

*IBM SPSS Statistics Server - Guida
dell'amministratore*



Nota

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in [“Informazioni particolari” a pagina 59.](#)

Informazioni sul prodotto

Questa edizione si applica alla versione 30, release 0, modifica 0 di IBM® SPSS Statistiche Server e a tutte le release e modifiche successive se non diversamente indicato in nuove edizioni.

© **Copyright International Business Machines Corporation .**

Indice

Capitolo 1. Osservazioni generali.....	1
Prodotti e Sistemi operativi.....	1
Architettura.....	1
Componenti software.....	3
Utilizzo Modalità Distribuita.....	4
Gestione del software Server.....	4
Utilizzo di questo documento.....	5
Capitolo 2. Installazione.....	7
Installazione del Software Server.....	7
Installazione dell'Applicazione client.....	7
Capitolo 3. Accesso ai dati.....	9
Vista dei dati.....	9
Tecnologia di accesso ai dati.....	9
Connetti ODBC.....	9
Accesso ai dati.....	10
Dati di riferimento.....	10
Controllo dell'accesso ai dati.....	10
Origini dati.....	11
Configurazione dell'ambiente UNIX per l'accesso ai dati.....	11
Capitolo 4. Configurazione, monitoraggio utilizzo e manutenzione.....	13
Gestione di Fine - Account utente e file.....	13
Account.....	13
Accesso ai dati.....	13
File.....	13
Profili.....	14
Gruppi e profili utente di IBM SPSS Statistiche Server.....	14
Configurazione delle origini dati ODBC.....	14
ODBC Origini dati e IBM SPSS Data Access Pack.....	14
Utilizzo di un motore di ordinamento di Terze Parti.....	15
Amministrazione di IBM SPSS Statistiche Server.....	15
Configurazione di Xtensions.....	15
Configurazione dell'interfaccia di linea di comando della funzione di produzione per Submit Jobs.....	16
Configurazione Istanze Multiple.....	17
Avvio Controllo del servizio.....	18
Parametri Riga Comandi Script di avvio.....	19
Altra manutenzione.....	19
Avvio e arresto del Software Server.....	19
Per avviare il servizio o Daemon.....	20
Per arrestare il servizio o Daemon.....	20
Configurazione per il miglioramento delle prestazioni.....	20
Capitolo 5. Supporto agli utenti finali.....	21
Autenticazione.....	21
Configurazione dell'autenticazione a livello OS.....	21
Configurazione di PAM.....	21
Configurazione dell'autenticazione interna.....	22
Configurazione dell'autenticazione unix2.....	23

Configurazione di Single Sign - On (SSO).....	24
Autorizzazioni.....	29
Autorizzazioni - Permessioni di livello.....	29
Autorizzazione del gruppo.....	29
Profili.....	30
Versioni client e server.....	30
Connessione utenti tramite un Firewall.....	30
Configurazione delle connessioni tramite un firewall.....	31
Connessione utenti con PPTP.....	33
Utilizzo di SSL per il trasferimento sicuro dei dati.....	33
Come funziona il protocollo SSL.....	33
Abilitazione SSL tramite GSKit.....	33
Abilitazione SSL utilizzando OpenSSL	38
Impostazione di una Locale.....	40
Connessione al Software del server.....	42
Accesso ai dati e ai file.....	42
Salvataggio di dati e file.....	42
Capitolo 6. Analisi e miglioramento delle prestazioni.....	45
Acquisizione di informazioni sulle prestazioni.....	45
Miglioramento dell'utilizzo del disco.....	46
Miglioramento dell'utilizzo della CPU.....	47
Miglioramento dell'utilizzo della memoria.....	47
Miglioramento dell'utilizzo della rete.....	47
Utilizzo di IBM SPSS Statistiche Efficientemente.....	47
Appendice A. Risoluzione dei problemi.....	49
Server software.....	49
Software client.....	49
Appendice B. La funzione di batch IBM SPSS Statistiche.....	51
Cosa devi sapere.....	51
Appendice C. Attività del sistema operativo Windows.....	53
Proprietà file.....	53
Proprietà di sistema.....	53
Gestore utente.....	54
Pannello di controllo dei servizi.....	54
Gestore attività.....	54
Amministratore ODBC.....	54
Per configurare un DSN di sistema.....	55
Per configurare un DSN utente.....	55
Appendice D. Attività del sistema operativo UNIX.....	57
chmod.....	57
env.....	57
Script.....	57
ps e uccidere.....	57
odbc.ini.....	58
Informazioni particolari.....	59
Marchi.....	60
Indice analitico.....	63

Capitolo 1. Osservazioni generali

La tecnologia server IBM SPSS Statistiche è un' **architettura distribuita** accoppiata con le ottimizzazioni di gestione dei dati chiave, supporta l'analisi scalabile. La tecnologia è basata su client / server. Distribuisce le richieste client per le operazioni intensive di risorse a potenti software server. Quando il client e il server funzionano insieme così, viene indicato come **modalità di analisi distribuita**. L'analisi distribuita consente agli utenti finali di eseguire analisi che i loro computer desktop non possono supportare.

Per la massima flessibilità, le applicazioni client che utilizzano la tecnologia server possono anche essere configurate per funzionare esclusivamente sul computer desktop dell'utente finale - questo è indicato come **modalità di analisi locale**. Gli utenti finali possono facilmente commutare le modalità.

Prodotti e Sistemi operativi

La tecnologia server supporta l'applicazione client IBM SPSS Statistiche e il software server esegue su diversi sistemi operativi (vedi le istruzioni di installazione per le specifiche). È possibile installare più versioni di software server presso il proprio sito, sullo stesso computer server o su diversi computer server.

Architettura

Il software server dispone di un'architettura a due livelli, distribuita. Distribuisce le operazioni software tra il client e i computer server. Le operazioni intensive di memoria, come l'accesso ad un grande database o l'analisi di un file di dati di grandi dimensioni, vengono effettuate sul computer server senza scaricare i dati sul computer client.

Livello client

L'applicazione **client** . È installato e viene eseguito sul computer desktop dell'utente finale.

L'applicazione client fornisce l'interfaccia grafica utente all'accesso e all'analisi dei dati. Presenta i risultati delle analisi di fine utente.

Livello server

Il software **server** . Viene installato e eseguito su un computer server netlavorato. Il software server fornisce il framework necessario per gestire più client, gli algoritmi utilizzati nell'analisi statistica e l'accesso ai dati.

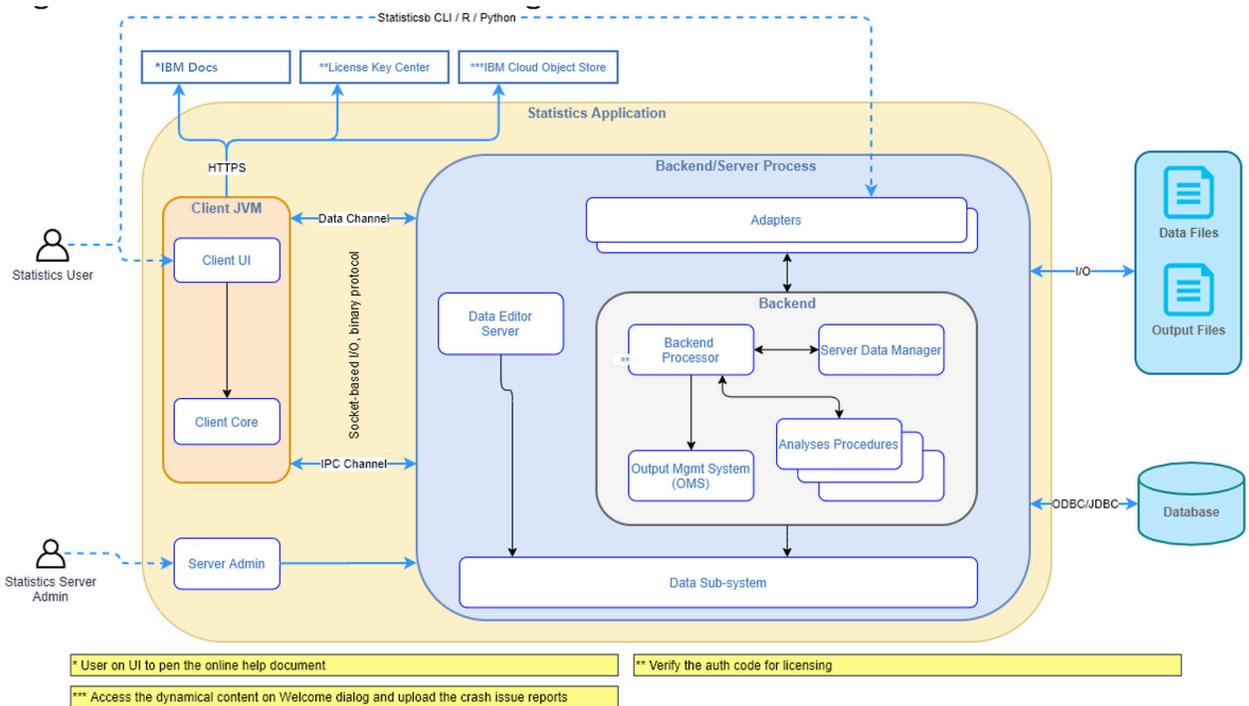
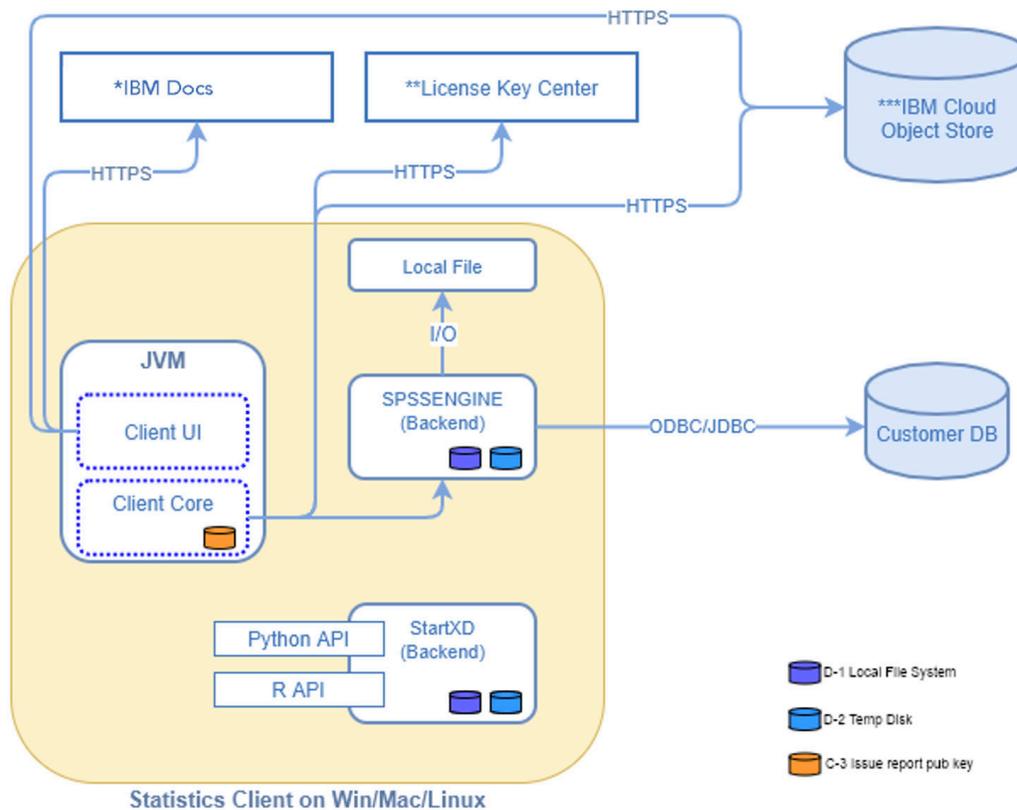


Figura 1. Modalità di analisi distribuita

Per le analisi che non richiedono l'accesso intensivo dei dati o l'elaborazione numerica, il software client può essere utilizzato come applicazione desktop standalone standard. Quando in modalità di analisi locale, tutti gli accessi ai dati e l'elaborazione statistica vengono gestiti sul computer desktop dell'utente finale.



* User on UI to pen the online help document

** Verify the auth code for licensing

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

Figura 2. Modalità di analisi locale

Componenti software

Come mostrato nella figura "Modalità di analisi distribuita", i componenti della tecnologia server sono i seguenti. (Consultare [Figura 1](#) a pagina 2.)

Software client. L'applicazione client è un'installazione completa del prodotto IBM Corp. dell'utente finale (ad esempio, IBM SPSS Statistiche). Quando viene utilizzato per l'analisi distribuita, vengono utilizzate solo l'interfaccia grafica utente e le funzionalità di modifica. Quando viene utilizzato per l'analisi locale, vengono utilizzati anche i relativi accessi ai dati e le capacità di elaborazione statistica.

Software Server. Il software server è costituito da componenti secondari: un framework che gestisce la comunicazione client / server, i processi client che gestiscono le richieste client e i moduli che accedono ai dati ed eseguono analisi.

- **Quadro.** Il framework del software server è un servizio (su Windows) o daemon (su UNIX). Gestisce tutta la comunicazione tra l'applicazione client e i moduli. Il framework viene eseguito continuamente sul computer server, in attesa delle connessioni client. Quando un client si connette, il framework lancia un processo che gestisce le richieste di quel client.
- **Processo client.** Un processo client è effettivamente una sessione per il client. Esiste un processo per ogni cliente. Un processo viene avviato quando il client si connette, e viene terminato quando il client si disconnette. Il processo gestisce le richieste dei suoi clienti per i dati e le analisi. Carica i moduli necessari per accedere e analizzare i dati. Scarica i moduli quando non sono più richiesti.
- **Moduli.** Un modulo è una libreria eseguibile, DLL o condivisa che accede ai dati e esegue procedure analitiche. Il software del server analitico dispone di diversi moduli. I moduli sono caricati su richiesta. I moduli possono caricare altri moduli.

Utilizzo Modalità Distribuita

I seguenti passaggi si verificano quando un utente finale esegue un prodotto in modalità di analisi distribuita:

1. **Avviare l'applicazione client.** L'utente finale lancia il software client sul proprio computer desktop. L'applicazione client presenta un'interfaccia utente completa.
2. **Connetti al server.** L'utente finale si connette al software del server collegando dall'applicazione client. Il servizio o il daemon del framework del server è sempre in esecuzione, in attesa di richieste di connessione. Quando viene effettuata una connessione, il software del server avvia un processo per gestire l'utente finale.
3. **Dati di accesso.** L'utente finale accede ai dati come di consueto dall'applicazione client, tranne che la sua visione di driver di database, file di dati, directory e unità rappresenta il computer server remoto, non il computer desktop. Il processo server carica i moduli di accesso dati appropriati e richiama i dati. Un piccolo segmento dei dati viene inviato all'applicazione client in modo che l'utente finale possa fare riferimento ad esso quando si seleziona un'analisi. La maggior parte dei dati rimangono sul server. È inoltre possibile configurare il software server per evitare che eventuali dati vengano inviati all'applicazione client. È possibile utilizzare l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, installata come parte di IBM SPSS Deployment Manager) per evitare che i dati vengano inviati a tutti i client. Consultare l'argomento Utenti nella *Guida per l'utente di distribuzione* (incluso nell'help per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni. È anche possibile configurare l'accesso per ogni utente o gruppo. Per ulteriori informazioni, consultare l'argomento IBM SPSS Statistics Server User Profiles and Groups, nel manuale *Deployment Manager User's Guide*.
4. **Analizzare i dati.** Utilizzando l'interfaccia utente dell'applicazione client, l'utente finale seleziona i dati e ne richiede il tipo di analisi. La richiesta viene inviata al processo server, che carica i pacchetti di analisi dei dati appropriati e elabora l'analisi. Tutte le attività relative ai dati, come la lettura dei dati, la trasformazione dei dati, il calcolo delle nuove variabili e il calcolo delle statistiche, vengono effettuate sul computer server.
5. **Rivista i risultati.** Il software server invia l'output dalla richiesta del client all'applicazione client. Solo i risultati vengono inviati, i dati rimangono sul server. L'utente finale può quindi utilizzare l'applicazione client per perfezionare e modificare i risultati.

Gestione del software Server

Questa guida è rivolta principalmente agli amministratori di sistema che si occupano di integrare la tecnologia server in un ambiente in rete in cui le applicazioni client vengono eseguite in modalità di analisi distribuita. Le attività amministrative includono:

Installazione. Il software server è progettato per funzionare continuamente e rispondere agli accessi e alle richieste dei computer desktop di fine utente. Selezionare un computer server appropriato per il software server - uno che ha poco tempo di fermo, è configurato per l'accesso agli utenti finali ed è collegato in rete agli appositi computer desktop. Più memoria e potenza di elaborazione del computer server ha, le richieste client più veloci vengono gestite. L'applicazione client deve essere installata sui computer desktop dell'utente finale. L'installazione client può essere effettuata da una postazione di rete. [Capitolo 2, "Installazione"](#), a [pagina 7](#) fornisce una panoramica su come installare il software del server e l'applicazione client. Le istruzioni di installazione dettagliate sono incluse nel prodotto DVD.

Accesso ai dati. Se è necessario fornire agli utenti finali l'accesso ai dati su un server remoto mentre stanno lavorando in modalità distribuita, il software server deve essere in grado di accedere a tali dati. I prodotti IBM Corp. possono accedere ai dati da una varietà di tipi di file di dati, inclusi i database. Per semplificare il tuo lavoro, i prodotti IBM Corp. vengono distribuiti con DataDirect Connect ODBC per l'accesso ai dati da un database. [Capitolo 3, "Accesso ai dati"](#), a [pagina 9](#) introduce l'accesso ai dati per i prodotti IBM Corp. . Ulteriore documentazione è inclusa sul prodotto DVD.

Configurazione e manutenzione. Poiché il software server è destinato al funzionamento continuo, dovrebbe essere monitorato ad intervalli regolari da un amministratore di sistema. Ci sono diverse opzioni di configurazione che ti danno il controllo su come funziona il software del server. [Capitolo](#)

4, “Configurazione, monitoraggio utilizzo e manutenzione”, a pagina 13 descrive come configurare e monitorare il software del server.

Supportare gli utenti finali. Gli utenti finali richiedono informazioni sui nomi server, gli account utente e dove trovare i dati. Potrebbe anche essere necessario assisterli nel risolvere i problemi. Capitolo 5, “Supporto agli utenti finali”, a pagina 21 descrive il tipo di supporto richiesto dagli utenti.

Prestazioni. Capitolo 6, “Analisi e miglioramento delle prestazioni”, a pagina 45 fornisce strategie per migliorare le prestazioni del software del server.

Risoluzione dei problemi. “Server software” a pagina 49 fornisce suggerimenti per la risoluzione dei problemi.

IBM SPSS Statistiche Batch Facility (solo IBM SPSS Statistiche Server). Il prodotto IBM SPSS Statistiche Server include IBM SPSS Statistiche Batch Facility, che è progettato per la produzione automatica di report statistici. Se si sta eseguendo IBM SPSS Statistiche Server sul proprio sito, leggere Appendice B, “La funzione di batch IBM SPSS Statistiche”, a pagina 51, che descrive IBM SPSS Statistiche Batch Facility e le attività che potrebbe essere necessario eseguire per supportarlo.

Utilizzo di questo documento

Questa guida è rivolta principalmente agli amministratori di sistema che si occupano di installare e mantenere il software server in un ambiente in rete in cui le applicazioni client vengono eseguite in modalità di analisi distribuita.

Capitolo 2. Installazione

I prodotti che utilizzano la tecnologia server sono confezionati su più supporti - uno DVD per il software server e uno DVD per l'applicazione client.

Per distribuire la tecnologia server, si:

- Installare il software server su un computer server netlavorato.
- Installare, o supervisionare l'installazione di, l'applicazione client in modo che sia accessibile dai computer desktop di fine utente.

Questo capitolo fornisce una panoramica del processo di installazione. Le istruzioni di installazione dettagliate sono disponibili sul prodotto DVD nella directory */Documentazione/<lingua>/InstallationDocuments*.

Fare riferimento a "Prodotti e Sistemi operativi" a pagina 1 per un elenco completo dei prodotti server e le relative applicazioni client associate.

Installazione del Software Server

Installare il software server su un computer server netlavorato. Il computer server deve eseguire la versione appropriata del sistema operativo. Se possibile, utilizzare un computer server configurato per, e dedicato a, elaborazione numerica rapida e accesso dati. Ulteriore potenza di elaborazione e memoria migliorano le prestazioni del software server. I requisiti hardware e software dettagliati, inclusi i requisiti del sistema operativo, appaiono nelle istruzioni di installazione.

Installazione del software di installazione della tecnologia server che gestisce l'accesso ai dati ed esegue i calcoli necessari per l'analisi statistica. Inoltre, installa un servizio (su Windows) o daemon (su UNIX) che ascolta le richieste di login degli utenti finali in arrivo e lancia un processo per gestire ogni utente finale.

Per installare il software del server, attenersi alle istruzioni riportate nella directory */Documentazione/<lingua>/InstallationDocuments* sul server DVD.

Installazione dell'Applicazione client

Installazione del software di installazione delle applicazioni client che gestisce l'interfaccia utente e la presentazione dei risultati. È necessario installare, o supervisionare l'installazione di, l'applicazione client sul computer desktop di ogni utente finale. Il computer desktop deve essere in esecuzione di Windows e deve soddisfare requisiti minimi hardware e di sistema operativo. I requisiti dettagliati vengono visualizzati nelle istruzioni di installazione, che si trovano nella directory */Documentazione/<lingua>/InstallationDocuments* sul client DVD.

Prima di leggere altri documenti di installazione, consultare *Getting Started with Installation and Licensing.pdf*.

Capitolo 3. Accesso ai dati

Se si desidera che gli utenti finali siano in grado di accedere ai dati sui server remoti, inclusi i dati dei database, è necessario pianificare, installare e configurare l'accesso ai dati. Per fare ciò è necessario capire come l'applicazione decide dove cercare i dati. È inoltre necessario decidere se si desidera utilizzare la tecnologia di accesso ai dati che offre DataDirect Connect ODBC. È inoltre possibile utilizzare le origini dati OLE DB.

Vista dei dati

Prima di iniziare a pianificare l'accesso ai dati per gli utenti finali, è importante capire come l'applicazione decide quali dati sono disponibili per l'utente finale. La visualizzazione dei dati che vengono presentati agli utenti finali dipende da come stanno eseguendo il programma - localmente o in modalità distribuita.

Modalità analisi locale. In modalità di analisi locale, in cui tutti gli accessi e le elaborazioni dei dati si verificano sul computer desktop dell'utente finale, la visualizzazione dei file di dati, le origini dati ODBC, le directory e le unità è dalla prospettiva del computer desktop - cioè quando l'utente finale cerca di aprire un file di dati, lui o lei vede i file di dati, le directory e le unità di rete sul proprio computer desktop.

Modalità analisi distribuita. In modalità di analisi distribuita, in cui l'accesso e l'elaborazione dei dati si verificano su un server remoto, la visualizzazione dei file di dati, delle origini dati ODBC, delle directory e delle unità è dalla prospettiva del computer server - cioè quando l'utente finale cerca di aprire un file di dati, lui o lei vede i file di dati, le directory e le unità montate sul computer server.

Il tuo lavoro consiste nel configurare l'accesso ai dati in modalità di analisi locale o in modalità di analisi distribuita, come richiesto dall'utente finale.

Tecnologia di accesso ai dati

Segue una breve descrizione di Connect ODBC. Per ulteriori informazioni su come la tecnologia di accesso ai dati funziona con i prodotti IBM Corp. e per i link alla documentazione dettagliata per specifici database, consultare *IBM SPSS Data Access Pack Istruzioni di installazione* nella directory / *Documentazione/<lingua>/InstallationDocuments* sul prodotto DVD.

Connetti ODBC

Connect ODBC è una serie completa di driver singoli, specifici di database che utilizzano ODBC per consegnare connettività a tutti i principali archivi dati, dai database relazionali ai dati di file flat.

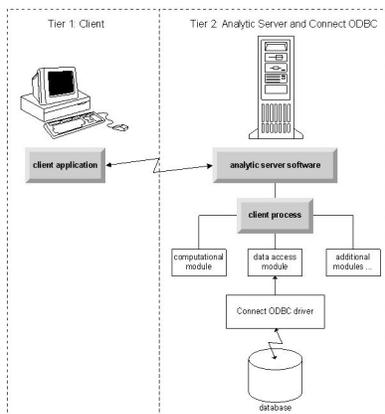


Figura 3. Connetti ODBC in modalità di analisi distribuita

Accesso ai dati

Come si imposta l'accesso ai dati, considerare quanto segue:

tecnologia di accesso ai dati. Decidi se vuoi utilizzare una delle tecnologie di accesso dati distribuite con il tuo prodotto IBM Corp. . Per ulteriori informazioni, consultare l'argomento [“Tecnologia di accesso ai dati”](#) a pagina 9. Una discussione più dettagliata su come scegliere una tecnologia viene visualizzata in *IBM SPSS Data Access Pack Istruzioni di installazione*(in /Documentazione/<lingua>/InstallationDocuments sul prodotto DVD).

Modalità di analisi. La modalità di analisi dell'utente finale determina quali dati può accedere. Per ulteriori informazioni, consultare l'argomento [“Vista dei dati”](#) a pagina 9.

prestazioni del file system (solo Windows). Se la maggior parte dei tuoi dati sono in formato proprietario da IBM Corp. (ad esempio i file .sav) piuttosto che in un database, ti consigliamo di memorizzare i tuoi dati su un'unità Windows NTFS di Windows per le migliori prestazioni.

Formato file. Il software gestisce l'apertura e la lettura dei file in formato UNIX automaticamente - te e i tuoi utenti finali non è necessario prendere alcuna azione per raccontare il software che un file è in formato UNIX.

Dati di riferimento

Alcuni software client consentono all'utente finale di salvare i riferimenti ai dati e ad altri file. Questi riferimenti devono essere scritti dalla prospettiva del computer che accederà ai dati. Ad esempio, se l'utente finale è in esecuzione in modalità di analisi locale, un riferimento a `C:\mydata\mydata.sav` fa sì che il software provi ad accedere al file sull'unità C locale del *computer desktop*. Se l'utente finale è in esecuzione in modalità di analisi distribuita, lo stesso riferimento a `C:\mydata\mydata.sav` fa in modo che il software tenti di accedere al file sull'unità C locale di *computer server*, causando probabilmente un errore.

Windows. Se si sta amministrando un sistema Windows, è possibile decidere di memorizzare i dati sullo stesso computer del software server. In tal caso, si consiglia agli utenti di fare riferimento all'ubicazione dei dati dalla prospettiva del computer server (ad esempio, `C:\ServerData\mydata.sav`). Le prestazioni sono più veloci perché la rete non è utilizzata per individuare il file. Se i dati si trovano su un altro computer di rete, si consiglia agli utenti di utilizzare riferimenti file UNC (ad esempio, `|mydataserver|ServerData\mydata.sav`). Si noti che i nomi UNC possono essere utilizzati solo quando le località di riferimento contengono il nome di una *risorsa condivisa* sulla rete. Gli utenti finali che passano frequentemente da distribuito alla modalità di analisi locale sono incoraggiati ad utilizzare i riferimenti del file UNC perché funzionano a prescindere dalla modalità.

UNIX. Se si sta amministrando una versione UNIX del software server, è possibile decidere di inserire file su un server UNIX. Gli utenti finali possono fare riferimento ai file su un server UNIX - indicare loro di utilizzare la specifica file completa e le barre (ad esempio, `/FILE = '/public/data/ourdata.txt`). Evitare di utilizzare il carattere di backslash nella directory UNIX e nelle riprese utilizzate con il software server.

Controllo dell'accesso ai dati

È possibile controllare l'accesso ai dati utilizzando il sistema operativo per impostare i permessi da parte di ID utente e gruppi. L'utente finale si connette al software del server collegando dall'applicazione client. Il software server utilizza il sistema operativo per far rispettare le autorizzazioni per tale utente.

Nota: La sicurezza dei dati aggiuntivi può essere esecutiva con il proprio software di database - il prompt dei moduli di accesso ai dati del software server per gli ID e le password quando il database li richiede.

Windows. Come impostare i permessi di accesso su Windows dipende da dove vengono memorizzati i dati.

- Se i file risiedono su un computer netlavorato altro poi il computer che esegue il software del server, assegnare i permessi alle risorse condivise.
- Se i file risiedono sul computer server, e su un'unità NTFS, utilizzare le impostazioni di sicurezza. Non è possibile controllare l'accesso file per i dati sul computer server su un'unità FAT.

Vedere “Proprietà file” a pagina 53 per informazioni sull'impostazione della condivisione e dei permessi di sicurezza su Windows.

UNIX. Quando l'utente finale si connette al software del server collegando dall'applicazione client, il software server passa l'ID di login e la password dell'utente al sistema operativo e avvia un processo per l'utente. Il processo avviato ha i diritti di accesso al file dell'account di login dell'utente finale.

Origini dati

ODBC

Il software server IBM SPSS Statistiche utilizza ODBC per accedere alla maggior parte dei dati che non sono in formato proprietario, inclusi i dati che vengono memorizzati nei database. ODBC richiede una fonte di dati ODBC . Un'origine dati ODBC è la combinazione di:

- Un nome descrittivo
- Un driver specifico
- Un riferimento a un database o ad altro tipo di file dati

Per accedere alla maggior parte dei dati è necessario configurare o aiutare gli utenti finali a configurare, le origini dati ODBC di cui hanno bisogno.

La posizione dell'origine dati configurata è critica. Deve essere configurato sul computer che sta accedendo e elaborando i dati - quindi configurare l'origine dati ODBC sul *computer server* per l'analisi distribuita e sul *computer desktop* per l'analisi locale. Ad esempio, confrontare la posizione dei driver ODBC nelle figure mostrate in “Connetti ODBC” a pagina 9 .

Se si sta solo iniziando ad utilizzare la tecnologia di accesso ai dati (introdotta in “Tecnologia di accesso ai dati” a pagina 9), è necessario effettuare alcune attività aggiuntive prima di poter configurare un'origine dati. Fare riferimento a *IBM SPSS Data Access Pack Istruzioni di installazione* (in /Documentazione/ <lingua>/InstallationDocuments sul prodotto DVD). La configurazione dell'origine dati viene discussa nuovamente in Capitolo 4, “Configurazione, monitoraggio utilizzo e manutenzione”, a pagina 13 di questa guida.

Configurazione dell'ambiente UNIX per l'accesso ai dati

Per la tecnologia di accesso ai dati al lavoro sui sistemi UNIX, lo script di avvio del software server deve essere configurato.

Aprire lo script di Startup

1. Passare alla sottodirectory */bin* nella directory di installazione del software server. Per esempio, digitare nel prompt di UNIX:

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

dove */usr/local/serverproduct/bin* è la sottodirectory */bin* della directory in cui è installato il software del server.

2. Aprire *statsenv.sh* con un editor di testo.

Specificare lo script DataDirect

1. Cerca il primo commento che contiene il testo:

```
MERANT_AMBIENT_SCRIPT
```

2. Individuare la riga che definisce l'ubicazione di **odbc.sh**.

3. Modificare la riga in modo che contenga il percorso corretto al tuo Connect ODBC *installazione cliente* rimuovere il carattere di commento se ne ha uno. Ad esempio, modificare:

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

A:

```
MERANT_ENVIRONMENT_SCRIPT=/usr/myDataAccess/slodbc50/5_01_00/odbc.sh
```

Aggiungi variabile di ambiente odbc.ini

1. Aggiungere le seguenti righe dopo le righe precedenti per creare una variabile di ambiente, ODBCINI, che consente a IBM SPSS Statistiche Server di trovare il file *odbc.ini* :

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

dove ODBCDir viene sostituito dal percorso alla directory di installazione di Connect ODBC .

Aggiungi Percorsi alle librerie di database

1. Aggiungere linee appropriate per il proprio database, di solito la *directory home database* e, se si è non utilizzando i driver del protocollo Data Direct Wire, un *percorso alle librerie di database*. Ad esempio, se si utilizza Oracle su Linux, aggiungere le seguenti righe:

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

dove */bigdisk/oracle/product/8.1.6* viene sostituito dal percorso alla tua directory di installazione Oracle e LD_LIBRARY_PATH è la variabile di percorso della libreria per il tuo sistema operativo.

Da notare che i driver di Data Direct Wire Protocol non richiedono l'installazione di librerie client di database. Tuttavia, altri driver Data Direct richiedono queste librerie.

Salvare lo script di Startup

1. Salvare *statsenv.sh*.

Modifica odbc.ini

1. Modificare *odbc.ini*, il file di configurazione ODBC , in modo che sia possibile accedere alle origini dati ODBC da IBM SPSS Statistiche Server. Consultare l'appendice "The UNIX Environment" in *DataDirect's DataDirect Connect ODBC Reference* (disponibile se è stata installata la documentazione DataDirect aggiuntiva quando è stato installato Connect ODBC) e i capitoli per driver specifici in *odbchelp.pdf* nella sottodirectory *doc* della directory di installazione di Connect ODBC .

La modifica avrà effetto la prossima volta che si avvia il software del server.

Nota: Se si prevede di utilizzare ODBC con IBM SPSS Statistiche Batch Facility, è necessario modificare lo script di avvio di IBM SPSS Statistiche Batch Facility nello stesso modo.

Capitolo 4. Configurazione, monitoraggio utilizzo e manutenzione

Dopo aver installato il software server, configurare il proprio ambiente tramite:

- Gestione degli account e dei file di fine utente
- Configurazione delle origini dati ODBC
- Utilizzo dell'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche) per configurare e monitorare il software server
- Controllo della startup del servizio

Questi compiti sono descritti nelle seguenti sezioni.

Gestione di Fine - Account utente e file

Questa sezione fornisce una panoramica di ciò che è necessario fare per supportare gli utenti finali sul proprio sito. Per ulteriori informazioni, consultare l'argomento [Capitolo 5, "Supporto agli utenti finali"](#), a [pagina 21](#).

Account

Gli utenti finali hanno bisogno di account per accedere al software server e ai dati di accesso. Questi account devono essere autenticati e devono essere in grado di leggere, scrivere e / o eseguire in cartelle specifiche sulla macchina server. Per ulteriori informazioni sulle autorizzazioni dei file, consultare l'argomento ["Autorizzazioni"](#) a [pagina 29](#). Per ulteriori informazioni sull'autenticazione, consultare l'argomento ["Autenticazione"](#) a [pagina 21](#).

Le autorizzazioni del database sono applicate dal software di database. Usa i tuoi usuali strumenti di gestione del database per gestire questi account. Se il database è limitato, i moduli di accesso ai dati del software del server richiedono all'utente di accedere e passare tali informazioni al database per la verifica prima di accedere ai dati.

Accesso ai dati

Per impostazione predefinita, ogni utente finale può visualizzare tutti i dati quando si apre un file mentre è collegato al software del server. La visualizzazione di tutti i dati può influire negativamente sulle prestazioni e aumentare il traffico di rete. È possibile scegliere di impedire ai computer client di fine utente di visualizzare i dati modificando l'impostazione globale con l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, installata come parte di IBM SPSS Deployment Manager). Consultare l'argomento [Utenti nella Guida per l'utente di distribuzione](#) (incluso nell'help per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni. È anche possibile modificare le impostazioni del profilo utente e dei gruppi per specificare l'accesso ai dati per singoli utenti o gruppi. Per ulteriori informazioni, consultare l'argomento [IBM SPSS Statistics Server User Profiles and Groups](#), nel manuale *Deployment Manager User's Guide*.

File

La maggior parte dei file che gli utenti finali devono salvare devono essere salvati sul computer desktop; tuttavia, è possibile consentire agli utenti di salvare i file di dati su un computer netlavorato. Quando l'utente finale accede al software del server analitico per la prima volta, la directory predefinita per l'apertura e il salvataggio dei file è la directory di installazione del software server. Chiaramente questa non è una località in cui si desidera che gli utenti scrivi file, così impostate una directory con autorizzazione di scrittura e distribuimmo quella posizione agli utenti finali. Una volta accesi a quella

posizione dall'interfaccia utente, l'applicazione client lo memorizzerà e diventerà la posizione predefinita per i file salvati.

Profili

Il software server consente anche di creare profili per gli utenti. Un profilo può specificare la directory temporanea, l'impostazione di UNIX umask, la priorità di processo della CPU, l'impostazione di accesso dei dati client e il numero massimo di thread per ogni utente o un gruppo di utenti.

Gruppi e profili utente di IBM SPSS Statistiche Server

Il software del server consente di creare profili per singoli utenti e gruppi di utenti. Il profilo specifica la directory dei file temporanei, l'impostazione umask UNIX, la priorità dei processi della CPU, l'accesso ai dati del client ed il numero massimo di thread per l'utente o il gruppo di utenti. Queste impostazioni sovrascrivono le impostazioni globali e predefinite associate.

File di profilo

Le impostazioni del gruppo e del profilo utente sono memorizzate nel file del profilo, *UserSettings.xml*. Per impostazione predefinita, questo file è contenuto nella sottodirectory *config* della directory di installazione di IBM SPSS Statistiche Server. Prima di apportare modifiche ai profili utente e ai gruppi, si consiglia di spostare il file predefinito e di specificare la nuova posizione nell'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche).

Come il server applica le impostazioni

Quando determina la directory dei file temporanei, l'impostazione umask, la priorità della CPU, l'accesso ai dati del client ed il numero massimo di thread per un particolare utente, il server effettua le seguenti operazioni.

1. Cercare un profilo utente per il nome utente ed il dominio dell'utente che effettua la connessione al server. Selezionare la prima corrispondenza trovata. In UNIX, il server ignora il dominio e le lettere maiuscole/minuscole per il nome utente. In Windows, le lettere maiuscole/minuscole del nome utente o del dominio non hanno importanza. Inoltre, se un utente ha eseguito l'accesso al server senza specificare un dominio, il server ricerca un nome utente con un dominio vuoto. Se non riesce a trovarne uno, utilizza una corrispondenza solo sul nome utente.
2. Se il profilo utente definisce delle impostazioni, applicare tali impostazioni al processo del server.
3. Se il profilo utente non definisce impostazioni o non definisce tutte le impostazioni, applicare le impostazioni del gruppo dell'utente al processo del server.
4. Se alcune impostazioni non sono ancora state definite o non c'è un profilo utente corrispondente, si applica l'umask predefinito, la directory dei file temporanei, l'impostazione di accesso ai dati del client e il numero massimo di thread definito dall'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche). Non viene utilizzata l'elaborazione predefinita della priorità della CPU.

Configurazione delle origini dati ODBC

Se gli utenti finali accedono ai dati dei database mentre stanno lavorando in modalità di analisi distribuita, è necessario configurare le origini dati ODBC sul computer su cui è installato il software server.

ODBC Origini dati e IBM SPSS Data Access Pack

Se si utilizza la tecnologia di accesso dei dati IBM Corp., leggi [Capitolo 3, "Accesso ai dati"](#), a pagina 9 in questo documento. Leggere le *Istruzioni di installazione* appropriate per una panoramica sulla configurazione dell'accesso al database e i link alla documentazione dettagliata sull'accesso ai dati per database specifici (il documento si trova in */Documentazione/<lingua>/InstallationDocuments* sul prodotto DVD).

Windows. Configurare le origini dati ODBC utilizzando l'amministratore ODBC . Per ulteriori informazioni, consultare l'argomento [“Amministratore ODBC”](#) a pagina 54.

UNIX. Modificare lo script dell'ambiente di avvio per il software del server come descritto in [“Configurazione dell'ambiente UNIX per l'accesso ai dati”](#) a pagina 11 e configurare le sorgenti dati ODBC utilizzando il file `odbc.ini` . Per ulteriori informazioni, consultare l'argomento [“odbc.ini”](#) a pagina 58 .

Utilizzo di un motore di ordinamento di Terze Parti

Per impostazione predefinita, il software server cerca di utilizzare un motore esterno, di terze parti per lo smistamento. Per utilizzare il motore di smistamento corretto, completare i seguenti passaggi:

1. Se il motore di ordinamento di terze parti non è installato sul computer server, installarlo. IBM Corp. non fornisce i motori. È necessario acquistare e concedere in licenza un motore da un fornitore di terze parti.
2. Assicurarsi che la libreria del motore di ordinamento sia sull'esecuzione del sistema o sulla variabile path della libreria. Su Windows, questa è la variabile di ambiente PATH; su UNIX si tratta di LD_LIBRARY_PATH o LIBPATH, a seconda del fornitore UNIX. Questo passo è necessario per consentire al software server di caricare la libreria di ordinamento di terze parti.
3. Utilizzando l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, che viene installata come parte di IBM SPSS Deployment Manager), impostare l'opzione di ordinamento all'appropriato motore di terze parti. Consultare l'argomento Utenti nella *Guida per l'utente di distribuzione* (incluso nell'help per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni.

Eventuali procedure che richiedono lo smistamento (ad esempio, SORT) utilizzeranno successivamente il motore di smistamento di terze parti. Il rilascio del comando di sintassi `SET SORT=INTERNAL` costringe il software server ad utilizzare l'algoritmo interno per l'ordinamento. Un utente finale può anche specificare esplicitamente l'ordinamento di terze parti emettendo il comando `SET SORT=EXTERNAL` . Tuttavia, questo non è necessario perché lo smistamento di terze parti è il default.

Verifica dell'opzione di ordinamento corrente

Per verificare quale opzione di smistamento viene utilizzata, è possibile emettere il comando della sintassi `SET MESSAGES ON` ed eseguire un lavoro SORT . È inoltre possibile utilizzare il comando di sintassi `SHOW SORT` .

Amministrazione di IBM SPSS Statistiche Server

IBM SPSS Console di amministrazione statistiche fornisce un'interfaccia utente per il monitoraggio e la configurazione delle installazioni di IBM SPSS Statistiche Server. Il IBM SPSS Console di amministrazione statistiche è installato come parte di IBM SPSS Deployment Manager. La documentazione completa per IBM SPSS Console di amministrazione statistiche è inclusa nella sezione *Administration Consoles* di *Deployment Manager User's Guide* (inclusa nella guida per IBM SPSS Servizi di collaborazione e distribuzione).

Configurazione di Xtensions

Un amministratore del server IBM SPSS Statistiche deve seguire la procedura per rendere disponibili le procedure di Xtension (`krr`, `lenr`, `lrr` e `lrr`) da eseguire nel server **statsb** e SPSS Statistiche . Le procedure di Xtension includono:

- Kernel Ridge Regression (KRR)
- Regressione Netta Elastica Lineare (LENR)
- Regressione Lineare Laica (LLR)
- Regressione Lineare Ridge (LRR)

Installazione di Xtensions su SPSS Statistiche Server

1. Sul client IBM SPSS Statistiche , installare le Xtensions (in modalità locale) dall'estensione Hub.
2. Accertarsi che la libreria **sklearn** sia installata sul server IBM SPSS Statistiche .

UNIX®

Eseguire il seguente comando come utente che ha installato SPSS Statistiche Server.

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

Nota: statisticspython3 si trova nella directory bin dell'installazione del server SPSS Statistiche .

Windows®

Immetti il seguente comando.

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

Nota: statisticspython3.bat Si trova nella directory di installazione del server SPSS Statistiche .

3. Copiare la directory xtensions e il relativo contenuto dal client SPSS Statistiche (%APPDATA%\IBM\SPSS Statistics\one\xtensions\ in Windows, \$HOME/Library/Application Support/IBM/SPSS Statistics/one/xtensions in macOS) alla directory di installazione del server SPSS Statistiche .

SPSS Statistiche Server è ora pronto a eseguire le procedure Xtension installate nella directory xtensions .

Configurazione dell'interfaccia di linea di comando della funzione di produzione per Submit Jobs

A partire da IBM SPSS Statistiche versione 26, è possibile utilizzare l'interfaccia della riga di comando di Produzione Facility per inoltrare i lavori al SPSS Statistiche Server. Quando l'interfaccia della riga comandi della funzione di produzione viene utilizzata insieme a Microsoft Windows Task Scheduler/ MacOS Automator per la pianificazione dei lavori, è possibile sostituire in modo efficace i lavori IBM SPSS Servizi di collaborazione e distribuzione per l'elaborazione SPSS Statistiche .

Il comando SPSS Statistiche **INSERT HIDDEN** può eseguire lavori che generano output. Quando si utilizza il comando, gli utenti non possono accedere o visualizzare la sintassi SPSS Statistiche di origine.

Nota: Il comando **INSERT HIDDEN** richiede un Server SPSS Statistiche . Il comando non funzionerà su una macchina client SPSS Statistiche autonoma.

INSERT HIDDEN funzione

Gli amministratori possono abilitare la funzione **INSERT HIDDEN** utilizzando la console di gestione del server SPSS Statistiche o modificando il file <install_path>/config/statisticsd.conf (**INSERT HIDDEN = Enabled**). Il campo **INSERT HIDDEN Feature** si trova nella scheda SPSS Statistiche Configurazione server della console di gestione del SPSS Statistiche Server (nella sezione **Utenti**).

1. Selezionare **Abilitato** come valore **INSERT HIDDEN Feature** . Notare che un asterisco (*) compare nella scheda Configurazione server SPSS Statistiche .
2. Salva il cambiamento. Fare clic sull'icona **Salva** sulla barra degli strumenti, Controlli - S oppure selezionare **File > Salva**.
3. Riavviare il SPSS Statistiche Server.
4. Dopo il riavvio del server sui server Windows, una finestra di dialogo richiede all'amministratore di inserire la password **INSERT HIDDEN Feature** . Sui server Linux , l'amministratore deve avviare manualmente il SPSS Statistiche Server. Quando il server si riavvia, richiede l'amministratore per la password.

La password viene memorizzata nel registro di sistema (simile ad una password SSL) e tutti i file di sintassi nascosti vengono crittografati tramite la stessa password.

Facoltativamente, l'amministratore può negare l'accesso dell'utente ai file **INSERT HIDDEN** tramite i controlli di accesso del file system.

Il processo daemon del server SPSS Statistiche richiede l'accesso in lettura ai file **INSERT HIDDEN**. Un comando OMS può essere utilizzato per avvolgere la sintassi per garantire che l'output non venga inviato al Viewer di Output.

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

La sintassi **INSERT HIDDEN** è simile alla sintassi **INSERT FILE**. Ad esempio:

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

L'autore del file **INSERT HIDDEN** fornisce i percorsi dei file nascosti agli utenti del client SPSS Statistiche. Durante il runtime, gli utenti del client eseguono la sintassi **INSERT HIDDEN SOURCE="<file_path>"**.

Fare riferimento alla *IBM SPSS Statistiche Guide Syntax Guide* per informazioni più dettagliate.

Il processo del client sul server SPSS Statistiche invia il percorso **SOURCE** al processo daemon del server. Il processo del daemon decodifica il file e lo restituisce al processo client per l'esecuzione.

Il processo client disabilita i log e i giornali, esegue il file decodificato e quindi ri - abilita log e giornali. Il risultato è che il SPSS Statistiche Output Viewer non contiene alcuna registrazione sintassi di origine (contiene output). Il giornale inoltre non contiene alcuna sintassi di origine.

Configurazione Istanze Multiple

È possibile creare più istanze del software server, ognuna con il proprio numero di porta. Questo viene spesso utilizzato insieme all'autorizzazione di gruppo per assegnare un gruppo di utenti ad un'istanza specifica. Tuttavia, le istanze multiple possono essere utilizzate indipendentemente dall'autorizzazione di gruppo. Per ulteriori informazioni sull'autorizzazione di gruppo, consultare [“Autorizzazione del gruppo”](#) a pagina 29.

Creazione di una nuova istanza

Per creare un'istanza di gruppo del software server, è necessario eseguire uno script.

Su Windows, eseguire il seguente script dalla directory di installazione del server.

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

Su UNIX e Linux, eseguire il seguente script dalla sottodirectory bin della directory di installazione.

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

<group_name> è un nome univoco per l'istanza e <port_number> è il numero di porta disponibile che verrà utilizzato dall'istanza.

Dopo aver eseguito lo script, ci sarà una cartella di configurazione specifica per l'istanza. Cercare config_<groupname> nella direzione di installazione del server. La cartella contiene diversi file di configurazione, come statisticsd.conf e UserSettings.xml. Quando si desidera aggiornare la configurazione per un'istanza specifica, assicurarsi di aggiornare il file di configurazione nella posizione corretta.

Avvio dell'istanza del server

Su Windows, l'istanza è un servizio separato denominato *IBM SPSS Statistiche NN.m*, dove *NN* è il numero di versione principale e *m* è il numero di versione secondario. È possibile avviare e arrestare questo servizio come qualsiasi altro servizio Windows.

Su Linux e UNIX è necessario specificare il nome del gruppo durante l'esecuzione dello script di avvio:

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

dove <group_name> è il nome del gruppo di istanze.

Eliminazione di un'istanza server

1. Su Windows, rimuovere la voce di servizio:
 - a. Aprire un prompt cmd come Amministratore.
 - b. Eseguire il comando riportato di seguito:

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

dove *NN* è il numero di versione principale, *m* è il numero di versione minore e <group_name> è il gruppo di istanza.

2. Eliminare la sottodirectory `config_<groupname>` nella directory di installazione del server.

Avvio Controllo del servizio

Il software server dispone di un componente quadro che gestisce tutta la comunicazione tra l'applicazione client e i moduli. Su Windows, il componente quadro è un servizio. Su UNIX, il componente quadro è un'applicazione, di solito si esegue come un daemon.

Windows

Per impostazione predefinita, il servizio è configurato per la startup automatica, il che significa che si riavvierà automaticamente quando il computer verrà riavviato. Quando è iniziato questo modo, il servizio viene eseguito in modo non presidiato e il computer server può essere scollegato senza influenzare il servizio. È possibile utilizzare il Pannello di controllo dei servizi di Windows per modificare i parametri di avvio del servizio. Per ulteriori informazioni, consultare l'argomento "Pannello di controllo dei servizi" a pagina 54. Se si eseguono più istanze, il Pannello dei Servizi includerà una voce per ogni istanza del server.

Nota: Se il computer server non supporta l'indirizzo IP dell'host locale (127.0.0.1::1), è necessario creare una variabile di ambiente di sistema denominata `STATS_LH_OVERRIDE` e impostarne il valore su `YES` prima di avviare il server. Per informazioni sull'avvio e l'arresto del server, consultare "Avvio e arresto del Software Server" a pagina 19.

UNIX

Uno script di avvio, `start_statistics_server`, è incluso nella sottodirectory `/bin` della directory di installazione. Lo script richiama `statsenv.sh` per configurare l'ambiente per il software del server e quindi avvia l'applicazione. È necessario avviare il software server con questo script. Lo script di avvio deve essere eseguito dalla sottodirectory `/bin`. Per eseguirlo è necessario essere collegati come **root** se si utilizza l'autenticazione unix predefinita o il PAM (Pluggable Authentication Module). In caso contrario, è necessario essere collegati come utente che possiede il daemon software server. Per ulteriori informazioni sull'autenticazione, consultare l'argomento "Autenticazione" a pagina 21. Il comando:

```
./start_statistics_server -d
```

avvierà il software server come un processo daemon, ovvero il modo consigliato per eseguire il software del server.

Se si eseguono più istanze del software server, questo comando avvierà l'istanza predefinita. Per avviare un'altra istanza, specifica il gruppo di istanze con lo switch -g :

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

dove <groupname> è il nome del gruppo di istanze.

Nota: Se il computer server non supporta l'indirizzo IP localhost (127.0.0.1/::1), è necessario impostare la variabile di ambiente `STATS_LH_OVERRIDE` su YES prima di avviare il server. La variabile di ambiente `STATS_LH_OVERRIDE` viene impostata da `statsenv.sh`, incluso nella sottodirectory `/bin` della directory di installazione. Per informazioni sull'avvio e l'arresto del server, consultare [“Avvio e arresto del Software Server”](#) a pagina 19.

Parametri Riga Comandi Script di avvio

Lo script `start_statistics_server` accetta i seguenti parametri di riga di comando (in qualsiasi ordine):

- **Daemon.** Eseguire il software del server come un processo del daemon specificando opzionalmente -d. Se si ometta il -d, il server inizierà come un processo di primo piano. Ad esempio, per avviare il software server come daemon, utilizzare il comando:

```
./start_statistics_server -d
```

- **Gruppo.** Se si eseguono più istanze del software server, specificare il gruppo associato all'istanza:

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

dove

<groupname> è il nome del gruppo appropriato.

- **Porta.** Un numero di porta può opzionalmente essere specificato sulla riga di comando dello script di avvio. Ad esempio, per specificare un numero di porta, utilizzare il comando:

```
start_statistics_server -p nnnn
```

dove

nnnn è il numero di porta desiderato.

Specificare un numero di porta solo se è necessario risolvere un conflitto del numero di porta. Il default funzionerà a meno che un'altra applicazione sul computer stia utilizzando lo stesso numero. Questa impostazione della riga di comando sovrascrive il valore impostato nell'applicazione di amministrazione.

Altra manutenzione

Rimuovi file non necessari. Controllare periodicamente la posizione del file temporaneo e la posizione del file di log per i file non necessari e rimuoverli. Le posizioni sono definite con l'applicazione di amministrazione.

Controllare i processi di esecuzione. Se non si reboot regolarmente il computer server, controllare periodicamente i processi in esecuzione sul computer e terminare eventuali processi non in uso. I nomi dei processi sono elencati in [“Avvio e arresto del Software Server”](#) a pagina 19 .

Avvio e arresto del Software Server

L'applicazione di amministrazione riavvierà il software server per te in modo che le modifiche di configurazione possano essere commesse; tuttavia, a volte potrebbe essere necessario avviare o arrestare il software server dal sistema operativo. Segui i passi riportati di seguito per il tuo sistema operativo, utilizzando il nome di processo del tuo prodotto server. Su Windows, il nome del servizio predefinito è *IBM SPSS Statistiche NN.m*, dove *NN* è il numero di versione principale e *m* è il numero di versione secondario. Se si stanno eseguendo più istanze, il nome del servizio è *IBM SPSS Statistiche NN.m*

< *groupname* >, dove *NN* è il numero di versione principale, *m* è il numero di versione secondario e < *groupname* > è il gruppo dell'istanza. Su UNIX e Linux, il nome daemon è *statisticsd*.

Nota di pianificazione: Arresto del servizio o del daemon disconnette gli utenti finali e termina i loro processi, quindi provare a programmare le attività di configurazione e manutenzione per un momento in cui ci si aspetta pochi utenti per accedere al sistema (ad esempio, inizio mattina o tarda sera).

Per avviare il servizio o Daemon

Windows. Utilizzare il Pannello di controllo dei servizi di Windows per avviare il servizio. Per ulteriori informazioni, consultare l'argomento [“Pannello di controllo dei servizi”](#) a pagina 54.

UNIX. Avviare il Server con lo script di avvio, *start_statistics_server*, incluso nella sottodirectory */bin* della directory di installazione. Lo script di avvio deve essere eseguito dalla sottodirectory */bin*. Per eseguirlo è necessario essere collegati come **root** se si utilizza l'autenticazione unix predefinita o il PAM (Pluggable Authentication Module). In caso contrario, è necessario essere collegati come utente che possiede il daemon software server. Per ulteriori informazioni sull'autenticazione, consultare l'argomento [“Autenticazione”](#) a pagina 21.

Per arrestare il servizio o Daemon

Windows. Utilizzare il Pannello di controllo dei servizi di Windows per arrestare il servizio. Per ulteriori informazioni, consultare l'argomento [“Pannello di controllo dei servizi”](#) a pagina 54.

UNIX. Uccidi il processo del server. (Vedi [“ps e uccidere”](#) a pagina 57 per un esempio.) Il daemon crea automaticamente un file (*statisticsd.pid*) che contiene l'ID processo per il daemon. È possibile utilizzare questo file insieme al comando kill eseguendo quanto segue dalla sottodirectory *config* della directory di installazione o dal *config_<group_name>* per un'altra istanza del software server:

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

Platform indipendente. Utilizzare l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, che viene installata come parte di IBM SPSS Deployment Manager). Per ulteriori informazioni, consultare l'argomento Controllo di IBM SPSS Statistics Server nel manuale *Deployment Manager User's Guide* (incluso nella guida per IBM SPSS Servizi di collaborazione e distribuzione).

Configurazione per il miglioramento delle prestazioni

Fare riferimento a [Capitolo 6, “Analisi e miglioramento delle prestazioni”](#), a pagina 45 per informazioni sulla modifica della configurazione del software server per migliorare le prestazioni.

Capitolo 5. Supporto agli utenti finali

Supportare gli utenti finali implica assicurarsi di avere le informazioni necessarie per eseguire il proprio prodotto IBM Corp. in modalità di analisi distribuita. Per utilizzare il software server, gli utenti finali devono sapere:

- Come connettersi al software server.
- Come accedere ai dati e ai file.
- Dove salvare dati e file.

Autenticazione

Si hanno diverse opzioni per l'autenticazione degli utenti. Alcune opzioni richiedono che il server venga eseguito con privilegi di root.

Metodo	Disponibilità OS	Server Must Run come System / Root?
Autenticazione di livello OS standard (account Windows o UNIX)	<ul style="list-style-type: none">• Windows• UNIX	Sì
Modulo di autenticazione collegabile (PAM)	<ul style="list-style-type: none">• UNIX	Sì
Autenticazione interna	<ul style="list-style-type: none">• Windows• UNIX	N
unix2	<ul style="list-style-type: none">• UNIX	N
SSO (Single Sign-On)	<ul style="list-style-type: none">• Windows• UNIX	N

Configurazione dell'autenticazione a livello OS

L'autenticazione di livello OS è il metodo di autenticazione predefinito. Utilizzare i consueti strumenti di amministrazione del sistema per creare e gestire gli account di fine utente di livello OS (consultare "Gestore utente" a pagina 54 per informazioni su come accedere a Windows User Manager).

Se si prova un altro metodo di autenticazione e si desidera ripristinare l'autenticazione a livello di sistema operativo, è necessario aggiornare l'elemento *userauth* nel file *statisticsd.conf* e modificare il parametro *value* in *unix* o *win32*.

Configurazione di PAM

Il software server su UNIX può utilizzare il PAM (Pluggable Authentication Module) per autenticare gli utenti. È necessario prima configurare il software server per utilizzare PAM. Quindi configurare PAM seguendo le istruzioni specifiche per il tuo fornitore UNIX. Passi di seguito per Linux. Questi possono variare, a seconda della versione e del fornitore.

Nota: se il software server è in esecuzione, è necessario riavviarlo dopo aver completato tutti i passaggi.

Configurare il Software Server per utilizzare la PAM

1. Accedi alla macchina UNIX come *root*.
2. Nella sottodirectory *configurazione* nella directory di installazione del software del server, aprire il file di configurazione (ad esempio, *statisticsd.conf*) in un editor di testo.
3. Trovare l'elemento *userauth* e modificare il parametro *value* da *unix* a *pam*.
4. Salvare il file.

Configurare PAM su Linux

1. Passare alla directory di configurazione PAM (ad esempio, */etc/pam.d*).
2. Utilizzare un editor di testo per creare un file denominato *statisticsd*.
3. Aggiungere le informazioni di configurazione PAM che si desidera utilizzare. Ad esempio:

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

Nota: queste righe possono variare in base alla tua particolare configurazione. Consultare la documentazione Linux per ulteriori informazioni.

4. Salvare il file.

Configurazione dell'autenticazione interna

L'autenticazione interna consente al software server di eseguire senza privilegi di *root*. Tuttavia, limita le connessioni client allo stesso accesso a disco. Ogni utente che si connette al software server ha la stessa sicurezza di accesso al disco. Pertanto, un utente può cancellare un altro file dell'utente. Se questa è una preoccupazione, si consiglia di utilizzare il metodo di autenticazione *unix2* invece. Questo metodo non limita le connessioni client perché utilizza il file UNIX *passwd* per l'autenticazione. Per ulteriori informazioni, consultare l'argomento "[Configurazione dell'autenticazione unix2](#)" a pagina 23.



Avvertenza: Non utilizzare l'autenticazione interna durante l'esecuzione del daemon / servizio come *root/SYSTEM*. Farlo è lo stesso che dare accesso *root/SYSTEM* al proprio server a qualsiasi utente che si connette.

Configurazione dell'autenticazione interna su UNIX

1. Creare un gruppo per gli utenti che si connettono al software server. Consigliamo di denominare questo gruppo **statistiche**.
2. Un membro di questo gruppo deve installare il software server. Questo utente sarà il proprietario del daemon software server.
3. Un altro membro di questo gruppo (diverso dal proprietario del daemon e tipicamente l'utente che mantiene gli utenti del software server) crea un file *statisticsusers* nella directory *config* nella directory di installazione del software server. Questo file dovrebbe avere accesso in lettura / scrittura per l'utente che lo ha creato. Avrebbe dovuto leggere l'accesso per il gruppo utenti. Nessun altro utente dovrebbe essere in grado di accederlo. Se non si crea questo file manualmente, viene creato automaticamente la prima volta che si esegue lo strumento della riga di comando *statisticsuser* (vedere il passo successivo). Lo strumento della riga di comando imposta le autorizzazioni appropriate.
4. Nella directory *config*, utilizzare lo strumento della riga di comando *statisticsuser* per aggiungere utenti. Come l'utente che ha creato il file *statisticsusers*, digitare *statisticsuser <username>* per creare un utente regolare (ad esempio, *statisticsuser jdoe*). Utilizzare l'opzione *-a* per creare un utente admin (ad esempio, *statisticsuser -a jdoe*). Lo strumento della riga di comando *statisticsuser* ti richiede una password. Un utente finale entra nel nome utente e nella password per connettersi al software server. Assicurarsi di distribuire opportunamente il nome utente e la password. Per eliminare un utente, utilizzare l'opzione *-d* (ad esempio, *statisticsuser -d jdoe*).

5. Collegati come proprietario del daemon del software del server, aprire il file di configurazione (ad esempio, *statisticsd.conf*) in un editor di testo.
6. Trovare l'elemento *userauth* e modificare il parametro *value* da *unix* a *internal*.
7. Collegato come proprietario del daemon software server, avviare il server.

Configurazione dell'autenticazione interna su Windows

1. Modificare la voce IBM SPSS Statistics Server da eseguire come utente specifico:
 - a. Aprire il pannello dei servizi di Windows e fare doppio clic sulla voce per *IBM SPSS Statistiche NN.m*, dove *NN* è il numero di versione principale e *m* è il numero di versione secondario.
 - b. Fare clic sulla scheda **Accedi**.
 - c. Sotto **Accedi come**, selezionare **Questo account**.
 - d. Inserire il domain\username e la password dell'utente che possederà il processo server. Questo utente avrà bisogno del privilegio *Logon as a service*.
2. Lo stesso utente deve creare un file *statisticsusers* nella directory *config* nella directory di installazione del software server. Questo file dovrebbe avere accesso in lettura / scrittura per l'utente che lo ha creato. Nessun altro utente dovrebbe avere accesso in scrittura. Se non si crea questo file manualmente, viene creato automaticamente la prima volta che si esegue lo strumento della riga di comando *statisticsuser* (vedere il passo successivo).
3. Nella directory *config*, utilizzare lo strumento della riga di comando *statisticsuser* per aggiungere utenti. Come utente che ha creato il file *statisticsusers*, immettere *statisticsuser <username>* per creare un utente regolare (ad esempio, *statisticsuser jdoe*). Utilizzare l'opzione *-a* per creare un utente admin (ad esempio, *statisticsuser -a jdoe*). Lo strumento della riga di comando *statisticsuser* richiede una password. Un utente finale entra nel nome utente e nella password per connettersi al software server. Assicurarsi di distribuire opportunamente il nome utente e le password. Per eliminare un utente, utilizzare l'opzione *-d* (ad esempio, *statisticsuser -d jdoe*).
4. Collegato come proprietario del daemon software server, aprire il file di configurazione (ad esempio, *statisticsd.conf*) in un editor di testo.
5. Trovare l'elemento *userauth* e modificare il parametro *value* da *win32* a *internal*.
6. Vai al Pannello dei servizi di Windows e avvia il servizio.

Configurazione dell'autenticazione unix2

L'autenticazione *unix2* consente al software server di eseguire senza privilegi di root e di autenticarsi contro il file UNIX *passwd* con account utente standard. Un file eseguibile (*suauth*) installato con il software server esegue l'autenticazione. Affinché funzioni correttamente, è necessario impostare le autorizzazioni necessarie.

Per configurare l'autenticazione *unix2*, completare i seguenti passaggi:

1. Utilizzando *setuid* e *setgid* o il controllo accessi basato su ruolo (RBAC), modificare le autorizzazioni dell'eseguibile *suauth* in modo che l'utente che eseguirà il daemon software server abbia i permessi di root necessari. Questo utente deve essere in grado di autenticare l'utente rispetto al file *passwd* e di modificare l'ID utente e il gruppo ID del processo server spedito per ogni utente finale. Dettagli sull'impostazione dei permessi di seguito. Notare che si utilizza *setuid* / *setgid* o RBAC. Non utilizzare entrambi i metodi.
2. Aprire il file di configurazione (ad esempio, *statisticsd.conf*) in un editor di testo.
3. Trovare l'elemento *userauth* e modificare il parametro *value* da *unix* a *unix2*.
4. Collegato come proprietario del daemon software server, avviare il server.

Impostazione Autorizzazioni con `setuid` e `setgid`

1. Creare un gruppo per l'utente che eseguirà il software server. Consigliamo di denominare questo gruppo **statistiche**. Consigliamo inoltre di limitare l'appartenenza del gruppo al solo utente che eseguirà il daemon software del server.
2. Un membro di questo gruppo deve installare il software server. Questo utente sarà il proprietario del daemon software server.
3. Avviare una sessione terminale come *root*.
4. Passare alla directory *bin* nella directory di installazione del software server.
5. Cambiare il proprietario del file *suauth* per essere *root*.

```
chown root suauth
```

6. Aggiungere i bit `setuid` e `setgid` a *suauth*. Questi bit consentono all'utente nel gruppo installer di eseguire il file ed eseguire temporaneamente come *root*. I privilegi di *root* sono richiesti per le ragioni indicate in precedenza in questo argomento.

```
chmod 6550 suauth
```

7. Uscire come *root* e accedere come proprietario del daemon software server.

Impostazione Autorizzazioni con controllo accessi basato su ruoli

È necessario inoltre essere in grado di utilizzare il controllo accessi basato su ruolo (RBAC) per impostare le autorizzazioni necessarie. Fare riferimento alla documentazione RBAC del tuo fornitore per informazioni. Sarà necessario effettuare quanto segue:

1. Creare un'autorizzazione per l'eseguibile *suauth*.
2. Creare un ruolo per questa autorizzazione.
3. Assegnare il proprietario del daemon software del server al ruolo.
4. Configurare l'autorizzazione per consentire le seguenti autorizzazioni:
 - Leggere il file *passwd*.
 - Modifica ID utente.
 - Modifica ID gruppo.

Configurazione di Single Sign - On (SSO)

È possibile utilizzare SSO (single sign - on) per collegarsi ad un server che è in esecuzione su qualsiasi piattaforma supportata. È necessario prima configurare le macchine IBM SPSS Statistiche Server, IBM SPSS Statistiche client e IBM SPSS Servizi di collaborazione e distribuzione. L'autenticazione interna consente al software server di eseguire senza privilegi di *root*.

Se si utilizza un SSO (Single Sign-On) per connettersi a IBM SPSS Statistiche Server e IBM SPSS Servizi di collaborazione e distribuzione, è necessario connettersi a IBM SPSS Servizi di collaborazione e distribuzione prima di connettersi a IBM SPSS Statistiche Server.

Per interagire con le installazioni Active Directory sicure più recenti, è necessario installare il package di crittografia ad elevata protezione per Java poiché gli algoritmi di crittografia richiesti non sono supportati in modo predefinito. È necessario installare il package sia per il client che per il server. Viene visualizzato un messaggio di errore come `Illegal key size` (Dimensione chiave non consentita) sul client quando la connessione del server non viene stabilita perché il package non è installato. Consultare ["Installazione della crittografia "Unlimited strength" a pagina 37](#).

Nota: Prima di configurare le macchine SPSS Statistiche Server, SPSS Statistiche client e IBM SPSS Servizi di collaborazione e distribuzione per single sign - on, è necessario assicurarsi che le macchine abbiano accesso al server controller di dominio.

Per informazioni sulla configurazione IBM SPSS Servizi di collaborazione e distribuzione per single sign - on, consultare [IBM SPSS Servizi di collaborazione e distribuzione Single Sign - On services overview](#).

Configurazione del Server per Single Sign - On

Configurare il Server su Windows

1. Assicurarsi che la macchina del server Windows sia un membro del dominio AD (Active Directory).
2. Nella posizione di installazione IBM SPSS Statistiche Server , individuare la cartella chiamata config.
3. Nella cartella config, creare una cartella secondaria denominata sso.
4. Nella cartella sso, creare un file krb5.conf. Le istruzioni su come creare il file krb5.conf si trovano all'indirizzo http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html. Di seguito è riportato un esempio di un file krb5.conf:

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

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

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

Configurare il Server su UNIX

Per configurare Single Sign - On per le macchine server UNIX, è possibile aggiungere la macchina UNIX al dominio Windows AD, quindi seguire le istruzioni per la configurazione di Single Sign - On su Windows. In alternativa, è possibile eseguire le seguenti operazioni:

1. Creare un account utente di dominio per la macchina UNIX.
2. Modifica il nome host. Se si sta utilizzando RedHat Linux, aprire il file /etc/sysconfig/network e modificare HOSTNAME nel modulo <name>.<realm>. Ciò consente all'AD di trovare le credenziali del server.
3. Per consentire al server DNS di trovare la macchina UNIX, effettuare una delle seguenti operazioni:
 - Aprire il file %windows%/system32/drivers/etc/hosts e aggiungere la mappatura IP/host, ad esempio:

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

Oppure

- Aggiungere una nuova voce di zona di ricerca inversa. In questo modo si aggiungerà una mappatura IP/host sul server DNS.

Se la voce DNS per la macchina UNIX non è corretta, è possibile aggiungere manualmente la voce di ricerca inversa sul server DNS.

Configurazione del Client per Single Sign - On

I passi sono comuni a tutti i client tranne i passi che vengono notati specificamente per Windows.

1. Assicurarsi che la macchina Windows locale che sta eseguendo IBM SPSS Statistiche sia membro del dominio Active Directory (AD).
2. Aggiungere l'utente del dominio come amministratore sulla macchina locale.
3. Abilitare Windows al fine di accedere alla chiave di sessione TGT:
 - a. Dal menu di **Avvio**, fare clic su **Esegui**.
 - b. Immettere `regedit` e fare clic su **OK** per aprire **Editor di registro**.

c. Naviga nella seguente posizione di registro:

```
My
Computer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\
Parameters
```

d. Fare clic con il tasto destro del mouse sulla cartella e selezionare **Nuovo > DWORD**. Il nome del nuovo valore deve essere `allowtgtsessionkey`.

e. Impostare il valore `allowtgtsessionkey` sul valore esadecimale 1, ovvero 0x0000001.

f. Chiudere l'**Editor di registro**.

g. Eseguire `kinit.exe`, che può essere trovato in `<IBM SPSS Statistiche installation location>\jre\bin`.

4. Nella cartella `config` dell'ubicazione di installazione IBM SPSS Statistiche, creare una cartella denominata `sso`.

5. Copiare il file `krb5.conf` dal server nella cartella `sso`.

6. Riavviare la macchina client e la macchina server.

Registrazione del Nome Principale di servizio (SPN)

Ogni istanza del server deve registrare un unico *nome principale del servizio (SPN, Service Principal Name)* per potersi identificare, mentre il client deve specificare lo stesso SPN quando si connette al server.

Un SPN per un'istanza del software server ha la forma:

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

Ad esempio:

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

Si noti che il nome `host` deve essere qualificato con il proprio dominio DNS (`ibm.com` in questo esempio) e il dominio deve mappare al dominio Kerberos.

La combinazione di nome `host` e numero porta rende l'SPN univoco (poiché ogni istanza su un dato `host` deve essere in ascolto su una porta differente). Sia il client che il server dispongono già del nome `host` e del numero di porta e quindi possono creare l'SPN appropriato per l'istanza. La procedura di configurazione aggiuntiva richiesta consiste nel registrare l'SPN nel database Kerberos.

Registrazione di SPN su Windows

Se si sta utilizzando Active Directory come implementazione Kerberos, utilizzare il comando `setspn` per registrare l'SPN. Per eseguire questo comando, è necessario che siano soddisfatte le seguenti condizioni:

- È necessario essere collegati a un controller del dominio
- È necessario eseguire il prompt dei comandi con privilegi elevati (esecuzione come amministratore)
- È necessario essere un membro del gruppo Domain Admins (o avere l'autorizzazione appropriata delegata da un amministratore di dominio)

Per ulteriori informazioni, fare riferimento ai seguenti articoli:

- [Setspn Command-Line Reference](#)
- [Delegating Authority to Modify SPNs](#)

Per l'istanza predefinita, in ascolto sulla porta standard (3023 per la versione 23, ad esempio) e in esecuzione sotto l'account Local System, è necessario registrare la SPN contro il nome del computer server. Ad esempio:

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

Per ogni istanza server successiva, in ascolto su una porta personalizzata (ad esempio, 3099) e in esecuzione sotto un account utente arbitrario (ad esempio, johndoe) con l'opzione `userauth` impostata su `internal` (cioè utilizzando l'autenticazione interna), è necessario registrare la SPN contro il nome dell'account utente del servizio:

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

Si noti che in questo caso (quando l'account del servizio è diverso da Sistema locale), la registrazione di SPN non è sufficiente per abilitare un client per la connessione. Le procedure di configurazione aggiuntive vengono descritte nella successiva sezione.

Per visualizzare gli SPN registrati per l'account `jdoe`:

```
setspn -l jdoe
```

Registrazione di SPN su UNIX

Se si sta utilizzando Active Directory come implementazione Kerberos, utilizzare il comando `setspn` come descritto nella precedente sezione Windows. Ciò presuppone che sia già stato creato il computer o l'account utente nella directory. Oppure è possibile sperimentare con `ktpass`, se desiderato (vedere [Ktpass Command - Line Reference](#)).

Se si sta utilizzando qualche altra implementazione Kerberos, utilizzare lo strumento di amministrazione Kerberos preferito per aggiungere il principal del servizio al database Kerberos. Per convertire l'SPN in un principal Kerberos, è necessario accodare il nome del realm di Kerberos. Ad esempio:

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

Aggiungere questo stesso principal e password al keytab del server. Il keytab deve contenere una voce per ogni istanza in esecuzione sull'host.

Configurazione SSO quando in esecuzione come non - Root / Sistema

Quando il servizio server / daemon è in esecuzione come utente arbitrario (non root su UNIX e non System su Windows), è necessario registrare l'account service / daemon. Hai bisogno della SPN che hai creato in precedenza.

1. Creare la directory `<STATISTICSSERVER>\config\sso`.
2. Copiare il file `krb5.conf` dalla directory SSO del client nella directory SSO del server creata al passo 1.
3. Utilizzare il seguente comando per creare il file `krb5.keytab` nella directory SSO del server:

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

Ad esempio:

```
"..\jre\bin\ktab.exe" -a statisticsserver/  
jdoemachine.ibm.com:3023@ibm.com  
-k krb5.keytab
```

Verrà richiesto l'immissione di una password. La password immessa deve essere la password dell'account di servizio. Pertanto, se l'account di servizio è `jdoe`, ad esempio, è necessario immettere la password per l'utente `jdoe`.

L'account di servizio stesso non è indicato nella keytab, ma in precedenza è stato registrato l'SPN per quell'account utilizzando `setspn`. Ciò indica che la password del principal del servizio e la password dell'account del servizio sono uguali e univoche.

Per ogni nuova istanza server creata è necessario registrare la SPN per tale istanza (utilizzando setspn) e creare un file keytab. Il file keytab deve essere copiato nella sottodirectory config_<group_name>/sso nella directory di installazione del server .. L'istanza predefinita non necessita di un file keytab.

Per essere certi che un'istanza sia inclusa nella keytab:

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

Si potrebbero visualizzare più voci di ciascun principal con tipi di codifica differenti, ma ciò è normale.

Configurazione Appartenenza Gruppo

Se si sta utilizzando l'autorizzazione di gruppo, è possibile configurare IBM SPSS Servizi di collaborazione e distribuzione per interrogare un provider LDAP per determinare il gruppo a cui appartiene un utente autenticato. Per ulteriori informazioni sull'autorizzazione di gruppo, consultare l'argomento [“Autorizzazione del gruppo”](#) a pagina 29.

Quindi, per la ricerca di gruppo per funzionare correttamente, è necessario configurare prima il proprio repository per aggiungere un provider LDAP o Active Directory e quindi abilitare SSO utilizzando quel provider:

1. Avviare IBM SPSS Deployment Manager client e selezionare **File > Nuovo > La connessione del server amministrato ...** per creare una connessione server amministrata per il proprio repository (se non ne avete già uno).
2. Accedere alla connessione al server amministrato ed espandere la cartella **Configurazione**.
3. Fare clic con il tasto destro del mouse su **Provider di sicurezza**, scegliere **Nuovo > Definizione del provider di sicurezza ...**, e inserire i valori appropriati. Per ulteriori informazioni, fare clic su **Guida** nella finestra visualizzata.
4. Espandere la cartella **Provider Single Sign-On**, fare clic con il tasto destro del mouse su **Provider SSO Kerberos** e selezionare **Apri**.
5. Fare clic su **Abilita**, selezionare il provider di sicurezza e quindi fare clic su **Salva**. Non è necessario inserire altri dettagli in questo punto a meno che non si desideri utilizzare l'SSO (far sì che il provider sia semplicemente abilitato è sufficiente per consentire la ricerca del gruppo).

Importante: Affinché l'attività di ricerca del gruppo funzioni correttamente, il provider Kerberos che si configura qui deve essere uguale al provider configurato per IBM SPSS Statistiche Server. Nello specifico, devono essere in esecuzione all'interno dello stesso realm Kerberos. Quindi se un utente accede al server tramite SSO e lo identifica come jdoe@ibm.com (dove ibm.com è il realm), ci si aspetterà il provider di sicurezza in IBM SPSS Servizi di collaborazione e distribuzione per riconoscere quel nome principal utente e restituire l'appartenenza del gruppo corrispondente dalla directory LDAP.

Configurazione SSO per le origini dati

È possibile connettersi al database da IBM SPSS Statistiche utilizzando Single Sign-On. Se si desidera creare una connessione al database utilizzando Single Sign-On, è necessario prima utilizzare il software di gestione ODBC per configurare correttamente un'origine dati e token Single Sign-On. Quindi, quando ci si connette a un database in IBM SPSS Statistiche, IBM SPSS Statistiche utilizzerà quello stesso token Single Sign-On e all'utente non verrà richiesto di collegarsi all'origine dati.

Tuttavia, se l'origine dati non è stata configurata correttamente per Single Sign-On, IBM SPSS Statistiche richiederà all'utente di collegarsi all'origine dati. L'utente sarà ancora in grado di accedere all'origine dati dopo aver fornito le credenziali valide.

Per i dettagli completi sulla configurazione delle origini dati ODBC sul sistema con Single Sign-On abilitato, consultare la documentazione del fornitore del database. Di seguito è riportato un esempio della procedura generale che potrebbe essere interessata:

1. Configurare il proprio database in modo che possa supportare il Single Sign-On Kerberos.
2. Sulla macchina server, creare un'origine dati ODBC e testarla. La connessione DSN non deve richiedere un ID utente e una password.

3. Collegarsi al server utilizzando SSO (single sign - on) e iniziare ad utilizzare l'origine dati ODBC creata e validata al passo 2.

Autorizzazioni

Se non si utilizza l'autenticazione interna o l'autorizzazione di gruppo con single sign - on, il software server avvia un processo per l'utente finale, superando l'ID e la password dell'utente al sistema operativo. Il processo avviato ha i diritti di accesso al file del conto dell'utente finale. Un utente che si collega al software server deve effettuare il login con un account che disponga dei seguenti permessi:

- Autorizzazioni di lettura ed esecuzione per la directory di installazione del server e le sue sottodirectory
- Leggere, eseguire e scrivere le autorizzazioni alla posizione della directory per i file temporanei

Per l'autenticazione interna e il single sign - on, l'utente client di connessione dispone delle autorizzazioni assegnate all'utente che ha avviato il servizio / daemon.

È possibile utilizzare l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, che viene installata come parte di IBM SPSS Deployment Manager) per modificare la posizione predefinita dei file temporanei. Consultare le Locazioni File di argomento nella Guida per l'utente di *Deployment Manager* (inclusa nella guida per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni. È anche possibile modificare la posizione per singoli utenti o gruppi. Per ulteriori informazioni, consultare l'argomento IBM SPSS Statistics Server User Profiles and Groups, nel manuale *Deployment Manager User's Guide*.

Autorizzazioni - Permessi di livello

Per impostazione predefinita, il gruppo di amministratori per il software server è il gruppo amministratori per la macchina su cui è in esecuzione il software server. È possibile modificare il gruppo di amministratori per il software server specificandolo nella casella di testo del gruppo Admin nell'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, installata come parte di IBM SPSS Deployment Manager). Consultare l'argomento Utenti nella *Guida per l'utente di distribuzione* (incluso nell'help per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni. Se si utilizza l'autenticazione interna su UNIX, è possibile creare direttamente gli amministratori. Per ulteriori informazioni, consultare l'argomento [“Configurazione dell'autenticazione interna”](#) a pagina 22.

Autorizzazione del gruppo

È possibile configurare il software server per supportare l'autorizzazione del gruppo. Un'istanza separata del daemon/servizio viene eseguita per ogni gruppo di utenti autorizzato.

Configurazione autorizzazione del gruppo

1. Creare un'istanza server per ogni gruppo. Per ulteriori informazioni relative alla creazione delle istanze server, consultare [“Configurazione Istanze Multiple”](#) a pagina 17.
2. Creare i gruppi in IBM SPSS Servizi di collaborazione e distribuzione e assegnare gli utenti ai gruppi.
3. Aprire l'applicazione di amministrazione ed aggiornare il valore di **URL servizio Autorizzazione del gruppo** nell'URL per IBM SPSS Servizi di collaborazione e distribuzione. Accertarsi di includere il numero di porta (ad esempio, `http://myserver.mydomain.com:9080`).

Controllo accesso DNS per gruppo

L'autenticazione multi-fattore (MFA) richiede che gli utenti abbiano un insieme limitato di nomi di origine dati (DSN) a cui possono accedere in base al relativo gruppo di appartenenza.

1. Aprire l'applicazione di gestione e impostare **Limita accesso al database** su Yes.
2. Nel campo **Origini database consentite**, immettere un elenco di DNS separati da punto e virgola (;) che sono consentiti per l'accesso (ad esempio, `Fraud - Analytic;Fraud - Operational`).

Quando questa limitazione è abilitata, determina quanto segue:

- Quando un utente ricerca le origini dati nella procedura guidata database, invece di venirgli presentati tutti i DNS definiti sul sistema server, gli verrà visualizzato solo il sottoinsieme di DNS che sono definiti dall'applicazione di amministrazione. Considerare che il percorso può contenere DNS che non sono definiti sul server. Questi vengono ignorati e l'utente non vedrà questi nomi.
- Se un utente modifica la sintassi GET DATA /TYPE=ODBC che specifica un DSN che non è specificato dall'applicazione di gestione, la sintassi non verrà eseguita e all'utente verrà visualizzato un errore simile a **Accesso negato all'origine dati: < X>**.

Profili

Il software del server consente di creare profili per singoli utenti e gruppi di utenti. Questi profili e gruppi di utenti consentono di definire le impostazioni per gli utenti specifici.

Versioni client e server

A partire dalla versione 20.0.1, il software client non deve essere allo stesso livello di release del software del server a cui si connette. Ad esempio, il client 20.0.1 può connettersi al software del server 21 e il client 21 può connettersi al server 20.0.1. Nota che è possibile eseguire anche più versioni del software server su un computer server.

I livelli di rilascio della miscelazione sono consentiti solo per semplificare gli aggiornamenti. I livelli di rilascio possono essere scagliati durante il periodo di aggiornamento e i client non devono essere aggiornati contemporaneamente. Tuttavia, non si consiglia di mantenere questa configurazione per un lungo periodo. Se il server è più recente del client, potrebbe creare un output che non può essere letto dal client. Se il client è più recente del server, la sintassi inoltrata dal client potrebbe non essere riconosciuta dal server. Pertanto, è necessario aggiornare il software client o server al più presto, a seconda di quale uno scorre l'altro.

Quando si distribuiscono le informazioni di connessione agli utenti finali, tenere presente quale versione del software client sono in esecuzione ed essere sicuri di avere le informazioni di connessione per una versione server corrispondente.

Connessione utenti tramite un Firewall

Se si utilizza un **firewall** per mantenere la rete sicura dagli intrusi, è possibile configurare il proprio firewall e il software server in modo che gli utenti finali al di fuori del firewall possano collegare il client al software server. Il tuo firewall può utilizzare **NAT** (Network Address Translation), ma non è richiesto.

Lo scenario tipico per la connessione degli utenti finali attraverso un firewall che utilizza NAT è il seguente:

1. L'utente finale connette l'applicazione client al software server utilizzando l' **IP mascherato** (l'indirizzo IP che NAT presenta al mondo esterno) e il numero di porta del server. Ad esempio, l'utente finale si connette con IP 10.10.10.2 e numero porta 3016.
2. Il firewall consente la connessione in quanto è stato configurato per accettare connessioni dall'IP mascherato.
3. Il firewall reindirizza l'IP mascherato al vero IP interno del server. Consente la connessione perché la porta (ad esempio, 3016) è abilitata sul firewall.
4. Il server svela un processo per la connessione client dell'utente finale e lo assegna un numero di porta dall'elenco nella variabile ambiente di sistema STATISTICS_CLIENT_PORTS. Ad esempio, il processo comunica attraverso la porta 3287.
5. Il firewall consente la comunicazione tramite quella porta (ad esempio, 3287) perché è abilitata sul firewall.

Configurazione delle connessioni tramite un firewall

Introduzione

IBM SPSS Statistiche Server re - utilizza lo stesso numero di porta per le connessioni client. Ciò significa che solo due porte devono essere aperte attraverso il firewall: il daemon SPSS Statistiche o la porta di ascolto (impostata per default su 3028, sebbene possa essere alterata se necessario) e la porta di risposta attraverso la quale i client SPSS Statistiche parlano ai propri processi child SPSS Statistiche Server.

Nota: Il riutilizzo della porta è legato alla capacità di ricollegamento del client. Per impostazione predefinita, il client - ricollegarsi è abilitato per 100 seconds minuti. Quando il client - ricollegarsi è abilitato, SPSS Statistiche Server ha un rapporto 1: 1 di client connessi per aprire le porte di risposta. Per consentire il riutilizzo della porta è necessario prima disabilitare il client - ricollegarsi. Questa operazione viene eseguita modificando l'impostazione **reconnect-timeout** in <Statistics Install Path>/config/statisticsd.conf. Ad esempio:

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

In un ambiente con molte possibili connessioni client-server, è possibile configurare più di una porta di risposta client. Quando un client SPSS Statistiche è in fase di connessione al SPSS Statistiche Server, la porta client è sostanzialmente bloccata e può essere utilizzata da un solo client fino a quando il processo di connessione non avrà concluso. Il tempo di connessione è compreso nell'intervallo di 1 - 3 seconds (questo tempo può variare a seconda del carico di sistema). Quando un secondo o terzo client SPSS Statistiche tenta di connettersi durante questo tempo, i client vengono bloccati fino a quando la porta client diventa disponibile. L'apertura di più porte client riduce il tempo di attesa durante la connessione in un ambiente in cui molti utenti avviano contemporaneamente le sessioni SPSS Statistiche .

Esempio

Supporre che cinque porte client siano elencate nella variabile di ambiente di sistema

STATISTICS_CLIENT_PORTS (porte 40001 - 40005) e che vi siano quattro possibili client. Un utente avvia una connessione con SPSS Statistiche Server e il primo contatto viene effettuato tramite la porta di ascolto (3028). Il server svela un processo child e continua la comunicazione attraverso la prima porta client disponibile (4001). Se la porta 40001 non è bloccata (perché la comunicazione con un altro client è appena iniziata), la porta verrà riutilizzata. Se la porta 40001 è bloccata, la comunicazione si sposta sulla porta successiva (4002), ipotizzando che non sia bloccata, e così via.

Dopo che tutti e quattro i client sono connessi, molto probabilmente tutti utilizzano lo stesso numero di porta (40001). C'è una piccola possibilità che uno o più clienti utilizzino la porta 40002, una possibilità minore che un client utilizzi la porta 40003, e una possibilità ancora più piccola che uno o più clienti utilizzino la porta 40004. Non c'è alcuna possibilità che un client utilizzi la porta 40005 perché ci sono solo quattro client e l'algoritmo inizia al primo numero di porta disponibile che è elencato nella variabile di ambiente di sistema **STATISTICS_CLIENT_PORTS** .

Esistono due metodi consigliati per la configurazione delle connessioni SPSS Statistiche Server tramite un firewall.

Configurare il firewall per consentire i processi

Utilizzando il software firewall, assicurarsi che i seguenti processi siano autorizzati ad accettare connessioni di rete.

statisticsproc.exe

Il processo **statisticsproc.exe** si apre, chiude e riutilizza le porte di risposta (o porte definite in **STATISTICS_CLIENT_PORTS**).

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

Il processo è il principale servizio Windows o UNIX/Linux e gestisce la porta di ascolto.

Fornire l'accesso ai processi consente efficacemente qualsiasi porta che il processo utilizzerà.

Nota: Le seguenti condizioni si applicano quando il valore di timeout di riconnessione è maggiore di 0 e `statisticsproc.exe` è consentito accettare connessioni di rete:

- `STATISTICS_CLIENT_PORTS` è irrilevante, tranne che per la diagnostica. Qualsiasi porta può essere utilizzata.
- Non esiste alcun limite al numero di connessioni a meno che le porte non siano definite in `STATISTICS_CLIENT_PORTS`. Il numero di porte `STATISTICS_CLIENT_PORTS` definite limita effettivamente le porte che SPSS Statistiche Server utilizzerà.

Configurare il firewall aprendo manualmente le porte

Per configurare manualmente il software server e il firewall, seguire questi passaggi:

1. Installare il software server come di consueto. È necessario conoscere l'indirizzo IP del computer su cui è installato il server e il numero di porta che il software server utilizza per le comunicazioni. Ad esempio, installare il server su `202.123.456.78` sulla porta di ascolto `3028`.
2. Configurare la variabile di ambiente del sistema `STATISTICS_CLIENT_PORTS` specificando almeno un numero di porta. La variabile di ambiente elenca le porte utilizzate per continuare le connessioni client con il server (porte **RESPONSE**). Se necessario, è possibile specificare un elenco delimitato da virgole e un intervallo di porte (ad esempio, `4001, 4002, 4003-4005`).

Importante:

- Quando si imposta il timeout di ricollocazione automatica su un valore superiore a 0, `STATISTICS_CLIENT_PORTS` definisce il numero massimo di connessioni client e server simultaneamente consentito.
- Non elencare la porta **LISTEN** (`3028`) nella variabile di ambiente `STATISTICS_CLIENT_PORTS`.

Microsoft® Windows™

Utilizzare le proprietà di Windows System per creare e configurare la variabile di ambiente. Consultare [“Proprietà di sistema”](#) a pagina 53 per le istruzioni.

UNIX

Modificare lo script di ambiente del software server, `statsenv.sh`, incluso nella sottodirectory `/bin` della directory di installazione. Definire la porta che può essere utilizzata dai processi client che il server avvia. Ad esempio, aggiungere le seguenti righe:

```
STATISTICS_CLIENT_PORTS=4001
export STATISTICS_CLIENT_PORTS
```

3. Quando si utilizza NAT (Network Address Translation), creare e mappare IP. Utilizzando il software firewall, creare un IP mascherato per uso esterno e associarlo all'IP interno del server. Ad esempio, creare un IP mascherato `10.10.10.2` e associarlo a `202.123.456.78`.
4. Utilizzando il software firewall, abilitare i numeri di porta sul firewall:
 - Numero di porta **LISTEN** del server. Ad esempio, abilitare la porta `3028`.
 - I numeri di porta specificati nella variabile di ambiente `STATISTICS_CLIENT_PORTS`. Ad esempio, abilitare la porta `4001`.
5. Distribuire le informazioni di connessione agli utenti che si connettono al software server dall'esterno del firewall.
 - Se utilizzato, l'IP mascherato del computer su cui è installato il software server (non distribuiamo l'IP interno del server). Ad esempio, distribuire `10.10.10.2` come IP del server.
 - Distribuire il numero di porta del software del server come di consueto. Ad esempio, distribuire `3028` come numero di porta **LISTEN** del server.

Connessione utenti con PPTP

Gli utenti finali possono collegare un computer client remoto al software server analitico con **Point - to - Point Tunneling Protocol (PPTP)**. PPTP è un protocollo di networking che supporta le reti private virtuali multiprotocollo (VPN). Consente agli utenti finali remoti di accedere alla propria rete in modo sicuro su Internet.

Per utilizzare le connessioni PPTP:

1. **Configurare un server di accesso remoto per PPTP.** Assicurarsi di creare sufficienti indirizzi IP per i client perché il software server supporta più connessioni client. Ogni connessione client richiede il proprio indirizzo IP.
2. **Configurare il computer desktop client.** Utilizzare il pannello di controllo di rete di Windows per aggiungere una connessione di rete privata tramite PPTP. Inserire un indirizzo IP che il server di accesso remoto riconoscerà come connessione PPTP.
3. **Abilita la connessione PPTP sul computer desktop client.** Quando gli utenti finali desiderano collegarsi al software server da una postazione remota, consentono la connessione PPTP e quindi utilizzano il software client per connettersi al server come di consueto.

Utilizzo di SSL per il trasferimento sicuro dei dati

SSL (Secure Sockets Layer) è un protocollo per la codifica dei dati trasferiti tra due computer. SSL assicura che la comunicazione tra i computer sia protetta. SSL può crittografare l'autenticazione di un nome utente/password e il contenuto di uno scambio tra un server e un client.

Nota: Dalla versione 30.0.0 in poi, SSL è obsoleto e gli utenti devono utilizzare GSKit.

Come funziona il protocollo SSL

SSL si basa sulle chiavi pubbliche e private del server, oltre a un certificato di chiave pubblica che collega l'identità del server alla relativa chiave pubblica.

1. Quando un client si connette a un server, il client autentica il server con il certificato di chiave pubblica.
2. Il client genera quindi un numero random, lo crittografa con la chiave pubblica del server e invia il messaggio crittografato al server.
3. Il server decrittografa il numero random tramite la chiave privata.
4. Dal numero random, sia il server sia il client creano le chiavi di sessione utilizzate per crittografare e decrittografare le informazioni successive.

Il certificato di chiave pubblica viene firmato solitamente 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 sintesi l'autorità di certificazione conferma l'identità del server. Solitamente l'autorità di certificazione applica una tariffa per l'emissione di un certificato, ma è possibile generare anche certificati autofirmati.

Abilitazione SSL tramite GSKit

Protezione client/server e comunicazioni server - server con GSKit

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. Abilitare e configurare un file di configurazione specificato nella directory di installazione di IBM SPSS Statistiche Server.

Nota: IBM SPSS Statistiche Server supporta il protocollo TLSv1.2 . GSKit attualmente non supporta altre versioni.

3. Se si utilizzano i certificati di crittografia con una forza maggiore di 2048, installare la crittografia a forza illimitata sui computer client.
4. Informare gli utenti finali che è necessario abilitare SSL quando ci si connette al server.

Nota: può capitare talvolta che un server si comporti come un client. Un esempio è IBM SPSS Statistiche Server che si connette al IBM SPSS Repository dei servizi di collaborazione e distribuzione. In questo caso, IBM SPSS Statistiche Server è il *client*.

Ottenere e installare il certificato e le chiavi SSL

I primi passi da seguire per configurare il supporto SSL sono:

1. Ottenere un file di chiave e un file certificato SSL. Ci sono vari modi in cui puoi fare questo:
 - Acquistarli da un'autorità di certificazione pubblica (come VeriSign, Thawte o Entrust). L'autorità di certificazione (CA) pubblica firma il certificato per controllare il server che lo utilizza.
 - Ottenere i file chiave e certificati da un'autorità di certificazione di terze parti. Se questo approccio viene assunto, il certificato root *.pfx di CA di terze parti deve essere importato nel file di memorizzazione chiave del server (spiegato qui sotto).
 - Generare i file della chiave e di certificato con un'autorità di certificazione autofirmata interna. I passi per effettuare ciò sono:
 - a. Preparare un database delle chiavi. Per ulteriori informazioni, consultare l'argomento [“Creazione di un database delle chiavi SSL”](#) a pagina 35.
 - b. Creare il certificato autofirmato. Per ulteriori informazioni, consultare l'argomento [“Creazione di un certificato SSL autofirmato”](#) a pagina 36.
2. Per i certificati CA (Certificate Authority) o autofirmati, copiare i file .kdb e .sth dal passo 1 in una directory a cui il Server IBM SPSS Statistiche ha accesso e specificare il percorso a tale directory nel file `statisticsd.conf`. Il file `statisticsd.conf` si trova in `<Statistics Server installation directory>/config/`; per i certificati di terze parti, copiare i file .pfx e .sth dal passo 1.
3. Impostare i seguenti parametri nel file `statisticsd.conf`:

Per l'autorità di certificazione (CA) o un autocertificazione:

- `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, dove `<value>` è 0 o 1 che indica se abilitare GSKit.
- `<gsk-keystore desc="GSKSSL Key store database filename." value="<filename>.kdb"/>`, dove `<filename>` è il nome del file di database delle chiavi.
- `<gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>`, dove `<filename>` è il nome del file stash della password del database delle chiavi.
- `<gsk-cert-label desc="GSKSSL certificate label." value=""/>`, dove `<label>` è l'etichetta del tuo certificato.

Per certificati di terze parti:

- `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, dove `<value>` è 0 o 1 che indica se abilitare GSKit.
- `<gsk-keystore = "<*.pfx_file_location>"`, dove `<*.pfx_file_location>` è la posizione e il nome del file certificato root *.pfx.
- `<gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>`, dove `<filename>` è il nome del file stash della password del database delle chiavi.
- `<gsk-cert-label desc="GSKSSL certificate label." value=""/>`, dove `<label>` è l'etichetta del tuo certificato.

4. Per certificati di terze parti:

- a. Estrarre il file `root.pem` dal file `*.pfx`, utilizzando come esempio il seguente comando GSK:

```
gsk8capiCmd_64.exe -cert -extract -db C:\SSL\<certificate_name>.pfx -stashed -label
<cert-certificate_issuing_server.com> -target C:\SSL\root.pem
```

- b. Copiare `root.pem` nella cartella `C:\ProgramData\IBM\SPSS\certificates` (Windows) o `/Library/Application Support/IBM/SPSS/certificates` (macOS) sul client.
 - c. Sul client, impostare la connessione utilizzando il nome del dominio completamente qualificato (ad esempio `cert-certificate_issuing_server.com`) " nel campo **Nome server** e abilitare l'opzione **SSL**.
5. Per i certificati autofirmati installare il certificato sui sistemi client. Per i certificati CA pubblici o di terze parti, questo passo non è richiesto. Verificare che le autorizzazioni di accesso vietino l'accesso casuale alla directory che contiene il certificato. Per ulteriori informazioni, consultare l'argomento ["Installazione di un certificato SSL autofirmato"](#) a pagina 36.

Configurazione dell'ambiente per l'esecuzione di GSKit

GSKCapiCmd è uno strumento della riga comandi non basato su Java e Java™ non deve essere installato sul sistema per utilizzare questo strumento; si trova nella cartella `<Statistics Server installation directory>/bin`. Il processo che configura il proprio ambiente per l'esecuzione di IBM Global Security Kit (GSKit) varia a seconda della piattaforma utilizzata.

Per configurare per Linux/Unix, aggiungere la directory delle librerie condivise `<Statistics Server installation directory>/lib` al tuo ambiente:

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

Il nome variabile del percorso della libreria condivisa dipende dalla propria piattaforma:

- Linux utilizza il nome variabile: `LD_LIBRARY_PATH`

Ad esempio, per impostare l'ambiente in Linux, utilizzare:

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

Accesso dell'account ai file

Accertarsi di concedere le autorizzazioni corrette per gli account che accederanno ai file SSL:

1. Per tutti gli account utilizzati da IBM SPSS Statistiche per la connessione, concedere l'accesso in lettura ai file SSL.

Nota: Ciò è valido anche per l'utente *Accedi come* definito nel servizio IBM SPSS Statistiche Server. In UNIX o Linux, si applica all'utente con cui viene avviato il server.

2. Per Windows, non è sufficiente che gli account siano contenuti nel gruppo Amministratori e che l'autorizzazione sia fornita a tale gruppo Amministratori quando UAC (User Access Control) è abilitato. Inoltre, è necessario eseguire una delle seguenti azioni:
 - Assegnare separatamente le autorizzazioni agli account.
 - Creare un nuovo gruppo, aggiungere gli account al nuovo gruppo ed assegnare al gruppo l'autorizzazione per l'accesso ai file SSL.
 - Disabilitare UAC.

Creazione di un database delle chiavi SSL

Utilizzare lo strumento GSKCapiCmd per creare il database delle chiavi. Prima di utilizzare lo strumento, è necessario configurare il proprio ambiente; consultare l'argomento ["Configurazione dell'ambiente per l'esecuzione di GSKit"](#) a pagina 35 per ulteriori informazioni

Per creare il database delle chiavi, eseguire GSKit e immettere il seguente comando:

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

dove <ver> è il numero di versione GSKit, <filename> è il nome che si desidera utilizzare per il file database delle chiavi e <password> è la password per il database delle chiavi.

L'opzione -stash crea un file stash nello stesso percorso di quello del database delle chiavi, con un'estensione file .sth. GSKit utilizza il file stash per ottenere la password del database delle chiavi in modo che non debba essere immessa sulla riga comandi ogni volta.

Nota: Si consiglia di utilizzare una protezione efficace del file system sul file .sth.

Creazione di un certificato SSL autofirmato

Per generare un certificato autofirmato e memorizzarlo nel database delle chiavi, utilizzare il seguente comando:

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

dove <ver> è il numero di versione GSKit, <filename> è il nome del file di database delle chiavi, <Number of days certificate is valid> è il numero fisico di giorni in cui il certificato è valido e <label> è un'etichetta descrittiva che consente di identificare il file (ad esempio, si potrebbe utilizzare un'etichetta come: myselfsigned).

Installazione di un certificato SSL autofirmato

Per le macchine client che si connettono al server utilizzando SSL, è necessario distribuire la parte pubblica del certificato ai client in modo che possa essere memorizzata nei loro database delle chiavi. A tal fine, effettuare i seguenti passi:

Nota: saltare questo passaggio se si sta utilizzando un certificato firmato da un'autorità di certificazione. Se si utilizza un certificato autofirmato, è necessario copiare l'autorità di certificazione attendibile sui computer client. Si ricordi che un computer server potrebbe fungere anche da client. Un esempio è IBM SPSS Statistiche Server che si connette a IBM SPSS Repository dei servizi di collaborazione e distribuzione. In tal caso, il server IBM SPSS Statistiche è il client ed è pertanto necessario copiare il certificato per il server IBM SPSS Repository dei servizi di collaborazione e distribuzione sul server IBM SPSS Statistiche .

1. Estrarre la parte pubblica in un file utilizzando il seguente comando:

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

2. Distribuire root .pem sui client. Se si dispone di più autorità di certificazione attendibili, copiarle in un singolo file root .pem. Le autorità di certificazione attendibili sono file di testo, per cui è possibile copiare e incollare il certificato o i certificati. Copiare root .pem nella seguente posizione sui computer client. Se nel client è già stato copiato un file root .pem per un altro prodotto IBM, accodare le informazioni sull'autorità di certificazione root attendibile dalla propria autorità nel file root .pem esistente. Per impostazione predefinita, tutti i prodotti client IBM ricercano in questo percorso i file di certificato autofirmati attendibili. Se si desidera utilizzare un'altra posizione, creare una variabile di ambiente SSL_CERT_DIR e impostare il valore della variabile nella posizione.

- Windows 7 e versioni successive: C:\ProgramData\IBM\SPSS\certificates
- Mac: /Library/Application Support/IBM/SPSS/certificates
- UNIX e Linux: /opt/IBM/SPSS/certificates

Configurazione dei certificati client

Quando SPSS Server di statistiche è configurato per utilizzare una connessione SSL e si sta utilizzando un'autocertificazione, è necessario copiare e configurare l'autorità di certificazione attendibile a tutte le workstation client.

Un esempio sarebbe quando IBM SPSS Servizi di collaborazione e distribuzione inoltra un lavoro a SPSS Server di statistiche (che è SSL abilitato). In questa situazione, IBM SPSS Servizi di collaborazione e distribuzione è il client. L'autorità di certificazione attendibile (`root.pem` sul SPSS Server di statistiche) deve essere copiata e configurata su tutte le macchine IBM SPSS Servizi di collaborazione e distribuzione.

Configurazione dei file certificato per IBM SPSS Servizi di collaborazione e distribuzione

Il supporto IBM SPSS Servizi di collaborazione e distribuzione può essere distribuito su un server delle applicazioni Web (ad esempio, EAP JBoss IBM WebSphere e RedHat).

Il primo passo nella configurazione dei file certificati per il supporto IBM SPSS Servizi di collaborazione e distribuzione è quello di richiamare il file SPSS Server di statistiche `root.pem` dal proprio amministratore.

Il processo di configurazione del certificato SSL dipende da quale Web Application Server è impiegato.

IBM WebSphere e RedHat JBoss EAP

Le istruzioni riportate di seguito si applicano a IBM WebSphere e RedHat JBoss EAP.

RedHat JBoss EAP - Nota: Quando l' SPSS Server di statistiche utilizza IBM GSKit SSL, è necessario utilizzare il JDK IBM quando si configura IBM SPSS Servizi di collaborazione e distribuzione su JBoss EAP.

1. Distribuire il file `root.pem` alla macchina IBM SPSS Servizi di collaborazione e distribuzione Server. Se si dispone di più autorità certificate attendibili, copiarle in un singolo file `root.pem` (le autorità certificate attendibili sono file di testo, così è possibile copiare e incollare i certificati) Copia `root.pem` nella seguente posizione su IBM SPSS Servizi di collaborazione e distribuzione Server.

Se hai già copiato un file `root.pem` al client per un altro prodotto IBM, accodare le informazioni sull'autorizzazione del certificato root attendibile dalla tua autorizzazione al file `root.pem` esistente. Creare una variabile di ambiente `SSL_CERT_DIR` e impostare il valore della variabile nella posizione server desiderata che contiene il file `root.pem`.

2. Verificare che IBM SPSS Servizi di collaborazione e distribuzione Server utente aggiunga la variabile di ambiente `SSL_CERT_DIR`.

Nota: Il server IBM SPSS Servizi di collaborazione e distribuzione deve essere riavviato dopo l'aggiunta della variabile di ambiente.

Installazione della crittografia "Unlimited strength"

Nel Java Runtime Environment, fornito con il prodotto, è attivata la cosiddetta crittografia "US export-strength". Per una maggiore protezione dei dati, si consiglia l'aggiornamento alla crittografia "Unlimited strength".

1. Estrarre i file di Unlimited Jurisdiction Policy che sono impacchettati nel file compresso. Il file compresso contiene un file `US_export_policy.jar` ed un file `local_policy.jar`.
2. Sostituire le copie esistenti dei file `US_export_policy.jar` e `local_policy.jar` con i due file scaricati ed estratti.

Istruzione agli utenti per l'attivazione di SSL

Quando gli utenti si connettono al server tramite un prodotto client, devono attivare SSL nella finestra di dialogo per connettersi al server. Assicurarsi di comunicare agli utenti la casella di controllo appropriata da selezionare.

Abilitazione SSL utilizzando OpenSSL

Sicurezza delle comunicazioni client/server e server-server con OpenSSL

Nota: Dalla versione 30.0.0 in poi, Open SSL 1.1 è deprecato.

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

1. Installare OpenSSL sul server.
2. Ottenere e installare il certificato e le chiavi SSL.
3. Abilitare e configurare SSL nell'applicazione di amministrazione del server (IBM SPSS Deployment Manager).

Nota: IBM SPSS Statistiche Server supporta il protocollo TLSv1 . Il protocollo SSLv3 risulta avere una vulnerabilità della sicurezza e non deve essere utilizzato.

4. Se si utilizzano i certificati di codifica superiore a 2048 bit, installare le codifica unlimited strength sui computer con client .
5. Se si utilizza un certificato autofirmato, copiare il certificato sul computer client.
6. Informare gli utenti finali che è necessario abilitare SSL quando ci si connette al server.

Nota: può capitare talvolta che un server si comporti come un client. Un esempio è IBM SPSS Statistiche Server che si connette al IBM SPSS Repository dei servizi di collaborazione e distribuzione. In questo caso, IBM SPSS Statistiche Server è il *client*.

Installazione di OpenSSL

Se sul server non è già disponibile OpenSSL, è necessario installarlo.

1. Scaricare OpenSSL da <http://www.openssl.org/>. Assicurarsi di utilizzare la versione di OpenSSL adatta alla versione del server:

Prodotto server	Versione OpenSSL compatibile
IBM SPSS Statistiche 29	1.1.1f o successivi
IBM SPSS Statistiche 28	1.1.1f o successivi
IBM SPSS Statistiche 27.0.1	1.1.1f o successivi Nota: Il supporto per il protocollo SSLv3 insicuro è stato obsoleto.
IBM SPSS Statistiche 26-27	1.0.2 o versioni successive
IBM SPSS Statistiche 24-25	1.0.1f o successivi
IBM SPSS Statistiche 20-23	1.0.0
IBM SPSS Statistiche 17-19 (no Linux® su System z®)	0.9.8 e le relative sottoversioni (0.9.8a, 0.9.8b e così via)
IBM SPSS Statistiche 19 (Linux® su System z®)	1.0.0

2. Seguire le istruzioni per l'installazione e la configurazione del software. Si consiglia di creare da soli OpenSSL , con le seguenti linee guida:

Windows. OpenSSL deve essere creato con DLL (che sono multithread di default).

UNIX. OpenSSL deve supportare i thread multipli (tale supporto non è sempre di default) e le librerie condivise.

3. Assicurarsi che i moduli OpenSSL siano inclusi nel percorso di sistema.

Nota: Se esiste più di una versione dei moduli OpenSSL sul computer server, copiare i moduli OpenSSL per IBM SPSS Statistiche Server nella directory in cui è installato IBM SPSS Statistiche Server.

Ottenere e installare il certificato e le chiavi SSL

1. Ottenere un file di chiave e un file certificato SSL. i metodi sono due:

- Acquistarli da un'autorità di certificazione pubblica (quale Comodo, Symantec, o GoDaddy) che firmerà i certificati per verificare il server che li utilizza. Questo rappresenta il metodo di migrazione consigliato.
- Generare i file di chiavi e certificato con un'autorità di certificazione firmata autonomamente. OpenSSL fornisce uno strumento di gestione certificati adatto allo scopo. In alternativa, ricercare su Internet le istruzioni per creare un certificato SSL autofirmato.

2. Copiare il file o i file della chiave e del certificato in una directory locale o nelle directory sul server. È possibile archiviare chiavi pubbliche e private in directory separate. Possono anche essere archiviate in un unico file. Assicurarsi che la chiave privata non si trova in una posizione che potrebbe essere riscontrata durante la consultazione casual del file system.

3. Copiare l'autorità di certificazione attendibile denominata *root.pem* nel seguente percorso sul computer del server. Se si desidera utilizzare un altro percorso, creare una variabile di ambiente `SSL_CERT_DIR` ed impostarne il valore sul percorso.

Windows 7 e versioni successive: `C:\ProgramData\IBM\SPSS\certificates`

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

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

Abilita e configura SSL in IBM SPSS Deployment Manager

1. Avviare l'applicazione di gestione del server (IBM SPSS Console di amministrazione statistiche, installata come parte di IBM SPSS Deployment Manager) ed effettuare la connessione al server.

2. Nella pagina di configurazione, impostare **SSL** su Yes.

3. In **File di chiave pubblica SSL**, specificare il percorso completo al file della chiave pubblica.

4. In **File di chiave privata SSL**, specificare il percorso completo al file della chiave privata.

Nota: se la chiave pubblica e privata sono archiviate in un solo file, specificare lo stesso file in **File di chiave pubblica SSL** e **File di chiave privata SSL**.

5. Dai menu, scegliere:

File > Salva

6. Riavviare il servizio o il daemon server. Al riavvio, verrà richiesta la password SSL. In Windows, è possibile selezionare **Memorizza password** per archiviare la password in modo sicuro. Questa opzione elimina la necessità di inserire la password ogni volta che il server viene avviato.

Installazione della crittografia "Unlimited strength"

Nel Java Runtime Environment, fornito con il prodotto, è attivata la cosiddetta crittografia "US export-strength". Per una maggiore protezione dei dati, si consiglia l'aggiornamento alla crittografia "Unlimited strength".

1. Estrarre i file di Unlimited Jurisdiction Policy che sono impacchettati nel file compresso. Il file compresso contiene un file `US_export_policy.jar` ed un file `local_policy.jar`.

2. Sostituire le copie esistenti dei file `US_export_policy.jar` e `local_policy.jar` con i due file scaricati ed estratti.

Copia del file di certificato ai computer client

Nota: saltare questo passaggio se si sta utilizzando un certificato firmato da un'autorità di certificazione.

Se si utilizza un certificato autofirmato, è necessario copiare l'autorità di certificazione attendibile sui computer *client*. Si ricordi che un computer server potrebbe fungere anche da client. Un esempio è IBM SPSS Statistiche Server che si connette al IBM SPSS Repository dei servizi di collaborazione e distribuzione. In questo caso, il server IBM SPSS Statistiche rappresenta il *client* ed è pertanto necessario copiare il certificato del server di IBM SPSS Repository dei servizi di collaborazione e distribuzione sul server di IBM SPSS Statistiche.

1. Creare un'autorità di certificazione attendibile denominata *root.pem*. Ad esempio, se si stava creando l'autorità di certificazione attendibile con OpenSSL, utilizzare lo switch `-out` per specificare il file di output come *root.pem*. Se si dispone di più autorità di certificazione attendibili, copiarle in un singolo file *root.pem*. Le autorità di certificazione attendibili sono file di testo, pertanto è possibile copiare e incollare il certificato o i certificati.
2. Copiare *root.pem* nella seguente posizione sui computer client. Se un file *root.pem* è già stato copiato sul client per un altro prodotto IBM Corp., accodare le informazioni sull'autorità di certificazione root attendibile dalla propria autorità al file *root.pem* esistente. Per impostazione predefinita, tutti i prodotti client IBM Corp. ricercano i file dei certificati autofirmati attendibili in questa ubicazione. Se si desidera utilizzare un altro percorso, creare una variabile di ambiente `SSL_CERT_DIR` ed impostarne il valore sul percorso.

Windows 7 e versioni successive: `C:\ProgramData\IBM\SPSS\certificates`

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

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

Istruzione agli utenti per l'attivazione di SSL

Quando gli utenti si connettono al server tramite un prodotto client, devono attivare SSL nella finestra di dialogo per connettersi al server. Assicurarsi di comunicare agli utenti la casella di controllo appropriata da selezionare.

Impostazione di una Locale

Il software server e il client che si connette deve essere eseguito nella stessa serie di caratteri, codifica e locale. Il software server ottiene il suo locale dal client. Per impostazione predefinita, questo è il locale *system* del client. Tuttavia, il client può sovrascrivere il default per elaborare file di dati in altre località. Sovrascrivendo il default, l'utente istruisce il software server da eseguire in un locale specificato senza modificare il locale di sistema del client.

Sintassi

L'utente sovrascrive il default utilizzando il comando di sintassi `SET LOCALE` :

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

`localeid` è una stringa che identifica il locale in cui verrà eseguito il software server. `SET LOCALE` scrive una voce di registro sulla macchina client. Questa voce persiste in modo che la prossima volta IBM SPSS Statistiche sia avviata sulla macchina client, IBM SPSS Statistiche eseguirà in quel locale.

La convenzione di denominazione per il locale ID può differire tra piattaforme e fornitori. Pertanto, esiste un file XML installato con il server che associa le località 'client alle località' del server. Questo file, *loclmap.xml*, si trova nella directory di installazione del server su Windows e nella sottodirectory */bin* su UNIX.

loclmap.xml

L'elemento root in *loclmap.xml* è il seguente. L'elemento root identifica anche la posizione dello schema.

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

L'elemento root contiene `<client-locale>` elementi con un attributo `name` che identifica il locale client. Gli elementi `<client-locale>` contengono uno o più elementi `<server-locale>`. Ogni elemento `<server-locale>` ha un attributo `name` che identifica un locale server che corrisponde al locale client. Il software server traduce l'ID locale del client in uno che può essere utilizzato sulla macchina server. Controlla ogni locale del server in ordine, fino a trovarne uno valido sulla macchina server.

Nessuna delle locale del server predefinite in *loclmap.xml* è locale di Windows. Le localine del sistema Windows generalmente non sono necessarie perché il software server cerca per la prima volta di utilizzare lo stesso locale del locale del client. Un server Windows dovrebbe avere il locale che corrisponde al locale client. Tuttavia, è possibile aggiungere le locale del server Windows a *loclmap.xml* se è necessario sostituire una locale Windows diversa ma simile.

È possibile modificare *loclmap.xml* in base alle necessità. Basta essere consapevoli che i propri elementi XML devono convalidare lo schema.

Esempio

Di seguito è riportato un esempio del contenuto di *loclmap.xml*:

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

In questo caso, se l'utente emette `SET LOCALE="French"`, il software server verifica prima `fr_FR.cp1252`. Considerare il caso di un server AIX. Il locale `fr_FR.cp1252` non funziona su AIX, quindi il software server continua la verifica fino a quando non raggiunge `fr_FR.windows-1252`, che funziona su AIX.

Utilizzo di un Server Locale

Se l'utente inoltra `SET LOCALE` utilizzando un ID locale del server non riconosciuto sulla macchina client, la macchina client utilizza *loclmap.xml* per trovare l'ID locale del client associato a un ID locale del server. Scrive questo ID locale al registro. Ad esempio, se l'utente emette `SET LOCALE="fr_FR.windows-1252"`, French viene scritto nel registro. Per vedere quale voce in *loclmap.xml* si applica al client, è possibile eseguire il comando `SHOW LOCALE` in modalità locale.

Problemi potenziali

Attenzione che utilizzare il comando `SET LOCALE` può causare problemi funzionali in alcuni casi:

- I nomi delle variabili correnti potrebbero non essere legali nella nuova pagina del codice.
- Le corrispondenze dei nomi insensibili potrebbero fallire. Il guasto potrebbe verificarsi perché le stringhe vengono convertite in caratteri maiuscoli in maiuscolo / minuscolo corrisponde (ad esempio, quando si confronta i nomi variabili). Se il locale è errato, questa conversione cambierebbe il carattere (ad esempio nella pagina del codice europeo centrale, 1250).

- Alcuni byte potrebbero essere interpretati erroneamente come i byte di piombo, e potrebbe verificarsi un problema a causa di un byte di scia inaspettato.
- SET LOCALE non modifica il locale di sistema del client. Pertanto, se il locale IBM SPSS Statistiche associato a SET LOCALE è diverso dal locale di sistema del client, ci saranno problemi di visualizzazione in vari luoghi. In questa situazione, anche un utente non è in grado di utilizzare un IME (Input Method Editor) per inserire caratteri nazionali.
- Il locale IBM SPSS Statistiche, l'impostazione OLANG e la codifica utilizzata per i dati devono essere compatibili. In caso contrario, l'output potrebbe essere inutilizzabile e illeggibile.

Connessione al Software del server

L'utente finale si connette al software del server collegando dall'applicazione client. Per effettuare il login un utente finale ha bisogno delle seguenti informazioni:

- **Nome computer o indirizzo IP.** Quando gli utenti terminano la connessione al software server, si collegano dall'applicazione client. Per farlo, devono specificare correttamente il nome del computer che esegue il software server. Il computer server può essere identificato da un nome alfanumerico (ad esempio, myserver) o da un indirizzo IP assegnato al computer server (ad esempio, 202.123.456.78), a seconda della scelta. Se si configurano i computer desktop del server e del client per utilizzare SSL (Secure Sockets Layer), l'utente finale deve utilizzare un nome dominio completo (ad esempio, myserver.mycompany.com).
- **Numero porta.** Gli utenti finali devono specificare correttamente la porta su cui il software server è in ascolto delle connessioni. Il numero di porta è quello predefinito per il server o qualunque sia stato specificato quando si è configurato il software server.
- **Nome dominio (solo Windows).** Gli utenti finali possono anche dover specificare un nome di dominio. Un nome di dominio è richiesto solo quando il computer server è in un dominio diverso rispetto ai computer desktop di fine utente.
- **ID utente e password.** Gli utenti finali sono tenuti ad accedere al computer server. Per fare questo, gli utenti hanno bisogno di un account valido, con autorizzazioni appropriate, per il computer su cui è in esecuzione il software server.
- **SSL (Secure Socket Layer).** Se si utilizza SSL per crittografare le comunicazioni che si verificano quando gli utenti finali si connettono al software del server, indicare agli utenti di abilitare SSL quando impostano la connessione server. I client non hanno bisogno di sapere quale protocollo SSL viene utilizzato dal server. Il software client proverà entrambi e userà quello che funziona.

Accesso ai dati e ai file

Quando gli utenti finali si collegano al software di sever analytic, la loro visualizzazione delle origini dati e dei file è dalla prospettiva del computer server, non dei loro computer desktop.

- **Origini dati ODBC.** Se gli utenti finali hanno bisogno di accedere alle origini dati ODBC definite sul computer server, distribuire i nomi, le descrizioni e le informazioni di accesso per tali origini dati. Vedere [Capitolo 3, "Accesso ai dati"](#), a pagina 9 per una discussione di accesso al database dal software server.
- **Accesso file.** Distribuire i nomi e le posizioni dei file presenti sul computer server che si desidera che gli utenti finali accedi. Per ulteriori informazioni, consultare l'argomento ["Dati di riferimento"](#) a pagina 10.

Salvataggio di dati e file

Quando gli utenti finali salvano i file mentre sono connessi al software server, la posizione predefinita per il salvataggio è la directory da cui è stato aperto il file. In molti casi, questo è il computer desktop locale; tuttavia per i file di dati sarà spesso una posizione protetta da scrittura sul computer server. Dire agli utenti dove salvare i file di dati. Di solito, la posizione è la directory home dell'utente da qualche parte sulla tua rete.

Nota UNIX: indicare agli utenti finali di utilizzare la specifica file completa e le barre quando si salvano i file (ad esempio, `/public/myhome/myserverdata/data.sav`). Evitare di utilizzare il carattere di backslash nella directory UNIX e nelle riprese utilizzate con il software server.

Capitolo 6. Analisi e miglioramento delle prestazioni

Se è necessario migliorare le prestazioni del software server, fare riferimento a questo capitolo per varie strategie, spaziando dalle modifiche di configurazione agli aggiornamenti hardware. Prima di apportare queste modifiche, ottenere informazioni sulle prestazioni così si sa quali aree sono problematiche.

Forniamo anche una carta bianca che include ulteriori informazioni sul miglioramento delle prestazioni. Vai a <http://www.ibm.com/developerworks/spsdevcentral> e cerca il link a "Libri e articoli".

Acquisizione di informazioni sulle prestazioni

Per verificare le prestazioni, confronta l'utilizzo nelle seguenti aree quando il server non viene utilizzato a quando viene pesantemente utilizzato.

- Utilizzo disco
- utilizzo della CPU
- Utilizzo memoria
- Utilizzo della rete

Registrazione

L'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, installata come parte di IBM SPSS Deployment Manager) consente di configurare il software server per registrare le informazioni sulle prestazioni. Utilizzando il nodo **Performance Log Interval** è possibile specificare quanto spesso il software server scrive le informazioni sulle prestazioni al log. Consultare l'argomento Logging nella *Guida per l'utente di Deployment Manager* (incluso nella guida per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni. È inoltre possibile ottenere informazioni sulle prestazioni direttamente dal sistema operativo.

Acquisizione di informazioni sulle prestazioni su Windows

Su Windows è possibile ottenere informazioni sulle prestazioni utilizzando Performance Monitor.

Tabella 3. Informazioni sulle prestazioni di Windows

Ad area	Oggetto Windows Performance Monitor	Contatore Utile
Utilizzo disco	PhysicalDisk	% tempo inattività
Utilizzo CPU	Processore	% tempo processore
Utilizzo memoria	Memoria	Byte con commit
Utilizzo rete	Interfaccia di rete	Byte totali / sec per ogni istanza di interfaccia fisica (non l'interfaccia loopback MS TSP)

Acquisizione di informazioni sulle prestazioni su UNIX

Su UNIX ci sono vari comandi per ottenere informazioni sulle prestazioni, a seconda del fornitore.

Tabella 4. Informazioni sulle prestazioni UNIX

Ad area	Fornitore	Comando	Nota
Utilizzo disco	Linux	iostat -x	Controllare la colonna %util .
Utilizzo disco	AIX	iostat -d	Controllare la colonna %tm_actl .
Utilizzo CPU	Linux	in alto	Utilizzare il comando interattivo P per ordinare tramite l'utilizzo della CPU.
Utilizzo CPU	AIX	ps aux	Pipe al comando sort per ordinare dalla colonna %CPU .
Utilizzo CPU	Tutto	tempo di attività	Controllare la media di carico.
Utilizzo memoria	Linux	in alto	Utilizzare il comando interattivo M per ordinare tramite l'utilizzo della CPU.
Utilizzo memoria	AIX	ps aux	Pipe al comando sort per ordinare dalla colonna RSS .
Utilizzo rete	Tutto	netsat	Utilizzare gli switch -i e -s per informazioni.

Passo successivo

Dopo aver raccolto queste informazioni, è necessario essere in grado di identificare l'area o le aree problematiche. Le seguenti sezioni descrivono possibili soluzioni e consigli per ogni area.

Miglioramento dell'utilizzo del disco

Considerare quanto segue per migliorare l'utilizzo del disco.

Spazio. Consentire sufficiente spazio su disco. Ogni utente in genere ha bisogno di spazio su disco temporaneo pari al doppio della dimensione del file di dati (SAV) in uso (lo spazio necessario è compreso tra 1 e 2.5 volte). Un utente che ordina un file potrebbe avere bisogno di spazio temporaneo più di tre volte la dimensione del file. Ad esempio, se sei utenti simultanei accedono ad un file e due si ordinano in una volta, potrebbero avere bisogno di ben 17 volte la dimensione del file. In pratica non saranno all'utilizzo di picco contemporaneamente, quindi 12 volte la dimensione del file sarebbe sufficiente.

Hardware. Utilizzare dischi SCSI per la performance più rapida. Non utilizzare IDE.

Configurazione di sistema. Tieni i file temporanei su un mandrino separato. È anche possibile definire più posizioni di file temporanei utilizzando l'applicazione di amministrazione. Assicurarsi che ogni posizione sia su un mandrino separato. Se si utilizza RAID, utilizzare RAID0 per il file di file temporanei. La velocità dei file di scratch acquisita da RAID0 è preferita rispetto alla ridondanza acquisita da RAID1. Se la tua CPU non è un problema e il computer server esegue Windows, puoi anche comprimere la directory dei dati o i file di dati su disco. Non assegnare più memoria virtuale.

IBM SPSS Statistiche configurazione. Se la memoria non è un problema ma l'utilizzo del disco è, aumentare lo spazio di lavoro in IBM SPSS Statistiche per prestazioni più veloci. Prova a impostarlo dividendo la quantità di RAM sul computer server dal numero previsto di utenti contemporanee. Ad esempio, se il computer server ha 1 GB di RAM, impostare l'area di lavoro su 0.25 GB di RAM.

Directory file temporanei. Modificare le impostazioni del profilo utente o dei gruppi in modo che le directory dei file temporanei per ogni utente si trovino su diverse unità fisiche.

Compressione della cache. Se i tuoi utenti stanno costantemente lavorando con file di dati di grandi dimensioni (soprattutto se la dimensione dei file è maggiore della metà della RAM del server), provare la compressione della cache nell'applicazione di gestione.

Miglioramento dell'utilizzo della CPU

Considerare quanto segue per migliorare l'utilizzo della CPU:

Numero. Aggiungere altri processori. Se si desidera avvicinarsi alla velocità che un utente sperimenterebbe durante l'esecuzione di IBM SPSS Statistiche localmente, provare ad avere un solo processore per ogni due utenti simultanei. Inoltre utilizzare i processori che sono veloci come, o più veloci, il processore sul computer desktop. Ad esempio, se si prevede una media di quattro utenti simultanei, configurare il computer server con due processori veloci.

Hardware. Utilizzare processori veloci. Aggiungere alcuni processori davvero veloci è meglio che aggiungere molti slow. Se l'utilizzo della CPU è ancora un problema con i processori veloci, considerare l'aggiunta di più computer server al proprio sistema.

Ubicazioni file SAV e accesso. Se alcuni file vengono utilizzati spesso da molti utenti simultanei, considerare di spostare i file su più server per bilanciare il carico utente. Ad esempio, se *TestScores.sav* e *GPA.sav* sono entrambi fortemente utilizzati, collocarli su server separati. Controllare l'accesso ai file con le autorizzazioni del sistema operativo (per gruppo o per utente) invece di controllare l'accesso tramite account server.

priorità CPU. Se alcuni utenti hanno bisogno di una priorità di CPU superiore rispetto ad altri utenti (ad esempio, gli utenti che eseguono lavori rapidi contro quelli che eseguono lavori lunghi), modificano il profilo utente o le impostazioni di gruppo.

Compressione della cache. La compressione della cache dispone di qualche sovraccarico di CPU per la compressione e la decompressione dei file di scratch. Se i tuoi utenti non stanno lavorando con file di dati di grandi dimensioni, potresti voler considerare la disattivazione.

Miglioramento dell'utilizzo della memoria

Considerare quanto segue per migliorare l'utilizzo della memoria:

Importo. Aggiungere quanto più RAM possibile. Prova ad avere 128 MB di RAM per ogni utente simultanea. Quindi, se ci sono quattro utenti simultanee, configurare il server con 512 MB di RAM.

IBM SPSS Statistiche configurazione. Diminuire lo spazio di lavoro in IBM SPSS Statistiche.

Miglioramento dell'utilizzo della rete

Considerare quanto segue per migliorare l'utilizzo della rete:

Configurazione di sistema. Pianificare le operazioni intensive di rete per i tempi in cui il software server non è in uso (ad esempio, eseguire i backup del sistema in una notte). Se si identifica un problema con il traffico di rete su un computer su cui il server è in esecuzione, IBM Corp. lavorerà con te per diagnosticare ulteriormente il problema.

Utilizzo di IBM SPSS Statistiche Efficientemente

Oltre a concentrarsi su specifiche aree problematiche, è anche possibile migliorare le prestazioni aderendo alle seguenti linee guida per l'utilizzo di IBM SPSS Statistiche in modo efficiente.

Gestione dei dati. Se si dispone di file di dati di grandi dimensioni che richiedono un aggiornamento regolare e sono condivisi dagli utenti, considerare di effettuare gli aggiornamenti una volta e poi rilasciando i file agli utenti per l'analisi. Ad esempio, se si aggiungono regolarmente i dati mensili ad un file, ordinarlo ed eseguire trasformazioni, designare una persona per eseguire il lavoro sul file. Gli

altri utenti possono ottenere i dati di cui hanno bisogno senza dover ripetere l'unione, l'ordinamento e le trasformazioni.

Interactive vs. batch. Se si dispone di operazioni regolari, a tempo determinato, che si fanno con IBM SPSS Statistiche, considerate di eseguirle dal IBM SPSS Statistiche Batch Facility piuttosto che da un client connesso al server. Utilizzare il client per la costruzione dei report, e eseguirli dal IBM SPSS Statistiche Batch Facility dopo che i report sono pronti.

Appendice A. Risoluzione dei problemi

Server software

Errore di accesso locale (solo Windows). Gli utenti potrebbero riscontrare una situazione in cui l'accesso non riesce perché non dispongono del privilegio di accesso locale sul server. Per risolvere questo problema è necessario apportare modifiche al `filespsprod.inf` file. Per ulteriori informazioni su questo problema noto e sulla relativa correzione temporanea, vedere [Soluzione alternativa per il requisito del server secondo cui gli utenti dispongono del privilegio "consenti accesso locale"](#).

conflitto numero di porta. Se c'è un conflitto del numero di porta, il software server potrebbe non riuscire ad avviarsi. Correggere il problema utilizzando l'applicazione di amministrazione (IBM SPSS Console di amministrazione statistiche, che viene installata come parte di IBM SPSS Deployment Manager) per modificare il numero di porta. Consultare il topic Connections nella *Guida per l'utente di Deployment Manager* (incluso nella guida per IBM SPSS Servizi di collaborazione e distribuzione) per ulteriori informazioni.

Funzioni errate. Il software del server potrebbe funzionare in modo non corretto se il relativo file di configurazione (ad esempio, `statisticsd.conf`) è danneggiato o mancante. Per correggere il problema, ripristinare il file di configurazione dalla copia di backup. Copiarlo nella posizione specificata nell'applicazione di amministrazione o nella variabile di ambiente del file di configurazione e riavviare il software server. Per ulteriori informazioni sul riavvio, consultare ["Avvio e arresto del Software Server"](#) a pagina 19 in.

L'applicazione di gestione non funziona (solo UNIX). Se si utilizza l'applicazione di gestione per controllare o configurare il software del server e non funziona (ad esempio, non è possibile arrestare il server), è possibile che il software del server non sia stato avviato con lo script di avvio fornito da IBM Corp.. Correggere il problema avviando il software del server con lo script di avvio `start_statistics_server`. Per ulteriori informazioni, consultare l'argomento ["Per arrestare il servizio o Daemon"](#) a pagina 20. Se si ottiene un messaggio di errore quando si tenta di controllare o configurare il software del server, potrebbe essere perché si è connessi con un account che non dispone dei permessi di amministratore.

Non è possibile modificare la posizione dei file temporanei (solo UNIX). Se si utilizza l'applicazione di amministrazione per modificare la posizione dei file temporanei e la modifica non è efficace, potrebbe essere perché la nuova posizione non dispone di autorizzazioni file sufficienti per gli utenti finali. Scegliere un'ubicazione che abbia un accesso **lettura, scrittura e esecuzione** per tutti gli utenti che si collegano al software del server.

Il server non viene avviato (solo UNIX) Se il software del server non viene avviato, è possibile che non si disponga delle patch del sistema operativo richieste. Per correggere il problema, scaricare e installare la patch appropriata. Le patch richieste sono elencate nelle istruzioni di installazione UNIX per il tuo prodotto server.

Software client

L'utente finale non può connettersi al server. L'utente potrebbe non avere autorizzazioni adeguate o il firewall potrebbe bloccare il software server. Per informazioni sulle autorizzazioni degli utenti, consultare ["Autorizzazioni"](#) a pagina 29. Per informazioni sulla configurazione del firewall, consultare ["Configurazione delle connessioni tramite un firewall"](#) a pagina 31.

Il login utente finale non riesce con il messaggio "non trovato il computer server remoto specificato". Il servizio o il daemon potrebbe non essere in esecuzione. Confermare ciò verificando lo stato del software server. Per correggere il problema, riavviare il servizio o il daemon. Per ulteriori informazioni, consultare l'argomento ["Avvio e arresto del Software Server"](#) a pagina 19.

Il login utente finale non riesce con il messaggio "errore di connessione al pacchetto". L'utente finale ha specificato il nome o l'indirizzo IP di un computer server che non è in rete. Per correggere il problema, chiedere all'utente finale di inserire un nome server valido.

DataDirect L'origine dati ODBC ha esito negativo con il messaggio "senza licenza". La tecnologia di accesso dati DataDirect viene distribuita con prodotti IBM Corp. . Funziona solo con i prodotti più recenti IBM Corp. - non funziona con le versioni precedenti, né funziona con applicazioni nonIBM Corp. . Se gli utenti finali tentano di utilizzare le origini dati DataDirect con un prodotto precedente o senza licenza, riceveranno un messaggio contenente il testo **Non si dispone della licenza per utilizzare il driver DataDirect ODBC.** Per correggere il problema con il prodotto IBM Corp. , aggiornare i propri utenti a una versione corrente. Per correggere il problema con i prodotti senza licenza, aggiornare la licenza con DataDirect oppure chiedere agli utenti finali di non tentare di utilizzare le origini dati definite per i prodotti IBM Corp. con applicazioni senza licenza.

L'utente finale non riesce a trovare un file di dati o l'origine dati ODBC . Quando gli utenti finali sono in esecuzione in modalità di analisi distribuita, avranno accesso solo ai file di dati e alle origini dati ODBC sul computer che sta eseguendo il software server. Quando gli utenti finali sono in esecuzione in modalità di analisi locale, avranno accesso solo ai file di dati e alle origini dati ODBC sui loro computer desktop. Per correggere il problema, chiedere all'utente finale di eseguire l'applicazione client nella modalità appropriata.

L'utente finale non può eseguire una procedura statistica (soloIBM SPSS Statistiche Server). Quando gli utenti finali sono connessi al software server, hanno accesso solo alle opzioni IBM SPSS Statistiche installate durante l'installazione di IBM SPSS Statistiche Server. Per correggere il problema, chiedere all'utente finale di eseguire la procedura mentre in modalità di analisi locale o installare la procedura richiesta sul computer server.

Appendice B. La funzione di batch IBM SPSS Statistiche

Nota: il IBM SPSS Statistiche Batch Facility è un'utility di elaborazione batch inclusa con **IBM SPSS Statistiche Server**.

Generalmente il client per IBM SPSS Statistiche Server è IBM SPSS Statistiche in esecuzione su un computer desktop. Tuttavia, il IBM SPSS Statistiche Batch Facility è un modo alternativo per utilizzare la potenza di IBM SPSS Statistiche Server, e si esegue sul computer server. Il IBM SPSS Statistiche Batch Facility è destinato alla **produzione automatizzata** di report statistici. La produzione automatizzata fornisce la possibilità di eseguire analisi senza l'intervento dell'utente. La produzione automatizzata è vantaggiosa se gli utenti del tuo sito richiedono regolarmente una serie di analisi di dispendio di tempo, come i report settimanali.

Il IBM SPSS Statistiche Batch Facility assume come input una richiesta di report contenuta in un file **sintassi di comando**. Il IBM SPSS Statistiche Batch Facility produce quindi automaticamente i report statistici specificati dalla sintassi.

Cosa devi sapere

Sistemi operativi. Il IBM SPSS Statistiche Batch Facility è attualmente disponibile con tutti i IBM SPSS Statistiche Server, UNIX e Windows.

del client DB2. Il IBM SPSS Statistiche Batch Facility viene installato automaticamente nella directory di installazione di IBM SPSS Statistiche Server su Windows e la sottodirectory */bin* della directory di installazione su UNIX.

Fatturazione. Il IBM SPSS Statistiche Batch Facility viene eseguito dalla riga di comando utilizzando il file eseguibile *statisticsb*. Si esegue indipendentemente da IBM SPSS Statistiche Server -IBM SPSS Statistiche Server non deve essere avviato per eseguirlo. Può anche essere eseguito in concomitanza con IBM SPSS Statistiche Server.

Modi di funzionamento. Comandi vengono inoltrati tothe IBM SPSS Statistiche Batch Facility in **batch** o **modalità interattiva**. In modalità batch, l'analista o il professionista IT sottopone un file di sintassi del comando al IBM SPSS Statistiche Batch Facility per l'esecuzione - i comandi nel file vengono letti e comportati come batch e l'output è diretto ad un file. Il IBM SPSS Statistiche Batch Facility esegue non presidiato e termina dopo l'esecuzione dell'ultimo comando. Questo è il modo tipico per utilizzare il IBM SPSS Statistiche Batch Facility. In modalità interattiva, i tipi di analista comandi uno alla volta ad un prompt dei comandi. I comandi vengono eseguiti immediatamente e l'output viene visualizzato nella finestra. Il IBM SPSS Statistiche Batch Facility attende il comando successivo.

Documentazione. La guida dell'utente, scritta per gli analisti e i professionisti IT di un sito che utilizzerà il IBM SPSS Statistiche Batch Facility, è su IBM SPSS Statistiche Server DVD in */Documentazione/<lingua>/Manuali*. La guida di riferimento della sintassi del comando che gli analisti avranno bisogno per creare file di sintassi dei comandi per il IBM SPSS Statistiche Batch Facility è su IBM SPSS Statistiche Server DVD in */Documentazione/<lingua>/Manuali*. Il IBM SPSS Statistiche Batch Facility for UNIX è distribuito anche con una pagina manuale, *statisticsb.1*, che si trova nella sottodirectory */bin* della directory di installazione di IBM SPSS Statistiche Server. Se si amministra un sistema UNIX, copiarlo nella posizione in cui si mantengono le pagine manuali.

Documentazione aggiuntiva. La guida dell'utente di IBM SPSS Statistiche Batch Facility contiene informazioni sufficienti per un analista esperto con il linguaggio di sintassi del comando IBM SPSS Statistiche per costruire file di sintassi dei comandi per il IBM SPSS Statistiche Batch Facility. Se gli analisti del tuo sito sono nuovi a IBM SPSS Statistiche, possono richiedere ulteriore documentazione. Se lo fanno, indirizzarli al nostro sito web all'indirizzo <http://www.ibm.com/software/analytics/spss/>, oppure chiedergli di contattare il tuo rappresentante di vendita.

Appendice C. Attività del sistema operativo Windows

È possibile effettuare la maggior parte delle attività amministrative con l'applicazione di amministrazione ; tuttavia potrebbero essere necessarie alcune attività con il sistema operativo Windows. Utilizzare le seguenti funzioni del sistema operativo per amministrare il software server in esecuzione su Windows:

- **Proprietà file.** Utilizzato per impostare l'accesso degli utenti finali alla directory di installazione del software server, la posizione del file temporaneo e i file di dati.
- **Proprietà di sistema.** Utilizzato per creare variabili di ambiente.
- **Gestore utenti.** Utilizzato per creare account utente finale.
- **Pannello di controllo dei servizi.** Utilizzato per avviare, arrestare e configurare il servizio.
- **ODBC Amministratore.** Utilizzato per configurare le origini dati.

Proprietà file

Utilizza Proprietà file per impostare i permessi sui file. Per i file di dati, come si fa dipende da dove vengono memorizzati i dati. Quando si memorizzano i dati sullo stesso computer del software server, si controlla l'accesso alla directory dei dati impostando i permessi su una directory su un'unità NTFS.

Sul computer server, collegato come amministratore:

1. Utilizzare Windows Explorer per navigare nella directory dei dati.
2. Fare clic sulla directory, fare clic con il tasto destro del mouse e fare clic su **Sharing** sul menu di contesto.
3. Fare clic sulla scheda **Sicurezza** e configurare i permessi.

Nota: la scheda di sicurezza è disponibile solo su unità NTFS. Se non sei sicuro di quale tipo di file system il tuo hardware utilizza, segui questi passaggi:

4. Utilizzare Windows Explorer per navigare all'unità.
5. Fare clic sull'unità, fare clic con il tasto destro del mouse e fare clic su **Proprietà** sul menu di contesto.
6. Clicca sulla scheda **Generale** e guarda il valore per File System.

Quando si memorizzano i dati su un computer sulla rete, è possibile controllare l'accesso alla directory dei dati creando una risorsa condivisa e impostando opportunamente le autorizzazioni.

Sul computer netlavorato, collegato come amministratore:

7. Utilizzare Windows Explorer per navigare nella directory dei dati.
8. Fare clic sulla directory, fare clic con il tasto destro del mouse e fare clic su **Sharing** sul menu di contesto.
9. Fare clic sulla scheda **Condivisione** nella finestra di dialogo, fare clic su **Condividi Come**, inserire un nome di condivisione e impostare l'accesso appropriato.

Proprietà di sistema

Utilizzare le proprietà del sistema per creare variabili di ambiente.

Sul computer server, collegato come amministratore:

1. Sul desktop di Windows, clicca con il tasto destro del mouse sull'icona per il computer. Ad esempio, fare clic con il tasto destro del mouse su **My Computer**.
2. Selezionare **Proprietà** dal menu.
3. Fare clic sulla scheda **Advanced** e quindi fare clic su **Variabili di ambiente**.
4. Fare clic su **Nuovo**.

5. Digitare il nome della nuova variabile.
6. Digitare il valore per la nuova variabile.

Gestore utente

Utilizzare User Manager per creare account utente finale.

Sul computer server, collegato come amministratore:

1. Fare clic sul pulsante Start di Windows e quindi scegliere:
Programmi > Strumenti amministrativi
 - Selezionare **Gestione informatica** e quindi **Utenti e gruppi locali**.
2. Creare gli account utente.

Pannello di controllo dei servizi

Utilizzare il Pannello di controllo dei servizi di Windows per:

- Stop e avvia il servizio.
- Modificare i parametri di avvio del servizio.
- Controllare lo stato del server.

Per accedere e utilizzare il Pannello di controllo dei servizi:

1. Fare clic sul pulsante Start di Windows e quindi scegliere:
Impostazioni > Pannello di controllo
2. Selezionare **Strumenti amministrativi** e quindi **Servizi**.
3. Seleziona il servizio. Ora è possibile controllare il proprio stato, avviare o arrestarlo e modificare i parametri di avvio.

Nota: è possibile avviare, arrestare e verificare lo stato del software server con l'applicazione di amministrazione.

Gestore attività

Utilizzare il Task Manager per vedere quanti processi relativi al server sono in esecuzione.

1. Aprire il Task Manager di Windows premendo Ctrl - Alt - Elimina e scegliendo **Task Manager**.
2. Fare clic sulla scheda **Processi**.
3. Fare clic su **Nome immagine** per ordinare alfabeticamente i processi.
4. Cercare il nome file del processo del server (*statisticsrvr.exe*).
5. Cercare il nome file del processo client (*statisticsproc.exe*). Esiste un processo per ogni utente finale attualmente connesso al software server.

Nota: è possibile monitorare i processi server e client con l'applicazione di amministrazione.

Amministratore ODBC

Utilizzare l'Amministratore ODBC per configurare le origini dati di sistema e utente per l'utilizzo con il software server.

Come viene creata l'origine dati ODBC influenza chi può visualizzare e utilizzarlo. Utilizzare i DSNs *system* quando si desidera consentire l'accesso generale all'origine dati. Utilizzare *utente* DSNs quando si desidera limitare l'accesso alle informazioni sensibili o quando si desidera personalizzare il DSN per un utente specifico.

Per configurare un DSN di sistema

I DSNs di sistema possono essere utilizzati da chiunque sia collegato al computer su cui sono definiti. I DSNs di sistema sono più facili da configurare e amministrare perché lo si fa una volta per tutti gli utenti.

Sul computer su cui si desidera che risieda l'origine dati, collegato come amministratore:

1. Fare clic sul pulsante Start di Windows e quindi scegliere:

Impostazioni > Pannello di controllo

2. Selezionare **Strumenti amministrativi** e poi **Origini dati**.
3. Fare clic sulla scheda **DSN di sistema**.
4. Fare clic su **Aggiungi**.
5. Selezionare un driver dall'elenco. Se si sta configurando una fonte di dati che utilizza la tecnologia di accesso dei dati IBM Corp., i nomi dei driver Connect ODBC sono etichettati con il testo IBM Corp. OEM.
6. Fare clic su **Fine**.
7. Inserire le informazioni appropriate nella finestra di dialogo **Impostazione driver**.
8. Fare clic su **OK**.

Per configurare un DSN utente

Gli utenti DSNs possono essere utilizzati solo dal conto dell'utente che li ha creati. Configurare DSNs utente quando si desidera limitare l'accesso alle informazioni sensibili o quando si desidera personalizzare il DSN per un utente specifico.

Accedi come utente e segui i passaggi per un sistema DSN, con questa eccezione:

- Fare clic sulla scheda **DSN utente** invece della scheda **DSN di sistema**.

Appendice D. Attività del sistema operativo UNIX

È possibile effettuare la maggior parte delle attività amministrative con l'applicazione di amministrazione ; tuttavia potrebbero essere necessarie alcune attività con il sistema operativo UNIX. Utilizzare le seguenti funzioni del sistema operativo per amministrare il software server in esecuzione su UNIX:

- **chmod**. Utilizzato per impostare l'accesso degli utenti finali ai file di dati.
- **env**. Utilizzato per controllare i valori delle variabili di ambiente.
- **scripts**. Utilizzato per avviare il software server e configurare il proprio ambiente.
- **ps e kill**. Utilizzato per controllare e arrestare i processi del server.
- **odbc.ini**. Utilizzato per configurare le origini dati ODBC .

chmod

Utilizzare il comando chmod (o chown) per modificare o assegnare la modalità di autorizzazioni per le directory e i file di dati. Ad esempio, per impostare la directory */usr/data* su sola lettura per tutti:

1. Accedi come super utente o come proprietario della directory.
2. Al prompt di UNIX digitare:

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

env

Utilizzare il comando env per verificare i valori correnti delle variabili di ambiente. Ad esempio, per utilizzare env per verificare i valori correnti delle variabili di ambiente per il software server:

1. Accedi come l'account che ha avviato il daemon, tipicamente *root*.
2. Al prompt di UNIX digitare:

```
env
```

3. Controllare le impostazioni per le variabili di interesse.

Script

Per modificare valore delle variabili di ambiente, modificare lo script di variabile dell'ambiente chiamato dallo script che avvia il software del server. Per modificare lo script della variabile d'ambiente:

1. Utilizzare un editor di testo per aprire lo script *statsenv.sh* , incluso nella directory secondaria */bin* della directory di installazione di IBM SPSS Statistiche Server. Ad esempio, aprire */usr/local/myserverproduct/bin/statsenv.sh*.
2. Se necessario, scommentare la riga che definisce la variabile e quindi inserire il nuovo valore per la variabile.
3. Salvare il file.

statsenv.sh viene chiamato dallo script *start_statistics_server* . Le variabili di ambiente impostate ed esportate in *statsenv.sh* influiscono solo sui processi avviati con lo script *start_statistics_server* .

ps e uccidere

Utilizzare il comando ps per acquisire le informazioni relative ai processi server in esecuzione e riportare lo stato del processo. Ad esempio:

1. Al prompt di UNIX digitare:

```
ps -efl.
```

2. Cerca il nomefile del processo del daemon (ad esempio, *statisticsd*). Questo processo ha l' **UID** dell'utente che ha avviato il processo del daemon software del server (di solito *root*).
3. Ricercare il nome file del processo client, *statisticsproc.exe*. Esiste un processo per ogni utente finale attualmente connesso al software server. La colonna *UID* visualizza l'ID di login dell'utente finale che possiede il processo client.

Utilizzare il comando `kill` per uccidere un processo. Ad esempio:

4. Accedi come utente che ha avviato il daemon.

5. Al prompt di UNIX digitare:

```
kill -9 pid
```

dove *pid* è l'id di processo del processo.

Il daemon software server crea anche automaticamente un file che contiene il suo ID di processo. Invece di trovare manualmente il PID con il comando `ps`, è possibile utilizzare questo file insieme al comando `kill` direttamente per uccidere direttamente il processo del daemon:

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

Nota: se si desidera utilizzare l'applicazione di amministrazione per monitorare e uccidere i processi, è necessario avviare il software server con lo script di avvio fornito da IBM Corp.. Per ulteriori informazioni, consultare l'argomento "Avvio Controllo del servizio" a pagina 18.

odbc.ini

Potrebbe essere necessario configurare le origini dati ODBC sul computer server se:

- Si utilizza il IBM Corp. Data Access Pack

e

- Il software server deve accedere ai database

Nessun amministratore ODBC esiste su UNIX. Per configurare un'origine dati ODBC su UNIX, modificare un file di testo delle informazioni di sistema, *odbc.ini*. *Odbc.ini* viene installato quando si installa il pacchetto di accesso dati per UNIX. Le istruzioni di installazione vengono visualizzate in *IBM Corp. Data Access Pack Installation Instructions for Unix.pdf* (il documento si trova nella directory */Documentazione/<lingua>/InstallationDocuments* sul prodotto DVD). Assicurarsi di installare la documentazione aggiuntiva in modo da avere accesso ai documenti elencati di seguito.

Connessione ODBC. Per informazioni sulla modifica del file *odbc.ini* e sull'impostazione di importanti variabili di ambiente, consultare la sezione "Configurazione di driver e origini dati" nel capitolo "Installazione su UNIX" di *Connect ODBC Installation Instructions* per istruzioni dettagliate.

La documentazione del prodotto DataDirectper Connect ODBC è inclusa, per impostazione predefinita, come parte dell'installazione di IBM SPSS Data Access Pack . Il programma di installazione crea la voce IBM SPSS OEM Connect e ConnectXE per ODBC insieme alle voci per altri programmi nel menu Start. È possibile accedere alla documentazione del prodotto DataDirect da questa voce di menu.

La documentazione del prodotto DataDirectper Connect ODBC si trova nella directory in cui sono stati estratti i file.

Nota: è possibile accedere alla documentazione anche dalla home page di DataDirect all'indirizzo <http://www.datadirect.com>

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, può essere necessario possedere una copia del prodotto o versione del prodotto in tale lingua per potervi accedere.

IBM può non offrire i prodotti, i servizi o le funzioni presentati in questo documento in altri paesi. Consultare il proprio rappresentante locale IBM per informazioni sui prodotti ed i servizi attualmente disponibili nella propria zona. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica o intende dichiarare che solo quel prodotto, programma o servizio IBM può essere utilizzato. Qualsiasi prodotto funzionalmente equivalente al prodotto, programma o servizio che non violi alcun diritto di proprietà intellettuale IBM può essere utilizzato. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri prodotti, programmi o servizi non IBM.

IBM può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura del presente documento non concede alcuna licenza a tali brevetti. È possibile inviare per iscritto richieste di licenze 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, Japan*

IBM (INTERNATIONAL BUSINESS MACHINES CORPORATION) FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIALIZZABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcune giurisdizioni non consentono la rinuncia ad alcune garanzie espresse o implicite in determinate transazioni, pertanto, la presente dichiarazione può non essere applicabile.

Queste informazioni potrebbero contenere imprecisioni tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. IBM si riserva il diritto di apportare miglioramenti e/o modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

I riferimenti in queste informazioni a siti Web non IBM vengono forniti solo per comodità e non implicano in alcun modo l'approvazione di tali siti web. I materiali presenti in tali siti web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti è a proprio rischio.

IBM può utilizzare o distribuire qualsiasi informazione fornita in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo verso l'utente.

Coloro che detengano la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'utilizzo reciproco di tali informazioni, dovrebbe rivolgersi a:

*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 descritto nel presente documento e tutto il materiale concesso in licenza disponibile sono forniti da IBM in base alle clausole dell'Accordo per Clienti IBM (IBM Customer Agreement), dell'IBM IPLA (IBM International Program License Agreement) o qualsiasi altro accordo equivalente tra le parti.

Gli esempi client e dati delle prestazioni citati sono presentati esclusivamente a scopo illustrativo. Gli effettivi risultati delle prestazioni possono variare in base alle configurazioni e alle condizioni operative specifiche.

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 testato quei prodotti e non può confermarne la precisione della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Le domande sulle funzionalità dei prodotti non IBM devono essere indirizzate ai fornitori di tali prodotti.

Le dichiarazioni relative all'orientamento o alle intenzioni future di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo mete e obiettivi.

Questa pubblicazione contiene esempi di dati e prospetti utilizzati quotidianamente nelle operazioni aziendali. Pertanto, per maggiore completezza, gli esempi includono nomi di persone, società, marchi e prodotti. Tutti i nomi contenuti nel manuale sono fittizi e ogni riferimento a persone o aziende reali è puramente casuale.

LICENZA DI COPYRIGHT:

Queste informazioni contengono programmi applicativi di esempio in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza 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. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi. I programmi di esempio sono forniti "NELLO STATO IN CUI SI TROVANO", senza alcun tipo di garanzia. IBM non intende essere responsabile per alcun danno derivante dall'uso dei programmi di esempio.

Ogni copia o qualsiasi parte di questi programmi di esempio o qualsiasi lavoro derivato, devono contenere le seguenti informazioni relative alle leggi sul diritto d'autore:

© Copyright IBM Corp. 2021. Le porzioni di questo codice derivano da IBM Corp. Programmi di esempio.

© Copyright IBM Corp. 1989 - 2021. Tutti i diritti riservati.

Marchi

IBM, il logo IBM e ibm.com sono marchi o marchi registrati di International Business Machines Corp., registrati in molte giurisdizioni in tutto il mondo. Altri nomi di prodotti e servizi possono essere marchi di IBM o di altre società. Un elenco corrente dei marchi IBM è disponibile sul web in "Copyright and trademark information" all'indirizzo www.ibm.com/legal/copytrade.shtml.

Adobe, il logo Adobe, PostScript e il logo PostScript sono marchi o marchi registrati 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 delle sue consociate negli Stati Uniti e in altri paesi.

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

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

UNIX è un marchio della The Open Group negli Stati Uniti e/o negli altri paesi.

Java e tutti i marchi e i logo basati su Java sono marchi o marchi registrati di Oracle e/o associate.

Indice analitico

A

- accesso a file di dati
 - cosa gli utenti finali devono sapere [42](#)
- accesso dati
 - configurazione delle origini dati ODBC per [14](#)
 - Connetti ODBC [9](#)
 - controllo [10](#)
 - Fattori da considerare [10](#)
 - in UNIX [11](#)
 - Origini dati ODBC per [10](#)
 - referenziare i dati del software client [10](#)
- accesso DSN [29](#)
- account [13](#)
- Ambiente UNIX e accesso dati [11](#)
- amministratori di sistema
 - cosa gli utenti finali devono sapere [21](#)
 - panoramica delle attività amministrative [4](#)
- applicazione client
 - installazione di [7](#)
 - risoluzione dei problemi [49](#)
- applicazione di amministrazione [15](#)
- architettura distribuita [1](#)
- Area di lavoro IBM SPSS Statistics [46, 47](#)
- attività del sistema operativo, Windows
 - creazione variabili di ambiente [53](#)
 - impostazione delle proprietà file [53](#)
 - utilizzando il pannello di controllo Servizi [54](#)
 - utilizzando il Task Manager [54](#)
 - utilizzando l'amministratore ODBC [54](#)
 - utilizzo di User Manager [54](#)
- attività di sistema operativo, UNIX
 - utilizzando il comando chmod per impostare i permessi dei file [57](#)
 - utilizzando il comando env per verificare le variabili di ambiente [57](#)
 - utilizzando il comando kill per arrestare i processi del server [57](#)
 - utilizzando il comando ps per controllare i processi del server [57](#)
 - utilizzando script per impostare le variabili di ambiente [57](#)
 - utilizzo di odbc.ini per la configurazione delle origini dati [58](#)
- autenticazione
 - autenticazione unica [24](#)
 - interno [22](#)
 - OS [21](#)
 - PAM [21](#)
 - unix2 [23](#)
- autenticazione unica
 - appartenenza ai gruppi [28](#)
 - Configurazione del client [25](#)
 - Configurazione del server [25](#)
 - nome principio di servizio [26, 27](#)
 - origini dati [28](#)
- autorizzazione del gruppo [17, 29](#)

autorizzazioni di livello amministratore [29](#)

C

- certificati
 - configurazione [37](#)
- configurazione
 - certificati [37](#)
 - estensioni [15](#)
- configurazione del software server [13](#)
- Connetti ODBC
 - impostazione dell'ambiente UNIX per [11](#)
 - multicloud [9](#)
 - panoramica di [9](#)
- console di amministrazione IBM SPSS Statistics [15](#)
- Controllo dell'accesso basato sul ruolo [23](#)
- crittografia
 - SSL [33](#)

D

- database
 - SSL [33](#)
- dati di visualizzazione [13](#)

E

esecuzione senza privilegi di root [22–24](#)

F

- file di configurazione
 - risoluzione dei problemi [49](#)
- file di profilo [14](#)
- firewall [30](#)
- Funzione Produzione
 - Inserisci nascosto [16](#)

G

- gestione [15](#)
- gruppi
 - cenni generali [14](#)
- gruppi di utenti
 - cenni generali [14](#)

I

- IBM SPSS Servizi di collaborazione e distribuzione
 - sostituzione [16](#)
- IBM SPSS Statistics Batch Facility
 - Cosa devi sapere [51](#)
 - introduzione a [51](#)
- ID utente e password
 - cosa gli utenti finali devono sapere [42](#)
- IDE [46](#)

Informazioni prestazione [45](#)
Inserisci nascosto
 Funzione Produzione [16](#)
installazione
 applicazione client [7](#)
 software server [7](#)

L

le autorizzazioni [29](#)
locale [40](#)

M

miglioramento prestazioni [45](#)
Modalità di analisi distribuita
 passi da utilizzare [1](#)
 software [1](#)
 vista dei dati [9](#)
modalità di analisi locale
 software [1](#)
 vista dei dati [9](#)
Modulo di autenticazione collegabile [21](#)

N

NAT [30](#)
Nome computer
 cosa gli utenti finali devono sapere [42](#)
nome dominio
 cosa gli utenti finali devono sapere [42](#)
nome principio di servizio [26](#), [27](#)
nomi di processo per prodotto [19](#)
numero porta
 cosa gli utenti finali devono sapere [42](#)
 risoluzione dei problemi [49](#)

O

ordinamento [15](#)
ordinamento di terze parti [15](#)
origine dati ODBC
 configurazione [14](#)
 cosa gli utenti finali devono sapere [42](#)
 e software server [11](#)
 risoluzione dei problemi [49](#)
origini dati
 autenticazione unica [28](#)
Origini dati ODBC , UNIX
 definito in odbc.ini [58](#)
Origini dati ODBC , Windows
 DSNs utente [54](#)
 sistema DSNs [54](#)

P

PAM [21](#)
PPTP [33](#)
prestazione
 Miglioramento [45](#)
privilegi di root [22-24](#)
processori [47](#)
prodotti e sistemi operativi [1](#)

produzione automatizzata con IBM SPSS Statistics Server [51](#)
profili
 cenni generali [14](#)
profili utente
 cenni generali [14](#)
protocollo di tunneling point-to-point [33](#)

R

RAID [46](#)
RAM [47](#)
RBAC [23](#)
Riferimenti file dati UNC [42](#)
risoluzione dei problemi
 applicazione client [49](#)
 file di configurazione [49](#)
 login client [49](#)
 numero porta [49](#)
 origine dati ODBC [49](#)
 software server [49](#)

S

SCSI [46](#)
software server
 amministratori [29](#)
 avvio e arresto [19](#)
 componenti [1](#)
 configurazione delle origini dati ODBC [14](#)
 configurazione di [13](#)
 controllo della startup [18](#)
 gestione degli account e dei file di fine utente [13](#)
 installazione di [7](#)
 istanze multiple [17](#)
 manutenzione ordinaria di [19](#)
 multicloud [1](#)
 nomi di processo per prodotto [19](#)
 prodotti [1](#)
 risoluzione dei problemi [49](#)
 software [1](#)
 utilizzando lo script di avvio UNIX [18](#)
spazio di lavoro [46](#), [47](#)
spazio su disco [46](#)
SSL
 cenni generali [33](#)
 protezione delle comunicazioni [33](#), [38](#)
SSL (Secure Socket Layer) [33](#)
SSO [24](#)
start_statistics_server [18](#)
statistica [51](#)
SyncSort [15](#)

T

tecnologia di accesso dati [9](#)

U

UNIX
 arresto dei processi server [57](#)
 controllo dei processi server [57](#)
 creazione e configurazione delle origini dati ODBC [58](#)
 impostazione dei permessi file [57](#)

UNIX (*Continua*)

- impostazione delle variabili di ambiente [57](#)
- verifica variabili di ambiente [57](#)

utenti finali

- accesso a file di dati [42](#)
- elenco di ciò che devono sapere [21](#)
- ID utente e password [42](#)
- Nome computer [42](#)
- nome dominio [42](#)
- numero porta [42](#)
- origine dati ODBC [42](#)
- sostegno [21](#)

utilizzo del disco

- Miglioramento [46](#)

utilizzo della CPU

- Miglioramento [47](#)

utilizzo della memoria

- Miglioramento [47](#)

Utilizzo rete

- Miglioramento [47](#)

V

versioni [30](#)

visualizzazione dati [13](#)

W

Windows

- avvio e arresto dei servizi [54](#)
- controllo dei processi server [54](#)
- creazione di account utente finale [54](#)
- creazione e configurazione delle origini dati ODBC [54](#)
- creazione variabili di ambiente [53](#)
- impostazione dei permessi file [53](#)
- modifica parametri di avvio del servizio [54](#)
- verifica stato del servizio [54](#)

X

xensioni

- configurazione [15](#)

