di server gestiti o di cluster, esso corrisponde al percorso del profilo del gestore di distribuzione. Altre impostazioni WebSphere, quali root di installazione WebSphere, topologia del profilo (per server autonomi), server e nodo, verranno compilati automaticamente in base alle informazioni del profilo. Se i valori non possono essere compilati automaticamente, specificarli manualmente.
 - **Root di installazione WebSphere** Percorso della directory in cui viene installato il server WebSphere.
 - **Topologia server** 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 installazioni in cluster, corrisponde all'URL del bilanciamento del carico o del server proxy per l'instradamento delle richieste avviate dal server.
 - **Server o cluster WebSphere** Nome del server o del cluster WebSphere.
 - **Nodo WebSphere** Per un server WebSphere gestito, corrisponde al nome del nodo su cui è ubicato il server di destinazione.
 - **Nome utente e password WebSphere** Solo se è stata abilitata la sicurezza amministrativa.
 - **JBoss**
 - **Percorso directory del server** Percorso della directory di installazione di JBoss.
 - **Server JBoss** Nome del server JBoss. Specificare il valore standalone.
 - **JVM** Posizione della directory del JVM di JBoss.
 - **Prefisso URL** URL per l'instradamento delle richieste avviate 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 conatteranno a IBM SPSS Collaboration and Deployment Services Repository.
 - **WebLogic**
 - **Directory root del dominio WebLogic** Percorso della directory nel dominio WebLogic. Altre impostazioni WebLogic come ad esempio il percorso della directory del server, la topologia del dominio, il nome del server o cluster e il percorso alla JVM WebLogic JVM, verranno automaticamente immesse in base alle informazioni del dominio. Se i valori non possono essere compilati automaticamente, specificarli manualmente.
 - **Percorso directory del server** Percorso della directory di installazione del server di WebLogic.
 - **Topologia del dominio** Topologia del dominio di WebLogic: server singolo o cluster.
 - **Prefisso URL** Per installazioni in cluster, corrisponde all'URL del bilanciamento del carico o del server proxy per l'instradamento delle richieste avviate dal server.
 - **Server o cluster WebLogic** Nome del server o del cluster WebLogic.
 - **Percorso del JVM di WebLogic** Percorso della directory del JVM di WebLogic.
 - **Nome utente e password di WebLogic.**
5. Specificare le informazioni sulla connessione al database:
 - **Tipo database** IBM DB2, SQL Server o Oracle.
 - **Host** Nome o indirizzo dell'host del server di database.
 - **Porta** Porta di accesso al server di database.
 - **Nome database** Nome del database utilizzato per il repository di contenuto.
 - **SID/Nome servizio** SID o nome del servizio di Oracle.

- **Esegui come servizio** In Oracle, indica che la connessione è stata effettuata utilizzando un servizio invece del SID del database.
 - **Nome utente** Nome dell'utente del database.
 - **Password** Password dell'utente del database.
6. Se si riutilizza un database di una installazione precedente, specificare se i dati presenti devono essere conservati o eliminati.
 7. 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.

8. 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.
9. 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.
10. Esaminare il riepilogo delle informazioni e procedere con la configurazione.
 - 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-installazione" a pagina 29.
 - Se si sceglie la modalità di distribuzione manuale, procedere con le fasi manuali. Per ulteriori informazioni, consultare la sezione "Distribuzione manuale" a pagina 23.
 - 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" a pagina 25.

Nota: la procedura di configurazione può impiegare dai 15 ai 30 minuti e oltre, in funzione dell'hardware, della velocità di rete, della complessità della topologia dei server delle applicazioni e così via. Qualora la procedura non dovesse rispondere o riportasse un errore, esaminare i file di log in `<Directory di installazione di IBM SPSS Collaboration and Deployment Services Repository>/log`.

Configurazione non presidiata

La configurazione di IBM SPSS Collaboration and Deployment Services Repository può essere automatizzata eseguendo il programma di utilità in modalità non presidiata prelevando l'input dal file delle proprietà. Il modello del file delle proprietà è disponibile in `<home repository>/setup/resources/properties/config.properties`. Se eseguito in modalità interattiva, il programma di utilità di configurazione crea `<home repository>/platform/engineConfig.properties`.

Per eseguire il programma di utilità di configurazione in modalità non presidiata:

```
<home installazione repository>/bin/engine.bat|.sh -config <percorso file proprietà config>
```

Per ripetere l'esecuzione del programma di utilità di configurazione in modalità non presidiata utilizzando i file delle proprietà creati in un momento precedente, ad esempio, dopo aver risolto i problemi provocati dalla mancata configurazione iniziale:

```
<home installazione repository>/bin/engine.bat|.sh -rerun
```

Per modificare il livello di accesso di una configurazione non presidiata, utilizzare il parametro `-antLogLevel <VERBOSE|DEBUG|INFO|WARN|ERROR>`.

Distribuzione manuale

La procedura di configurazione manuale è destinata agli utenti avanzati nel caso si richieda un maggiore controllo dell'ambiente del server delle applicazioni. Il programma di utilità della configurazione eseguito in modalità distribuzione manuale, richiede di apportare modifiche al database, ma non al server delle applicazioni. I file delle applicazioni distribuibili, gli script di installazione e i file delle proprietà J2EE generati nella directory `<directory installazione repository>/toDeploy/<timestamp>`. Tali risorse possono essere utilizzate per distribuire IBM SPSS Collaboration and Deployment Services Repository.

Importante: È necessario eseguire l'installazione, se prevista, degli adattatori dei prodotti IBM SPSS in IBM SPSS Collaboration and Deployment Services Repository prima di eseguire la distribuzione manuale. Se vengono installati dopo l'avvenuta distribuzione manuale del repository, è necessario innanzitutto annullare la distribuzione delle risorse del repository sul server dell'applicazione. Dopo di che, è possibile installare gli adattatori e ridistribuire il repository utilizzando le seguenti procedure relative a ciascun tipo di server delle applicazioni. Per informazioni su come annullare la distribuzione del repository, consultare "Disinstallazione" a pagina 33.

Distribuzione manuale su WebSphere

1. Eseguire la procedura di installazione di IBM SPSS Collaboration and Deployment Services Repository. Durante la fase di configurazione, selezionare l'opzione manuale sul pannello informazioni del server delle applicazioni. Per ulteriori informazioni, consultare la sezione "Configurazione" a pagina 20.
 - La directory `<directory installazione repository>/toDeploy/<timestamp>` conterrà i file per la configurazione del server WebSphere e la distribuzione dell'applicazione. Lo script `CrtCDSresources.py` genera le risorse del server delle applicazioni, quali provider JDBC, origini dati, e motori di messaggistica. Lo script `DeployCDS.py` distribuisce flag delle applicazioni.
2. Verificare che il server delle applicazioni sia nel seguente stato:
 - **WebSphere autonomo:** arrestato.
 - **WebSphere gestito/in cluster:** interrompere il server gestito/i membri del cluster, lasciare in esecuzione il server di Deployment Manager.
3. Eseguire gli script nella directory `<directory installazione repository>/toDeploy/<time stamp>`.

Se si sta eseguendo una distribuzione manuale su un server WebSphere autonomo, utilizzare l'opzione `-connType NONE`:

Windows

```
<root profilo WAS root>/bin/wsadmin -lang jython -connType NONE  
-wsadmin_classpath <directory installazione repository>/setup/lib/crypto-server.jar  
-f CrtCDSResources.py
```

```
<WAS profile root>/bin/wsadmin -lang jython -connType NONE -f DeployCDS.py
```

UNIX

```
<WAS profile root>/bin/wsadmin.sh -lang jython -connType NONE
-wsadmin_classpath <directory installazione repository>/setup/lib/crypto-server.jar
-f CrtCDSResources.py
```

```
<WAS profile root>/bin/wsadmin.sh -lang jython -connType NONE -f DeployCDS.py
```

Se è stata abilitata la protezione amministratore sul server WebSphere, è necessario includere anche i parametri dell'ID utente e della password dell'amministratore:

Windows

```
<root profilo WAS>/bin/wsadmin -lang jython -user <admin_user> -password <admin_password>
-wsadmin_classpath <directory installazione repository>/setup/lib/crypto-server.jar
-f CrtCDSresources.py
```

```
<root profilo WAS>/bin/wsadmin -lang jython -user <admin_user> -password <admin_password>
-f DeployCDS.py
```

UNIX

```
<WAS profile root>/bin/wsadmin.sh -lang jython -user <admin_user> -password <admin_password>
-wsadmin_classpath <directory installazione repository>/setup/lib/crypto-server.jar
-f CrtCDSresources.py
```

```
<WAS profile root>/bin/wsadmin.sh -lang jython -user <admin_user> -password <admin_password>
-f DeployCDS.py
```

4. Avviare il server.

Per un cluster, completare tutte le fasi richieste per tutti i membri. Per ulteriori informazioni, consultare la sezione "Cluster WebSphere" a pagina 26.

Per eseguire la distribuzione manuale su JBoss

1. Eseguire la procedura di installazione di IBM SPSS Collaboration and Deployment Services Repository. Durante la fase di configurazione, selezionare l'opzione manuale sul pannello informazioni del server delle applicazioni. Per ulteriori informazioni, consultare la sezione "Configurazione" a pagina 20.
 - La directory *<directory installazione repository>/toDeploy/<timestamp>* conterrà i file per la configurazione del server JBoss e la distribuzione dell'applicazione. Lo script *CrtCDSresources.bat* o *CrtCDSresources.sh* genera le risorse del server delle applicazioni, quali provider, origini dati, motori di messaggistica JDBC e così via, mentre lo script *DeployCDS.bat* o *DeployCDS.sh* distribuiscono gli indicatori delle applicazioni.
2. Verificare che il server delle applicazioni sia stato interrotto.
3. Eseguire gli script nella directory *<directory installazione repository>/toDeploy/<timestamp>*.

Windows

```
CrtCDSresources.bat
DeployCDS.bat
```

UNIX

```
CrtCDSresources.sh
DeployCDS.sh
```

4. Avviare il server.

Distribuzione manuale del repository su WebLogic

1. Eseguire la procedura di installazione di IBM SPSS Collaboration and Deployment Services Repository. Durante la fase di configurazione, selezionare l'opzione manuale sul pannello informazioni del server delle applicazioni. Per ulteriori informazioni, consultare la sezione "Configurazione" a pagina 20.
 - La directory *<directory installazione repository>/toDeploy/current* conterrà i file per la configurazione del server WebLogic e la distribuzione dell'applicazione. *DeployCDS.bat* o *DeployCDS.sh* genera le risorse del server delle applicazioni, quali provider, origini dati, motori di messaggistica JDBC e così, e distribuisce i file di applicazioni.

- a. Verificare che il server delle applicazioni sia nel seguente stato:
 - **WebLogic autonomo:** Avviato.
 - **WebLogic gestito/in cluster:** I membri server/cluster gestito devono essere arrestati, il server di amministrazione deve essere in esecuzione.
2. Eseguire i seguenti comandi dalla directory *<directory installazione repository>/toDeploy/current*:
Windows
`deploy.bat -user <weblogic_user> -password <weblogic_password> -resources -deploy`
UNIX
`deploy.sh user <weblogic_user> -password <weblogic_password> -resources -deploy`
3. Aggiornare lo script di avvio del server WebLogic includendo la chiamata allo script che imposta le variabili di ambiente. Questi file si trovano nella directory *<directory installazione repository>/toDeploy/current* e anche nella directory *<dominio WebLogic>/bin*.
Windows
`setCDSEnv.cmd`
UNIX
`setCDSEnv.sh`
4. Avviare il server.
Per un cluster, completare tutte le fasi richieste per tutti i membri. Per ulteriori informazioni, consultare la sezione "Cluster WebLogic" a pagina 27.

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. Un'architettura di questo tipo consente la distribuzione dell'elaborazione tra più server delle applicazioni, oltre a offrire ridondanza, nell'eventualità di errori su server singoli.

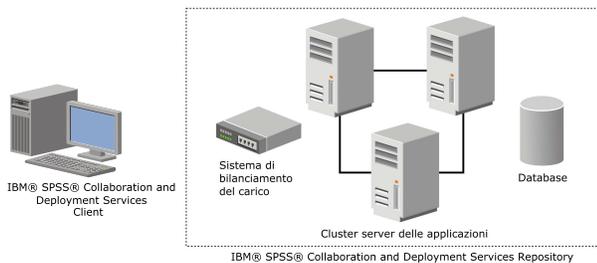


Figura 2. Architettura di distribuzione in cluster

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.

Al momento, IBM SPSS Collaboration and Deployment Services Repository supporta il clustering dei server delle WebSphere e WebLogic. 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" a pagina 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" a pagina 28.
8. Avviare il cluster.

Cluster WebLogic

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" a pagina 19.
3. Configurare la condivisione della directory di installazione per consentire l'accesso a tutti i membri del cluster.
4. Per garantire il failover JMS, configurare il server JMS su una destinazione di migrazione:
 - Per la migrazione automatica, WebLogic richiede un'origine dati munita di una tabella specifica. Il database di IBM SPSS Collaboration and Deployment Services Repository può essere utilizzato a tale scopo, ma la tabella deve essere creata manualmente. Accedere a `<directory server WebLogic>/server/db` e selezionare la sottocartella corrispondente al produttore del database utilizzato con il repository. Per creare la tabella richiesta da WebLogic, utilizzare l'SQL specifico per il database nel file `leasing.ddl`, ad esempio, `<directory server WebLogic>/server/db/db2/leasing.ddl`. Si noti che il nome della tabella predefinita è *ACTIVE*. Utilizzare gli strumenti del produttore del database per creare la tabella nel database del repository.
 - Utilizzando WebLogic Administration Console, in **Ambiente > Cluster > Configurazione > Migrazione**, impostare Base migrazione su *Database* e Origine dai per migrazione automatica su *CDS_DataSource*. Essa rappresenta l'origine dati del repository, che deve essere già stata creata e indirizzata al cluster.
 - In **Ambiente > Destinazioni di migrazione**, impostare Politica di migrazione servizio su *Auto-Migrate Exactly-Once Services*. Ciò promuoverà il trasferimento automatico dei servizi JMS su un server diverso, qualora uno dovesse guastarsi. Le modifiche apportate alla destinazione di migrazione potrebbero richiedere il riavvio dei server.

- In **Servizi > Archivi permanenti > PlatformStore > Configurazione**, modificare l'impostazione di Destinazione in modo che faccia riferimento alla destinazione di migrazione configurata nella fase precedente. Se si riceve un messaggio di errore concernente PlatformJMSServer non indirizzato verso la stessa destinazione, ignorarlo.
 - In **Servizi > Messaging > Server JMS > PlatformJMSServer**, modificare l'impostazione di Destinazione in modo che faccia riferimento alla destinazione di migrazione configurata nella fase precedente.
5. Aggiornare lo script di avvio del server WebLogic includendo una chiamata allo script *setCDSEnv.sh* o *setCDSEnv.cmd* per impostare le variabili d'ambiente. Si precisa che quando gli adattatori del repository sono installati, il file di script viene aggiornato in base alle nuove impostazioni. Il modo più semplice per garantire che le impostazioni di tutti i server siano sempre aggiornate è fare riferimento direttamente al file di script nella directory *<directory installazione repository>/toDeploy/current* utilizzando il percorso di rete condiviso.
 6. 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".
 7. Avviare il cluster.

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 WebLogic e WebSphere offrono programmi di utilità integrati per il bilanciamento del carico basato su software, quali WebLogic Apache Plugin e 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 "Configurazione" a pagina 20.

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" a pagina 26.
4. Riavviare il cluster.

WebLogic

1. Creare ulteriori server WebLogic e aggiungerli al cluster utilizzando la console WebLogic.
2. Aggiornare lo script di avvio del server WebLogic includendo una chiamata allo script *setCDSEnv.sh* o *setCDSEnv.cmd* per impostare le variabili d'ambiente. Si precisa che quando gli adattatori del repository sono installati, il file di script viene aggiornato in base alle nuove impostazioni. Il modo più semplice per garantire che le impostazioni di tutti i server siano sempre aggiornate è fare riferimento direttamente al file di script nella directory *<directory installazione repository>/toDeploy/current* utilizzando il percorso di rete condiviso.
3. Riavviare il server appena aggiunto al cluster.

Post-installazione

Lasciarsi guidare dal seguente elenco di controllo nel corso delle fasi di post-installazione:

- Avviare il server e verificare la connettività. Se necessario, configurare l'avvio automatico del server.
- Installare eventuali adattatori di contenuto per utilizzare IBM SPSS Collaboration and Deployment Services Repository insieme ad altri prodotti IBM SPSS, quali IBM SPSS Statistics e IBM SPSS Modeler.
- 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, consultare *IBM SPSS Collaboration and Deployment Services Remote Process Server 8.1 Istruzioni sull'installazione* e *IBM SPSS Collaboration and Deployment Services - Essentials for Python 8.1 Istruzioni sull'installazione*.
- Se necessario, modificare la password master del database.
- Se necessario, installare driver JDBC aggiuntivi.
- Installare i client IBM SPSS Collaboration and Deployment Services e IBM SPSS Deployment Manager. Per ulteriori informazioni, consultare le istruzioni di installazione dell'applicazione client.
- Utilizzando Deployment Manager, creare utenti singoli e gruppi del repository e assegnarvi le autorizzazioni di accesso alle applicazioni attraverso ruoli. Per ulteriori informazioni, consultare *IBM SPSS Collaboration and Deployment Services 8.1 Administrator's Guide*.

Per problemi durante le fasi di post-installazione, consultare *IBM SPSS Collaboration and Deployment Services 8.1 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.

Nota: 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.

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.

WebLogic

Per le configurazioni di singoli server WebLogic, utilizzare i seguenti script a corredo dell'installazione del server di repository:

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

Il server delle applicazioni WebLogic può essere avviato utilizzando un meccanismo a scelta, tuttavia è necessario verificare che le variabili di ambiente siano corrette e che le proprietà Java siano impostate. Per assistere con la procedura, la configurazione crea i seguenti script nella directory *toDeploy/current*:

- *setCDSEnv.cmd* o *setCDSEnv.sh*
- *startCDSWebLogic.cmd* o *startCDSWebLogic.sh*
- *startManagedCDSWebLogic.cmd* o *startManagedCDSWebLogic.sh*

Se viene selezionata la distribuzione automatica durante la configurazione, i file vengono copiati nel dominio e nella directory *<dominio>/bin*. Ispezionarli per determinare quale ambiente e proprietà Java è necessario impostare. Le proprietà specifiche varieranno in funzione degli adattatori IBM SPSS installati. Se si avvia il server utilizzando uno script di avvio, è possibile chiamare *setCDSEnv.cmd/setCDSEnv.sh* da tale script. Se si avvia il server attraverso gestione nodi, definire le opportune impostazioni.

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
- Internet Explorer 9

- Internet Explorer 8
- Firefox 10 ESR
- Safari 5
- Safari 4

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	CDS_DataSource
JBoss	jdbc/spss/PlatformDS
WebLogic	CDS_DataSource

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 viene configurato sul server delle applicazioni WebSphere o WebLogic utilizzando la distribuzione automatica (con il programma di utilità per la configurazione) o la distribuzione manuale mediante gli script generati dal programma di utilità per la configurazione, la password viene trasferita al server delle applicazioni in formato testo semplice e quindi mantenuta in base alle impostazioni del server delle applicazioni. Sebbene le impostazioni WebSphere e WebLogic predefinite prevedono la memorizzazione delle password in formato crittografato, potrebbe essere necessario verificare che la password non sia memorizzata in formato di testo semplice. 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.

Nota:

- Se si utilizza il server delle applicazioni WebLogic con il repository, modificare la password in IBM SPSS Collaboration and Deployment Services prima modificarla nel database.

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. La password modificata utilizzando la console WebLogic viene automaticamente crittografata.

Driver JDBC

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

IBM SPSS Collaboration and Deployment Services include un insieme di driver JDBC IBM Corp. per tutti i principali sistemi di database: IBM DB2, Microsoft SQL Server e 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`
- Oracle WebLogic: `<directory installazione repository>/<nome dominio>/lib`

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.

Compatibilità con i prodotti IBM SPSS

La funzionalità di IBM SPSS Collaboration and Deployment Services Repository può essere estesa con il supporto di altre applicazioni IBM SPSS, installando package di adattatori di contenuto aggiuntivi.

Per le informazioni aggiornate relative alla compatibilità, fare riferimento ai report di compatibilità dei prodotti software al sito IBM Technical Support all'indirizzo: <http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html>

Nota:

- Alcuni prodotti richiedono l'applicazione di patch. Rivolgersi all'assistenza tecnica di IBM Corp. per determinare se il livello di patch utilizzato sia corretto.
- È necessario verificare che i requisiti di installazione e di runtime delle applicazioni IBM SPSS (ad esempio, server delle applicazioni e database) siano compatibili con i requisiti di IBM SPSS Collaboration and Deployment Services Repository. Per informazioni dettagliate, consultare i report sulla compatibilità dei prodotti software e la documentazione dei singoli prodotti IBM SPSS .

I client IBM SPSS Statistics e IBM SPSS Modeler non sono essenziali per l'utilizzo di IBM SPSS Collaboration and Deployment Services. Tuttavia, le interfacce di tali applicazioni consentono di utilizzare IBM SPSS Collaboration and Deployment Services Repository per archiviare e recuperare oggetti. Le versioni server di questi prodotti sono necessari per lavori contenenti oggetti IBM SPSS Statistics o IBM SPSS Modeler da eseguire.

Per impostazione predefinita, il repository viene installato senza adattatori per gli altri prodotti IBM SPSS demandando agli utenti il compito di installare i package degli adattatori associati con le versioni dei prodotti utilizzati. I package sono inclusi nel supporto di distribuzione prodotti.

Si precisa che è necessario evitare la memorizzazione degli oggetti del prodotto IBM SPSS nel repository finché non è stata eseguita l'installazione dei package degli adattatori richiesti. In caso contrario, il tipo oggetto non verrà riconosciuto, anche dopo l'installazione dei package degli adattatori, costringendo a eliminare e ad aggiungere nuovamente gli oggetti nel repository. Ad esempio, se un flusso IBM SPSS Modeler viene memorizzato nel repository prima di avere installato l'adattatore IBM SPSS Modeler, risultando sconosciuto, il tipo MIME verrà impostato su un tipo generico, rendendo il file di flusso inutilizzabile.

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>/deICDS.py
```

- Server gestito o cluster WebSphere

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

- WebLogic

- ```
<directory installazione repository>/toDeploy/current/deploy[.sh]
-user <user ID> -password <password> -undeploy
```

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*.

---

## Capitolo 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), il server (JBoss) o il dominio (WebLogic) già utilizzati per eseguire l'istanza precedente 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 "Compatibilità con i prodotti IBM SPSS" a pagina 33.

**Nota:** 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 8.1, la migrazione dalla versione 7 è supportata.

---

### Installazione utilizzando una copia del database del repository

L'utilizzo di una copia di un database del repository consente di tenere in linea l'istanza preesistente finché la nuova installazione non è pronta per l'attivazione.

Questa procedura è riservata a migrazioni eseguite utilizzando una copia del database del repository in cui i database di origine e destinazione sono uguali, ad esempio, da DB2 a DB2. Per informazioni su come commutare sistemi database, consultare "Migrazione su un database diverso"

- Eseguire una copia del database del repository preesistente. La copia del database può essere eseguita utilizzando strumenti del produttore del database o di terze parti.
- Eseguire il programma di utilità per la configurazione di IBM SPSS Collaboration and Deployment Services indirizzandola verso la nuova copia del database del repository. Verificare che l'opzione Mantieni i dati esistenti sia stata selezionata per non perdere i dati archiviati.
- Reinstallare i package aggiuntivi.

---

## Installazione utilizzando un database del repository preesistente

L'aggiornamento a IBM SPSS Collaboration and Deployment Services Repository è eseguibile dall'installazione del sistema anche con un database del repository preesistente.

- Interrompere il repository.
- Eseguire il backup del database del repository preesistente.
- Installare IBM SPSS Collaboration and Deployment Services ed eseguire il programma di utilità per la configurazione. Verificare che l'opzione Mantieni i dati esistenti sia stata selezionata per non perdere i dati archiviati.
- Reinstallare i package aggiuntivi.

---

## Migrazione su un database diverso

La migrazione su un database diverso può includere il passaggio ad un fornitore di database differente (ad esempio, da SQL Server a IBM DB2 oppure da Oracle a DB2) oppure la migrazione su un database su un sistema operativo differente (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.

Si precisa che date le differenze tra gli ambienti dei database e gli strumenti di copia del fornitore, come DB2 backup, MS-SQL Server backup o Oracle RMAN, durante la migrazione, è necessario appurare che lo strumento selezionato supporti le seguenti funzioni del database:

- Tabelle XML (*SPSSDMRESPONSE\_LOG* e *SPSSSCORE\_LOG*)
- Dati binari/BLOB, CLOB
- Date dal formato speciale

Ad esempio, Oracle 11g 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'assistenza tecnica IBM Corp. prima di eseguire la migrazione del database.

---

## Ulteriori considerazioni sulla migrazione

In base alla configurazione prescelta, potrebbero essere necessarie ulteriori attività per una corretta migrazione di quanto segue:

- 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 cambiare fornitore o dimensioni in bit di Java (ad esempio, quando si migra da WebLogic 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.

## Migrazione dell'archivio JMS su WebSphere

Quando si installa IBM SPSS Collaboration and Deployment Services Repository con WebSphere Application Server, il provider JMS predefinito di WebSphere, SIB (Service Integration Bus), viene configurato in modo da utilizzare il database del repository come archivio dei messaggi JMS. All'avvio, il repository crea automaticamente nel database le opportune tabelle JMS, se non sono già presenti. Si precisa che quando si utilizza WebSphere su z/OS con DB2, le tabelle dell'archivio messaggi JMS devono essere create manualmente.

Quando si utilizza una copia del database per migrare il contenuto di un repository su una nuova istanza eseguita su WebSphere, prima di avviare IBM SPSS Collaboration and Deployment Services, eliminare le tabelle dell'archivio messaggi JMS (le tabelle con i nomi che iniziano con SIB\*) dal database. Le tabelle verranno create automaticamente, con l'eccezione di WebSphere su z/OS.

Per creare manualmente le tabelle dell'archivio messaggi JMS di WebSphere su z/OS con DB2, utilizzare il comando WebSphere *sibDDLGenerator* per generare il DDL e applicarlo al database per creare le tabelle. Per ulteriori informazioni su *sibDDLGenerator*, consultare la documentazione WebSphere.

## **Migrazione dell'archivio JMS su WebLogic**

Durante la migrazione dell'archivio messaggi JMS di IBM SPSS Collaboration and Deployment Services Repository installato con WebLogic, è necessario tenere presenti alcune considerazioni speciali.

Quando viene utilizzata la copia del database per migrare il contenuto del repository in una nuova istanza in esecuzione su WebLogic, è necessario eliminare il contenuto della tabella di archiviazione messaggi JMS *SPSSWLStore* dal database prima di avviare IBM SPSS Collaboration and Deployment Services.

## **Migrazione dei modelli di notifica**

Dopo la configurazione iniziale della nuova installazione, al fine di conservare le personalizzazioni eseguite sui modelli di notifica in un repository preesistente, copiare i modelli da *<directory installazione repository>/components/notification/templates* nella medesima directory della nuova installazione. Per ulteriori informazioni sui modelli di notifica, consultare *IBM SPSS Collaboration and Deployment Services Repository 8.1 Administrator's Guide*.

---

## Capitolo 5. Gestione dei package

Gli aggiornamenti, i componenti facoltativi e gli adattatori di contenuto per prodotti IBM SPSS sono installati sul server IBM SPSS Collaboration and Deployment Services Repository come package con IBM Installation Manager.

Per i dettagli, consultare le istruzioni di installazione per singoli componenti.

È possibile inoltre utilizzare il programma di utilità IBM SPSS Collaboration and Deployment Services Package Manager per risolvere problemi relativi alla configurazione del package IBM SPSS Collaboration and Deployment Services e per installare componenti aggiuntivi, come ad esempio, adattatori di contenuti personalizzati e provider di sicurezza.

---

### 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:

- WebSphere: il server autonomo deve essere arrestato. Il server gestito deve essere interrotto, mentre il nodo di Deployment Manager deve restare in esecuzione. Tutti i membri del cluster devono essere arrestati, mentre il nodo di Deployment Manager deve restare in esecuzione.
- JBoss: arrestato.
- WebLogic: il server autonomo deve essere arrestato. Nel caso di un server gestito o di cluster, il server di amministrazione di WebLogic deve restare in esecuzione, mentre il server/cluster di destinazione interrotto.

**Importante:** Se il repository è stato inizialmente distribuito manualmente, anche l'aggiornamento della distribuzione deve avvenire manualmente dopo l'esecuzione di IBM SPSS Collaboration and Deployment Services Package Manager. Per ulteriori informazioni, consultare la sezione "Distribuzione manuale" a pagina 23. Le risorse create manualmente non subiscono modifiche durante l'esecuzione del gestore package e quindi, non è necessario aggiornarle.

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.

**Nota:** 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`.

---

## Capitolo 6. Single sign-on

IBM SPSS Collaboration and Deployment Services propone capacità single sign-on autenticando inizialmente gli utenti attraverso un servizio di directory estero basato sul protocollo di sicurezza *Kerberos* e successivamente, utilizzando le credenziali in tutte le applicazioni IBM SPSS Collaboration and Deployment Services (ad esempio, IBM SPSS Deployment Manager, IBM SPSS Collaboration and Deployment Services Deployment Portal, o un server del portale) senza ulteriore autenticazione.

**Nota:** Il single sign-on (SSO) non è possibile con IBM SPSS Deployment Manager basato su browser.

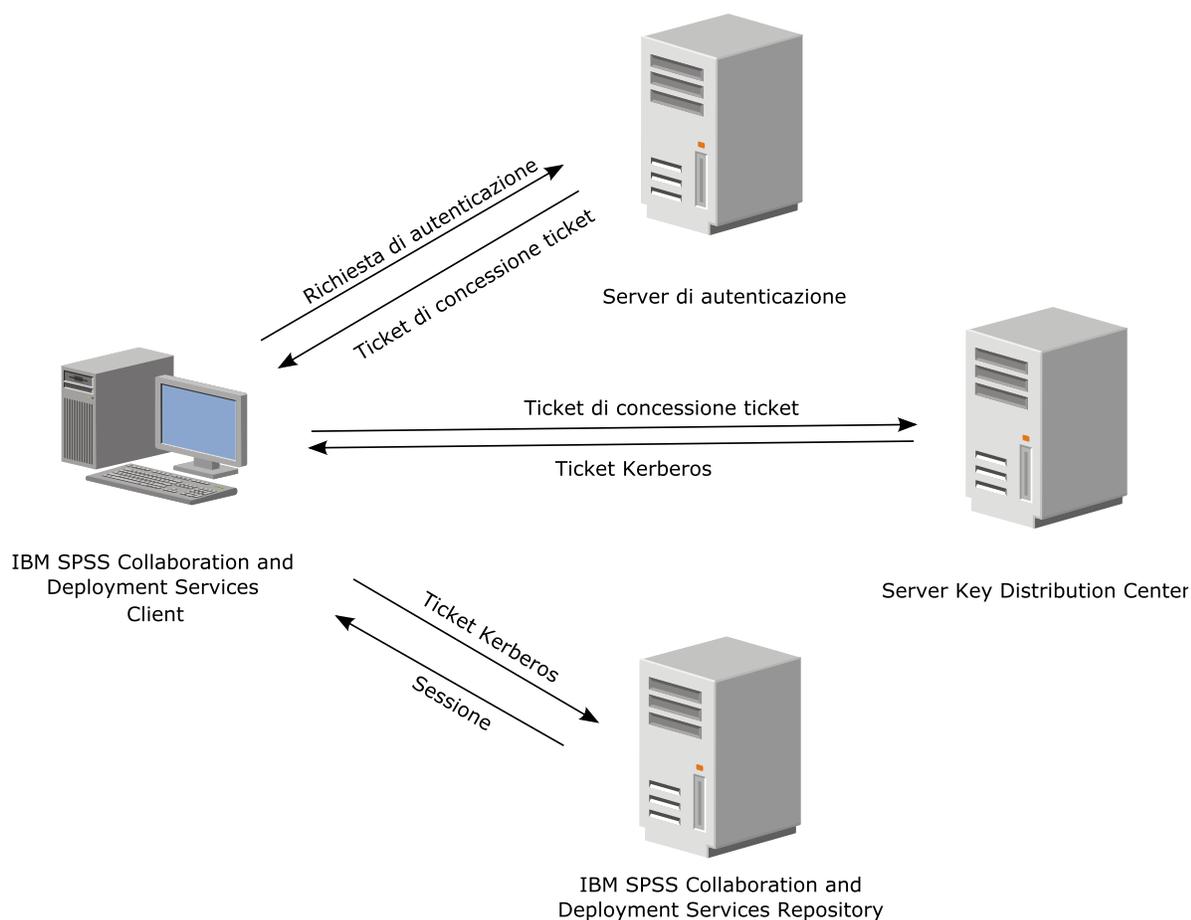


Figura 3. Architettura SSO di IBM SPSS Collaboration and Deployment Services

Ad esempio, quando si utilizzano congiuntamente IBM SPSS Collaboration and Deployment Services e Windows Active Directory, è necessario configurare il servizio *Kerberos Key Distribution Center (KDC)* per abilitare il protocollo single sign-on. Il servizio fornirà ticket di sessione e chiavi di sessione temporanee agli utenti e ai computer che operano nel dominio Active Directory. È necessario che KDC esegua ciascun controller di dominio nell'ambito di Active Directory Domain Services (AD DS). Quando il protocollo single sign-on è abilitato, le applicazioni IBM SPSS Collaboration and Deployment Services si collegano al dominio Kerberos utilizzando token Kerberos per l'autenticazione dei servizi Web. Se il protocollo single sign-on è abilitato, si consiglia vivamente di configurare le comunicazioni SSL del repository.

Applicazioni client desktop, quali Deployment Manager, creano un oggetto Java il cui contesto viene utilizzato per stabilire una sessione GSS con il repository. Una volta stabilito il contesto GSS, il repository

restituisce al client un ticket di servizio Kerberos. Anche le applicazioni thin client, quali Deployment Portal, ricevono un ticket di servizio Kerberos dal repository. Prima, tuttavia, eseguono l'autenticazione multiplatforma basata su HTTP attraverso il protocollo Negotiate. Sia le applicazioni desktop che thin client richiedono l'accesso a un dominio Kerberos, ad esempio, il dominio Microsoft Active Directory/Windows.

La configurazione di single sign-on in IBM SPSS Collaboration and Deployment Services include le seguenti fasi:

- Configurazione del sistema di directory.
- Configurazione del sistema di directory quale *provider di sicurezza* di IBM SPSS Collaboration and Deployment Services utilizzando la scheda Amministratore server di IBM SPSS Deployment Manager. Per ulteriori informazioni, consultare la documentazione dell'amministratore di IBM SPSS Collaboration and Deployment Services.
- Configurazione del server Kerberos Key Distribution Center. Abilitare la delega delle credenziali per il principal di servizio Kerberos sul server Kerberos Key Distribution Center. La procedura per abilitare la delega delle credenziali varierà in funzione del directory server utilizzato e dell'ambiente Kerberos in cui si opera.
- Configurazione del server Kerberos Key Distribution Center quale provider di single sign-on per IBM SPSS Collaboration and Deployment Services utilizzando la scheda Amministrazione server di IBM SPSS Deployment Manager. Per ulteriori informazioni, consultare la documentazione dell'amministratore di IBM SPSS Collaboration and Deployment Services.
- Configurazione del server delle applicazioni per il single sign-on.
- Nei sistemi client Windows, è necessario aggiornare il registro di sistema per accedere all'autorità di sicurezza locale (LSA) Kerberos.
- In base al repository utilizzato, potrebbe essere necessario aggiornare la configurazione del server delle applicazioni.
- Nei sistemi client Windows è necessario aggiornare il valore del registro di sistema HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\. Per ulteriori informazioni, consultare la sezione "Aggiornamento del registro di sistema Windows con il single sign-on" a pagina 47.
- Per accedere al repository con il thin client (ad esempio, con IBM SPSS Collaboration and Deployment Services Deployment Portal), è necessario abilitare SPNEGO (Simple and Protected GSS-API Negotiation) nel browser Web.

L'abilitazione di Server Process Credential nel repository prevede fasi aggiuntive. Per ulteriori informazioni, consultare la sezione "Configurazione di Server Process Credential" a pagina 48.

---

## Configurazione della directory per il single sign-on

Il single sign-on di IBM SPSS Collaboration and Deployment Services richiede la configurazione di una directory esterna. L'autenticazione della directory per il single sign-on di IBM SPSS Collaboration and Deployment Services può basarsi sui seguenti sistemi di directory:

- Directory OpenLDAP
- Microsoft Active Directory

### OpenLDAP

La configurazione complessiva prevede le seguenti fasi:

- Configurazione del provider di sicurezza OpenLDAP. Per ulteriori informazioni, consultare *IBM SPSS Collaboration and Deployment Services 8.1 Administrator's Guide*.
- Modifiche alla configurazione OpenLDAP specifiche per server Kerberos sul server Kerberos utilizzato.

## OpenLDAP su server Kerberos con Windows

Se la directory OpenLDAP viene utilizzata su server Kerberos con Windows, in cui OpenLDAP funge da provider di sicurezza per IBM SPSS Collaboration and Deployment Services e il server Kerberos con Windows funge da provider di single sign-on, verificare che lo schema OpenLDAP coincida con lo schema Active Directory. In caso contrario, modificare il mapping utente sul server OpenLDAP.

### Server MIT Kerberos

Se si utilizza il server MIT Kerberos con OpenLDAP, potrebbe essere necessario configurare SSL sul server e sul client OpenLDAP per garantire che il servizio KDC e il server LDAP sono su un host diverso. Per informazioni aggiornate, consultare la documentazione del server MIT Kerberos specifica per la versione utilizzata.

### Active Directory

Le seguenti istruzioni si riferiscono al controller di dominio di Windows Server 2003. I sistemi Windows Server 2008 avranno fasi analoghe.

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.

---

## Configurazione del server Kerberos

In ambienti Microsoft Windows, si consiglia l'utilizzo di Active Directory Server con server Kerberos con Windows integrato). Aggiornare i registri di sistema dei computer client con l'accesso LSA Kerberos. È necessario, inoltre, apportare modifiche specifiche ai browser per utilizzare Kerberos. Per i server Kerberos senza Microsoft Windows, potrebbe essere necessario installare software aggiuntivo sia sul computer host del repository che su ciascun computer client. In tutti i casi, il principal del servizio Kerberos deve essere impostato sulla delega delle credenziali. È necessario, inoltre, apportare modifiche specifiche su ciascun computer client per la delega delle credenziali.

---

## Configurazione del server delle applicazioni per il single sign-on

In base al repository utilizzato, potrebbe essere necessario aggiornare le impostazioni del server delle applicazioni.

## WebSphere

La configurazione del single sign-on su IBM SPSS Collaboration and Deployment Services per WebSphere 7 e 8 prevede le seguenti fasi:

- Definizione del file keytab di Kerberos.
- Definizione della politica JAAS-JGSS.

### Definizione del file keytab di Kerberos

1. Nella console di gestione, scegliere:  
**Server > Server delle applicazioni > <Nome server> > Infrastruttura server > Definizione del processo > Java Virtual Machine > Proprietà personalizzate**
2. Aggiungere la proprietà personalizzata *KRB5\_KTNAME* recante il valore del percorso del file keytab.

### Definizione della politica JAAS-JGSS

1. Nella console di gestione, scegliere:  
**Sicurezza > Protezione amministrazione, applicazione e infrastruttura > Java Authentication and Authorization Service > Accessi alle applicazioni**
2. Definire una proprietà *JGSSServer*.
3. In Proprietà aggiuntive alla voce *JGSSServer*, definire la classe modulo *com.ibm.security.auth.module.Krb5LoginModule* munita di strategia di autenticazione **REQUIRED**.
4. Definire le seguenti proprietà personalizzate per *com.ibm.security.auth.module.Krb5LoginModule*.

| Nome proprietà   | Valore                                                                |
|------------------|-----------------------------------------------------------------------|
| credsType        | entrambi                                                              |
| principal        | <nome principal>, ad esempio, <i>HTTP/cdsserver.spss.com@SPSS.COM</i> |
| useDefaultKeytab | true                                                                  |

## JBoss

Il server di applicazioni JBoss richiede almeno una configurazione JAAS (Java Authentication and Authorization Service) per JGSSServer. Il modello della politica dell'applicazione single sign-on (SSO) si trova nell'elemento JGSSServer di <JBoss installation directory>/standalone/configuration/standalone.xml o *cds\_server.xml*. Potrebbe essere necessario modificare il nome del modulo di accesso Kerberos in modo che corrisponda al server delle applicazioni JRE.

Come minimo, è necessario fornire almeno una configurazione JAAS per JGSSServer con i seguenti parametri:

- **JGSSServer** obbligatorio
- **KerberosLocalUser** opzionale
- **JDBC\_DRIVER\_01** opzionale

1. Per Sun JRE, viene creata la seguente configurazione JGSSServer predefinita:

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

2. La configurazione **KerberosLocalUser** facoltativa è utilizzata per consentire di ignorare NTLM. Questa configurazione consente all'utente di creare credenziali Kerberos quando un browser client invia un token NTLM (invece di un token Kerberos) durante una sfida Negotiate. Si precisa che nei sistemi

Windows, i browser del computer su cui è installato IBM SPSS Collaboration and Deployment Services, invieranno sempre token NTLM. L'invio di richieste NTLM a IBM SPSS Collaboration and Deployment Services può essere disattivato omettendo questa configurazione dal relativo file di configurazione JAAS.

Per JRE IBM:

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

Per JRE Sun:

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

3. La configurazione JDBC\_DRIVER\_01 opzionale viene utilizzata sui server di database per l'autenticazione Kerberos.

Per JRE IBM:

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

Per JRE Sun:

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

4. È altresì possibile specificare l'appropriato nome classe, tipo requisito e altre opzioni richieste dal modulo di accesso per ogni configurazione JAAS. La classe del modulo di accesso deve essere nel percorso della classe. Per ulteriori informazioni, consultare la documentazione del produttore del server delle applicazioni JRE.

## WebLogic

Se si sta eseguendo WebLogic 12c utilizzando JDK7, sono necessarie ulteriori operazioni di configurazione.

1. Creare un file di configurazione JAAS, jaas.conf, sulla macchina server. Il contenuto deve essere simile a quello riportato di seguito:

```
JGSSServer {
 com.sun.security.auth.module.Krb5LoginModule required
 useKeyTab=true
 storeKey=true
 keyTab="C:/sso/winwlprin.keytab"
 principal="HTTP/winwlsrv.mysso.com@MYSSO.COM"
 debug=true;
};
```

2. Modificare il file C:\Oracle12c\Middleware\Oracle\_Home\user\_projects\domains\C60B246\bin\setDomainEnv.cmd in modo da includere la seguente proprietà Java, sostituendo <conf\_path> con il percorso del proprio file di configurazione:

```
-Djava.security.auth.login.config="<conf_path>/jaas.conf"
```

3. Quando viene configurato SSO (single sign-on) in IBM SPSS Deployment Manager, specificare parametro URL tabella chiavi:

```
C:/sso/winwlprin.keytab
```

**Nota:** Se vengono rilevati errori Kerberos nella configurazione, verificare che il server delle applicazioni utilizzi un JRE recente.

---

## Aggiornamento del registro di sistema Windows con il single sign-on

Affinché SSO funzioni correttamente, il TGT (Ticket-Granting Ticket) Kerberos deve includere la chiave di sessione. Per consentire questa inclusione, il registro Windows deve essere aggiornato. Per ulteriori informazioni, consultare <http://support.microsoft.com/kb/308339>.

Il supporto di installazione di IBM SPSS Collaboration and Deployment Services contiene i file di aggiornamento del registro di sistema per la configurazione dei sistemi Windows XP SP2, Windows Vista e Windows 2003 per il single sign-on basato su Kerberos. È possibile trovare i file nella directory /Documentation/Utility\_Files/Windows/registry del package della documentazione (scaricato da IBM Passport Advantage). I file sono i seguenti:

- /Server/Kerberos/Win2003\_Kerberos.reg
- /Server/Kerberos/WinXPSP2\_Kerberos.reg

Per i sistemi Windows Vista e successivi, utilizzare il file Win2003\_Kerberos.reg.

I file del registro di sistema consentono all'amministratore di sistema di inserire modifiche nel registro di tutti i sistemi in rete dotati di accesso single sign-on al repository.

---

## Configurazione di relazioni attendibili unidirezionali

È possibile configurare il proprio ambiente per l'autenticazione realm per il controllo dell'accesso utente.

Ad esempio, si supponga di avere due domini, AppDomain e UserDomain. I due domini hanno una relazione attendibile unidirezionale, con AppDomain configurato per l'attendibilità in uscita e UserDomain configurato per l'attendibilità in entrata. È possibile installare il server IBM SPSS Collaboration and Deployment Services nel dominio AppDomain e IBM SPSS Deployment Manager nel dominio UserDomain.

Per configurare IBM SPSS Collaboration and Deployment Services per un'attendibilità unidirezionale, è necessario modificare sia il server IBM SPSS Collaboration and Deployment Services sia IBM SPSS Deployment Manager.

## Configurazione del server IBM SPSS Collaboration and Deployment Services

1. Arrestare il server IBM SPSS Collaboration and Deployment Services.
2. Creare un file di configurazione Kerberos krb5.conf valido sul file system del server. Il file deve avere un contenuto simile alle seguenti righe, con i domini sostituiti da valori corrispondenti al proprio sistema:

```
[libdefaults]
default_realm = APPDOMAIN.COM

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

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

3. Impostare la proprietà di sistema Java java.security.krb5.conf sull'ubicazione del file krb5.conf. Ad esempio:

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

Consultare la documentazione del proprio server delle applicazioni per istruzioni sull'impostazione delle proprietà di sistema Java.

4. Avviare il server IBM SPSS Collaboration and Deployment Services.

## Configurazione di IBM SPSS Deployment Manager

1. Chiudere IBM SPSS Deployment Manager.
2. Creare un file di configurazione Kerberos krb5.ini valido nella cartella di installazione Windows, come c:\windows\krb5.ini. Il file deve avere un contenuto valido per l'autenticazione realm simile alle seguenti righe, con i domini sostituiti dai valori corrispondenti al proprio sistema:

```
[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. Avviare IBM SPSS Deployment Manager.

---

## Configurazione di Server Process Credential

Server Process Credential è la definizione integrata delle credenziali del profilo utente secondo cui viene eseguito il server del repository server. Nell'ambiente single sign-on di Active Directory o OpenLDAP, è possibile utilizzare Server Process Credential al posto delle regolari credenziali utente per repository per:

- Eseguire le fasi di lavoro di creazione report e pianificare lavori a tempo
- Inviare query al provider di sicurezza per ottenere l'elenco dei profili di utenti e gruppi

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>
```

## Configurazione dell'accesso utente di livello intermedio su WebLogic

Aggiungere la seguente politica dell'applicazione al file di configurazione accesso JAAS (*jaas.conf*).

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

Qualora il file non fosse presente, crearlo e definirlo come argomento di avvio `-Djava.security.auth.login.config` del server di WebLogic.

## 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.

**Nota:** 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.

---

## Configurazione dei browser per il single sign-on

Per abilitare single sign-on per IBM SPSS Collaboration and Deployment Services Deployment Portal e altri thin client di IBM SPSS Collaboration and Deployment Services, è necessario configurare il browser web per supportare il protocollo SPNEGO (Simple and Protected GSS-API Negotiation).

### Microsoft Internet Explorer

Per informazioni su come configurare il supporto di SPNEGO in Microsoft Internet Explorer, consultare la pagina <http://msdn.microsoft.com/en-us/library/ms995329.aspx>.

### Mozilla Firefox

Per impostazione predefinita, il supporto di SPNEGO è disattivato in Firefox. Per attivarlo:

1. Recarsi all'URL *about:config* (editor del file di configurazione di Firefox).
2. Modificare i seguenti valori delle preferenze:
  - **network.negotiate-auth.allow-non-fqdn** = false
  - **network.negotiate-auth.allow-proxies** = true
  - **network.negotiate-auth.delegation-uris** = Includere il nome dominio Intranet locale come *.your-domain.com*, in cui il periodo iniziale rappresenta un carattere jolly.
  - **network.negotiate-auth.trusted-uris** = Includere il nome dominio Intranet locale come *.your-domain.com*, in cui il periodo iniziale rappresenta un carattere jolly.
  - **network.negotiate-auth.using-native-gsslib** = true

### Google Chrome

Il supporto SPNEGO per Chrome è disabilitato per impostazione predefinita. Per abilitarlo, è necessario includere il nome server IBM SPSS Collaboration and Deployment Services in una whitelist:

- Per Windows, definire la politica del gruppo `AuthNegotiateDelegateWhitelist` Per ulteriori informazioni, consultare [Chrome Policy List, Issue 472145](#) e [Issue 469171](#).

In quanto membro della whitelist, il server IBM SPSS Collaboration and Deployment Services viene trattato come una destinazione attendibile per l'inoltro del ticket Kerberos.

### Safari

Single sign-on non è supportato da Safari.

---

## Ticket che è possibile inoltrare e IBM SPSS Deployment Manager

Sebbene non sia necessario si potrebbe utilizzare lo strumento **kinit.exe** di JDK per ottenere e memorizzare nella cache TGT (Ticket-Granting Ticket) Kerberos. Ad esempio, dalla directory `jre\bin` di installazione IBM SPSS Deployment Manager si può immettere il seguente comando:

```
kinit.exe -f
```

L'opzione `-f` crea un ticket che è possibile inoltrare. Questo comando crea un file di cache nella directory `Windows user` in cui JVM ricerca automaticamente una cache.

Se si è immesso questo comando utilizzando IBM JDK 7 precedente rispetto a `170_SR8`, può essere necessario modificare il file `krb5.ini` per accedere a questa cache correttamente.

1. Aprire il file `krb5.ini` in un editor di testo. Questo file è spesso ubicato nella directory `C:\Windows`
2. Nella sezione **[libdefaults]**: aggiungere la seguente impostazione:  
`forwardable = true`

3. Salvare il file aggiornato.

Questa modifica è necessaria solo per il client. Nessuna corrispondente modifica è necessaria per il server IBM SPSS Collaboration and Deployment Services Repository.



---

## Capitolo 7. Root di contesto dell'applicazione

La root di contesto di un'applicazione definisce il percorso di accesso al modulo. La root di contesto fa parte dell'URL utilizzato per connettersi all'applicazione.

Il riferimento a un URL di un'applicazione IBM SPSS Collaboration and Deployment Services include i seguenti elementi:

### **prefisso URL**

È costituito da protocollo, nome server o indirizzo IP e numero porta

### **Root di contesto**

Definisce il percorso di accesso all'applicazione. Per impostazione predefinita, la root di contesto corrisponde alla root del server in sé, indicato da una singola barra.

### **Root dell'applicazione**

Specifica la root dell'applicazione in sé

Ad esempio, quando il server del repository viene eseguito localmente sulla porta 8080, l'URL di IBM SPSS Collaboration and Deployment Services Deployment Portal è:

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

Il prefisso dell'URL è `http://localhost:8080` e la root di contesto corrisponde alla root del server delle applicazioni. La root dell'applicazione corrisponde a `peb`.

Nulla nell'URL identifica il modulo Web come facente parte di IBM SPSS Collaboration and Deployment Services. Se si aggiungono altre applicazioni al server, la gestione dei vari moduli presenti nella root del server diventa sempre più difficile.

Se si configura il server del repository con una root di contesto, è possibile isolare i componenti di IBM SPSS Collaboration and Deployment Services dalle altre applicazioni. Ad esempio, è possibile definire una root di contesto `ibm/spss` per i moduli di IBM SPSS Collaboration and Deployment Services. In questo caso, l'URL per l'interfaccia di IBM SPSS Collaboration and Deployment Services Deployment Portal è:

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

**Importante:** Utilizzando una root di contesto per il repository del server, tutte le applicazioni sul client devono contenere la medesima root di contesto nel collegarsi al server. L'URL di una qualsiasi applicazione in esecuzione nell'ambiente IBM SPSS Collaboration and Deployment Services, ad esempio IBM Analytical Decision Management, deve essere aggiornato conseguentemente.

---

## 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.
  - "Aggiornamento delle root di contesto di WebSphere" a pagina 54
  - "Aggiornamento delle root di contesto di JBoss" a pagina 55
  - "Aggiornamento delle root di contesto di WebLogic" a pagina 55

## 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.

## Aggiunta di una root di contesto al prefisso URL

Se il sistema utilizza un prefisso URL personalizzato per accedere a IBM SPSS Collaboration and Deployment Services Repository, aggiungere la root di contesto alla specifica del prefisso URL.

### Prima di iniziare

- Le credenziali di login devono essere associate all'azione di Configurazione.
- L'utilizzo dell'impostazione Prefisso URL deve essere abilitato mediante il IBM SPSS Deployment Manager basato sul browser.

### Procedura

1. Accedere a IBM SPSS Deployment Manager basato su browser.
2. Nel pannello **Configurazione**, fare clic sull'opzione **Prefisso URL** nel gruppo **Installazione**.
3. Aggiungere la root di contesto alla definizione del **Prefisso URL**. Ad esempio, se il prefisso URL è `http://mioserver:8080` e si desidera utilizzare come root di contesto `ibm/spss`, impostare il nuovo valore su `http://mioserver:8080/ibm/spss`.

**Limitazione:** Non terminare la specifica URL con una barra. Ad esempio, specificare un valore `http://myserver:8080/myroot` anziché `http://myserver:8080/myroot/`.

4. Riavviare il server delle applicazioni.

## Operazioni successive

Aggiornare la root di contesto di ciascuna applicazione. La procedura dipende dal server delle applicazioni.

## Aggiornamento delle root di contesto di WebSphere

Modificare il percorso di accesso alle applicazioni distribuite su WebSphere utilizzando la console di gestione.

### Prima di iniziare

“Aggiunta di una root di contesto al prefisso URL”

### Procedura

1. Accedere alla console di WebSphere.
2. Accedere all'applicazione IBM SPSS Collaboration and Deployment Services.
3. Aggiornare le impostazioni di **Root di contesto per moduli Web** con il valore di root. Se sul sistema è stato abilitato il prefisso URL, il valore di root per ciascun modulo deve corrispondere al valore aggiunto nel campo Prefisso URL. La root dell'applicazione deve restare invariata. Ad esempio: `/IBM/SPSS/CDS/admin`
4. Riavviare i nodi di WebSphere in cui è stato distribuito IBM SPSS Collaboration and Deployment Services

## Aggiornamento delle root di contesto di JBoss

Modificare il percorso di accesso alle applicazioni distribuite su JBoss, aggiornando i file EAR contenenti la definizione dello stesso.

### Prima di iniziare

“Aggiunta di una root di contesto al prefisso URL” a pagina 54

### Procedura

1. Eseguire una copia di backup del file cds80.ear nella directory toDeploy/timestamp dell'installazione JBoss.
2. Con un programma di utilità per archivi, modificare il file META-INF/application.xml nel file EAR originale. Aggiungere il valore della nuova root di contesto come prefisso in ciascun elemento context-root della root dell'applicazione. È necessario che il valore aggiunto sia il medesimo per ciascun elemento context-root.
3. Copiare il file EAR contenente l'aggiornamento, nel file application.xml nella directory deploy del server delle applicazioni.
4. Riavviare il server delle applicazioni.

### Esempio

Si supponga che il file application.xml contenga le seguenti specifiche:

```
<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>
```

Per aggiungere la root di contesto ibm/spss, aggiornare le definizioni di context-root con i seguenti valori:

```
<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>
```

## Aggiornamento delle root di contesto di WebLogic

Modificare il percorso di accesso alle applicazioni distribuite su WebLogic, aggiornando i file EAR contenenti la definizione dello stesso.

### Prima di iniziare

“Aggiunta di una root di contesto al prefisso URL” a pagina 54

## Procedura

1. Eseguire una copia di backup del file `cds80.ear` nella directory `toDeploy/current` dell'installazione WebLogic.
2. Con un programma di utilità per archivi, modificare il file `META-INF/application.xml` nel file EAR originale. Aggiungere il valore della nuova root di contesto come prefisso in ciascun elemento `context-root` della root dell'applicazione. È necessario che il valore aggiunto sia il medesimo per ciascun elemento `context-root`.
3. Utilizzare la console WebLogic per ridistribuire il file EAR contenente l'aggiornamento nel file `application.xml`.
4. Riavviare il server delle applicazioni.

## Capitolo 8. Conformità FIPS 140-2

La pubblicazione 140-2 del Federal Information Processing Standard (FIPS PUB 140-2) è uno standard di sicurezza informatica del governo statunitense utilizzato per accreditare i moduli di crittografia. Il documento specifica i requisiti dei moduli di crittografia, che includono i componenti software e hardware, corrispondenti a quattro diversi gradi di sicurezza obbligatori per le organizzazioni che trattano con il governo degli Stati Uniti. IBM SPSS Collaboration and Deployment Services può essere configurato per offrire il livello di sicurezza 1 (Security Level 1), secondo quanto specificato da FIPS 140-2.

La configurazione della sicurezza per la conformità a FIPS 140-2 deve uniformarsi alle seguenti direttive:

- Le comunicazioni tra le applicazioni del repository e del client devono utilizzare SSL per la sicurezza del livello di trasporto dei trasferimenti generali di dati. Ulteriore crittografia AES viene fornita per le password di credenziali utilizzando una chiave condivisa archiviata nel codice dell'applicazione. Per ulteriori informazioni, consultare la sezione Capitolo 9, "Utilizzo di SSL per proteggere il trasferimento di dati", a pagina 59.
- Il server del repository utilizza l'algoritmo AES con la chiave archiviata nel keystore del file system del server per crittografare le password nei file di configurazione, nei file di configurazione del server delle applicazioni, nei file di configurazione del provider di sicurezza e così via.
- Le comunicazioni tra il server del repository e il server del database possono, facoltativamente, utilizzare SSL per la sicurezza del livello di trasporto dei trasferimenti generali di dati. La crittografia AES viene fornita per le password di credenziali, le password di configurazione, le password delle preferenze utente, e così via, utilizzando una chiave condivisa archiviata in un keystore nel file system del server del database.

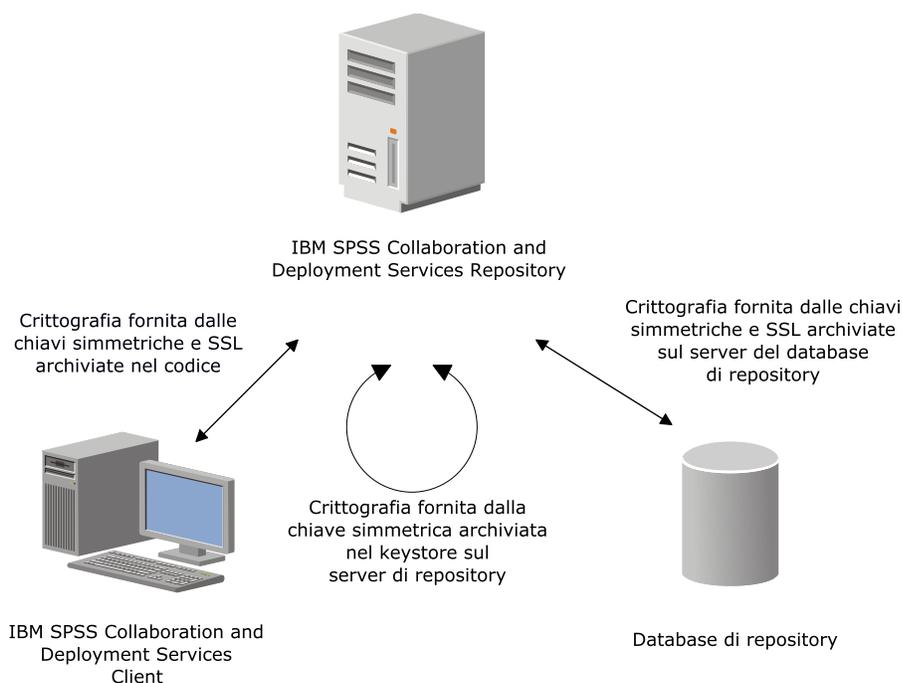


Figura 4. Configurazione della sicurezza di IBM SPSS Collaboration and Deployment Services conforme FIPS 140-2

---

## Configurazione del repository

Nel configurare il repository per la conformità a FIPS 140-2 è necessario attenersi alle seguenti indicazioni:

- Impostare il database in modo che accetti comunicazioni SSL; configurare anche il modulo di crittografia JCE.
- Se il repository viene installato su UNIX, il JRE predefinito deve essere configurato con un modulo JCE.
- Anche il JRE del server delle applicazioni deve essere configurato utilizzando un modulo JCE.
- Impostare il server delle applicazioni in modo che accetti comunicazioni SSL; configurare anche il modulo di crittografia JCE.
- Se il repository viene installato su Windows, nella schermata di configurazione uscire dall'installazione, configurare un modulo JCE e riavviare la configurazione, selezionando nell'opportuna schermata l'esecuzione in modalità conforme a FIPS 140-2.
- Se il repository viene distribuito in un ambiente cluster, replicare il keystore su tutti i nodi del cluster.
- Gli JRE utilizzati dalle applicazioni di IBM Corp. Server che interagiscono con IBM SPSS Collaboration and Deployment Services, quali IBM SPSS Statistics Server e IBM SPSS Modeler Server, devono tutti essere dotati di certificati SSL.

---

## Configurazione del client desktop

Per eseguire le applicazioni client desktop IBM SPSS Collaboration and Deployment Services, quali IBM SPSS Deployment Manager, è necessario abilitare l'utilizzo del JRE sul modulo di crittografia JCE. Il JRE richiede l'installazione dei certificati SSL.

---

## Configurazione del browser

- Modificandone le opzioni, è possibile configurare Mozilla Firefox per eseguirlo in modalità conforme a FIPS 140-2. Per ulteriori informazioni, consultare .
- Per configurare Internet Explorer è necessaria abilitare la crittografia Windows e modificare le impostazioni del. Per ulteriori informazioni, consultare .
- Apple Safari non può essere utilizzato in modalità conforme a FIPS 140-2.

---

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

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

---

### Come funziona il protocollo SSL

SSL si basa sulle chiavi pubbliche e private del server, nonché su un certificato di chiave pubblica che vincola l'identità del server alla relativa chiave pubblica.

1. Nel connettersi a un server, il client lo autentica utilizzando il certificato di chiave pubblica.
2. Il client quindi genera un numero random, lo crittografa con la chiave pubblica del server, ritrasmettendolo al server.
3. Il server decrittografa il numero random e la propria chiave privata.
4. Dal numero random, sia il server che il client generano le chiavi di sessione utilizzate per crittografare e decrittografare le informazioni trasmesse successivamente.

Il certificato di chiave pubblica di norma viene firmato da un'autorità di certificazione. Le autorità di certificazione, quali VeriSign e Thawte, sono organizzazioni che emettono, autenticano e gestiscono le credenziali di sicurezza contenute nei certificati di chiave pubblica. In sostanza, è l'autorità di certificazione a confermare l'identità del server. Di solito l'autorità di certificazione applica una tariffa a un certificato, ma è possibile generare anche certificati autofirmati.

---

### Protezione delle comunicazioni client-server e server-server con SSL

Le fasi principali per garantire la protezione delle comunicazioni client-server e server-server con SSL sono:

1. Ottenere e installare il certificato e le chiavi SSL.
2. Se si utilizza certificati di crittografia con resistenza superiore a 2048 bit, installare crittografia con forza illimitata sul computer client Deployment Manager. Per ulteriori informazioni, consultare "Installazione della crittografia "Unlimited Strength""
3. Aggiungere il certificato al keystore sul client.
4. Informare gli utenti finali che è necessario abilitare SSL quando ci si connette al server.

**Nota:** A volte un prodotto server può agire da client. Ad esempio, il server di IBM SPSS Statistics che si collega a IBM SPSS Collaboration and Deployment Services Repository. In questo caso, il server di IBM SPSS Statistics rappresenta il *client*.

### Installazione della crittografia "Unlimited Strength"

Nel Java Runtime Environment, a corredo del prodotto, è stata abilitata la crittografia minima per esportazione degli Stati Uniti. Per ottimizzare la protezione dei dati, si consiglia di aggiornare alla crittografia "Unlimited Strength".

#### IBM J9

1. Scaricare i file JCE (Java Cryptography Extension) Unlimited Strength Jurisdiction Policy relativi alla propria versione SDK dal sito web IBM.com.

2. Estrarre i file di Unlimited Jurisdiction Policy contenuti nel file compresso. Il file compresso contiene un file `US_export_policy.jar` ed un file `local_policy.jar`. Nell'installazione di WebSphere Application Server, selezionare la directory `$JAVA_HOME/jre/lib/security` ed eseguire il back up dei file `US_export_policy.jar` e `local_policy.jar`.
3. Sostituire le copie esistenti dei file `US_export_policy.jar` e `local_policy.jar` con i due file scaricati ed estratti.

**Nota:** E' necessario installare anche il file `*.jar` sulla cartella `<DeploymentManager_Client_Install>/jre/lib/security`.

4. Nella console di gestione di WebSphere Application Server, abilitare la protezione. Verificare innanzitutto che tutti gli agenti del nodo all'interno della cella siano attivi. Per ulteriori informazioni, consultare la documentazione WebSphere. Si ribadisce che è necessario selezionare la definizione dell'area di autenticazione dall'elenco contenuto in **Sicurezza e amministrazione, applicazioni e infrastrutture protette** e fare clic su **Imposta come corrente** per abilitare la protezione al riavvio del server.
5. Eseguire il logoff dalla console di gestione.
6. Interrompere il server.
7. Riavviare il server.

## Sun Java

1. Scaricare i file JCE (Java Cryptography Extension) Unlimited Strength Jurisdiction Policy relativi alla propria versione SDK dal sito web Sun Java.
2. Estrarre il file scaricato.
3. Copiare i due file `.jar`, `local_policy.jar` e `US_export_policy.jar`, in `<installation folder>/jre/lib/security`, dove `<installation folder>` è la cartella di installazione del prodotto.

## Aggiunta del certificato al keystore sul client (per le connessioni al repository di )

**Nota:** Ignorare questo passaggio se si utilizza un certificato firmato da un'autorità di certificazione.

Se si utilizza SSL per collegarsi a un repository IBM SPSS Collaboration and Deployment Services mediante certificati autofirmati, è necessario aggiungere il certificato al keystore Java del client. Completare la seguente procedura sul computer *client*.

1. Aprire il prompt dei comandi e ridefinire il percorso della directory con quanto segue e in cui `<dir installazione prodotto>` rappresenta la directory in cui è stato installato il prodotto:  
`<dir installazione prodotto>/jre/bin`
2. Inserire il seguente comando:  
`keytool -import -alias <nome alias> -file <percorso a cert> -keystore <percorso a keystore>`  
dove `<nome alias>` è un nome alias arbitrario attribuito al certificato, `<percorso a cert>` rappresenta il percorso completo del certificato e `<percorso a keystore>` rappresenta il percorso completo al keystore Java, che potrebbe essere `<dir installazione prodotto>/lib/security/jssecacerts` o `<dir installazione prodotto>/lib/security/cacerts`.
3. Quando richiesto, inserire la password del keystore, che per impostazione predefinita è `changeit`.
4. Quando richiesto, confermare l'attendibilità del certificato inserendo `yes`.

## Importazione del file certificato per connessioni client basate su browser

Quando ci si connette a IBM SPSS Collaboration and Deployment Services Repository tramite SSL con un client basato su browser, ad esempio IBM SPSS Collaboration and Deployment Services Deployment

Portal, il browser potrebbe richiedere di accettare il certificato non attendibile senza firma oppure visualizza un messaggio per indicare che il sito non è sicuro e fornisce un collegamento per l'importazione del certificato nel truststore del browser. Questo processo è diverso per browser differenti e potrebbe essere diverso a seconda della configurazione del browser. È possibile inoltre installare manualmente il certificato nel truststore del browser.

## Istruzione agli utenti per l'abilitazione di SSL

Quando gli utenti si connettono al server tramite un prodotto client, devono abilitare SSL nella finestra di dialogo per connettersi al server. Informare gli utenti di selezionare l'opportuna casella di controllo.

---

## Configurazione del prefisso URL

Se IBM SPSS Collaboration and Deployment Services Repository è impostato per l'accesso SSL, il valore dell'impostazione di configurazione del Prefisso URL deve essere modificato come segue:

1. Utilizzando la console basata sul browser, accedere al repository.
2. Aprire l'opzione di configurazione del *Prefisso URL*.  
**Configurazione > Configurazione > Prefisso URL**
3. Impostare il valore del prefisso su `https` anziché `http` e il valore della porta sul numero della porta SSL. Ad esempio:

```
[default]
http://<nomehost>:<porta>
[abilitato SSL]
https://<nomehost>:<portaSSL>
```

---

## Protezione di LDAP mediante SSL

Lightweight Directory Access Protocol (LDAP) è uno standard Internet Engineering Task Force (IETF) per lo scambio di informazioni tra directory e database in rete contenenti informazioni di qualsiasi livello. Per i sistemi che richiedono un livello di sicurezza supplementare, provider LDAP, come Microsoft Active Directory, sono in grado di operare su connessioni SSL (Secure Socket Layer), a patto che il Web o il server delle applicazioni supporti LDAP con connessioni SSL. Abbinando SSL a LDAP può garantire che password di accesso, informazioni delle applicazioni e altri dati sensibili non vengano manomessi, compromessi o sottratti.

Il seguente esempio illustra come abilitare LDAPS utilizzando Active Directory di Microsoft come provider di sicurezza. Per informazioni più particolareggiare su qualsiasi fase della procedura oppure per approfondimenti su una versione specifica del provider di sicurezza, consultare la documentazione originale del produttore.

1. Verificare che Active Directory e Enterprise Certificate Authority siano installati e funzionanti.
2. Utilizzare l'autorità di certificazione per generare un certificato e importarlo nell'archivio certificati dell'installazione di IBM SPSS Deployment Manager. Così facendo è possibile stabilire una connessione LDAPS tra IBM SPSS Collaboration and Deployment Services Repository e un server Active Directory.

Per configurare IBM SPSS Deployment Manager per connessioni protette da Active Directory, verificare che esista una connessione al repository.

3. Avviare IBM SPSS Deployment Manager.
4. Dal menu **Strumenti** scegliere **Amministrazione server**.
5. Accedere a un server amministrato predefinito.
6. Fare doppio clic sull'icona **Configurazione** del server per espandere la gerarchia.
7. Fare doppio clic sull'icona **Provider di sicurezza** per espandere la gerarchia.
8. Fare doppio clic sul provider di sicurezza Active Directory.
9. Immettere i valori di configurazione per l'istanza di Active Directory dotata dei certificati di sicurezza.

10. Selezionare la casella di controllo **Utilizza SSL**.
11. Annotare il nome nel campo Utente dominio. Da questo momento in poi, tutti gli accessi mediati da Active Directory verranno autenticati da SSL.

Per ulteriori informazioni su installazione, configurazione e implementazione di LDAPS su server delle applicazioni specifici, consultare la documentazione originale del produttore.

---

## Capitolo 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 installazione repository>/platform/log4j.properties
- **JBoss:** <directory server JBoss>/deploy/jboss-logging.xml
- **WebLogic:** <directory installazione repository>/toDeploy/current/log4j.properties

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:

Tabella 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/*
- **WebLogic:** *<directory dominio WebLogic>/servers/<nome server>/logs/*

---

## Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti. Questo materiale potrebbe essere disponibile da IBM in altre lingue. Tuttavia, all'utente potrebbe essere richiesto di possedere una copia del prodotto o una versione del prodotto in tale lingua per accedervi.

È possibile che IBM non offra in altri paesi i prodotti, i servizi o le funzioni illustrati in questa documentazione. Consultare il proprio rappresentante locale IBM per informazioni sui prodotti ed i servizi attualmente disponibili nella propria zona. Ogni riferimento a prodotti, programmi o servizi IBM non implica che possano essere utilizzati solo quei prodotti, programmi o servizi IBM. In sostituzione a quelli forniti da IBM, è possibile utilizzare prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti IBM. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM potrebbe avere brevetti o domande di brevetti in corso relativi agli argomenti discussi nella presente pubblicazione. La fornitura del presente documento non concede alcuna licenza a tali brevetti. Chi desiderasse ricevere informazioni relative alle licenze può rivolgersi per iscritto a:

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

Per richieste di licenze relative ad informazioni double-byte (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA", SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, MA NON LIMITATE A, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIALIZZABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcune giurisdizioni non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi la presente dichiarazione potrebbe non essere a voi applicabile.

Queste informazioni potrebbero includere imprecisioni tecniche o errori tipografici. Le informazioni incluse al suo interno vengono modificate su base periodica e tali modifiche verranno inserite nelle nuove edizioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nella presente pubblicazione in qualsiasi momento e senza alcun preavviso.

Tutti i riferimenti a siti web non-IBM sono forniti unicamente a scopo di consultazione e non devono essere in alcun modo considerati come complementari a tali siti web. I materiali disponibili sui siti web non fanno parte di questo prodotto IBM e l'utilizzo di questi è a discrezione dell'utente.

IBM può utilizzare o distribuire qualsiasi informazione fornita dall'utente nel modo che ritenga più idoneo senza incorrere in alcun obbligo nei confronti dell'utente stesso.

Coloro che detengono la licenza su questo programma e che desiderano ricevere informazioni su di essa allo scopo di consentire: (i) uno scambio di informazioni tra programmi creati in modo indipendente e altri programmi (incluso questo) e (ii) l'utilizzo reciproco delle informazioni scambiate, devono contattare:

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

Tali informazioni possono essere disponibili, in base ad appropriate clausole e condizioni, includendo in alcuni casi, il pagamento di una tassa.

Il programma concesso in licenza e descritto nella presente documentazione e tutto il materiale su licenza ad esso relativo vengono forniti da IBM nel rispetto dei termini dell'IBM Customer Agreement, dell'IBM International Program License Agreement o di qualunque altro accordo equivalente tra le parti.

I dati di prestazione e gli esempi client citati vengono solo rappresentati per fini illustrativi. I risultati di prestazione reali possono variare a seconda delle configurazioni specifiche e delle condizioni di operazione.

Le informazioni relative a prodotti non-IBM sono ottenute dai fornitori di quei prodotti, dagli annunci pubblicati o da altre fonti disponibili al pubblico. IBM non ha eseguito test dei prodotti e non può confermare l'accuratezza della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non-IBM products. Eventuali commenti relativi alle prestazioni dei prodotti non-IBM devono essere indirizzati ai fornitori di tali prodotti.

Le dichiarazioni concernenti le strategie e le intenzioni future di IBM sono soggette a modifiche o a ritiro senza preavviso, inoltre sono limitate alla rappresentazione esclusiva di scopi e obiettivi.

Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con persone reali o aziende business è puramente casuale. *no actual people or business enterprises is entirely coincidental.*

#### LICENZA DI COPYRIGHT:

Queste informazioni contengono esempi di programmi applicativi in lingua originale che illustrano le tecniche di programmazione su diverse piattaforme operative. Il licenziatario può copiare, modificare e distribuire tali programmi di esempio, in qualsiasi formato, senza versare alcun pagamento a IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (application programming interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. La IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi. Questi programmi di esempio vengono fornite "nello stato in cui si trovano" senza garanzie di alcun tipo. IBM declina ogni responsabilità per eventuali danni derivanti dall'uso degli stessi.

---

## **Considerazioni sulla politica della privacy**

I prodotti software IBM incluso le soluzioni Software-as-a service, ("Offerte Software") possono utilizzare cookie o altre tecnologie per raccogliere informazioni sull'utilizzo del prodotto, per consentire di migliorare l'esperienza dell'utente finale, per personalizzare le interazioni con l'utente finale o per altri scopi. In molti casi le offerte software non raccolgono informazioni che consentono l'identificazione personale. Alcune delle Offerte Software possono abilitare la raccolta di informazioni che consentono

l'identificazione personale. Se questa Offerta software utilizza cookie per raccogliere informazioni che consentono l'identificazione personale, di seguito sono riportate le informazioni specifiche sull'uso dei cookie di questa offerta.

Questa Offerta Software non utilizza cookie o altre tecnologie per raccogliere informazioni che consentono l'identificazione personale.

Se le configurazioni distribuite per questa Offerta Software forniscono al cliente la possibilità di raccogliere informazioni che consentono l'identificazione personale da utenti finali tramite cookie e altre tecnologie, è necessario richiedere un parere legale sulle leggi applicabili in materia di raccolta di dati, incluso i requisiti di avviso e consenso.

Per ulteriori informazioni sull'uso a tale scopo di diverse tecnologie, incluso i cookie fare riferimento alla Politica della privacy IBM all'indirizzo <http://www.ibm.com/privacy> e alla dichiarazione sulla privacy online IBM all'indirizzo <http://www.ibm.com/privacy/details> la sezione "Cookies, Web Beacons and Other Technologies" e alla sezione "IBM Software Products and Software-as-a-Service Privacy Statement" all'indirizzo <http://www.ibm.com/software/info/product-privacy>.

---

## Marchi

IBM, il logo IBM e [ibm.com](http://www.ibm.com) sono marchi commerciali o marchi registrati di International Business Machines Corp., in numerose giurisdizioni di tutto il mondo. Altri nomi di prodotti e servizi possono essere marchi commerciali di IBM o di altre aziende. Un elenco aggiornato di marchi IBM è disponibile sul web in "Copyright and trademark information" su [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, il logo Adobe, PostScript e il logo PostScript sono sia marchi registrati o marchi di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Intel, il logo Intel, Intel Inside, il logo Intel Inside, Intel Centrino, il logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium e Pentium sono marchi o marchi registrati di Intel Corporation o relative controllate negli Stati Uniti e altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e/o in altri paesi.

Microsoft, Windows, Windows NT e il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Java e tutti i marchi e i loghi basati su Java sono marchi o marchi registrati di Oracle e/o delle sue affiliate.

Altri nomi di prodotti e servizi possono essere marchi commerciali di IBM o di altre aziende.



---

## Indice analitico

### A

accesso 50  
accesso utente di livello intermedio 48  
Active Directory 41, 43  
AES 57, 58  
affinità di sessione 28  
aggiornamenti del client 39  
aggiornamenti del repository 39  
aggiornamenti del server 39  
aggiunta di nodi al cluster 29  
applicazioni  
    versioni supportate 33  
applicazioni supportate 33  
archivio messaggi JMS 16  
attendibilità unidirezionale  
    configurazione 47  
autenticazione 41  
autorizzazioni 11, 15  
autorizzazioni del database 15

### B

bilanciamento del carico  
    basato su hardware 25, 28  
    basato su software 25, 28  
browser 60  
    single sign-on 50  
Bus di integrazione sistema 16

### C

cache dei ticket Kerberos 48  
calcolo del punteggio 6  
certificati 58  
certificato  
    importazione 60  
Chrome  
    single sign-on 50  
Citrix Presentation Server 11  
clipackagemanager.bat 39  
clipackagemanager.sh 39  
cluster  
    espansione 29  
    WebLogic 29  
    WebSphere 29  
clustering 25, 26, 27, 28  
clustering di server 25, 26, 27, 28  
clustering di server delle  
    applicazioni 25, 26, 27, 28  
collaborazione 1  
componenti opzionali 39  
condivisione su Windows 26, 27  
configurare  
    database Oracle 18  
    DB2 16  
    MS SQL Server 17  
configurazione  
    database del repository 20  
    distribuzione automatica 20  
    distribuzione manuale 20

configurazione (*Continua*)  
    non presidiata 20  
    server delle applicazioni 20  
confronto senza distinzione tra carattere  
    maiuscolo/minuscolo 17  
connettività del database 31  
controllo dipendenza 39  
controllo versione 39  
credenziali 36, 37  
crittografia 36, 37, 57, 58  
    SSL 59  
crittografia simmetrica 57, 58

### D

database  
    requisiti 15  
database Oracle  
    configurazione 18  
DB2  
    configurazione 16  
DB2 for Linux, UNIX e Windows 15  
DB2 UDB 15  
directory di output 20  
disinstallazione 33  
distribuzione 2  
    automatica 20  
    manuale 20, 23  
distribuzione automatica 20  
distribuzione con script su un cluster  
    WebLogic 27  
distribuzione manuale 20  
    WebLogic 23  
    WebSphere 23

### E

encrypt.bat 31  
encrypt.sh 31  
espansione del cluster 29  
eventi del repository  
    registrazione 63  
eventi di gestione report  
    registrazione 63  
eventi di importazione/esportazione  
    registrazione 63  
eventi di lavoro  
    registrazione 63  
eventi di notifica  
    registrazione 63  
eventi di sicurezza  
    registrazione 63

### F

failover 25, 28  
failover JMS 27  
file di aggiornamento del registro di  
    sistema 47  
FIPS 140-2 57, 58

funzioni  
    rimosso 7

### G

Google Chrome  
    single sign-on 50

### I

IBM HTTP Server 28  
IBM Installation Manager 19, 33  
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 39  
IBM SPSS Collaboration and Deployment  
    Services Password Utility 31  
IBM SPSS Collaboration and Deployment  
    Services Repository 2, 3  
IBM SPSS Modeler Decision  
    Management 6  
IBM SPSS Modeler versione 33  
IBM SPSS Statistics versione 33  
importazione  
    certificato 60  
installazione 10, 19  
    package 39

### J

Java 12  
JBoss 12, 48  
    single sign-on 45  
JMS 37  
    WebLogic 38  
JRE (64 bit) 12  
Jython 23, 26

### K

Kerberos 47  
    dominio 41  
    Key Distribution Center 41  
    Ticket di servizio 41

### L

LDAP 61  
    protezione 61  
log 63  
log4j 63  
    configurazione 63

## M

- manuale 12
- manutenzione del database 18
- manutenzione del database del repository 18
- Microsoft Internet Explorer
  - single sign-on 50
- Microsoft SQL Server 15
  - configurazione 17
- migrazione
  - con una copia del database del repository 36
  - modelli di notifica 38
  - password 37
  - su un altro database 36
  - su un server diverso 35
  - su una versione successiva del repository 35
  - utilizzando un database del repository preesistente 36
- migrazione della password 36, 37
- migrazione modelli di notifica 38
- MIT Kerberos 42
- modulo JCE 26, 27, 57, 58
- Mozilla Firefox
  - single sign-on 50

## N

- Netezza 32
- non presidiata
  - configurazione 20
  - disinstallazione 33
  - IBM Installation Manager 19, 33
  - installazione 19
  - installazione del package 39

## O

- OpenLDAP 42
- Oracle 10g 15
- Oracle Database 15
- Oracle WebLogic 12

## P

- package
  - installazione 39
  - in modalità riga di comando 39
  - non presidiata 39
- password
  - crittografare 31
  - modifica 31
- peggiore delle prestazioni 11
- percorso condiviso 27
- preferenze utente 4
- prefisso URL 20, 28, 54, 61
- privilegi utente 11
- processo remoto
  - server di esecuzione 2, 5
- programma di utilità per password 31
- protezione
  - LDAP 61
  - SSL 59

## R

- requisiti 11
  - applicazione 33
  - database 15
  - server delle applicazioni 12
- ridondanza 25, 28
- riga di comando 39
- root di contesto 53
  - di JBoss 55
  - di WebLogic 55
  - di WebSphere 54
  - prefisso URL 54

## S

- Safari 50
- SAS
  - server di esecuzione 2, 5
- script di installazione 23
- Secure Sockets Layer 59
- server del punteggio distribuiti in remoto 5
- server delle applicazioni
  - requisiti 12
- server di calcolo del punteggio 5
- server di esecuzione 5
  - processo remoto 2, 5
  - SAS 2, 5
- server Kerberos 44
- Servizi terminal di Windows 11
- SIB 37
- single sign-on 41, 44
  - Active Directory 43
  - attendibilità unidirezionale 47
  - configurazione del server delle applicazioni 45
  - file di aggiornamento del registro di sistema 47
  - Google Chrome 50
  - JBoss 45
  - Microsoft Internet Explorer 50
  - MIT Kerberos 42
  - Mozilla Firefox 50
  - OpenLDAP 42
  - Server Kerberos con Windows 42
  - WebLogic 46
  - WebSphere 45
- SPNEGO 50
- SSL 57, 59
  - certificati 58
  - panoramica 59
  - protezione delle comunicazioni 59
- strumenti di registrazione 63

## T

- truststore del browser 60

## U

- UNC 26, 27

## V

- versioni
  - IBM SPSS Modeler 33
  - IBM SPSS Statistics 33
- virtualizzazione 11
- VMWare 11

## W

- WebLogic 25, 48
  - cluster 27
  - destinazione della migrazione 27
  - distribuzione con script 27
  - distribuzione manuale 27
  - JMS 27
  - single sign-on 46
- WebLogic Apache Plugin 25, 28
- WebSphere 12, 25, 28, 37, 48
  - cluster 26
  - distribuzione automatica 26
  - distribuzione manuale 26
  - single sign-on 45





Stampato in Italia