IBM SPSS Statistics Server -Guide d'administration

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 65.

Notice d'édition

La présente édition s'applique à la version 32.0.0 d'IBM® SPSS Statistiques Server et à toutes les éditions et modifications ultérieures sauf mention contraire dans les nouvelles éditions.

Table des matières

Chapitre 1. Présentation

La technologie du serveur IBM SPSS Statistiques est une **architecture répartie**et, associée à des optimisations de gestion des données clés, elle prend en charge l'analyse évolutive. La technologie est basée sur le client/serveur. Il distribue les demandes des clients pour les opérations gourmandes en ressources à des logiciels serveur puissants. Lorsque le client et le serveur fonctionnent ensemble de la sorte, ils sont appelés **mode d'analyse distribué**. L'analyse distribuée permet aux utilisateurs finaux d'effectuer des analyses que leurs ordinateurs de bureau ne peuvent pas prendre en charge.

Pour une flexibilité maximale, les applications client qui utilisent la technologie du serveur peuvent également être configurées pour s'exécuter uniquement sur l'ordinateur de bureau de l'utilisateur final-ce que l'on appelle le **mode d'analyse locale**. Les utilisateurs finaux peuvent facilement changer de mode.

Produits et systèmes d'exploitation

La technologie serveur prend en charge l'application IBM SPSS Statistiques cliente, et le logiciel serveur fonctionne sur plusieurs systèmes d'exploitation (voir les instructions d'installation pour plus de détails). Vous pouvez installer plusieurs versions de logiciels serveur sur votre site, sur le même ordinateur serveur ou sur des ordinateurs serveur différents.

Remarque importante concernant l'installation SPSS Statistics de Server sur Red Hat Enterprise Linux s 10

Sous Red Hat Enterprise Linux (RHEL) 10, IBM SPSS Statistics Server nécessite le `libxcrypt-compat` paquet.

RHEL 10 ne fournit plus `libcrypt.so.1` dans le cadre des bibliothèques système par défaut. SPSS Statistics Le serveur 32 contient des binaires qui dépendent de cette bibliothèque. L'installation `libxcrypt-compat` fournit la bibliothèque de compatibilité requise et permet au serveur de fonctionner sous RHEL 10.

Architecture

Le logiciel serveur possède une architecture répartie à deux niveaux. Il répartit les opérations logicielles entre le client et les ordinateurs serveur. Les opérations gourmandes en mémoire, telles que l'accès à une base de données volumineuse ou l'analyse d'un fichier de données volumineux, sont effectuées sur l'ordinateur serveur sans télécharger les données sur l'ordinateur client.

Niveau Client

L'application **client** . Il est installé et s'exécute sur l'ordinateur de bureau de l'utilisateur final. L'application client fournit l'interface graphique permettant d'accéder aux données et de les analyser. Il présente les résultats des analyses de l'utilisateur final.

Niveau serveur

Le logiciel **server** . Il est installé et s'exécute sur un ordinateur serveur en réseau. Le logiciel serveur fournit l'infrastructure nécessaire pour gérer plusieurs clients, les algorithmes utilisés dans l'analyse statistique et l'accès aux données.

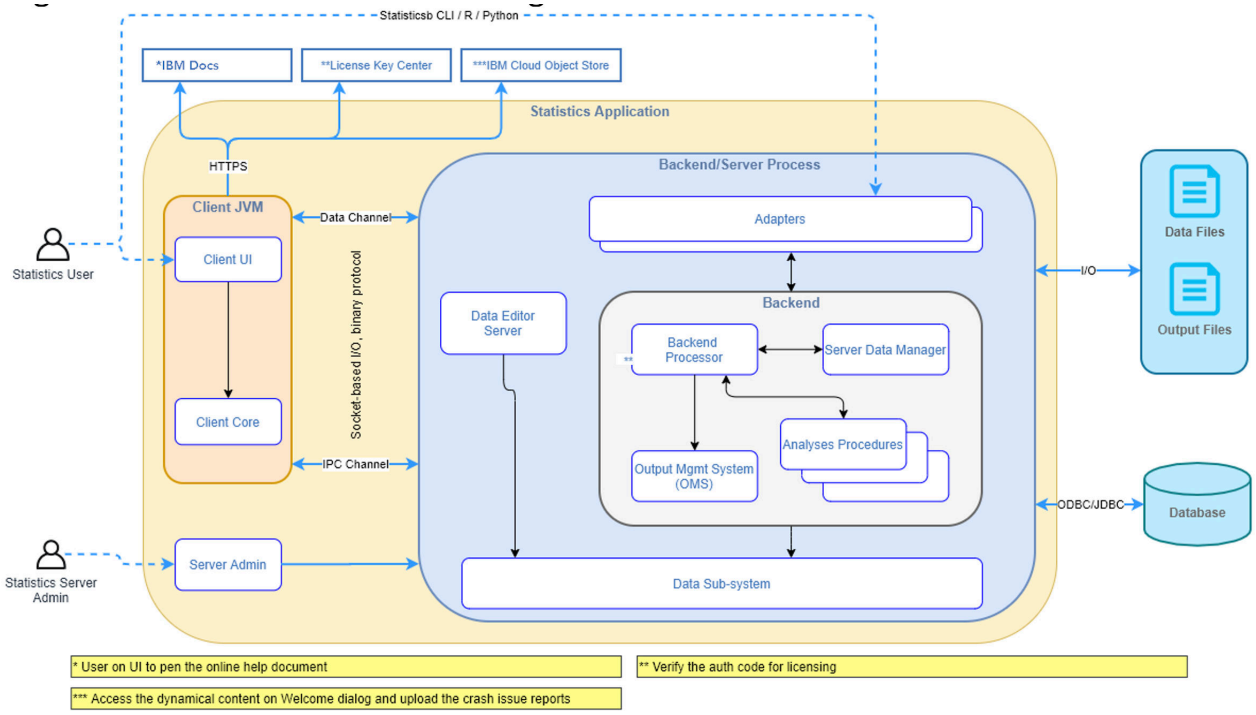

Figure 1. Mode d'analyse distribuée

Pour les analyses qui ne nécessitent pas d'accès intensif aux données ou de traitement numérique, le logiciel client peut être utilisé en tant qu'application de bureau autonome standard. En mode d'analyse locale, tous les accès aux données et les traitements statistiques sont gérés sur l'ordinateur de bureau de l'utilisateur final.

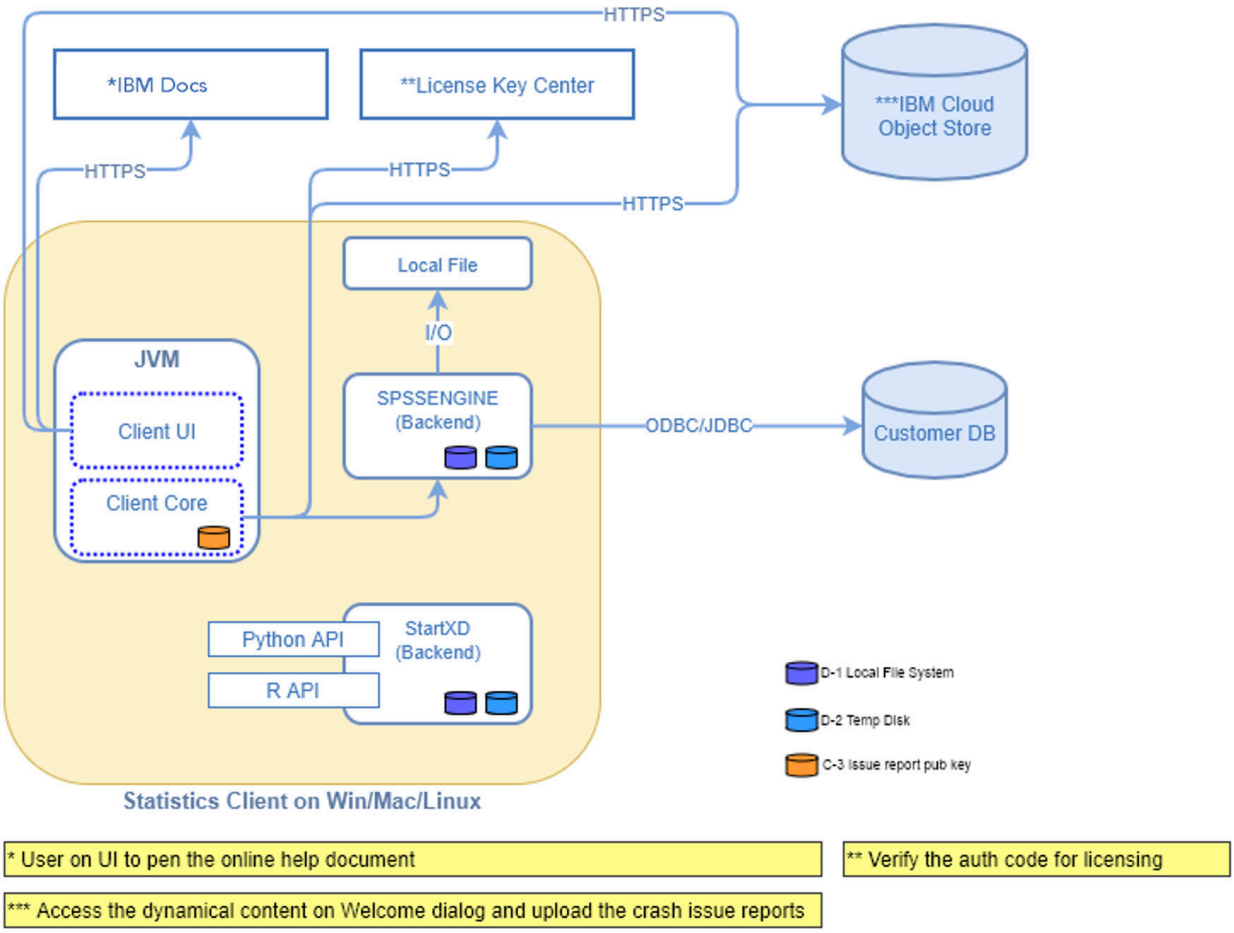

Figure 2. Mode d'analyse locale

Composants logiciels

Comme illustré dans la figure "Mode d'analyse distribué", les composants de la technologie du serveur sont les suivants. (Voir Figure 1, à la page 2.)

Logiciel client. L'application client est une installation complète du produit IBM Corp. de l'utilisateur final (par exemple, IBM SPSS Statistiques). Lorsqu'il est utilisé pour l'analyse répartie, seules l'interface graphique et les fonctions d'édition sont utilisées. Lorsqu'il est utilisé pour l'analyse locale, ses capacités d'accès aux données et de traitement statistique sont également utilisées.

Logiciel serveur. Le logiciel serveur est constitué de sous-composants: une infrastructure qui gère la communication client/serveur, des processus client qui gèrent les demandes client et des modules qui accèdent aux données et effectuent des analyses.

- **Infrastructure**. L'infrastructure du logiciel serveur est un service (sous Windows) ou un démon (sous UNIX). Il gère toutes les communications entre l'application client et les modules. L'infrastructure s'exécute en continu sur l'ordinateur serveur, en attendant les connexions client. Lorsqu'un client se connecte, l'infrastructure lance un processus qui gère les demandes pour ce client.
- **Processus client**. Un processus client est effectivement une session pour le client. Il existe un processus pour chaque client. Un processus est lancé lorsque le client se connecte et il est arrêté lorsque le client se déconnecte. Le processus gère les demandes de données et d'analyses de son client. Il charge les modules nécessaires pour accéder aux données et les analyser. Il décharge les modules lorsqu'ils ne sont plus nécessaires.
- **Modules**. Un module est une bibliothèque exécutable, DLL ou partagée qui accède aux données et exécute des procédures analytiques. Le logiciel du serveur analytique comporte plusieurs modules. Les modules sont chargés à la demande. Les modules peuvent charger d'autres modules.

Utilisation du mode réparti

Les étapes suivantes se produisent lorsqu'un utilisateur final exécute un produit en mode d'analyse distribuée:

1. **Lancez l'application client**. L'utilisateur final lance le logiciel client sur son ordinateur de bureau. L'application client présente une interface utilisateur complète.
2. **Connectez-vous au serveur**. L'utilisateur final se connecte au logiciel serveur en se connectant à partir de l'application client. Le service ou le démon de l'infrastructure du serveur est toujours en cours d'exécution et attend les demandes de connexion. Lorsqu'une connexion est créée, le logiciel serveur lance un processus pour prendre en charge l'utilisateur final.
3. **Accès aux données.** L'utilisateur final accède aux données comme d'habitude à partir de l'application client, sauf que sa vue des pilotes de base de données, des fichiers de données, des répertoires et des unités représente l'ordinateur serveur distant, et non l'ordinateur de bureau. Le processus serveur charge les modules d'accès aux données appropriés et extrait les données. Un petit segment des données est envoyé à l'application client afin que l'utilisateur final puisse y faire référence lors de la sélection d'une analyse. La plupart des données restent sur le serveur. Vous pouvez également configurer le logiciel serveur pour empêcher l'envoi de données à l'application client. Vous pouvez utiliser l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée avec IBM SPSS Responsable du déploiement) pour empêcher l'envoi des données à tous les clients. Pour plus d'informations, voir la rubrique Utilisateurs dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement). Vous pouvez également configurer l'accès pour chaque utilisateur ou groupe. Pour plus d'informations, voir la rubrique IBM SPSS Statistics Server dans le document *Deployment Manager User's Guide*.
4. **Analyser les données**. A l'aide de l'interface utilisateur de l'application client, l'utilisateur final sélectionne les données et demande le type d'analyse qu'il souhaite. La demande est envoyée au processus serveur, qui charge les packs d'analyse de données appropriés et traite l'analyse. Toutes les tâches liées aux données, telles que la lecture de données, la transformation de données, le calcul de nouvelles variables et le calcul de statistiques, sont effectuées sur l'ordinateur serveur.
5. **Consultez les résultats**. Le logiciel serveur renvoie la sortie de la demande du client à l'application client. Seuls les résultats sont envoyés, les données restent sur le serveur. L'utilisateur final peut ensuite utiliser l'application client pour affiner et éditer les résultats.

Administration du logiciel serveur

Ce guide est destiné principalement aux administrateurs système chargés d'intégrer la technologie du serveur dans un environnement en réseau dans lequel les applications client sont exécutées en mode d'analyse distribuée. Les tâches d'administration sont les suivantes:

Installation. Le logiciel serveur est conçu pour s'exécuter en continu et répondre aux connexions et aux demandes des ordinateurs de bureau des utilisateurs finaux. Sélectionnez un ordinateur serveur approprié pour le logiciel serveur-un ordinateur qui a peu de temps d'indisponibilité, qui est configuré pour l'accès de l'utilisateur final et qui est en réseau avec les ordinateurs de bureau appropriés. Plus la mémoire et la puissance de traitement de l'ordinateur serveur sont nombreuses, plus les demandes client sont traitées rapidement. L'application client doit être installée sur les ordinateurs de bureau de l'utilisateur final. L'installation du client peut être effectuée à partir d'un emplacement réseau. Chapitre 2, «Installation», à la page 7 fournit une présentation de l'installation du logiciel serveur et de l'application client. Des instructions d'installation détaillées sont fournies sur le produit Fichier ISO .

Accès aux données. Si vous devez fournir aux utilisateurs finaux l'accès aux données sur un serveur distant alors qu'ils travaillent en mode réparti, le logiciel serveur doit pouvoir accéder à ces données. Les produits IBM Corp. peuvent accéder aux données à partir de différents types de fichiers de données, y compris les bases de données. Pour faciliter votre travail, les produits IBM Corp. sont distribués avec DataDirect Connect ODBC pour l'accès aux données à partir d'une base de données. Chapitre 3, «Accès aux données», à la page 9 introduit l'accès aux données pour les produits IBM Corp. . Une documentation supplémentaire est incluse sur le produit Fichier ISO .

Configuration et maintenance. Etant donné que le logiciel serveur est destiné à un fonctionnement continu, il doit être surveillé à intervalles réguliers par un administrateur système. Il existe plusieurs options de configuration qui vous permettent de contrôler le fonctionnement du logiciel serveur. Chapitre 4, «Configuration, surveillance de l'utilisation et de la maintenance», à la page 15 décrit la configuration et la surveillance du logiciel serveur.

Prise en charge des utilisateurs finaux. Les utilisateurs finaux ont besoin d'informations sur les noms de serveur, les comptes utilisateur et l'emplacement des données. Vous devrez peut-être également les aider à résoudre les problèmes. Chapitre 5, «Prise en charge des utilisateurs finaux», à la page 25 décrit le type de prise en charge requis par les utilisateurs finaux.

Performances. Chapitre 6, «Analyse et amélioration des performances», à la page 49 fournit des stratégies permettant d'améliorer les performances du logiciel serveur.

Traitement des incidents. «logiciel serveur», à la page 53 fournit des conseils de traitement des incidents.

IBM SPSS Statistiques Batch Facility (IBM SPSS Statistiques Server uniquement). Le produit IBM SPSS Statistiques Server inclut IBM SPSS Statistiques Batch Facility, qui est destiné à la production automatisée de rapports statistiques. Si vous exécutez IBM SPSS Statistiques Server sur votre site, lisez la rubrique Annexe B, «IBM SPSS Statistiques Batch Facility», à la page 55, qui décrit IBM SPSS Statistiques Batch Facility et les tâches que vous devrez peut-être effectuer pour le prendre en charge.

Utilisation du présent document

Ce guide est destiné principalement aux administrateurs système chargés de l'installation et de la maintenance du logiciel serveur dans un environnement réseau dans lequel les applications client sont exécutées en mode d'analyse distribuée.

Chapitre 2. Installation

Les produits qui utilisent la technologie serveur sont conditionnés sur plusieurs supports: un Fichier ISO pour le logiciel serveur et un Fichier ISO pour l'application client.

Pour déployer la technologie du serveur, procédez comme suit:

- Installez le logiciel serveur sur un ordinateur serveur en réseau.
- Installez ou supervisez l'installation de l'application client afin qu'elle soit accessible à partir des ordinateurs de bureau de l'utilisateur final.

Ce chapitre fournit une présentation du processus d'installation. Des instructions d'installation détaillées sont disponibles sur votre produit Fichier ISO dans le répertoire */Documentation/<langue>/InstallationDocuments* répertoire.

Pour obtenir la liste complète des produits serveur et des applications client associées, voir «Produits et systèmes d'exploitation», à la page 1 .

Installation du logiciel serveur

Installez le logiciel serveur sur un ordinateur serveur en réseau. L'ordinateur serveur doit exécuter la version appropriée du système d'exploitation. Si possible, utilisez un ordinateur serveur configuré pour, et dédié à, un traitement numérique rapide et un accès aux données. La puissance de traitement et la mémoire supplémentaires améliorent les performances du logiciel serveur. La configuration matérielle et logicielle requise détaillée, y compris la configuration requise pour le système d'exploitation, apparaît dans les instructions d'installation.

L'installation de la technologie du serveur installe un logiciel qui gère l'accès aux données et effectue les calculs requis pour l'analyse statistique. Il installe également un service (sous Windows) ou un démon (sous UNIX) qui écoute les demandes de connexion d'utilisateur final entrantes et lance un processus pour traiter chaque utilisateur final.

Pour installer le logiciel serveur, suivez les instructions figurant dans le répertoire */Documentation/<langue>/InstallationDocuments* sur le serveur Fichier ISO .

Dépendance de compatibilité avec RHEL 10

Lorsque vous installez IBM SPSS Statistiques Server sur Red Hat Enterprise Linux s 10, le programme d'installation tente automatiquement d'installer le package de compatibilité requis (`libxcrypt-compat`).

Ce paquet fournit `libcrypt.so.1`, qui est nécessaire au fonctionnement du serveur sur les systèmes RHEL 10.

Le programme d'installation détecte la version du système d'exploitation lors de l'installation et n'installe le paquet que si nécessaire.

Installation de l'application client

L'installation de l'application client installe un logiciel qui gère l'interface utilisateur et la présentation des résultats. Vous devez installer ou superviser l'installation de l'application client sur l'ordinateur de bureau de chaque utilisateur final. L'ordinateur de bureau doit fonctionner sous Windows et doit répondre aux exigences minimales en matière de matériel et de système d'exploitation. Les exigences détaillées figurent dans les instructions d'installation, qui se trouvent dans le répertoire */Documentation/<langue>/InstallationDocuments* sur le client Fichier ISO .

Avant de lire d'autres documents d'installation, voir `Getting Started with Installation and Licensing.pdf`.

Chapitre 3. Accès aux données

Si vous souhaitez que vos utilisateurs finaux puissent accéder aux données des serveurs distants, y compris les données des bases de données, vous devez planifier, installer et configurer l'accès aux données. Pour ce faire, vous devez comprendre comment l'application décide où rechercher des données. Vous devez également décider si vous souhaitez utiliser la technologie d'accès aux données qui offre DataDirect Connect ODBC. Vous pouvez également utiliser des sources de données OLE DB.

Vue des données

Avant de commencer à planifier l'accès aux données pour les utilisateurs finaux, il est important de comprendre comment l'application décide quelles données sont disponibles pour l'utilisateur final. La vue des données présentées aux utilisateurs finaux dépend de la façon dont ils exécutent le programme-localement ou en mode réparti.

Mode d'analyse locale : En mode d'analyse locale, dans lequel tous les accès aux données et tous les traitements sont effectués sur l'ordinateur de bureau de l'utilisateur final, la vue des fichiers de données, des sources de données, des répertoires et des unités ODBC est du point de vue de l'ordinateur de bureau, c'est-à-dire que lorsque l'utilisateur final tente d'ouvrir un fichier de données, il voit les fichiers de données, les répertoires et les unités réseau sur son ordinateur de bureau.

Mode d'analyse distribuée : En mode d'analyse répartie, dans lequel l'accès aux données et le traitement des données se produisent sur un serveur distant, la vue des fichiers de données, des sources de données, des répertoires et des unités ODBC est du point de vue de l'ordinateur serveur, c'est-à-dire que lorsque l'utilisateur final tente d'ouvrir un fichier de données, il voit les fichiers de données, les répertoires et les unités montées sur l'ordinateur serveur.

Votre travail consiste à configurer l'accès aux données en mode d'analyse locale ou en mode d'analyse distribuée, selon les besoins de l'utilisateur final.

technologie Data Access

Vous trouverez ci-après une brève description de Connect ODBC . Pour plus d'informations sur le fonctionnement de la technologie d'accès aux données avec les produits IBM Corp. et pour des liens vers une documentation détaillée pour des bases de données spécifiques, voir *IBM SPSS Data Access Pack Installation Instructions* dans le répertoire */Documentation/<langue>/InstallationDocuments* sur le produit Fichier ISO .

Connect ODBC

Connect ODBC est un ensemble complet de pilotes individuels spécifiques à une base de données qui utilisent ODBC pour fournir la connectivité à tous les principaux magasins de données, des bases de données relationnelles aux données de fichiers à plat.

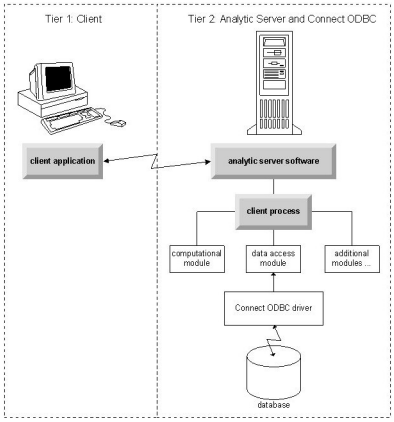

Figure 3. Connect ODBC en mode d'analyse distribuée

Accès aux données

Lorsque vous configurez l'accès aux données, tenez compte des points suivants:

Technologie d'accès aux données. Décidez si vous souhaitez utiliser l'une des technologies d'accès aux données distribuées avec votre produit IBM Corp. . Pour plus d'informations, voir «technologie Data Access», à la page 9. Une discussion plus détaillée sur le choix d'une technologie figure dans les *instructions d'installation de IBM SPSS Data Access Pack* (en anglais) */Documentation/<langue>/InstallationDocuments* sur le produit Fichier ISO).

Mode d'analyse. Le mode d'analyse de l'utilisateur final détermine les données auxquelles il peut accéder. Pour plus d'informations«Vue des données», à la page 9, voir la rubrique .

Performances du système de fichiers (Windows uniquement). Si la plupart de vos données sont dans un format propriétaire provenant de IBM Corp. (par exemple, des fichiers *.sav*) plutôt que dans une base de données, nous vous recommandons de les stocker sur une unité Windows NTFS en réseau pour des performances optimales.

Format de fichier. Le logiciel gère automatiquement l'ouverture et la lecture des fichiers au format UNIX-vous et vos utilisateurs finaux n'avez pas besoin d'effectuer d'action pour indiquer au logiciel qu'un fichier est au format UNIX.

Données de référencement

Certains logiciels client permettent à l'utilisateur final de sauvegarder des références à des données et à d'autres fichiers. Ces références doivent être écrites du point de vue de l'ordinateur qui va accéder aux données. Par exemple, si l'utilisateur final s'exécute en mode d'analyse locale, une référence à *C:\mydata\mydata.sav* fait que le logiciel tente d'accéder au fichier sur l'unité *C* locale du *ordinateur de bureau*. Si l'utilisateur final s'exécute en mode d'analyse distribuée, la même référence à *C:\mydata\mydata.sav* fait que le logiciel tente d'accéder au fichier sur l'unité *C* locale du *ordinateur serveur*, ce qui peut entraîner une erreur.

Windows. Si vous administrez un système Windows, vous pouvez décider de stocker des données sur le même ordinateur que le logiciel serveur. Si vous le faites, nous recommandons aux utilisateurs de se référer à l'emplacement des données du point de vue de l'ordinateur serveur (par exemple, *C:\ServerData\mydata.sav*). Les performances sont plus rapides car le réseau n'est pas utilisé pour localiser le fichier. Si vos données se trouvent sur un autre ordinateur en réseau, nous recommandons à vos utilisateurs d'utiliser des références de fichiers UNC (par exemple, *\\mydataserver\ServerData\mydata.sav*). Notez que les noms UNC ne peuvent être utilisés que lorsque les emplacements référencés contiennent le nom d'une *ressource partagée* sur le réseau. Les utilisateurs finaux qui passent fréquemment du mode d'analyse distribué au mode d'analyse local sont encouragés à utiliser les références de fichier UNC car ils fonctionnent quel que soit le mode.

UNIX. Si vous administrez une version UNIX du logiciel serveur, vous pouvez décider de placer des fichiers sur un serveur UNIX. Les utilisateurs finaux peuvent référencer des fichiers sur un serveur UNIX-

leur demander d'utiliser la spécification de fichier complète et des barres obliques (par exemple, */FILE ='/public/data/ourdata.txt'*). Evitez d'utiliser la barre oblique inversée dans le répertoire UNIX et dans les noms de fichier utilisés avec le logiciel serveur.

Contrôle de l'accès aux données

Vous pouvez contrôler l'accès aux données à l'aide du système d'exploitation pour définir les droits par ID utilisateur et groupes. L'utilisateur final se connecte au logiciel serveur en se connectant à partir de l'application client. Le logiciel serveur utilise le système d'exploitation pour appliquer les droits de cet utilisateur.

Remarque: Une sécurité de données supplémentaire peut être applicable avec votre logiciel de base de données-les modules d'accès aux données du logiciel serveur demandent des ID et des mots de passe lorsque la base de données les requiert.

Windows. La manière dont vous définissez les droits d'accès sous Windows dépend de l'emplacement de stockage des données.

- Si les fichiers résident sur un ordinateur réseau autre que l'ordinateur exécutant le logiciel serveur, affectez des droits d'accès aux ressources partagées.
- Si les fichiers résident sur l'ordinateur serveur et sur une unité NTFS, utilisez les paramètres de sécurité. Vous ne pouvez pas contrôler l'accès aux fichiers pour les données de l'ordinateur serveur sur une unité FAT.

Pour plus d'informations sur la définition des droits de partage et de sécurité sous Windows, voir «Propriétés de fichier», à la page 57 .

UNIX. Lorsque l'utilisateur final se connecte au logiciel serveur en se connectant à partir de l'application client, le logiciel serveur transmet l'ID de connexion et le mot de passe de l'utilisateur au système d'exploitation et lance un processus pour l'utilisateur. Le processus lancé dispose des droits d'accès aux fichiers du compte de connexion de l'utilisateur final.

Sources de données

ODBC

Le logiciel serveur IBM SPSS Statistiques utilise ODBC pour accéder à la plupart des données qui ne sont pas dans un format propriétaire, y compris les données stockées dans les bases de données. ODBC requiert une source de données ODBC . Une source de données ODBC est la combinaison des éléments suivants:

- Nom descriptif
- Un pilote spécifique
- Référence à une base de données ou à un autre type de fichier de données

Pour accéder à la plupart des données, vous devez configurer ou aider les utilisateurs finaux à configurer les sources de données ODBC dont ils ont besoin.

L'emplacement de la source de données configurée est critique. Il doit être configuré sur l'ordinateur qui accède aux données et les traite. Par conséquent, configurez la source de données ODBC sur l' *ordinateur serveur* pour l'analyse distribuée et sur l' *ordinateur de bureau* pour l'analyse locale. Par exemple, comparez l'emplacement des pilotes ODBC dans les figures indiquées dans «Connect ODBC», à la page 9 .

Si vous commencez tout juste à utiliser la technologie d'accès aux données (introduite dans «technologie Data Access», à la page 9), vous devez effectuer des tâches supplémentaires avant de pouvoir configurer une source de données. Reportez-vous aux *instructions d'installation IBM SPSS Data Access Pack* (dans / Documentation/<langue>*/Documents* d'installation sur le produit Fichier ISO). La configuration de la source de données est abordée à nouveau dans la section Chapitre 4, «Configuration, surveillance de l'utilisation et de la maintenance», à la page 15 de ce guide.

Configuration de l'environnement UNIX pour l'accès aux données

Pour que la technologie d'accès aux données fonctionne sur les systèmes UNIX, le script de démarrage du logiciel serveur doit être configuré.

Ouvrir le script de démarrage

1. Accédez au sous-répertoire */bin* dans le répertoire d'installation du logiciel serveur. Par exemple, à l'invite UNIX, saisissez :

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

   où */usr/local/serverproduct/bin* est le sous-répertoire */bin* du répertoire dans lequel le logiciel serveur est installé.
2. Ouvrez *statsenv.sh* à l'aide d'un éditeur de texte.

Spécifiez le script DataDirect

1. Recherchez le premier commentaire contenant le texte:

   MERANT_ENVIRONNEMENT_SCRIPT
2. Recherchez la ligne qui définit l'emplacement de **odbc.sh**.
3. Modifiez la ligne de sorte qu'elle contienne le chemin d'accès correct à votre installation client Connect ODBC et supprimez le caractère de commentaire s'il en comporte un. Par exemple, remplacez le code suivant :

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

pour :

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

Ajouter une variable d'environnement odbc.ini

1. Ajoutez les lignes suivantes après les lignes ci-dessus pour créer une variable d'environnement, ODBCINI, qui permet à IBM SPSS Statistiques Server de trouver le fichier *odbc.ini* :

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

où ODBCDIR est remplacé par le chemin d'accès à votre répertoire d'installation Connect ODBC .

Ajouter des chemins aux bibliothèques de base de données

1. Ajoutez des lignes adaptées à votre base de données, généralement le *répertoire de base de la base de données* et, si vous n'utilisez *pas* les pilotes DataDirect Wire Protocol, un *chemin d'accès aux bibliothèques de base de données*. Par exemple, si vous utilisez Oracle sous Linux, ajoutez les lignes suivantes:

```
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
```

où */disque/oracle/produit/8.1.6* est remplacé par le chemin d'accès à votre répertoire d'installation Oracle et LD_LIBRARY_PATH correspond à la variable du chemin de bibliothèque pour votre système d'exploitation.

Les pilotes DataDirect Wire Protocol ne nécessitent pas l'installation de bibliothèques client de base de données. Toutefois, d'autres pilotes DataDirect exigent ces bibliothèques.

Sauvegarder le script de démarrage

1. Sauvegardez *statsenv.sh*.

Editez odbc.ini

1. Editez *odbc.ini*, le fichier de configuration ODBC , de sorte que les sources de données ODBC soient accessibles à partir de IBM SPSS Statistiques Server. Reportez-vous à l'annexe sur l'environnement UNIX du document DataDirect intitulé *DataDirect Connect ODBC Reference* (disponible si vous avez installé la documentation DataDirect supplémentaire au moment de l'installation de Connect ODBC) et aux chapitres relatifs aux pilotes spécifiques dans le document *odbchelp.pdf*, situé dans le sous-répertoire *doc* de votre répertoire d'installation Connect ODBC.

La modification sera prise en compte lors du prochain démarrage du logiciel serveur.

Remarque : Si vous prévoyez d'utiliser ODBC avec IBM SPSS Statistiques Batch Facility, vous devez modifier le script de démarrage de IBM SPSS Statistiques Batch Facility de la même manière.

Chapitre 4. Configuration, surveillance de l'utilisation et de la maintenance

Après avoir installé le logiciel serveur, configurez son environnement en:

- Gestion des comptes et des fichiers de l'utilisateur final
- Configuration des sources de données ODBC
- Utilisation de l'application d'administration (IBM SPSS Statistics Administration Console) pour configurer et surveiller le logiciel serveur
- Contrôle du démarrage du service

Ces tâches sont décrites dans les sections suivantes.

Gestion des comptes et des fichiers d'utilisateur final

Cette section fournit une vue d'ensemble de ce que vous devez faire pour prendre en charge les utilisateurs finaux sur votre site. Pour plus d'informations, voir Chapitre 5, «Prise en charge des utilisateurs finaux», à la page 25.

Comptes

Les utilisateurs finaux ont besoin de comptes pour se connecter au logiciel serveur et accéder aux données. Ces comptes doivent être authentifiés et pouvoir lire, écrire et / ou exécuter dans des dossiers spécifiques sur la machine du serveur. Pour plus d'informations sur les droits d'accès aux fichiers, voir la rubrique «Autorisations», à la page 33. Pour plus d'informations sur l'authentification, voir la rubrique «Authentification», à la page 25.

Les droits d'accès à la base de données sont appliqués par le logiciel de base de données. Utilisez vos outils d'administration de base de données habituels pour gérer ces comptes. Si la base de données est restreinte, les modules d'accès aux données du logiciel serveur invitent l'utilisateur à se connecter et à transmettre ces informations à la base de données pour vérification avant d'accéder aux données.

Accès aux données

Par défaut, chaque utilisateur final peut voir toutes les données lors de l'ouverture d'un fichier lorsqu'il est connecté au logiciel serveur. L'affichage de toutes les données peut avoir un impact négatif sur les performances et augmenter le trafic réseau. Vous pouvez choisir d'empêcher les ordinateurs client de l'utilisateur final d'afficher les données en modifiant le paramètre global avec l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée dans le cadre de IBM SPSS Responsable du déploiement). Pour plus d'informations, voir la rubrique Utilisateurs dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement). Vous pouvez également modifier les paramètres du profil utilisateur et des groupes afin de spécifier l'accès aux données pour des utilisateurs ou des groupes individuels. Pour plus d'informations, voir la rubrique IBM SPSS Statistics Server dans le document *Deployment Manager User's Guide*.

Fichiers

La plupart des fichiers que les utilisateurs finaux doivent enregistrer doivent être enregistrés sur l'ordinateur de bureau ; cependant, vous pouvez être amené à autoriser les utilisateurs à enregistrer des fichiers de données sur un ordinateur en réseau. Lorsque l'utilisateur final se connecte au logiciel du serveur analytique pour la première fois, le répertoire par défaut pour l'ouverture et la sauvegarde des fichiers est le répertoire d'installation du logiciel du serveur. Il est clair qu'il ne s'agit pas d'un emplacement où vous voulez que les utilisateurs écrivent des fichiers. Par conséquent, configurez un

répertoire avec des droits d'accès en écriture et distribuez cet emplacement aux utilisateurs finaux. Une fois qu'ils accèdent à cet emplacement à partir de l'interface utilisateur, l'application client le stocke et devient l'emplacement par défaut pour les fichiers sauvegardés.

Profils

Le logiciel serveur vous permet également de créer des profils pour les utilisateurs. Un profil peut spécifier le répertoire temporaire, le paramètre UNIX `umask` , la priorité du processus d'UC, le paramètre d'accès aux données client et le nombre maximal d'unités d'exécution pour chaque utilisateur ou groupe d'utilisateurs.

Profils utilisateur et groupes d'utilisateurs d'IBM SPSS Statistiques Server

Le logiciel serveur permet de créer des profils utilisateur et des groupes d'utilisateurs spécifiques. Le profil indique le répertoire des fichiers temporaires, le paramètre `umask` UNIX, la priorité de processus d'UC, l'accès aux données client et le nombre maximal d'unités d'exécution d'un utilisateur ou d'un groupe d'utilisateurs. Ces paramètres remplacent les paramètres globaux par défaut associés. .

Fichier de profil

Les paramètres appliqués aux profils utilisateur et aux groupes d'utilisateurs sont stockés dans le fichier de profil, *UserSettings.xml*. Par défaut, ce fichier se trouve dans le sous-répertoire `config` du répertoire d'installation du serveur IBM SPSS Statistiques. Avant de modifier les profils d'utilisateurs et les groupes, il est recommandé de déplacer le fichier par défaut et de spécifier le nouvel emplacement dans l'application d'administration (IBM SPSS Statistics Administration Console).

Application des paramètres par le serveur

Le serveur suit les étapes ci-dessous pour identifier les fichiers temporaires, le paramètre umask, la priorité d'UC, l'accès aux données client et le nombre maximal d'unités d'exécution d'un utilisateur spécifique.

1. Recherchez un profil utilisateur correspondant au nom d'utilisateur et au domaine de l'utilisateur qui se connecte au serveur. Sélectionnez la première entrée concordante trouvée. Sous UNIX, le serveur ignore le domaine et fait une distinction entre les majuscules et les minuscules pour le nom d'utilisateur. Sous Windows, il n'y a pas de distinction entre les majuscules et les minuscules pour le nom d'utilisateur et le domaine. Si un utilisateur connecté au serveur s'est connecté sans indiquer de domaine, le serveur recherche un nom d'utilisateur dont le nom de domaine est vide. S'il n'en trouve pas, il utilise une entrée concordante incluant uniquement le nom d'utilisateur.
2. Si le profil utilisateur définit des paramètres, appliquez-les au processus serveur.
3. Si le profil utilisateur ne définit pas de paramètres ou n'en définit qu'une partie, appliquez les paramètres du groupe d'utilisateurs au processus serveur.
4. Si certains paramètres ne sont toujours pas définis ou s'il n'y a pas de profil d'utilisateur correspondant, appliquez l'umask par défaut, le répertoire de fichiers temporaires, le paramètre d'accès aux données du client et le nombre maximal de threads défini par l'application d'administration (IBM SPSS Statistics Administration Console). Aucun traitement par défaut de la priorité du processeur n'est utilisé. .

Configuration des sources de données ODBC

Si vos utilisateurs finaux accèdent à des données à partir de bases de données alors qu'ils travaillent en mode d'analyse distribuée, vous devez configurer des sources de données ODBC sur l'ordinateur sur lequel le logiciel serveur est installé.

ODBC Data Sources et IBM SPSS Data Access Pack

Si vous utilisez la technologie d'accès aux données IBM Corp. , lisez Chapitre 3, «Accès aux données», à la page 9 dans ce document. Lisez les *instructions d'installation* appropriées pour obtenir une vue d'ensemble de la configuration de l'accès aux bases de données et des liens vers la documentation détaillée sur l'accès aux données pour des bases de données spécifiques (le document se trouve dans la rubrique */Documentation/<langue>/InstallationDocuments* sur le site du produit Fichier ISO).

Fenêtres. Configurez les sources de données ODBC à l'aide de l'administrateur ODBC . Pour plus d'informations«Administrateur ODBC», à la page 58, voir la rubrique .

UNIX. Editez le script d'environnement de démarrage du logiciel serveur comme décrit dans «Configuration de l'environnement UNIX pour l'accès aux données», à la page 12 et configurez les sources de données ODBC à l'aide du fichier *odbc.ini* . Pour plus d'informations, voir la rubrique «odbc.ini», à la page 62 .

Utilisation d'un moteur de tri tiers

Par défaut, le logiciel serveur tente d'utiliser un moteur tiers externe pour le tri. Pour utiliser le moteur de tri approprié, procédez comme suit:

1. Si le moteur de tri tiers n'est pas installé sur l'ordinateur serveur, installez-le. IBM Corp. ne fournit pas les moteurs. Vous devez acheter un moteur auprès d'un fournisseur tiers et lui attribuer une licence.
2. Vérifiez que la bibliothèque du moteur de tri se trouve dans la variable de chemin d'exécution ou de bibliothèque du système. Sous Windows, il s'agit de la variable d'environnement PATH ; sous UNIX, il s'agit de LD_LIBRARY_PATH ou LIBPATH, selon le fournisseur UNIX. Cette étape est requise pour permettre au logiciel serveur de charger la bibliothèque de tri tierce.
3. A l'aide de l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée dans le cadre de IBM SPSS Responsable du déploiement), définissez l'option Trier sur le moteur tiers approprié. Pour plus d'informations, consultez la rubrique Utilisateurs dans le *Guide de l'utilisateur de Deployment Manager* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement).

Toutes les procédures nécessitant un tri (par exemple, SORT) utiliseront ensuite le moteur de tri tiers. L'émission de la commande de syntaxe `SET SORT=INTERNAL` force le logiciel serveur à utiliser l'algorithme interne pour le tri. Un utilisateur final peut également spécifier explicitement le tri par des tiers en émettant la commande `SET SORT=EXTERNAL` . Toutefois, cela n'est pas nécessaire car le tri par des tiers est la valeur par défaut.

Vérification de l'option de tri en cours

Pour vérifier quelle option de tri est utilisée, vous pouvez exécuter la commande de syntaxe `SET MESSAGES ON` et exécuter un travail `SORT` . Vous pouvez également utiliser la commande de syntaxe `SHOW SORT` .

Administration d'IBM SPSS Statistiques Server

IBM SPSS Statistics Administration Console fournit une interface utilisateur pour surveiller et configurer les installations d'IBM SPSS Statistiques Server. Le IBM SPSS Statistics Administration Console est installé avec IBM SPSS Responsable du déploiement. La documentation complète de IBM SPSS Statistics Administration Console est incluse dans la section *Administration Consoles* du document *Deployment Manager User's Guide* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement).

Configuration de Xtensions

Un administrateur IBM SPSS Statistiques Server doit suivre les étapes pour que les procédures Xtension (krr, lenr, lrr et lrr) soient disponibles pour une exécution dans **`statsb`** et SPSS Statistics Server. Les procédures Xtension comprennent:

- Régression de crête du noyau (KRR)

- Régression linéaire élastique nette (LENR)
- Régression lasso linéaire (LLR)
- Régression linéaire de crête (LRR)

Installation de Xtensions sur SPSS Statistics Server

1. Sur le client IBM SPSS Statistiques , installez les Xtensions (en mode local) à partir du concentrateur d'extension.
2. Vérifiez que la bibliothèque **sklearn** est installée sur le serveur IBM SPSS Statistiques .

   UNIX
   Exécutez la commande suivante en tant qu'utilisateur ayant installé SPSS Statistics Server.

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

   Remarque : statisticspython3 se trouve dans le répertoire `bin` de l'installation du serveur SPSS Statistics .

   Windows ®
   Exécutez la commande suivante.

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

   Remarque : statisticspython3.bat se trouve dans le répertoire d'installation de SPSS Statistics Server.
3. Copiez le répertoire `xtensions` et son contenu du client SPSS Statistics (`%APPDATA%\IBM\SPSS Statistics\one\xtensions\` sous Windows, `$HOME/Library/Application Support/IBM/SPSS Statistics/one/xtensions` sous macOS) dans le répertoire d'installation de SPSS Statistics Server.

SPSS Statistics Le serveur est maintenant prêt à exécuter les procédures Xtension qui sont installées dans le répertoire `xtensions` .

Configuration de l'interface de ligne de commande de l'environnement de production en vue de la soumission de travaux

Depuis IBM SPSS Statistiques version 26, vous pouvez utiliser l'interface de ligne de commande de l'environnement de production pour soumettre des travaux à SPSS Statistics Server. Lorsque l'interface de ligne de commande de l'environnement de production est utilisée avec le Planificateur de tâches Microsoft Windows ou MacOS Automator pour la planification des travaux, vous pouvez remplacer IBM SPSS Services de collaboration et de déploiement de manière efficace pour le traitement des travaux SPSS Statistics.

La commande SPSS Statistics **INSERT HIDDEN** peut exécuter des travaux qui génèrent une sortie. Lorsque cette commande est employée, les utilisateurs ne peuvent pas accéder à la syntaxe SPSS Statistics source, ni l'afficher.

Remarque : La commande **INSERT HIDDEN** requiert un serveur SPSS Statistics Server. Cette commande ne fonctionne pas sur une machine client SPSS Statistics autonome.

Fonction INSERT HIDDEN

Les administrateurs peuvent activer la fonction **INSERT HIDDEN** à l'aide de la console d'administration du serveur SPSS Statistics ou en éditant le fichier `<install_path>/config/statisticsd.conf` (**INSERT HIDDEN = Enabled**). La zone **INSERT HIDDEN Feature** se trouve dans l'onglet SPSS Statistics Server Configuration de la console d'administration de SPSS Statistics Server (sous la section **Users**).

1. Sélectionnez **activée** pour la valeur de **INSERT HIDDEN Feature**. Notez qu'un astérisque(*) apparaît dans l'onglet de configuration de SPSS Statistics Server.
2. Sauvegardez la modification. Cliquez sur l'icône **Enregistrer** de la barre d'outils, appuyez sur Ctrl+S ou sélectionnez **Fichier** > **Enregistrer**.
3. Redémarrez le serveur SPSS Statistics.
4. Après le redémarrage du serveur sur les serveurs Windows, une boîte de dialogue invite les administrateurs à entrer le mot de passe de la fonction **INSERT HIDDEN Feature**. Sur les serveurs Linux, l'administrateur doit démarrer manuellement SPSS Statistics Server. Lorsque le serveur redémarre, il invite l'administrateur à saisir le mot de passe.

   Le mot de passe est stocké dans le registre système (comme un mot de passe SSL) et tous les fichiers de syntaxe masqués sont chiffrés avec le même mot de passe.

L'administrateur peut éventuellement refuser l'accès utilisateur aux fichiers **INSERT HIDDEN** via les contrôles d'accès au système de fichiers.

Le processus démon de SPSS Statistics Server requiert un accès en lecture aux fichiers **INSERT HIDDEN**. Il est possible d'utiliser une commande OMS pour encapsuler la syntaxe afin de s'assurer que la sortie n'est pas envoyée au visualiseur de sortie.

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

La syntaxe de **INSERT HIDDEN** est similaire à celle de **INSERT FILE**. Par exemple :

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

L'auteur du fichier **INSERT HIDDEN** fournit les chemins d'accès au fichier caché aux utilisateurs de la machine client SPSS Statistics. Lors de l'exécution, les utilisateurs du client exécutent la syntaxe **INSERT HIDDEN SOURCE="<file_path>"** .

Le processus client sur SPSS Statistics Server envoie le chemin **SOURCE** au processus démon du serveur. Le processus démon déchiffre le fichier, puis le renvoie au processus client en vue de son exécution.

Le processus client désactive les journaux, exécute le fichier déchiffré, puis réactive les journaux. Le visualiseur de sortie de SPSS Statistics ne contient donc aucune journalisation de syntaxe source (il contient la sortie). Le journal ne contient non plus aucune syntaxe source.

Configuration de plusieurs instances

Vous pouvez créer plusieurs instances du logiciel serveur, chacune avec son propre numéro de port. Ceci est souvent utilisé en conjonction avec l'autorisation de groupe pour affecter un groupe d'utilisateurs à une instance spécifique. Toutefois, plusieurs instances peuvent être utilisées indépendamment de l'autorisation de groupe. Pour plus d'informations sur l'autorisation de groupe, voir «Autorisation de groupe», à la page 33.

Création d'une nouvelle instance

Pour créer une instance de groupe du logiciel serveur, vous devez exécuter un script.

Sous Windows, exécutez le script suivant à partir du répertoire d'installation du serveur.

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

Sous UNIX et Linux, exécutez le script suivant à partir du sous-répertoire `bin` du répertoire d'installation.

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

`<group_name>` est un nom unique pour l'instance et `<port_number>` est le numéro de port disponible qui sera utilisé par l'instance.

Une fois le script exécuté, il existe un dossier de configuration spécifique à l'instance. Recherchez `config_<groupname>` dans la direction d'installation du serveur. Le dossier contient plusieurs fichiers de configuration, tels que `statisticsd.conf` et `UserSettings.xml`. Lorsque vous souhaitez mettre à jour la configuration d'une instance spécifique, veillez à mettre à jour le fichier de configuration à l'emplacement approprié.

Démarrage de l'instance de serveur

Sous Windows, l'instance est un service distinct nommé *IBM SPSS Statistiques NN.m*, où *NN* est le numéro de version principale et *m* est le numéro de version secondaire. Vous pouvez démarrer et arrêter ce service comme n'importe quel autre service Windows.

Sous Linux et UNIX, vous devez spécifier le nom de groupe lors de l'exécution du script de démarrage:

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

où `<group_name>` est le nom du groupe d'instances.

Suppression d'une instance de serveur

1. Sous Windows, supprimez l'entrée de service:
   a. Ouvrez une invite de commande en tant qu'administrateur.
   b. Exécutez la commande suivante :

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

      où *NN* est le numéro de version principale, *m* est le numéro de version secondaire et *<nom_groupe>* est le groupe d'instances.
2. Supprimez le sous-répertoire `config_<groupname>` du répertoire d'installation du serveur.

Contrôle du démarrage du service

Le logiciel serveur possède un composant d'infrastructure qui gère toutes les communications entre l'application client et les modules. Sous Windows, le composant d'infrastructure est un service. Sous UNIX, le composant d'infrastructure est une application, généralement exécutée en tant que démon.

Fenêtres

Par défaut, le service est configuré pour le démarrage automatique, ce qui signifie qu'il redémarrera automatiquement lorsque l'ordinateur sera redémarré. Lorsqu'il est démarré de cette manière, le service s'exécute sans surveillance et l'ordinateur serveur peut être déconnecté sans affecter le service. Vous pouvez utiliser le panneau de configuration des services Windows pour modifier les paramètres de démarrage du service. Pour plus d'informations, voir la rubrique «Panneau de configuration des services», à la page 58. Si vous exécutez plusieurs instances, le panneau Services inclut une entrée pour chaque instance de serveur.

Remarque : Si l'ordinateur serveur ne prend pas en charge l'adresse IP du système hôte local (127.0.0.1/::1), vous devez créer une variable d'environnement système nommée `STATS_LH_OVERRIDE` et définir sa valeur sur YES avant de démarrer le serveur. Pour plus d'informations sur le démarrage et l'arrêt du serveur, voir «Démarrage et arrêt du logiciel serveur», à la page 22.

UNIX

Un script de démarrage, *start_statistics_server*, est inclus dans le sous-répertoire */bin* du répertoire d'installation. Le script appelle *statsenv.sh* pour configurer l'environnement du logiciel serveur, puis démarre l'application. Vous devez démarrer le logiciel serveur avec ce script. Le script de démarrage doit être exécuté à partir du sous-répertoire */bin* . Pour l'exécuter, vous devez être connecté en tant que **root** si vous utilisez l'authentification unix par défaut ou le module PAM (Pluggable Authentication Module). Sinon, vous devez être connecté en tant qu'utilisateur propriétaire du démon du logiciel serveur. Pour plus d'informations sur l'authentification, voir la rubrique «Authentification», à la page 25. La commande :

```
./start_statistics_server -d
```

démarrera le logiciel serveur en tant que processus démon, ce qui est la méthode recommandée pour exécuter le logiciel serveur.

Si vous exécutez plusieurs instances du logiciel serveur, cette commande démarre l'instance par défaut. Pour démarrer une autre instance, spécifiez le groupe d'instances avec le commutateur `-g` :

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

où `<groupname>` est le nom du groupe d'instances.

Remarque : Si l'ordinateur du serveur ne prend pas e charge l'adresse IP de l'hôte local (127.0.0.1/::1), vous devez affecter à la variable d'environnement `STATS_LH_OVERRIDE` la valeur YES avant de démarrer le serveur. La variable `STATS_LH_OVERRIDE` est définie à partir du fichier `statsenv.sh`, qui se trouve dans le sous-répertoire `/bin` du répertoire d'installation. Pour plus d'informations sur le démarrage et l'arrêt du serveur, voir «Démarrage et arrêt du logiciel serveur», à la page 22.

Paramètres de ligne de commande du script de démarrage

Le script *start_statistics_server* accepte les paramètres de ligne de commande suivants (dans n'importe quel ordre):

- **Démon**. Exécutez le logiciel serveur en tant que processus démon en spécifiant éventuellement `-d`. Si vous omettez `-d`, le serveur démarre en tant que processus d'avant-plan. Par exemple, pour démarrer le logiciel serveur en tant que démon, utilisez la commande suivante:

  ```
  ./start_statistics_server -d
  ```

- **Groupe.** Si vous exécutez plusieurs instances du logiciel serveur, indiquez le groupe associé à l'instance:

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

  où

  `<groupname>` est le nom de groupe approprié.

- **Port.** Un numéro de port peut éventuellement être spécifié sur la ligne de commande du script de démarrage. Par exemple, pour spécifier un numéro de port, utilisez la commande suivante:

  ```
  start_statistics_server -p nnnn
  ```

  où

  nnnn est le numéro de port souhaité.

  Indiquez un numéro de port uniquement si vous devez résoudre un conflit de numéro de port. La valeur par défaut fonctionne sauf si une autre application de l'ordinateur utilise le même numéro. Ce paramètre de ligne de commande remplace la valeur définie dans l'application d'administration.

Autre maintenance

Supprimez les fichiers inutiles. Recherchez régulièrement les fichiers inutiles dans l'emplacement du fichier temporaire et dans l'emplacement du fichier journal, puis supprimez-les. Les emplacements sont définis avec l'application d'administration.

Vérifiez les processus en cours d'exécution. Si vous ne réamorcez pas régulièrement l'ordinateur serveur, vérifiez régulièrement les processus en cours d'exécution sur l'ordinateur et arrêtez les processus qui ne sont pas utilisés. Les noms de processus sont répertoriés dans le «Démarrage et arrêt du logiciel serveur», à la page 22 .

Démarrage et arrêt du logiciel serveur

L'application d'administration redémarre le logiciel serveur pour vous afin que les modifications de configuration puissent être validées. Toutefois, il peut être nécessaire de démarrer ou d'arrêter le logiciel serveur à partir du système d'exploitation. Suivez les étapes ci-dessous pour votre système d'exploitation, en utilisant le nom de processus de votre produit serveur. Sous Windows, le nom de service par défaut est *IBM SPSS Statistiques NN.m*, où *NN* est le numéro de version principale et *m* est le numéro de version secondaire. Si vous exécutez plusieurs instances, le nom de service est *IBM SPSS Statistiques NN.m < groupname>*, où *NN* est le numéro de version principale, *m* est le numéro de version secondaire et *< groupname>* est le groupe de l'instance. Sous UNIX et Linux, le nom du démon est *statisticsd*.

Remarque concernant la planification: L'arrêt du service ou du démon déconnecte les utilisateurs finaux et met fin à leurs processus. Par conséquent, essayez de planifier les tâches de configuration et de maintenance à un moment où vous prévoyez que peu d'utilisateurs accèdent au système (par exemple, tôt le matin ou tard le soir).

Pour démarrer le service ou le démon

Windows. Utilisez le panneau de configuration des services Windows pour démarrer le service. Pour plus d'informations«Panneau de configuration des services», à la page 58, voir la rubrique .

UNIX. Démarrez le serveur avec le script de démarrage, *start_statistics_server*, qui est inclus dans le sous-répertoire */bin* du répertoire d'installation. Le script de démarrage doit être exécuté à partir du sous-répertoire */bin* . Pour l'exécuter, vous devez être connecté en tant que **root** si vous utilisez l'authentification unix par défaut ou le module PAM (Pluggable Authentication Module). Sinon, vous devez être connecté en tant qu'utilisateur propriétaire du démon du logiciel serveur. Pour plus d'informations sur l'authentification, voir la rubrique «Authentification», à la page 25.

Pour arrêter le service ou le démon

Windows. Utilisez le panneau de configuration des services Windows pour arrêter le service. Pour plus d'informations«Panneau de configuration des services», à la page 58, voir la rubrique .

UNIX. Arrêtez le processus serveur. (Voir «ps et kill», à la page 62 pour un exemple.) Le démon crée automatiquement un fichier (*statisticsd.pid*) qui contient l'ID de processus du démon. Vous pouvez utiliser ce fichier avec la commande kill en exécutant la commande suivante à partir du sous-répertoire `config` du répertoire d'installation ou du fichier `config_<group_name>` pour une autre instance du logiciel serveur:

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

Indépendante de la plateforme. Utilisez l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée avec IBM SPSS Responsable du déploiement). Pour plus d'informations, voir la rubrique Contrôle du serveur IBM SPSS Statistics Server dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement).

Configuration pour l'amélioration des performances

Pour plus d'informations sur la modification de la configuration du logiciel serveur afin d'améliorer les performances, voir Chapitre 6, «Analyse et amélioration des performances», à la page 49 .

Chapitre 5. Prise en charge des utilisateurs finaux

La prise en charge des utilisateurs finaux implique de s'assurer qu'ils disposent des informations dont ils ont besoin pour exécuter leur produit IBM Corp. en mode d'analyse distribuée. Pour utiliser le logiciel serveur, les utilisateurs finaux doivent savoir:

- Comment se connecter au logiciel serveur.
- Comment accéder aux données et aux fichiers.
- Emplacement de sauvegarde des données et des fichiers.

Authentification

Vous disposez de plusieurs options pour l'authentification des utilisateurs. Certaines options nécessitent que le serveur s'exécute avec des privilèges de superutilisateur.

Tableau 1. Options d'authentification

Méthode	**Disponibilité du système d'exploitation**	**Le serveur doit être exécuté en tant que système / racine?**
Authentification standard au niveau du système d'exploitation (compte Windows ou UNIX)	• Fenêtres • UNIX	Oui
Module PAM (Pluggable Authentication Module)	• UNIX	Oui
Authentification interne	• Fenêtres • UNIX	Non
unix2	• UNIX	Non
Connexion unique	• Fenêtres • UNIX	Non

Configuration de l'authentification au niveau du système d'exploitation

L'authentification au niveau du système d'exploitation est la méthode d'authentification par défaut. Utilisez vos outils d'administration système habituels pour créer et gérer des comptes d'utilisateur final de niveau système d'exploitation standard (voir «Gestionnaire des utilisateurs», à la page 58 pour plus d'informations sur l'accès au gestionnaire d'utilisateurs Windows).

Si vous essayez une autre méthode d'authentification et que vous souhaitez rétablir l'authentification au niveau du système d'exploitation, vous devez mettre à jour l'élément *userauth* dans le fichier `statisticsd.conf` et remplacer le paramètre *value* par `unix` ou `win32`.

Configuration du module PAM

Le logiciel serveur sous UNIX peut utiliser le module PAM (Pluggable Authentication Module) pour authentifier les utilisateurs. Vous devez d'abord configurer le logiciel serveur pour utiliser PAM. Ensuite, vous configurez PAM en suivant les instructions spécifiques à votre fournisseur UNIX. Pour Linux, procédez comme suit. Elles peuvent varier en fonction de la version et du fournisseur.

Remarque: Si le logiciel serveur est en cours d'exécution, vous devez le redémarrer après avoir effectué toutes les étapes.

Configuration du logiciel serveur pour l'utilisation de PAM

1. Connectez-vous à la machine UNIX en tant que *root*.
2. Dans le sous-répertoire *config* du répertoire d'installation du logiciel serveur, ouvrez le fichier de configuration (par exemple, *statisticsd.conf*) dans un éditeur de texte.
3. Recherchez l'élément *userauth* et remplacez le paramètre *value* `unix` par `pam`.
4. Sauvegardez le fichier.

Configuration de PAM sous Linux

1. Accédez au répertoire de configuration PAM (par exemple, */etc/pam.d*).
2. Utilisez un éditeur de texte pour créer un fichier nommé *statisticsd*.
3. Ajoutez les informations de configuration PAM que vous souhaitez utiliser. Par exemple :

```
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
```

   Remarque: ces lignes peuvent varier en fonction de votre configuration particulière. Pour plus d'informations, consultez la documentation Linux .
4. Sauvegardez le fichier.

Configuration de l'authentification interne

L'authentification interne permet au logiciel serveur de s'exécuter sans privilèges de superutilisateur. Cependant, il limite les connexions client au même accès au disque. Chaque utilisateur qui se connecte au logiciel serveur dispose de la même sécurité d'accès au disque. Par conséquent, un utilisateur peut supprimer le fichier d'un autre utilisateur. Dans ce cas, il est recommandé d'utiliser la méthode d'authentification unix2 à la place. Cette méthode ne restreint pas les connexions client car elle utilise le fichier *passwd* UNIX pour l'authentification. Pour plus d'informations«Configuration de l'authentification unix2», à la page 27, voir la rubrique .

Avertissement : N'utilisez pas l'authentification interne lors de l'exécution du démon / service en tant que root/SYSTEM. Cela revient à accorder l'accès root/SYSTEM à votre serveur à n'importe quel utilisateur qui se connecte.

Configuration de l'authentification interne sous UNIX

1. Créez un groupe pour les utilisateurs qui se connecteront au logiciel serveur. Il est recommandé de nommer ce groupe **statistics**.
2. Un membre de ce groupe doit installer le logiciel serveur. Cet utilisateur sera le propriétaire du démon du logiciel serveur.
3. Un autre membre de ce groupe (différent du propriétaire du démon et généralement de l'utilisateur qui gère les utilisateurs du logiciel serveur) crée un fichier *statisticsusers* dans le répertoire *config* du répertoire d'installation du logiciel serveur. Ce fichier doit disposer d'un accès en lecture / écriture pour l'utilisateur qui l'a créé. Il doit disposer d'un accès en lecture pour le groupe d'utilisateurs. Aucun autre utilisateur ne doit pouvoir y accéder. Si vous ne créez pas ce fichier manuellement, il est automatiquement créé la première fois que vous exécutez l'outil de ligne de commande `statisticsuser` (voir l'étape suivante). L'outil de ligne de commande définit les droits appropriés.
4. Dans le répertoire *config* , utilisez l'outil de ligne de commande `statisticsuser` pour ajouter des utilisateurs. En tant qu'utilisateur ayant créé le fichier *statisticsusers* , entrez `statisticsuser <username>` pour créer un utilisateur standard (par exemple, `statisticsuser jdoe`). Utilisez l'option `-a` pour créer un administrateur (par exemple, `statisticsuser -a jdoe`). L'outil de ligne de commande `statisticsuser` vous invite à entrer un mot de passe. Un utilisateur final entre le nom d'utilisateur et le mot de passe pour se connecter au logiciel serveur. Veillez à distribuer le

nom d'utilisateur et les mots de passe de manière appropriée. Pour supprimer un utilisateur, utilisez l'option `-d` (par exemple, `statisticsuser -d jdoe`).

5. Connecté en tant que propriétaire du démon du logiciel serveur, ouvrez le fichier de configuration (par exemple, *statisticsd.conf*) dans un éditeur de texte.
6. Recherchez l'élément *userauth* et remplacez le paramètre *value* `unix` par `internal`.
7. Si vous êtes connecté en tant que propriétaire du démon du logiciel serveur, démarrez le serveur.

Configuration de l'authentification interne sous Windows

1. Editez l'entrée IBM SPSS Statistics Server pour l'exécuter en tant qu'utilisateur spécifique:
   a. Ouvrez le panneau des services Windows et cliquez deux fois sur l'entrée pour *IBM SPSS Statistiques NN.m*, où *NN* est le numéro de version principale et *m* est le numéro de version secondaire.
   b. Cliquez sur l'onglet **Connexion**.
   c. Sous **Se connecter en tant que**, sélectionnez **Ce compte**.
   d. Entrez le domaine \username et le mot de passe de l'utilisateur qui sera propriétaire du processus serveur. Cet utilisateur aura besoin du privilège *Connexion en tant que service* .
2. Le même utilisateur doit créer un fichier `statisticsusers` dans le répertoire `config` du répertoire d'installation des logiciels du serveur. Ce fichier doit disposer d'un accès en lecture / écriture pour l'utilisateur qui l'a créé. Aucun autre utilisateur ne doit disposer d'un accès en écriture. Si vous ne créez pas ce fichier manuellement, il est automatiquement créé la première fois que vous exécutez l'outil de ligne de commande `statisticsuser` (voir l'étape suivante).
3. Dans le répertoire `config` , utilisez l'outil de ligne de commande `statisticsuser` pour ajouter des utilisateurs. En tant qu'utilisateur ayant créé le fichier `statisticsusers` , entrez `statisticsuser <username>` pour créer un utilisateur standard (par exemple, `statisticsuser jdoe`). Utilisez l'option `-a` pour créer un administrateur (par exemple, `statisticsuser -a jdoe`). L'outil de ligne de commande `statisticsuser` vous invite à entrer un mot de passe. Un utilisateur final entre le nom d'utilisateur et le mot de passe pour se connecter au logiciel serveur. Veillez à distribuer le nom d'utilisateur et les mots de passe de manière appropriée. Pour supprimer un utilisateur, utilisez l'option `-d` (par exemple, `statisticsuser -d jdoe`).
4. Si vous êtes connecté en tant que propriétaire du démon du logiciel serveur, ouvrez le fichier de configuration (par exemple, `statisticsd.conf`) dans un éditeur de texte.
5. Recherchez l'élément *userauth* et remplacez le paramètre *value* `win32` par `internal`.
6. Accédez au panneau des services Windows et démarrez le service.

Configuration de l'authentification unix2

L'authentification unix2 permet au logiciel serveur de s'exécuter sans privilèges de superutilisateur et s'authentifie par rapport au fichier *passwd* UNIX avec des comptes utilisateur standard. Un fichier exécutable (*suauth*) installé avec le logiciel serveur effectue l'authentification. Pour qu'il fonctionne correctement, vous devez définir les droits nécessaires.

Pour configurer l'authentification unix2 , procédez comme suit:

1. A l'aide de setuid et de setguid ou du contrôle d'accès basé sur les rôles (RBAC), modifiez les droits de l'exécutable *suauth* de sorte que l'utilisateur qui exécutera le démon du logiciel serveur dispose des droits d'accès root nécessaires. Cet utilisateur doit être en mesure d'authentifier l'utilisateur par rapport au fichier *passwd* et de modifier l'ID utilisateur et l'ID de groupe du processus serveur généré pour chaque utilisateur final. Vous trouverez ci-dessous des détails sur la définition des droits d'accès. Notez que vous utilisez *soit* setuid / setguid *, soit* RBAC. N'utilisez pas les deux méthodes.
2. Ouvrez le fichier de configuration (par exemple, *statisticsd.conf*) dans un éditeur de texte.
3. Recherchez l'élément *userauth* et remplacez le paramètre *value* `unix` par `unix2`.
4. Si vous êtes connecté en tant que propriétaire du démon du logiciel serveur, démarrez le serveur.

Définition des droits avec setuid et setguid

1. Créez un groupe pour l'utilisateur qui exécutera le logiciel serveur. Il est recommandé de nommer ce groupe **statistics**. Nous vous recommandons également de limiter l'appartenance à un groupe uniquement à l'utilisateur qui exécutera le démon du logiciel serveur.
2. Un membre de ce groupe doit installer le logiciel serveur. Cet utilisateur sera le propriétaire du démon du logiciel serveur.
3. Démarrez une session de terminal en tant que *superutilisateur*.
4. Accédez au répertoire *bin* dans le répertoire d'installation des logiciels du serveur.
5. Remplacez le propriétaire du fichier *suauth* par *root*.

   ```
   chown root suauth
   ```

6. Ajoutez les bits setuid et setgid à *suauth*. Ces bits permettent à l'utilisateur du groupe d'installation d'exécuter le fichier et de l'exécuter temporairement en tant que *superutilisateur*. Des privilèges de superutilisateur sont requis pour les raisons indiquées précédemment dans cette rubrique.

   ```
   chmod 6550 suauth
   ```

7. Quittez l'application en tant que *superutilisateur* et connectez-vous en tant que propriétaire du démon du logiciel serveur.

Définition des droits avec le contrôle d'accès basé sur les rôles

Vous devez également pouvoir utiliser le contrôle d'accès basé sur les rôles (RBAC) pour définir les droits nécessaires. Pour plus d'informations, reportez-vous à la documentation RBAC de votre fournisseur. Vous devez effectuer les opérations suivantes:

1. Créez une autorisation pour l'exécutable *suauth* .
2. Créez un rôle pour cette autorisation.
3. Affectez le propriétaire du démon du logiciel serveur au rôle.
4. Configurez l'autorisation pour autoriser les droits suivants:
   - Lisez le fichier *passwd* .
   - Modifiez l'ID utilisateur.
   - Modifier l'ID de groupe.

Configuration de la connexion unique (SSO)

Vous pouvez utiliser la connexion unique pour vous connecter à un serveur qui s'exécute sur n'importe quelle plateforme prise en charge. Vous devez d'abord configurer votre serveur IBM SPSS Statistiques , votre client IBM SPSS Statistiques et vos machines IBM SPSS Services de collaboration et de déploiement . L'authentification interne permet au logiciel serveur de s'exécuter sans privilèges de superutilisateur.

Si vous utilisez une connexion unique pour vous connecter à IBM SPSS Statistiques Server et à IBM SPSS Services de collaboration et de déploiement, vous devez vous connecter à IBM SPSS Services de collaboration et de déploiement avant de vous connecter à IBM SPSS Statistiques Server.

Pour pouvoir interagir avec les installations Active Directory les plus récentes et les plus sécurisées, vous devez installer le pack de chiffrement haute résistance pour Java, car les algorithmes de chiffrement requis ne sont pas pris en charge par défaut. Vous devez installer le pack à la fois pour le client et pour le serveur. Un message d'erreur tel que `Illegal key size` s'affiche sur le client en cas d'échec de la connexion serveur due à l'absence d'installation du pack. Voir «Installation du codage de type Unlimited Strength», à la page 42.

Remarque : Avant de configurer votre serveur SPSS Statistics , votre client SPSS Statistics et vos machines IBM SPSS Services de collaboration et de déploiement pour la connexion unique, vous devez vous assurer que les machines ont accès au serveur de contrôleur de domaine.

Pour plus d'informations sur la configuration de IBM SPSS Services de collaboration et de déploiement pour la connexion unique, voir Présentation des services de connexion uniqueIBM SPSS Services de collaboration et de déploiement.

Configuration du serveur pour la connexion unique

Configurer le serveur sous Windows

1. Vérifiez que la machine du serveur Windows est membre du domaine Active Directory (AD).
2. Dans l'emplacement d'installation de IBM SPSS Statistiques Server , localisez le dossier `config`.
3. Dans le dossier `config` , créez un sous-dossier appelé `sso`.
4. Dans le dossier `sso`, créez un fichier `krb5.conf`. Les instructions de création du fichier `krb5.conf` se trouvent à l'adresse http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html. Voici un exemple de fichier `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
```

Configuration du serveur sous UNIX

Pour configurer la connexion unique pour les machines serveur UNIX, vous pouvez ajouter la machine UNIX au domaine Windows AD, puis suivre les instructions de configuration de la connexion unique sous Windows. Vous pouvez également effectuer les étapes suivantes:

1. Créez un compte utilisateur de domaine pour la machine UNIX.
2. Modifiez le nom d'hôte. Si vous utilisez RedHat Linux, ouvrez le fichier `/etc/sysconfig/network` et remplacez HOSTNAME par le format <*name*>.<*realm*>. Cela permet à AD de trouver les données d'identification du serveur.
3. Pour permettre au serveur DNS de trouver la machine UNIX, effectuez l'une des opérations suivantes:
   - Ouvrez le fichier `%windows%/system32/drivers/etc/hosts` et ajoutez le mappage IP/hôte, par exemple:

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

     Ou
   - Ajoutez une nouvelle entrée de zone de recherche inversée. Cette opération va ajouter un mappage d'IP/hôte sur le serveur DNS.

   Si l'entrée DNS de la machine UNIX n'est pas correcte, vous pouvez ajouter manuellement l'entrée de recherche inversée sur le serveur DNS.

Configuration du client pour la connexion unique

Les étapes sont communes à tous les clients à l'exception des étapes qui sont notées spécifiquement pour Windows.

1. Vérifiez que la machine Windows locale qui exécute IBM SPSS Statistiques est membre du domaine Active Directory (AD).

2. Ajoutez l'utilisateur de domaine en tant qu'administrateur sur la machine locale.
3. Activez Windows pour accéder à la clé de session TGT:
   a. Dans le menu **Démarrer**, cliquez sur l'option **Exécuter**.
   b. Entrez `regedit` et cliquez sur **OK** pour ouvrir l'**éditeur de registre**.
   c. Accédez à l'emplacement de registre suivant:

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

   d. Cliquez avec le bouton droit de la souris sur le dossier et sélectionnez **Nouveau** > **DWORD**. Le nom de la nouvelle valeur doit être `allowtgtsessionkey`.
   e. Définissez la valeur de `allowtgtsessionkey` à la valeur hexadécimale de 1, c'est-à-dire `0x0000001`.
   f. Fermez l'**éditeur de registre**.
   g. Exécutez `kinit.exe`, qui se trouve dans <IBM SPSS Statistiques *installation location*>`\jre\bin`.
4. Dans le dossier `config` de l'emplacement d'installation de IBM SPSS Statistiques, créez un dossier appelé `sso`.
5. Copiez le fichier `krb5.conf` du serveur dans le dossier `sso` .
6. Redémarrez la machine client et la machine serveur.

Enregistrement du nom de principe de service (SPN)

Chaque instance de serveur doit enregistrer un *nom principal de service (SPN)* unique pour s'identifier, et le client doit spécifier le même SPN lorsqu'il se connecte au serveur.

Un SPN pour une instance du logiciel serveur se présente sous la forme suivante:

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

Par exemple :

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

Notez que le nom d'hôte doit être qualifié avec son domaine DNS (`ibm.com` dans cet exemple) et que le domaine doit être mappé au domaine Kerberos .

L'association du nom d'hôte et du numéro de port rend le SPN unique (car chaque instance sur un hôte donné doit utiliser un port d'écoute différent). Le client et le serveur disposent déjà du nom d'hôte et du numéro de port, ils peuvent donc construire le SPN approprié pour l'instance. L'étape de configuration supplémentaire requise consiste à enregistrer le SPN dans la base de données Kerberos.

Enregistrement du SPN sous Windows

Si vous utilisez Active Directory comme implémentation Kerberos, utilisez la commande `setspn` pour enregistrer le SPN. Pour exécuter cette commande, les conditions ci-dessous doivent être satisfaites.

- Vous devez être connecté à un contrôleur de domaine.
- Vous devez exécuter l'invite de commande avec des privilèges élevés (en tant qu'administrateur).
- Vous devez être membre du groupe Domain Admins (ou avoir reçu la permission appropriée d'un administrateur de domaine).

Pour plus d'informations, voir les articles suivants :

- Setspn Command-Line Reference
- Delegating Authority to Modify SPNs

Pour l'instance par défaut, en mode écoute sur le port standard (3023 pour la version 23, par exemple) et en cours d'exécution sous le compte Système local, vous devez enregistrer le SPN sur le nom de l'ordinateur serveur. Par exemple :

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

Pour chaque instance de serveur suivante, à l'écoute sur un port personnalisé (par exemple, 3099) et en cours d'exécution sous un compte utilisateur arbitraire (par exemple, johndoe) avec l'option `userauth` définie sur `internal` (c'est-à-dire, à l'aide de l'authentification interne), vous devez enregistrer le SPN par rapport au nom de compte utilisateur de service:

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

Notez que dans ce cas (lorsque le compte de service n'est pas Local System), l'enregistrement du SPN ne suffit pas pour permettre au client de se connecter. D'autres étapes de configuration sont décrites dans la section suivante.

Pour voir les SPN enregistrés sur le compte `jdoe` :

```
setspn -l jdoe
```

Enregistrement du SPN sous UNIX

Si vous utilisez Active Directory comme implémentation Kerberos , utilisez la commande `setspn` comme décrit dans la section Windows précédente. Cela suppose que vous avez déjà créé l'ordinateur ou le compte utilisateur dans le répertoire. Vous pouvez également tester `ktpass`, si vous le souhaitez (voir Ktpass Command-Line Reference).

Si vous utilisez une autre implémentation Kerberos , utilisez votre outil d'administration Kerberos favori pour ajouter le principal de service à la base de données Kerberos . Pour convertir le SPN à un principal Kerberos, vous devez ajouter le nom du domaine Kerberos. Par exemple :

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

Ajoutez ce principal et le mot de passe au fichier keytab du serveur. Le fichier keytab doit contenir une entrée pour chaque instance qui s'exécute sur l'hôte.

Configuration de la connexion unique lors de l'exécution en tant que non-racine / système

Lorsque le service / démon du serveur s'exécute en tant qu'utilisateur arbitraire (non root sous UNIX et non système sous Windows), vous devez enregistrer le compte de service / démon. Vous avez besoin du SPN que vous avez créé précédemment.

1. Créez le répertoire `<STATISTICSSERVER>\config\sso`.
2. Copiez le fichier `krb5.conf` du répertoire SSO du client vers le répertoire SSO du serveur que vous avez créé à l'étape 1.
3. Utilisez la commande suivante pour créer le fichier `krb5.keytab` dans le répertoire SSO serveur :

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

   Par exemple :

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

Vous êtes invité à entrer un mot de passe. Il doit s'agir du mot de passe du compte de service. Ainsi, si le compte de service est `jdoe`, par exemple, vous devez entrer le mot de passe de l'utilisateur `jdoe`.

Le compte de service lui-même n'est pas mentionné dans le fichier keytab, mais vous avez précédemment enregistré le SPN dans ce compte à l'aide de `setspn`. Cela signifie que le mot de passe du principal du service et celui du compte du service sont identiques.

Pour chaque nouvelle instance de serveur que vous créez, vous devez enregistrer le SPN pour cette instance (à l'aide de `setspn`) et créer un fichier de clés. Le fichier de clés doit être copié dans le sous-répertoire `config_<group_name>/sso` du répertoire d'installation du serveur. L'instance par défaut n'a pas besoin de fichier de clés.

Pour vérifier si une instance est incluse dans le fichier keytab :

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

Vous pouvez voir plusieurs entrées pour chaque principal avec différents types de chiffrement, ce qui est normal.

Configuration de l'appartenance à un groupe

Si vous utilisez l'autorisation par groupe, vous pouvez configurer le IBM SPSS Services de collaboration et de déploiement système pour qu'il interroge un fournisseur d' LDAP s afin de déterminer le groupe auquel appartient un utilisateur authentifié. Pour plus d'informations sur l'autorisation de groupe, voir la rubrique «Autorisation de groupe», à la page 33.

Pour que la recherche par groupe fonctionne correctement, vous devez d'abord configurer votre référentiel afin d'y ajouter un fournisseur LDAP ou Active Directory, puis activer l'authentification unique (SSO) à l'aide de ce fournisseur :

1. Démarrez le client IBM SPSS Responsable du déploiement et sélectionnez **Fichier** > **Nouveau** > **Administered Server Connection...** pour créer une connexion au serveur administré pour votre référentiel (si vous n'en avez pas déjà).
2. Connectez-vous via la connexion au serveur administré et développez le dossier **Configuration**.
3. Cliquez avec le bouton droit de la souris sur **Fournisseurs de sécurité**, sélectionnez **Nouveau** > **Définition du fournisseur de sécurité...** et entrez les valeurs appropriées. Pour plus d'informations, cliquez sur **Aide** dans la boîte de dialogue.
4. Développez le dossier **Fournisseurs de connexion unique**, cliquez avec le bouton droit de la souris sur **Fournisseur SSO Kerberos**, et sélectionnez **Ouvrir**.
5. Cliquez sur **Activer**, sélectionnez votre fournisseur de sécurité, puis cliquez sur **Enregistrer**. Il n'est pas nécessaire d'indiquer d'autres détails ici, sauf si vous souhaitez utiliser SSO (il suffit que le fournisseur soit activé pour permettre la recherche du groupe).

Important : Pour que la recherche de groupe fonctionne correctement, le fournisseur Kerberos que vous configurez ici doit être le même que le fournisseur configuré pour IBM SPSS Statistiques Server. En particulier, ils doivent fonctionner dans le même domaine Kerberos. Ainsi, si un utilisateur se connecte au serveur via l'authentification unique (SSO) et que celui-ci l'identifie comme `jdoe@ibm.com` (où `ibm.com` correspond au domaine), il attendra du fournisseur de sécurité situé dans IBM SPSS Services de collaboration et de déploiement qu'il reconnaisse ce nom principal d'utilisateur et qu'il renvoie l'appartenance au groupe correspondante à partir de l'annuaire LDAP.

Configuration de la connexion unique pour les sources de données

Vous pouvez vous connecter à des bases de données à partir de IBM SPSS Statistiques via une connexion unique. Si vous souhaitez créer une connexion de base de données via une connexion unique, vous devez d'abord utiliser votre logiciel de gestion ODBC pour configurer correctement une source de données et un jeton de connexion unique. Ensuite, lorsque vous vous connecterez à une base de données dans IBM SPSS Statistiques, IBM SPSS Statistiques utilisera ce jeton de connexion unique et l'utilisateur ne sera pas invité à se connecter à la source de données.

Cependant, si la source de données n'a pas été configurée correctement pour une connexion unique, IBM SPSS Statistiques invitera l'utilisateur à se connecter à la source de données. L'utilisateur pourra toujours accéder à la source de données après avoir fourni des données d'identification valides.

Pour les détails complets de la configuration des sources de données ODBC sur votre système avec une connexion unique, consultez la documentation du fournisseur de base de données. Vous trouverez ci-dessous un exemple de la procédure générale à suivre.

1. Configurez votre base de données pour qu'elle prenne en charge la connexion unique Kerberos.
2. Sur la machine serveur, créez une source de données ODBC et testez cette dernière. La connexion DSN ne doit nécessiter ni ID utilisateur, ni mot de passe.
3. Connectez-vous au serveur à l'aide de la connexion unique et commencez à utiliser la source de données ODBC créée et validée à l'étape 2.

Autorisations

Si vous n'utilisez pas l'authentification interne ou l'autorisation de groupe avec la connexion unique, le logiciel serveur lance un processus pour l'utilisateur final, en transmettant l'ID et le mot de passe de l'utilisateur au système d'exploitation. Le processus lancé dispose des droits d'accès aux fichiers du compte de l'utilisateur final. Un utilisateur qui se connecte au logiciel serveur doit se connecter avec un compte disposant des droits suivants:

- Droits de lecture et d'exécution sur le répertoire d'installation du serveur et sur ses sous-répertoires.
- Droits de lecture, d'exécution et d'écriture sur l'emplacement du répertoire pour les fichiers temporaires

Pour l'authentification interne et la connexion unique, l'utilisateur du client de connexion dispose des droits qui sont affectés à l'utilisateur qui a démarré le service / démon.

Vous pouvez utiliser l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée avec IBM SPSS Responsable du déploiement) pour modifier l'emplacement par défaut des fichiers temporaires. Pour plus d'informations, voir la rubrique relative aux emplacements des fichiers dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide relative à IBM SPSS Services de collaboration et de déploiement). Vous pouvez également modifier l'emplacement pour des utilisateurs ou des groupes individuels. Pour plus d'informations, voir la rubrique IBM SPSS Statistics Server dans le document *Deployment Manager User's Guide*.

Autorisations de niveau administrateur

Par défaut, le groupe d'administrateurs du logiciel serveur correspond au groupe d'administrateurs de la machine sur laquelle le logiciel serveur s'exécute. Vous pouvez modifier le groupe d'administrateurs du logiciel serveur en le spécifiant dans la zone de texte Groupe d'administrateurs de l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée avec IBM SPSS Responsable du déploiement). Pour plus d'informations, voir la rubrique Utilisateurs dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement). Si vous utilisez l'authentification interne sous UNIX, vous pouvez créer des administrateurs directement. Pour plus d'informations, voir «Configuration de l'authentification interne», à la page 26.

Autorisation de groupe

Vous pouvez configurer le logiciel du serveur pour prendre en charge l'autorisation de groupe. Une instance distincte du service/démon est exécutée pour chaque groupe d'utilisateurs autorisé.

Configuration de l'autorisation de groupe

1. Créez une instance de serveur pour chaque groupe. Pour plus d'informations sur la création des instances de serveur, voir «Configuration de plusieurs instances», à la page 19.
2. Créez les groupes dans IBM SPSS Services de collaboration et de déploiement et affecter des utilisateurs aux groupes.
3. Ouvrez l'application d'administration et mettez à jour la valeur de l'**URL de service d'autorisation du groupe** par l'URL de IBM SPSS Services de collaboration et de déploiement. Veillez à inclure le numéro de port (par exemple, `http://myserver.mydomain.com:9080`).

Contrôle de l'accès aux sources de données (DSN) par groupe

L'authentification multi-facteur (MFA) exige que les utilisateurs puissent être limités dans l'accès aux DSN ODBC accessibles, en fonction de leur appartenance au groupe.

1. Ouvrez l'application d'administration et définissez **Restrict Database Access** sur `Yes`.
2. Dans la zone **Permitted Database Sources**, entrez une liste de sources de données délimitées par des points-virgules (;) et dont l'accès est autorisé (par exemple, `Fraud - Analytic;Fraud - Operational`).

Lorsque cette restriction est activée, les résultats obtenus sont les suivants :

- Lorsqu'un utilisateur recherche des sources de données dans l'assistant de base de données, au lieu de disposer de toutes les sources de données DSN définies sur le système serveur, l'utilisateur ne voit que le sous-ensemble de sources de données DSN défini par l'application d'administration. Notez que le chemin peut contenir des sources de données DSN qui ne sont pas définies sur le serveur. Elles sont ignorées. L'utilisateur ne voit pas ces noms.
- Si un utilisateur modifie la syntaxe `GET DATA /TYPE=ODBC` qui spécifie un DSN qui n'est pas spécifié par l'application d'administration, la syntaxe ne s'exécute pas et l'utilisateur reçoit une erreur similaire à **Accès refusé à la source de données: < X>**.

Profils

Le logiciel serveur permet de créer des profils utilisateur et des groupes d'utilisateurs spécifiques. Ces profils et groupes d'utilisateurs vous permettent de définir des paramètres pour des utilisateurs spécifiques.

Versions client et serveur

A partir de la version 20.0.1, le logiciel client n'a pas besoin d'être au même niveau d'édition que le logiciel serveur auquel il se connecte. Par exemple, le client 20.0.1 peut se connecter au logiciel serveur 21 et le client 21 peut se connecter à un serveur 20.0.1 . Notez que vous pouvez également exécuter plusieurs versions du logiciel serveur sur un ordinateur serveur.

Le mélange des niveaux d'édition n'est autorisé que pour simplifier les mises à niveau. Les niveaux d'édition peuvent être échelonnés pendant la période de mise à niveau et les clients n'ont pas besoin d'être mis à niveau simultanément. Toutefois, il n'est pas recommandé de conserver cette configuration de manière prolongée. Si le serveur est plus récent que le client, il peut créer des sorties qui seront illisibles pour le client. Si le client est plus récent que le serveur, il se peut que la syntaxe soumise par le client ne soit pas reconnue par le serveur. Par conséquent, vous devez mettre à niveau le logiciel client ou serveur dès que possible, en fonction de la valeur de l'un par rapport à l'autre.

Lorsque vous distribuez des informations de connexion aux utilisateurs finaux, gardez à l'esprit la version du logiciel client qu'ils exécutent et assurez-vous qu'ils disposent des informations de connexion pour une version de serveur correspondante.

Connexion d'utilisateurs via un pare-feu

Si vous utilisez un **pare-feu** pour protéger votre réseau des intrus, vous pouvez configurer votre pare-feu et le logiciel serveur de sorte que les utilisateurs finaux en dehors du pare-feu puissent connecter le client au logiciel serveur. Votre pare-feu peut utiliser la conversion d'adresses réseau (**NAT**), mais elle n'est pas obligatoire.

Le scénario typique de connexion d'utilisateurs finaux via un pare-feu qui utilise la conversion d'adresses réseau est le suivant:

1. L'utilisateur final connecte l'application client au logiciel serveur à l'aide de l' **adresse IP masquée** (adresse IP que NAT présente au monde extérieur) et du numéro de port du serveur. Par exemple, l'utilisateur final se connecte avec l'adresse IP `10.10.10.2` et le numéro de port `3016`.

2. Le pare-feu autorise la connexion car il a été configuré pour accepter les connexions à partir de l'adresse IP masquée.
3. Le pare-feu redirige l'adresse IP masquée vers l'adresse IP interne réelle du serveur. Elle autorise la connexion car le port (par exemple, 3016) est activé sur le pare-feu.
4. Le serveur génère un processus pour la connexion client de l'utilisateur final et lui affecte un numéro de port dans la liste de la variable d'environnement système STATISTICS_CLIENT_PORTS. Par exemple, le processus communique via le port 3287.
5. Le pare-feu autorise la communication via ce port (par exemple, 3287) car il est activé sur le pare-feu.

Configuration des connexions via un pare-feu

Introduction

Pour les connexions de clients à travers le pare-feu, deux ports doivent être ouverts :

- Le démon des statistiques ou le port d'écoute. Par défaut, le numéro de port se situe dans la plage 3000 et varie en fonction du numéro de version. Par exemple, le numéro de port peut être 3031 pour la version 31.
- Le port de réponse utilisé par les processus enfants du serveur de statistiques pour communiquer avec plusieurs connexions de clients de statistiques. Dans le cas de connexions client/serveur multiples, il est possible que vous souhaitiez configurer plus d'un port de réponse client.

Lorsqu'un client SPSS Statistics se connecte au serveur SPSS Statistics , le port client est verrouillé et ne peut être utilisé que par un seul client jusqu'à la fin du processus de connexion. Le temps de connexion est de l'ordre de 1 à 3 secondes (ce temps peut varier en fonction de la charge du système). Lorsqu'un deuxième ou un troisième client SPSS Statistics tente de se connecter pendant cette période, les clients sont bloqués jusqu'à ce que le port client soit disponible. L'ouverture de plusieurs ports clients réduit le temps d'attente lors de la connexion dans un environnement où de nombreux utilisateurs lancent simultanément des sessions SPSS Statistics . Le nombre de ports de réponse est contrôlé par la variable d'environnement STATISTICS_CLIENT_PORTS.

Remarque : IBM SPSS Statistiques Le serveur peut réutiliser le même numéro de port pour les connexions des clients. Mais la réutilisation des ports dépend de la capacité de reconnexion du client. Par défaut, la reconnexion des clients est activée pendant 100 minutes. Lorsque la fonction de reconnexion des clients est activée, le serveur SPSS Statistics a un rapport de 1:1 entre les clients connectés et les ports de réponse ouverts. Pour activer la réutilisation des ports, vous devez d'abord désactiver la reconnexion client. Pour ce faire, il suffit de modifier le paramètre **`reconnect-timeout`** dans `<Statistics Install Path>/config/statisticsd.conf`. Par exemple :

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

Exemple

Supposons que cinq ports clients soient répertoriés dans la variable d'environnement du système **STATISTICS_CLIENT_PORTS** (ports 40001-40005) et qu'il y ait quatre clients possibles. Un utilisateur établit une connexion avec le serveur SPSS Statistics et le premier contact est établi via le port d'écoute (3031). Le serveur génère un processus enfant et poursuit la communication via le premier port client disponible (4001). Si le port 40001 n'est pas verrouillé (car la communication avec un autre client vient de démarrer), le port sera réutilisé. Si le port 40001 est verrouillé, la communication passe au port suivant (4002), en supposant qu'il n'est pas verrouillé, et ainsi de suite.

Une fois que les quatre clients sont connectés, ils utiliseront probablement tous le même numéro de port (40001). Il est peu probable qu'un ou plusieurs clients utilisent le port 40002, qu'un client utilise le port 40003 et qu'un ou plusieurs clients utilisent le port 40004. Il n'est pas possible qu'un client utilise le port 40005 car il n'y a que quatre clients et l'algorithme démarre au premier numéro de port disponible répertorié dans la variable d'environnement système STATISTICS_CLIENT_PORTS .

Il existe deux méthodes recommandées pour configurer les connexions SPSS Statistics Server via un pare-feu.

Configurer le pare-feu pour autoriser les processus

A l'aide de votre logiciel de pare-feu, assurez-vous que les processus suivants sont autorisés à accepter les connexions réseau.

`statisticsproc.exe`
Le processus `statisticsproc.exe` ouvre, ferme et réutilise les ports de réponse (ou les ports définis dans `STATISTICS_CLIENT_PORTS`).

`statisticssrvr.exe` (Microsoft Windows) ou `statisticsd` (UNIX ou Linux)
Le processus est le service Windows principal, ou démon UNIX/Linux , et gère le port d'écoute.

Le fait de fournir un accès aux processus permet d'utiliser efficacement n'importe quel port que le processus utilisera.

Remarque : Les conditions suivantes s'appliquent lorsque la valeur de délai de reconnexion est supérieure à 0 et que `statisticsproc.exe` est autorisé à accepter les connexions réseau:

- `STATISTICS_CLIENT_PORTS` n'est pas pertinent, à l'exception des diagnostics. N'importe quel port peut être utilisé.
- Il n'y a pas de limite au nombre de connexions sauf si les ports sont définis dans **`STATISTICS_CLIENT_PORTS`**. Le nombre de ports **`STATISTICS_CLIENT_PORTS`** définis limite efficacement les ports utilisés par SPSS Statistics Server.

Configurez le pare-feu en ouvrant manuellement les ports

Pour configurer manuellement le logiciel serveur et le pare-feu, procédez comme suit:

1. Installez le logiciel serveur comme d'habitude. Vous devez connaître l'adresse IP de l'ordinateur sur lequel le serveur est installé et le numéro de port utilisé par le logiciel serveur pour les communications. Par exemple, installez le serveur sur `202.123.456.78` sur le port d'écoute `3031`.
2. Configurez la variable d'environnement système `STATISTICS_CLIENT_PORTS` en spécifiant au moins un numéro de port. La variable d'environnement répertorie les ports utilisés pour continuer les connexions client avec le serveur (ports**`RESPONSE`**). Si nécessaire, vous pouvez spécifier une liste délimitée par des virgules et une plage de ports (par exemple, `4001`, `4002`, `4003-4005`).

   Important :

   - Lorsque le délai d'attente de reconnexion automatique est défini sur une valeur supérieure à 0, `STATISTICS_CLIENT_PORTS` définit le nombre maximal de connexions client et serveur simultanées autorisées.
   - Ne pas indiquer le port **`LISTEN`** (3031) dans la variable d'environnement `STATISTICS_CLIENT_PORTS` .

   Microsoft® Windows™
   Utilisez les propriétés du système Windows pour créer et configurer la variable d'environnement. Pour plus d'informations, voir «Propriétés système», à la page 57 .

   UNIX
   Editez le script d'environnement du logiciel serveur, `statsenv.sh`, qui est inclus dans le sous-répertoire `/bin` du répertoire d'installation. Définissez le port qui peut être utilisé par les processus client que le serveur démarre. Par exemple, ajoutez les lignes suivantes :

   ```
   STATISTICS_CLIENT_PORTS=4001

   export STATISTICS_CLIENT_PORTS
   ```

3. Lorsque vous utilisez la conversion d'adresses réseau (NAT), créez et mappez des adresses IP. A l'aide de votre logiciel de pare-feu, créez une adresse IP masquée pour une utilisation externe et mappez-la à l'adresse IP interne du serveur. Par exemple, créez une adresse IP de masquage `10.10.10.2` et mappez-la à `202.123.456.78`.

4. A l'aide de votre logiciel de pare-feu, activez les numéros de port sur le pare-feu:
   - Numéro de port **LISTEN** du serveur. Par exemple, activez le port `3031`.
   - Numéros de port que vous avez spécifiés dans la variable d'environnement `STATISTICS_CLIENT_PORTS` . Par exemple, activez le port `4001`.
5. Distribuez les informations de connexion aux utilisateurs qui se connectent au logiciel serveur depuis l'extérieur du pare-feu.
   - S'il est utilisé, l'adresse IP masquée de l'ordinateur sur lequel le logiciel serveur est installé (ne distribuez pas l'adresse IP interne du serveur). Par exemple, distribuez `10.10.10.2` en tant qu'adresse IP du serveur.
   - Distribuez le numéro de port du logiciel serveur comme d'habitude. Par exemple, distribuez `3031` en tant que numéro de port **LISTEN** du serveur.

Connexion d'utilisateurs à PPTP

Les utilisateurs finaux peuvent connecter un ordinateur client distant au logiciel du serveur analytique à l'aide du **protocole PPTP (Point-to-Point Tunneling Protocol)** . PPTP est un protocole réseau qui prend en charge les réseaux privés virtuels (VPN) multiprotocoles. Il permet aux utilisateurs finaux distants d'accéder à votre réseau en toute sécurité sur Internet.

Pour utiliser des connexions PPTP:

1. **Configurez un serveur d'accès distant pour PPTP.** Veillez à créer suffisamment d'adresses IP pour les clients car le logiciel serveur prend en charge plusieurs connexions client. Chaque connexion client requiert sa propre adresse IP.
2. **Configurez l'ordinateur de bureau du client.** Utilisez le panneau de configuration du réseau Windows pour ajouter une connexion de réseau privé à l'aide de PPTP. Entrez une adresse IP que le serveur d'accès distant reconnaîtra comme une connexion PPTP.
3. **Activez la connexion PPTP sur l'ordinateur de bureau du client.** Lorsque les utilisateurs finaux souhaitent se connecter au logiciel serveur à partir d'un emplacement distant, ils activent la connexion PPTP, puis utilisent le logiciel client pour se connecter au serveur comme d'habitude.

Utilisation du protocole SSL pour sécuriser le transfert de données

Le protocole SSL (Secure Sockets Layer) permet de coder les données transférées entre deux ordinateurs. Le protocole SSL sécurise la communication entre les ordinateurs. SSL peut chiffrer l'authentification d'un nom utilisateur/mot de passe et le contenu d'un échange entre un serveur et un client.

Remarque : À partir de la version 30.0.0, SSL est obsolète et les utilisateurs doivent désormais utiliser GSKit.

Fonctionnement de SSL

Le protocole SSL repose sur des clés publiques et privées de serveur, en plus d'un certificat de clé publique qui relie l'identité du serveur à sa clé publique.

1. Lorsqu'un client se connecte à un serveur, le client authentifie ce serveur avec le certificat de clé publique.
2. Le client génère ensuite un chiffre au hasard, code ce chiffre avec la clé publique du serveur et renvoie le message chiffré au serveur.
3. Le serveur décode ce chiffre aléatoire avec sa clé privée.
4. Avec le chiffre aléatoire, le serveur et le client créent les clés de session utilisées pour le codage et le décodage des informations suivantes.

Le certificat de clé publique est généralement signé par une autorité de certification. Les autorités de certification, comme VeriSign et Thawte, sont des organismes qui fournissent, authentifient et gèrent les informations de sécurité contenues dans les certificats de clé publique. L'autorité de certification a

pour rôle principal de confirmer l'identité du serveur. Le certificat délivré par l'autorité de certification est généralement payant, mais des certificats signés peuvent également être délivrés.

Activation de l' SSL ation à l'aide de GSKit

Sécurisation des communications client-serveur et serveur-serveur avec GSKit

Les principales étapes de sécurisation des communications client-serveur et serveur-serveur avec le protocole SSL sont les suivantes :

1. Obtenez et installez le certificat et les clés SSL.
2. Activez et configurez un fichier de configuration spécifié situé dans le répertoire d'installation du serveur IBM SPSS Statistiques .

   Remarque : IBM SPSS Statistiques Server prend en charge le protocole TLSv1.2 . GSKit ne prend actuellement en charge aucune autre version.
3. Si vous utilisez des certificats de chiffrement dont la puissance est supérieure à 2048 bits, installez un chiffrement de niveau illimité sur les ordinateurs client.
4. Demandez aux utilisateurs d'activer SSL lors de la connexion au serveur.

Remarque : Parfois, un produit serveur agit comme un client. Par exemple, le Serveur IBM SPSS Statistiques se connectant au IBM SPSS Référentiel des services de collaboration et de déploiement. Dans ce cas, IBM SPSS Statistiques Server est le *client*.

Obtention et installation du certificat et des clés SSL

Pour configurer la prise en charge de SSL, vous devez tout d'abord suivre les étapes ci-après.

1. Procurez-vous un certificat et un fichier de clé SSL. Vous pouvez effectuer cette opération de différentes manières:
   - Achetez-les auprès d'une autorité de certification publique (comme VeriSign, Thawte ou Entrust). L'autorité de certification publique (CA) signe le certificat pour vérifier le serveur qui l'utilise.
   - Procurez-vous les fichiers de clés et de certificats auprès d'une autorité de certification tierce. Si cette approche est adoptée, le certificat racine `*.pfx` de l'autorité de certification tierce doit être importé dans le fichier de clés du serveur (expliqué ci-dessous).
   - Générez les fichiers de clé et de certificat par le biais d'une autorité de certification signée interne. Pour ce faire :
     a. Préparez une base de données de clés. Pour plus d'informations, voir la rubrique «Création d'une base de données de clés SSL», à la page 40.
     b. Créez le certificat autosigné. Pour plus d'informations, voir la rubrique «Création d'un certificat SSL autosigné», à la page 40.
2. Pour les certificats d'autorité de certification ou les certificats autosignés, copiez les fichiers `.kdb` et `.sth` de l'étape 1 dans un répertoire auquel le IBM SPSS Statistiques Server a accès et indiquez le chemin d'accès à ce répertoire dans le fichier `statisticsd.conf` . Le fichier `statisticsd.conf` se trouve dans `<Statistics Server installation directory>/config/`; pour les certificats tiers, copiez les fichiers `.pfx` et `.sth` de l'étape 1.
3. Définissez les paramètres suivants dans le fichier `statisticsd.conf` :

   Pour les autorités de certification (CA) ou les certificats autosignés:
   - `<gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>`, où `<value>` est `0` ou `1` qui indique si GSKit doit être activé.
   - `<gsk-keystore desc="GSKSSL Key store database filename." value="<filename>.kdb"/>`, où `<filename>` est le nom du fichier de base de données de clés.

- <gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>, où <filename> est le nom du fichier de mot de passe secret de la base de données de clés.
- <gsk-cert-label desc="GSKSSL certificate label." value=""/>, où <label> est l'étiquette de votre certificat.

Pour les certificats de tiers:

- <gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>, où <value> est 0 ou 1 qui indique si GSKit doit être activé.
- <gsk-keystore ="<*.pfx_file_location>", où <*.pfx_file_location> est l'emplacement et le nom du fichier de certificat racine *.pfx .
- <gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>, où <filename> est le nom du fichier de mot de passe secret de la base de données de clés.
- <gsk-cert-label desc="GSKSSL certificate label." value=""/>, où <label> est l'étiquette de votre certificat.

4. Pour les certificats de tiers:
   a. Extrayez le fichier root.pem du fichier *.pfx en utilisant la commande GSK suivante comme exemple:

```
gsk8capicmd_64.exe -cert -extract -db C:\SSL\<certificate_name>.pfx -stashed -label
<cert-certificate_issuing_server.com> -target C:\SSL\root.pem
```

   b. Copiez le fichier root.pem dans le dossier C:\ProgramData\IBM\SPSS\certificates (Windows) ou /Library/Application Support/IBM/SPSS/certificates (macOS) sur le client.
   c. Sur le client, configurez la connexion en indiquant le nom de domaine complet (par exemple, cert-certificate_issuing_server.com) dans le champ « **Nom du serveur** », puis activez l'option « **SSL** ».
5. Pour les certificats autosignés, installez le certificat sur les systèmes client. Pour les certificats de l'autorité de certification publique ou tiers achetés, cette étape n'est pas requise. Assurez-vous que les droits d'accès interdisent la navigation dans le répertoire contenant le certificat. Pour plus d'informations, voir la rubrique «Installation d'un certificat SSL autosigné», à la page 41.

Configuration de l'environnement pour l'exécution de GSKit

GSKCapiCmd est un outil de ligne de commande non Java, et Java™ n'a pas besoin d'être installé sur votre système pour que vous puissiez utiliser cet outil ; il se trouve dans le dossier <Statistics Server installation directory>/bin . Le processus de configuration de votre environnement d'exécution d'IBM Global Security Kit (GSKit) varie en fonction de la plateforme utilisée.

Pour configurer pour Linux/Unix, ajoutez le répertoire des bibliothèques partagées <Statistics Server installation directory>/lib à votre environnement :

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

Le nom de la variable du chemin de bibliothèque partagée dépend de la plateforme.

- Linux utilise le nom de variable : LD_LIBRARY_PATH

Par exemple, pour définir l'environnement sous Linux, utilisez :

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

Accès du compte aux fichiers

Veillez à accorder les droits d'accès appropriés aux comptes qui devront accéder aux fichiers SSL :

1. Pour tous les comptes qui sont utilisés par IBM SPSS Statistiques pour la connexion, accordez un droit d'accès en lecture aux fichiers SSL.

   Remarque : Cela s'applique également à l'utilisateur *Se connecter en tant que* défini dans le service IBM SPSS Statistiques Server. Sous UNIX ou Linux, il s'applique à l'ID utilisateur que vous utilisez pour démarrer le serveur.
2. Pour Windows, il ne suffit pas que les comptes soient dans le groupe Administrateurs et qu'un droit d'accès soit accordé à ce groupe lorsque le contrôle d'accès utilisateur (UAC) est activé. Vous devez en plus exécuter l'une des actions suivantes :
   - Accorder des droits aux comptes de façon distincte.
   - Créer un nouveau groupe, ajouter les comptes à ce groupe et accorder au groupe le droit d'accès aux fichiers SSL.
   - Désactiver le contrôle d'accès utilisateur.

Création d'une base de données de clés SSL

Utilisez l'outil GSKCapiCmd pour créer votre base de données de clés. Avant d'utiliser cet outil, vous devez configurer votre environnement. Pour plus d'informations, voir la rubrique «Configuration de l'environnement pour l'exécution de GSKit», à la page 39.

Pour créer la base de données de clés, exécutez GSKit et entrez la commande suivante :

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

Où `<ver>` est le numéro de version du GSKit, `<filename>` est le nom que vous souhaitez utiliser pour le fichier de la base de données de clés et `<password>` est le mot de passe de la base de données de clés.

L'option `-stash` crée un fichier de dissimulation au même chemin que la base de données de clés, avec une extension de fichier `.sth`. GSKit utilise le fichier de dissimulation pour se procurer le mot de passe de la base de données de clés pour ne pas avoir à le saisir sur la ligne de commande à chaque fois.

Remarque : Il est conseillé d'utiliser une protection de système de fichiers renforcée pour le fichier `.sth`.

Création d'un certificat SSL autosigné

Vous pouvez générer un certificat auto-signé et le stocker dans la base de données des clés à l'aide de la commande suivante.

```
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>
```

Attribut	Descriptif
`<ver>`	Numéro de version du GSKit
`<filename>`	Nom du fichier de la base de données des clés
`<Number of days certificate is valid>`	Le nombre physique de jours de validité du certificat
`<label>`	Une étiquette descriptive pour vous aider à identifier le fichier. Par exemple, vous pouvez utiliser une étiquette, telle que, `myselfsigned`
`CN`	Le nom de domaine complet (FQDN) du système sur lequel IBM SPSS Statistics Server est installé

Installation d'un certificat SSL autosigné

Pour les machines client qui se connectent au serveur via SSL, vous devez distribuer la part publique du certificat aux clients pour qu'elle puisse être stockée dans leurs bases de données de clés. Pour ce faire, procédez comme suit :

Remarque : Ignorez cette étape si vous utilisez un certificat signé par une autorité de certification. Si vous utilisez un certificat signé, vous devez copier l'autorité de certification sécurisée sur les ordinateurs clients. N'oubliez pas qu'un ordinateur serveur peut également agir comme un client. Par exemple, IBM SPSS Statistiques Server se connecte à IBM SPSS Référentiel des services de collaboration et de déploiement. Dans ce cas, IBM SPSS Statistiques Server est le client et vous devez donc copier le certificat du serveur IBM SPSS Référentiel des services de collaboration et de déploiement sur le serveur IBM SPSS Statistiques .

1. Extrayez la partie publique dans un fichier via la commande suivante :

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

2. Distribuez `root.pem` aux clients. Si vous disposez de plusieurs autorités de certification sécurisées, copiez-les dans un fichier `root.pem` unique. Les autorités de certification autorisées sont des fichiers texte qui vous permettent de copier et de coller le ou les certificats. Copiez `root.pem` à l'emplacement suivant des ordinateurs clients. Si vous avez déjà copié un fichier `root.pem` sur le client pour un autre produit IBM, ajoutez les informations de l'autorité de certification racine sécurisée à partir de l'autorité dans le fichier `root.pem` existant. Par défaut, tous les produits clients IBM recherchent les fichiers de certificat signés sécurisés à cet emplacement. Si vous souhaitez utiliser un autre emplacement, créez une variable d'environnement `SSL_CERT_DIR` et définissez la valeur de la variable sur l'emplacement.
   - Windows 7 et versions ultérieures : `C:\ProgramData\IBM\SPSS\certificates`
   - Mac : `/Library/Application Support/IBM/SPSS/certificates`
   - UNIX et Linux : `/opt/IBM/SPSS/certificates`

Configuration de certificats client

Lorsque SPSS Statistics Server le système est configuré pour utiliser une connexion SSL et que vous utilisez un certificat auto-signé, vous devez copier et configurer l'autorité de certification de confiance sur tous les postes de travail clients.

Par exemple, lorsque IBM SPSS Services de collaboration et de déploiement soumet une tâche à SPSS Statistics Server (qui prend en charge la fonctionnalité « SSL »). Dans ce cas, IBM SPSS Services de collaboration et de déploiement est le client. L'autorité de certification de confiance (`root.pem` sur le SPSS Statistics Server) doit être copiée et configurée sur toutes les machines IBM SPSS Services de collaboration et de déploiement .

Configuration des fichiers de certificat pour IBM SPSS Services de collaboration et de déploiement

La prise en charge de IBM SPSS Services de collaboration et de déploiement peut être déployée sur un serveur d'applications Web (par exemple, IBM WebSphere et RedHat JBoss EAP).

La première étape de la configuration des fichiers de certificat pour le support IBM SPSS Services de collaboration et de déploiement consiste à extraire le fichier SPSS Statistics Server `root.pem` de votre administrateur.

La procédure de configuration des certificats d' SSL s dépend du serveur d'applications Web utilisé.

IBM WebSphere et RedHat JBoss EAP

Les instructions suivantes s'appliquent à la fois à IBM WebSphere et à RedHat JBoss EAP.

RedHat JBoss EAP-Remarque : Lorsque l'application SPSS Statistics Server utilise GSKit (IBM) SSL, vous devez utiliser le JDK IBM lors de la configuration IBM SPSS Services de collaboration et de déploiement sur JBoss EAP.

1. Distribuez le fichier `root.pem` sur la machine IBM SPSS Services de collaboration et de déploiement Server. Si vous disposez de plusieurs autorités de certification de confiance, copiez-les dans un seul fichier `root.pem` (les autorités de certification de confiance sont des fichiers texte, de sorte que vous pouvez copier et coller les certificats). Copiez `root.pem` à l'emplacement suivant sur le serveur IBM SPSS Services de collaboration et de déploiement .

   Si vous avez déjà copié un fichier `root.pem` sur le client pour un autre produit IBM , ajoutez les informations de l'autorité de certification racine accréditée de votre autorité dans le fichier `root.pem` existant. Créez une variable d'environnement `SSL_CERT_DIR` et définissez la valeur de la variable sur l'emplacement de serveur souhaité qui contient le fichier `root.pem` .
2. Vérifiez que l'utilisateur IBM SPSS Services de collaboration et de déploiement Server ajoute la variable d'environnement `SSL_CERT_DIR` .

   Remarque : Le serveur IBM SPSS Services de collaboration et de déploiement doit être redémarré après l'ajout de la variable d'environnement.

Installation du codage de type Unlimited Strength

Le codage de type US Export-Strength est activé dans le logiciel Java Runtime Environment livré avec le produit. Pour améliorer la sécurité de vos données, il est recommandé de mettre à niveau le codage vers le système Unlimited Strength.

1. Extrayez les fichiers de la politique Unlimited Strength contenus dans le fichier compressé. Le fichier compressé contient un fichier `US_export_policy.jar` et un fichier `local_policy.jar`.
2. Remplacez les copies existantes des fichiers *US_export_policy.jar* et *local_policy.jar* par les deux fichiers que vous avez téléchargés et extraits.

Indiquer aux utilisateurs d'activer SSL

Lorsque les utilisateurs se connectent au serveur via un produit client, ils doivent activer SSL dans la boîte de dialogue pour se connecter au serveur. N'oubliez pas d'avertir vos utilisateurs de sélectionner la case à cocher appropriée.

Activation de SSL avec OpenSSL

Sécurisation des communications client-serveur et serveur-serveur avec le protocole OpenSSL

Remarque : À partir de la version 30.0.0, l'utilisation de SSL 1.1 est déconseillée.

Les principales étapes de sécurisation des communications client-serveur et serveur-serveur avec le protocole SSL sont les suivantes :

1. Installez OpenSSL sur l'ordinateur serveur.
2. Obtenez et installez le certificat et les clés SSL.
3. Activez et configurez SSL dans l'application d'administration du serveur (IBM SPSS Responsable du déploiement).

   Remarque : IBM SPSS Statistiques Server prend en charge le protocole TLSv1. SSLv3 souffre d'une vulnérabilité de sécurité démontrée et ne doit pas être utilisé.
4. Si vous utilisez des certificats de chiffrement d'une force supérieure à 2048 bits, installez un chiffrement de force illimitée sur les ordinateurs des clients .
5. Si vous utilisez un certificat auto-signé, copiez le certificat sur l'ordinateur client.

6. Demandez aux utilisateurs d'activer SSL lors de la connexion au serveur.

Remarque : Parfois, un produit serveur agit comme un client. Par exemple, le Serveur IBM SPSS Statistiques se connectant au IBM SPSS Référentiel des services de collaboration et de déploiement. Dans ce cas, IBM SPSS Statistiques Server est le *client*.

Installation d'OpenSSL

Si OpenSSL n'est pas disponible sur le serveur, vous devez l'installer.

1. Téléchargez OpenSSL depuis http://www.openssl.org/. Vérifiez que vous utilisez la version d'OpenSSL qui correspond à la version du serveur :

Tableau 2. Versions d'OpenSSL

Produit serveur	**Version d'OpenSSL compatible**
IBM SPSS Statistiques 29	1.1.1f ou version ultérieure
IBM SPSS Statistiques 28	1.1.1f ou version ultérieure
IBM SPSS Statistiques 27.0.1	1.1.1f ou version ultérieure **Remarque :** La prise en charge du protocole SSLv3 non sécurisé a été dépréciée.
IBM SPSS Statistiques 26-27	1.0.2 ou version ultérieure
IBM SPSS Statistiques 24-25	1.0.1f ou version ultérieure
IBM SPSS Statistiques 20-23	1.0.0
IBM SPSS Statistiques 17-19 (*non* Linux® sur System z®)	0.9.8 et ses sous-versions (0.9.8a, 0.9.8b, etc.)
IBM SPSS Statistiques 19 (Linux® sur System z®)	1.0.0

2. Suivez les instructions d'installation et de configuration du logiciel. Il est recommandé de générer OpenSSL vous-même, avec les instructions suivantes:

   Windows. OpenSSL doit être créé avec des DLL (qui sont multi-unité d'exécution par défaut).

   UNIX. OpenSSL doit prendre en charge plusieurs unités d'exécution (fonction qui n'est pas toujours activée par défaut) et les bibliothèques partagées.

3. Vérifiez que les modules OpenSSL sont inclus dans le système path.

   Remarque : S'il existe plusieurs versions des modules OpenSSL sur l'ordinateur serveur, copiez les modules OpenSSL du serveur IBM SPSS Statistiques dans le répertoire où le serveur IBM SPSS Statistiques est installé.

Obtention et installation du certificat et des clés SSL

1. Procurez-vous un certificat et un fichier de clé SSL. Ceci peut être fait de deux manières :
   - Achetez-les auprès d'une autorité de certification publique (comme Comodo, Symantec ou GoDaddy). L'autorité de certification publique signe le certificat pour vérifier le serveur qui l'utilise. Il s'agit de la méthode recommandée.
   - Générez les fichiers de clés et de certificat avec une autorité de certificat autosigné. OpenSSL fournit un outil de gestion des certificats dans ce but ; vous pouvez aussi effectuer une recherche sur Internet pour obtenir des instructions sur la création d'un certificat SSL signé.
2. Copiez les fichiers de certificat et de clé dans un ou plusieurs répertoires locaux du serveur. Les clés publiques et privées peuvent être stockées dans des répertoires distincts. Elles peuvent

également être stockées dans un fichier unique. Assurez-vous que la clé privée ne se trouve pas à un emplacement qui peut être rencontré lors d'une navigation dans le système de fichiers.

3. Copiez l'autorité de certification de confiance nommée *root.pem* à l'emplacement suivant sur l'ordinateur serveur. Si vous souhaitez utiliser un autre emplacement, créez une variable d'environnement SSL_CERT_DIR et définissez la valeur de la variable à cet emplacement.

   Windows 7 et versions ultérieures : `C:\ProgramData\IBM\SPSS\certificates`

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

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

Activation et configuration de SSL dans IBM SPSS Responsable du déploiement

1. Démarrez l'application d'administration du serveur (IBM SPSS Statistics Administration Console qui est installée avec IBM SPSS Responsable du déploiement) et connectez-vous au serveur.
2. Sur la page de configuration, réglez **Secure Sockets Layer** sur `Yes`.
3. Dans **fichier de clé publique SSL**, indiquez le chemin d'accès complet au fichier de clé publique.
4. Dans **fichier de clé privée SSL**, indiquez le chemin d'accès complet au fichier de clé privée.

   Remarque : Si les clés publique et privée sont stockées dans un seul fichier, indiquez le même fichier dans **fichier de clé publique SSL** et dans **fichier de clé privée SSL**.
5. A partir des menus, sélectionnez :

   Fichier > **Enregistrer**
6. Redémarrez le service ou le démon du serveur. Au redémarrage, le mot de passe SSL vous sera demandé. Sous Windows, vous pouvez sélectionner **Se souvenir de ce mot de passe** pour stocker le mot de passe de manière sécurisée. Cette option permet de ne pas avoir à saisir le mot de passe à chaque démarrage du serveur.

Installation du codage de type Unlimited Strength

Le codage de type US Export-Strength est activé dans le logiciel Java Runtime Environment livré avec le produit. Pour améliorer la sécurité de vos données, il est recommandé de mettre à niveau le codage vers le système Unlimited Strength.

1. Extrayez les fichiers de la politique Unlimited Strength contenus dans le fichier compressé. Le fichier compressé contient un fichier `US_export_policy.jar` et un fichier `local_policy.jar`.
2. Remplacez les copies existantes des fichiers *US_export_policy.jar* et *local_policy.jar* par les deux fichiers que vous avez téléchargés et extraits.

Copie du fichier de certificat sur les ordinateurs clients

Remarque : Ignorez cette étape si vous utilisez un certificat signé par une autorité de certification.

Si vous utilisez un certificat signé, vous devez copier l'autorité de certification sécurisée sur les ordinateurs *clients*. N'oubliez pas qu'un ordinateur serveur peut également agir comme un client. Par exemple, le Serveur IBM SPSS Statistiques se connectant au IBM SPSS Référentiel des services de collaboration et de déploiement. Dans ce cas, le Serveur IBM SPSS Statistiques est le *client*, et vous devez alors copier le certificat du serveur IBM SPSS Référentiel des services de collaboration et de déploiement sur le Serveur IBM SPSS Statistiques.

1. Créez une autorité de certification sécurisée nommée *root.pem*. Par exemple, si vous créez l'autorité de certification sécurisée avec OpenSSL, utilisez le commutateur `-out` pour spécifier le fichier de sortie en tant que *root.pem*. Si vous disposez de plusieurs autorités de certification sécurisées, copiez-les dans un fichier *root.pem* unique. Les autorités de certification autorisées sont des fichiers texte qui vous permettent de copier et de coller le ou les certificats.

2. Copiez *root.pem* à l'emplacement suivant des ordinateurs clients. Si vous avez déjà copié un fichier *root.pem* sur le client pour un autre produit IBM Corp., ajoutez les informations de l'autorité de certification racine sécurisée à partir de l'autorité dans le fichier *root.pem* existant. Par défaut, tous les produits clients IBM Corp. recherchent les fichiers de certificat signés sécurisés à cet emplacement. Si vous souhaitez utiliser un autre emplacement, créez une variable d'environnement `SSL_CERT_DIR` et définissez la valeur de la variable à cet emplacement.

   Windows 7 et versions ultérieures : `C:\ProgramData\IBM\SPSS\certificates`

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

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

Indiquer aux utilisateurs d'activer SSL

Lorsque les utilisateurs se connectent au serveur via un produit client, ils doivent activer SSL dans la boîte de dialogue pour se connecter au serveur. N'oubliez pas d'avertir vos utilisateurs de sélectionner la case à cocher appropriée.

Définition d'un environnement local

Le logiciel serveur et le client qui s'y connecte doivent s'exécuter dans le même jeu de caractères, le même codage et les mêmes paramètres régionaux. Le logiciel serveur obtient son environnement local du client. Par défaut, il s'agit de l'environnement local *système* du client. Toutefois, le client peut remplacer la valeur par défaut pour le traitement des fichiers de données dans d'autres environnements locaux. En remplaçant la valeur par défaut, l'utilisateur demande au logiciel serveur de s'exécuter dans un environnement local spécifié sans modifier l'environnement local du système du client.

Syntaxe

L'utilisateur remplace la valeur par défaut à l'aide de la commande de syntaxe `SET LOCALE` :

```
SET LOCALE=”localeid”
```

`localeid` est une chaîne qui identifie l'environnement local dans lequel le logiciel serveur sera exécuté. `SET LOCALE` écrit une entrée de registre sur la machine client. Cette entrée est conservée de sorte que la prochaine fois que IBM SPSS Statistiques sera démarré sur la machine client, IBM SPSS Statistiques s'exécutera dans cet environnement local.

La convention de dénomination de l'ID d'environnement local peut varier d'une plateforme à l'autre et d'un fournisseur à l'autre. Par conséquent, un fichier XML est installé avec le serveur qui mappe les environnements locaux du client aux environnements locaux du serveur. Ce fichier, *loclmap.xml*, se trouve dans le répertoire d'installation du serveur sous Windows et dans le sous-répertoire */bin* sous UNIX.

loclmap.xml

L'élément racine dans *loclmap.xml* est le suivant. L'élément racine identifie également l'emplacement du schéma.

```
<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'élément racine contient des éléments `<client-locale>` avec un attribut `name` identifiant l'environnement local du client. Les éléments `<client-locale>` contiennent un ou plusieurs éléments `<server-locale>` . Chaque élément `<server-locale>` possède un attribut `name` identifiant l'environnement local du serveur qui correspond à l'environnement local du client. Le logiciel serveur convertit l'ID d'environnement local du client en un ID pouvant être utilisé sur la machine du serveur. Il vérifie chaque environnement local du serveur dans l'ordre, jusqu'à ce qu'il en trouve un qui soit valide sur la machine du serveur.

Aucun des environnements locaux de serveur par défaut dans *loclmap.xml* n'est un environnement local Windows. Les paramètres régionaux du système Windows ne sont généralement pas nécessaires car le logiciel serveur tente d'abord d'utiliser les mêmes paramètres régionaux que ceux du système du client. Un serveur Windows doit avoir l'environnement local qui correspond à l'environnement local du client. Toutefois, vous pouvez ajouter des environnements locaux de serveur Windows à *loclmap.xml* si vous devez remplacer un environnement local Windows différent mais similaire.

Vous pouvez modifier *loclmap.xml* si nécessaire. Sachez simplement que vos éléments XML doivent être validés par rapport au schéma.

Exemple

Voici un exemple de contenu de *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>
```

Dans ce cas, si l'utilisateur émet une commande SET LOCALE="French", le logiciel serveur vérifie d'abord `fr_FR.cp1252` . Prenons le cas d'un serveur AIX . L'environnement local `fr_FR.cp1252` ne fonctionne pas sous AIX, de sorte que le logiciel serveur continue de vérifier jusqu'à ce qu'il atteigne `fr_FR.windows-1252`, ce qui fonctionne sous AIX.

Utilisation d'un environnement local de serveur

Si l'utilisateur utilise SET LOCALE à l'aide d'un ID d'environnement local de serveur non reconnu sur la machine client, la machine client utilise *loclmap.xml* pour rechercher l'ID d'environnement local de client associé à un ID d'environnement local de serveur. Il écrit cet ID d'environnement local dans le registre. Par exemple, si l'utilisateur émet SET LOCALE="fr_FR.windows-1252", French est écrit dans le registre. Pour savoir quelle entrée du fichier *loclmap.xml* s'applique au client, vous pouvez exécuter la commande SHOW LOCALE en mode local.

Problèmes éventuels

Sachez que l'utilisation de la commande SET LOCALE peut entraîner des problèmes fonctionnels dans certains cas:

- Les noms de variable en cours peuvent ne pas être légaux dans la nouvelle page de codes.
- Les correspondances de noms insensibles à la casse peuvent échouer. L'échec peut se produire parce que les chaînes sont converties en caractères majuscules dans les correspondances de noms insensibles à la casse (par exemple, lors de la comparaison de noms de variables). Si l'environnement local est incorrect, cette conversion modifie le caractère (par exemple, dans la page de codes d'Europe centrale, 1250).
- Certains octets peuvent être interprétés de manière incorrecte comme des octets de début et un problème peut se produire en raison d'un octet de trace inattendu.
- SET LOCALE ne modifie pas les paramètres régionaux du système du client. Par conséquent, si l'environnement local IBM SPSS Statistiques associé à SET LOCALE est différent de l'environnement local du système du client, des problèmes d'affichage se produisent à différents endroits. Dans cette situation, un utilisateur ne peut pas non plus utiliser un éditeur de méthode d'entrée (IME) pour entrer des caractères nationaux.

- L'environnement local IBM SPSS Statistiques , le paramètre OLANG et le codage utilisé pour les données doivent être compatibles. Sinon, la sortie peut être inutilisable et illisible.

Connexion au logiciel serveur

L'utilisateur final se connecte au logiciel serveur en se connectant à partir de l'application client. Pour vous connecter à un utilisateur final, vous devez fournir les informations suivantes:

- **Nom de l'ordinateur ou adresse IP.** Lorsque les utilisateurs se connectent au logiciel serveur, ils se connectent à partir de l'application client. Pour ce faire, ils doivent spécifier correctement le nom de l'ordinateur exécutant le logiciel serveur. L'ordinateur serveur peut être identifié par un nom alphanumérique (par exemple, `myserver`) ou par une adresse IP affectée à l'ordinateur serveur (par exemple, `202.123.456.78`), selon votre choix. Si vous configurez le serveur et les ordinateurs de bureau clients pour qu'ils utilisent le protocole SSL (SSL), l'utilisateur final doit utiliser un nom de domaine complet (par exemple, `myserver.mycompany.com`).
- **Numéro de port.** Les utilisateurs finaux doivent spécifier correctement le port sur lequel le logiciel serveur écoute les connexions. Le numéro de port est la valeur par défaut du serveur, ou tout autre numéro que vous avez spécifié lors de la configuration du logiciel serveur.
- **Nom de domaine (Windows uniquement).** Les utilisateurs finaux peuvent également avoir besoin de spécifier un nom de domaine. Un nom de domaine est requis uniquement lorsque l'ordinateur serveur se trouve dans un domaine différent de celui des ordinateurs de bureau de l'utilisateur final.
- **ID utilisateur et mot de passe :** Les utilisateurs finaux doivent se connecter à l'ordinateur serveur. Pour ce faire, les utilisateurs ont besoin d'un compte valide, avec les droits appropriés, pour l'ordinateur sur lequel le logiciel serveur est en cours d'exécution.
- **Secure Socket Layer (SSL).** Si vous utilisez le protocole SSL pour chiffrer les communications qui ont lieu lorsque les utilisateurs finaux se connectent au logiciel serveur, demandez aux utilisateurs d'activer le protocole SSL lorsqu'ils configurent la connexion au serveur. Les clients n'ont pas besoin de savoir quel protocole SSL est utilisé par le serveur. Le logiciel client essaiera les deux et utilisera celui qui fonctionne.

Accès aux données et aux fichiers

Lorsque les utilisateurs finaux se connectent au logiciel du serveur analytique, leur vue des sources de données et des fichiers est du point de vue de l'ordinateur serveur et non de leur ordinateur de bureau.

- **Sources de donnéesODBC .** Si vos utilisateurs finaux ont besoin d'accéder aux sources de données ODBC définies sur l'ordinateur serveur, distribuez les noms, les descriptions et les informations de connexion de ces sources de données. Pour plus d'informations sur l'accès à la base de données à partir du logiciel serveur, voir Chapitre 3, «Accès aux données», à la page 9 .
- **Accès aux fichiers.** Distribuez les noms et les emplacements des fichiers sur l'ordinateur serveur auquel les utilisateurs finaux doivent accéder. Pour plus d'informations, reportez-vous à la rubrique «Données de référencement», à la page 10.

Enregistrement de données et de fichiers

Lorsque les utilisateurs finals sauvegardent des fichiers alors qu'ils sont connectés au logiciel serveur, l'emplacement par défaut de la sauvegarde est le répertoire à partir duquel le fichier a été ouvert. Dans de nombreux cas, il s'agit de l'ordinateur de bureau local ; cependant, pour les fichiers de données, il s'agit souvent d'un emplacement protégé en écriture sur l'ordinateur serveur. Indiquez aux utilisateurs où sauvegarder les fichiers de données. Généralement, l'emplacement est le répertoire de base de l'utilisateur quelque part sur votre réseau.

Remarque UNIX: Demandez aux utilisateurs finaux d'utiliser la spécification de fichier complète et les barres obliques lors de la sauvegarde des fichiers (par exemple, */public/myhome/myserverdata/data.sav*). Evitez d'utiliser la barre oblique inversée dans le répertoire UNIX et les noms de fichier utilisés avec le logiciel serveur.

Chapitre 6. Analyse et amélioration des performances

Si vous avez besoin d'améliorer les performances du logiciel serveur, consultez ce chapitre pour connaître les différentes stratégies, allant des changements de configuration aux mises à niveau matérielles. Avant d'effectuer ces modifications, obtenez des informations sur les performances afin de savoir quelles sont les zones problématiques.

Nous fournissons également un livre blanc qui contient des informations supplémentaires sur l'amélioration des performances. Accédez à http://www.ibm.com/developerworks/spssdevcentral et recherchez le lien vers "Livres et articles".

Obtention d'informations sur les performances

Pour vérifier les performances, comparez l'utilisation dans les zones suivantes lorsque le serveur n'est pas utilisé lorsqu'il est fortement utilisé.

- Utilisation du disque
- Utilisation de l'unité centrale
- Utilisation de la mémoire
- Utilisation du réseau

Journalisation

L'application d'administration (IBM SPSS Statistics Administration Console, qui est installée dans le cadre de IBM SPSS Responsable du déploiement) vous permet de configurer le logiciel serveur pour qu'il consigne les informations de performances. A l'aide du noeud **Intervalle du journal des performances** , vous pouvez spécifier la fréquence à laquelle le logiciel serveur écrit les informations de performances dans le journal. Pour plus d'informations, voir la rubrique relative à la connexion dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide relative à IBM SPSS Services de collaboration et de déploiement). Vous pouvez également obtenir des informations sur les performances directement à partir du système d'exploitation.

Obtention d'informations sur les performances sous Windows

Sous Windows, vous pouvez obtenir des informations sur les performances à l'aide du moniteur de performances.

Tableau 3. Informations sur les performances Windows

Zone	**Objet du moniteur de performances Windows**	**Compteur utile**
Utilisation du disque	PhysicalDisk	% de temps d'inactivité
Utilisation de l'UC	Processeur	% Temps de processeur
Utilisation de la mémoire	Mémoire	Octets mobilisés
Utilisation réseau	Interface réseau	Nombre total d'octets par seconde pour chaque instance d'interface physique (pas l'interface de bouclage TSP MS)

Obtention d'informations sur les performances sous UNIX

Sous UNIX, il existe différentes commandes permettant d'obtenir des informations sur les performances, en fonction du fournisseur.

Tableau 4. Informations sur les performances UNIX

Zone	Vendeur	Commande	Remarque
Utilisation du disque	Linux	iostat -x	Vérifiez la colonne **%util** .
Utilisation du disque	AIX	iostat -d	Vérifiez la colonne **% tm_actl** .
Utilisation de l'UC	Linux	haut	Utilisez la commande interactive P pour trier par utilisation de l'UC.
Utilisation de l'UC	AIX	ps aux	Accédez à la commande `sort` pour effectuer un tri en fonction de la colonne **%CPU** .
Utilisation de l'UC	Tous	temps de disponibilité	Vérifiez la charge moyenne.
Utilisation de la mémoire	Linux	haut	Utilisez la commande interactive `M` pour trier par utilisation de l'UC.
Utilisation de la mémoire	AIX	ps aux	Accédez à la commande `sort` pour effectuer un tri en fonction de la colonne **RSS** .
Utilisation réseau	Tous	netsat	Utilisez les commutateurs `-i` et `-s` pour plus d'informations.

Etape suivante

Après avoir recueilli ces informations, vous devriez être en mesure d'identifier la ou les zones qui posent problème. Les sections suivantes décrivent les solutions et recommandations possibles pour chaque domaine.

Amélioration de l'utilisation du disque

Tenez compte des points suivants pour améliorer l'utilisation du disque.

Espace. Prévoyez suffisamment d'espace disque. Chaque utilisateur a généralement besoin d'un espace disque temporaire égal à deux fois la taille du fichier de données (SAV) utilisé (l'espace requis est compris entre 1 et 2.5 fois). Un utilisateur triant un fichier peut avoir besoin d'un espace temporaire supérieur à trois fois la taille du fichier. Par exemple, si six utilisateurs simultanés accèdent à un fichier et que deux d'entre eux effectuent un tri à la fois, ils peuvent avoir besoin de 17 fois la taille du fichier. Dans la pratique, ils ne seront pas en période d'utilisation maximale simultanément, donc 12 fois la taille du fichier serait suffisante.

Matériel. Utilisez des disques SCSI pour des performances plus rapides. N'utilisez pas l'environnement de développement intégré.

Configuration du système. Conservez les fichiers temporaires sur une broche distincte. Vous pouvez également définir plusieurs emplacements de fichiers temporaires à l'aide de l'application d'administration. Assurez-vous que chaque emplacement se trouve sur une broche distincte. Si vous utilisez RAID, utilisez RAID0 comme fuseau de fichier temporaire. La vitesse des fichiers utilisables obtenue à partir de RAID0 est préférée à la vitesse de redondance obtenue à partir de RAID1. Si votre unité centrale n'est pas un problème et que l'ordinateur serveur exécute Windows, vous pouvez également compresser le répertoire de données ou les fichiers de données sur le disque. N'allouez pas plus de mémoire virtuelle.

IBM SPSS Statistiques . Si la mémoire n'est pas un problème mais que l'utilisation du disque l'est, augmentez l'espace de travail dans IBM SPSS Statistiques pour des performances plus rapides. Essayez de le définir en divisant la quantité de mémoire RAM sur l'ordinateur serveur par le nombre attendu d'utilisateurs simultanés. Par exemple, si l'ordinateur serveur dispose de 1 Go de mémoire RAM, définissez l'espace de travail sur 0.25 Go de mémoire RAM.

Répertoire des fichiers temporaires. Modifiez les paramètres du profil utilisateur ou des groupes de sorte que les répertoires de fichiers temporaires de chaque utilisateur se trouvent sur des unités physiques différentes.

Compression du cache. Si vos utilisateurs utilisent régulièrement des fichiers de données volumineux (en particulier si la taille des fichiers est supérieure à la moitié de la mémoire RAM du serveur), essayez d'activer la compression du cache dans l'application d'administration.

Amélioration de l'utilisation de l'UC

Tenez compte des points suivants pour améliorer l'utilisation de l'unité centrale:

Nombre. Ajoutez d'autres processeurs. Si vous souhaitez vous approcher de la vitesse à laquelle un utilisateur peut s'approcher lors de l'exécution de IBM SPSS Statistiques en local, essayez de disposer d'un processeur pour deux utilisateurs simultanés. Utilisez également des processeurs qui sont aussi rapides ou plus rapides que le processeur de l'ordinateur de bureau. Par exemple, si vous prévoyez une moyenne de quatre utilisateurs simultanés, configurez l'ordinateur serveur avec deux processeurs rapides.

Matériel. Utilisez des processeurs rapides. L'ajout de quelques processeurs très rapides est préférable à l'ajout de beaucoup de processeurs lents. Si l'utilisation de l'unité centrale pose toujours problème avec les processeurs rapides, envisagez d'ajouter d'autres ordinateurs serveur à votre système.

Emplacement et accès aux fichiers SAV. Si certains fichiers sont souvent utilisés par de nombreux utilisateurs simultanés, envisagez de déplacer les fichiers sur plusieurs serveurs pour équilibrer la charge utilisateur. Par exemple, si *TestScores.sav* et *GPA.sav* sont tous deux fortement utilisés, placez-les sur des serveurs distincts. Contrôlez l'accès aux fichiers avec les droits du système d'exploitation (par groupe ou par utilisateur) au lieu de contrôler l'accès via les comptes serveur.

Priorité de l'unité centrale. Si certains utilisateurs ont besoin d'une priorité d'UC plus élevée que d'autres utilisateurs (par exemple, les utilisateurs qui exécutent des travaux rapides par rapport à ceux qui exécutent des travaux longs), modifiez les paramètres de profil utilisateur ou de groupe.

Compression du cache. La compression du cache entraîne une surcharge de l'unité centrale pour la compression et la décompression des fichiers de travail. Si vos utilisateurs ne travaillent pas avec des fichiers de données volumineux, vous pouvez envisager de le désactiver.

Amélioration de l'utilisation de la mémoire

Tenez compte des points suivants pour améliorer l'utilisation de la mémoire:

Montant : Ajoutez autant de mémoire RAM que possible. Essayez de disposer de 128 Mo de mémoire RAM pour chaque utilisateur simultané. Par conséquent, s'il y a quatre utilisateurs simultanés, configurez le serveur avec 512 Mo de mémoire RAM.

IBM SPSS Statistiques . Réduisez l'espace de travail dans IBM SPSS Statistiques.

Amélioration de l'utilisation du réseau

Tenez compte des points suivants pour améliorer l'utilisation du réseau:

Configuration du système. Planifiez des opérations de réseau intensif pour les périodes où le logiciel serveur n'est pas utilisé (par exemple, exécutez les sauvegardes du système pendant la nuit). Si vous identifiez un problème de trafic réseau sur un ordinateur sur lequel le serveur est en cours d'exécution, IBM Corp. vous aide à diagnostiquer le problème plus en détail.

Utilisation d' IBM SPSS Statistiques de manière efficace

En plus de vous concentrer sur des domaines problématiques spécifiques, vous pouvez également améliorer les performances en vous conformant aux instructions suivantes pour une utilisation efficace de IBM SPSS Statistiques .

Gestion des données : Si vous avez des fichiers de données volumineux qui nécessitent une mise à jour régulière et qui sont partagés par les utilisateurs, envisagez d'effectuer les mises à jour une fois, puis de les publier pour analyse. Par exemple, si vous ajoutez régulièrement des données mensuelles à un fichier, que vous les triez et que vous effectuez des transformations, désignez une personne pour exécuter le travail sur le fichier. Les autres utilisateurs peuvent obtenir les données dont ils ont besoin sans avoir à répéter la fusion, le tri et les transformations.

Interactif par rapport au traitement par lots. Si vous effectuez régulièrement des opérations longues et fastidieuses avec IBM SPSS Statistiques, envisagez de les exécuter à partir de IBM SPSS Statistiques Batch Facility plutôt qu'à partir d'un client connecté au serveur. Utilisez le client pour générer les rapports et exécutez-les à partir de IBM SPSS Statistiques Batch Facility une fois que les rapports sont prêts.

Annexe A. Traitement des incidents

logiciel serveur

Échec de la connexion locale (Windows uniquement). Les utilisateurs peuvent rencontrer une situation dans laquelle la connexion échoue car ils ne disposent pas du privilège de connexion locale sur le serveur. Pour résoudre ce problème, vous devez apporter des modifications `auspssprod.inf` déposer. Pour plus d'informations sur ce problème connu et le correctif temporaire associé, consultez Solution de contournement pour l'exigence du serveur selon laquelle les utilisateurs disposent du privilège « Autoriser la connexion locale » .

Conflit de numéro de port. En cas de conflit de numéro de port, le démarrage du logiciel serveur risque d'échouer. Corrigez le problème en utilisant l'application d'administration (IBM SPSS Statistics Administration Console, qui est installée avec IBM SPSS Responsable du déploiement) pour modifier le numéro de port. Pour plus d'informations, voir la rubrique Connexions dans le *Guide d'utilisation du gestionnaire de déploiement* (inclus dans l'aide de IBM SPSS Services de collaboration et de déploiement).

Comportement erratique. Le logiciel serveur peut se comporter de manière erratique si son fichier de configuration (par exemple, `statisticsd.conf`) est endommagé ou manquant. Pour corriger le problème, restaurez le fichier de configuration à partir de votre copie de sauvegarde. Copiez-le à l'emplacement indiqué dans l'application d'administration ou dans la variable d'environnement du fichier de configuration et redémarrez le logiciel serveur. Pour plus d'informations sur le redémarrage, voir «Démarrage et arrêt du logiciel serveur», à la page 22 dans.

L'application d'administration ne fonctionne pas (UNIX uniquement). Si vous utilisez l'application d'administration pour contrôler ou configurer le logiciel serveur et qu'il ne fonctionne pas (par exemple, vous ne pouvez pas arrêter le serveur), cela peut être dû au fait que vous n'avez pas démarré le logiciel serveur avec le script de démarrage fourni par IBM Corp.. Corrigez le problème en démarrant le logiciel serveur avec le script de démarrage *start_statistics_server* . Pour plus d'informations, voir «Pour arrêter le service ou le démon», à la page 22. Si vous recevez un message d'erreur lorsque vous tentez de contrôler ou de configurer le logiciel serveur, cela peut être dû au fait que vous êtes connecté à un compte qui ne dispose pas des droits d'administrateur.

Impossible de modifier l'emplacement des fichiers temporaires (UNIX uniquement). Si vous utilisez l'application d'administration pour modifier l'emplacement des fichiers temporaires et que la modification n'est pas effective, il se peut que le nouvel emplacement ne dispose pas de droits suffisants pour les utilisateurs finaux. Choisissez un emplacement doté d'un accès **en lecture**, **en écriture**et **en exécution** pour tous les utilisateurs qui se connectent au logiciel serveur.

Le serveur ne démarre pas (UNIX uniquement). Si le logiciel serveur ne démarre pas, cela peut être dû au fait que vous ne disposez pas des correctifs de système d'exploitation requis. Pour corriger le problème, téléchargez et installez le correctif approprié. Les correctifs requis sont répertoriés dans les instructions d'installation UNIX de votre produit serveur.

Logiciel client

Impossible pour l'utilisateur final de se connecter au serveur. Il se peut que l'utilisateur ne dispose pas des droits appropriés ou que le pare-feu bloque le logiciel serveur. Pour plus d'informations sur les droits utilisateur, voir «Autorisations», à la page 33 . Pour plus d'informations sur la configuration du pare-feu, voir «Configuration des connexions via un pare-feu», à la page 35 .

La connexion de l'utilisateur final échoue avec le message " l'ordinateur serveur distant spécifié est introuvable. Le service ou le démon n'est peut-être pas en cours d'exécution. Confirmez-le en vérifiant le statut du logiciel serveur. Pour résoudre le problème, redémarrez le service ou le démon. Pour plus d'informations, reportez-vous à la rubrique «Démarrage et arrêt du logiciel serveur», à la page 22.

La connexion de l'utilisateur final échoue avec le message " erreur lors de la connexion au package. L'utilisateur final a spécifié le nom ou l'adresse IP d'un ordinateur serveur qui ne se trouve pas sur le réseau. Pour résoudre le problème, demandez à l'utilisateur final d'entrer un nom de serveur valide.

La source de donnéesDataDirect ODBC échoue avec le message " not licensed message. La technologie d'accès aux données DataDirect est distribuée avec les produits IBM Corp. . Il ne fonctionne qu'avec les produits IBM Corp. plus récents-il ne fonctionne pas avec les versions antérieures, ni avec les applications nonIBM Corp. . Si les utilisateurs finaux tentent d'utiliser des sources de données DataDirect avec un produit plus ancien ou sans licence, ils reçoivent un message contenant le texte **Vous n'êtes pas autorisé à utiliser le pilote DataDirect ODBC**. Pour résoudre le problème lié au produit IBM Corp. , mettez à niveau vos utilisateurs vers une version en cours. Pour résoudre le problème lié aux produits sans licence, mettez à niveau votre licence avec DataDirect ou demandez aux utilisateurs finaux de ne pas tenter d'utiliser les sources de données que vous avez définies pour les produits IBM Corp. avec des applications sans licence.

Impossible de trouver un fichier de données ou une source de données ODBC . Lorsque les utilisateurs finaux s'exécutent en mode d'analyse distribuée, ils n'ont accès qu'aux fichiers de données et aux sources de données ODBC sur l'ordinateur qui exécute le logiciel serveur. Lorsque les utilisateurs finaux s'exécutent en mode d'analyse locale, ils n'ont accès qu'aux fichiers de données et aux sources de données ODBC sur leurs ordinateurs de bureau. Pour résoudre le problème, demandez à l'utilisateur final d'exécuter l'application client en mode approprié.

L'utilisateur final ne peut pas exécuter de procédure statistique (IBM SPSS Statistiques Server uniquement). Lorsque les utilisateurs finaux sont connectés au logiciel serveur, ils n'ont accès qu'aux options IBM SPSS Statistiques qui ont été installées lors de l'installation du serveur IBM SPSS Statistiques . Pour résoudre le problème, demandez à l'utilisateur final d'exécuter la procédure en mode d'analyse locale ou installez la procédure demandée sur l'ordinateur serveur.

Annexe B. IBM SPSS Statistiques Batch Facility

Remarque: IBM SPSS Statistiques Batch Facility est un utilitaire de traitement par lots inclus avec **IBM SPSS Statistiques Server**.

Généralement, le client pour IBM SPSS Statistiques Server est IBM SPSS Statistiques exécuté sur un ordinateur de bureau. Toutefois, IBM SPSS Statistiques Batch Facility est un autre moyen d'utiliser la puissance de IBM SPSS Statistiques Server et il s'exécute sur l'ordinateur serveur. IBM SPSS Statistiques Batch Facility est destiné à la **production automatisée** de rapports statistiques. La production automatisée permet d'exécuter des analyses sans intervention de l'utilisateur. La production automatisée est avantageuse si les utilisateurs de votre site ont régulièrement besoin d'un ensemble d'analyses longues, telles que des rapports hebdomadaires.

IBM SPSS Statistiques Batch Facility utilise comme entrée une demande de rapport contenue dans un fichier de **syntaxe de commande** . IBM SPSS Statistiques Batch Facility génère ensuite automatiquement les rapports statistiques spécifiés par la syntaxe.

Ce que vous devez connaître

Systèmes d'exploitation. IBM SPSS Statistiques Batch Facility est actuellement disponible avec tous les serveurs IBM SPSS Statistiques , UNIX et Windows.

Installation. IBM SPSS Statistiques Batch Facility est automatiquement installé dans le répertoire d'installation de IBM SPSS Statistiques Server sous Windows et dans le sous-répertoire */bin* du répertoire d'installation sous UNIX.

Appel. IBM SPSS Statistiques Batch Facility est exécuté à partir de la ligne de commande à l'aide du fichier exécutable *statisticsb* . Il s'exécute indépendamment de IBM SPSS Statistiques Server-IBM SPSS Statistiques Server n'a pas besoin d'être démarré pour qu'il s'exécute. Il peut également être exécuté simultanément avec IBM SPSS Statistiques Server.

Modes de fonctionnement. Les commandes sont soumises à IBM SPSS Statistiques Batch Facility en mode **batch** ou en **mode interactif**. En mode de traitement par lots, l'analyste ou l'informaticien soumet un fichier de syntaxe de commande à IBM SPSS Statistiques Batch Facility pour exécution-les commandes du fichier sont lues et traitées en tant que lot et la sortie est dirigée vers un fichier. IBM SPSS Statistiques Batch Facility s'exécute sans surveillance et s'arrête après l'exécution de la dernière commande. Il s'agit de la méthode standard d'utilisation de IBM SPSS Statistiques Batch Facility. En mode interactif, l'analyste entre les commandes une par une dans une invite de commande. Les commandes sont exécutées immédiatement et la sortie s'affiche dans la fenêtre. IBM SPSS Statistiques Batch Facility attend la commande suivante.

Documentation. Le guide de l'utilisateur, rédigé à l'intention des analystes et des professionnels de l'informatique d'un site qui utiliseront IBM SPSS Statistiques Batch Facility, se trouve sur le serveur IBM SPSS Statistiques Fichier ISO dans */Documentation/<langue>/Manuals*. Le guide de référence de la syntaxe de commande dont les analystes auront besoin pour créer des fichiers de syntaxe de commande pour IBM SPSS Statistiques Batch Facility se trouve sur le serveur IBM SPSS Statistiques Fichier ISO dans */Documentation/<langue>/Manuals*. IBM SPSS Statistiques Batch Facility for UNIX est également distribué avec une page manuelle, *statisticsb.1*, qui se trouve dans le sous-répertoire */bin* du répertoire d'installation de IBM SPSS Statistiques Server. Si vous administrez un système UNIX, copiez-le à l'emplacement où vous conservez vos pages manuelles.

Une documentation supplémentaire Le guide d'utilisation de IBM SPSS Statistiques Batch Facility contient suffisamment d'informations pour permettre à un analyste expérimenté avec le langage de syntaxe de commande IBM SPSS Statistiques de générer des fichiers de syntaxe de commande pour IBM SPSS Statistiques Batch Facility. Si les analystes de votre site sont nouveaux dans IBM SPSS Statistiques, ils peuvent avoir besoin d'une documentation supplémentaire. Si c'est le cas, vous pouvez les diriger vers notre site Web à l'adresse http://www.ibm.com/software/analytics/spss/ou leur demander de contacter votre représentant commercial.

Annexe C. Tâches du système d'exploitation Windows

Vous pouvez effectuer la plupart des tâches d'administration avec l'application d'administration ; toutefois, il peut être nécessaire d'effectuer quelques tâches avec le système d'exploitation Windows. Utilisez les fonctions de système d'exploitation suivantes pour administrer les logiciels serveur exécutés sous Windows:

- **Propriétés du fichier.** Permet de définir l'accès de l'utilisateur final au répertoire d'installation du logiciel serveur, à l'emplacement du fichier temporaire et aux fichiers de données.
- **Propriétés système.** Utilisé pour créer des variables d'environnement.
- **Gestionnaire d'utilisateurs.** Permet de créer des comptes d'utilisateur final.
- **Panneau de configuration des services.** Utilisé pour démarrer, arrêter et configurer le service.
- **AdministrateurODBC .** Utilisé pour configurer les sources de données.

Propriétés de fichier

Utilisez les propriétés de fichier pour définir les droits d'accès aux fichiers. Pour les fichiers de données, la façon dont vous effectuez cette opération dépend de l'emplacement de stockage des données. Lorsque vous stockez des données sur le même ordinateur que le logiciel serveur, vous contrôlez l'accès au répertoire de données en définissant des droits sur un répertoire d'une unité NTFS.

Sur l'ordinateur serveur, connecté en tant qu'administrateur:

1. Utilisez l'explorateur Windows pour accéder au répertoire de données.
2. Cliquez sur le répertoire, cliquez avec le bouton droit de la souris, puis cliquez sur **Partage** dans le menu contextuel.
3. Cliquez sur l'onglet **Sécurité** et configurez les droits.

   Remarque: l'onglet Sécurité est disponible uniquement sur les unités NTFS. Si vous n'êtes pas sûr du type de système de fichiers utilisé par votre matériel, procédez comme suit:
4. Utilisez l'explorateur Windows pour accéder à l'unité.
5. Cliquez sur l'unité, cliquez avec le bouton droit de la souris, puis cliquez sur **Propriétés** dans le menu contextuel.
6. Cliquez sur l'onglet **Général** et examinez la valeur du système de fichiers.

   Lorsque vous stockez des données sur un ordinateur de votre réseau, vous pouvez contrôler l'accès au répertoire de données en créant une ressource partagée et en définissant les droits de manière appropriée.

   Sur l'ordinateur en réseau, connecté en tant qu'administrateur:
7. Utilisez l'explorateur Windows pour accéder au répertoire de données.
8. Cliquez sur le répertoire, cliquez avec le bouton droit de la souris, puis cliquez sur **Partage** dans le menu contextuel.
9. Cliquez sur l'onglet **Partage** dans la boîte de dialogue, cliquez sur **Partagé en tant que**, entrez un nom de partage et définissez l'accès approprié.

Propriétés système

Utilisez les propriétés système pour créer des variables d'environnement.

Sur l'ordinateur serveur, connecté en tant qu'administrateur:

1. Sur le bureau Windows, cliquez avec le bouton droit de la souris sur l'icône de l'ordinateur. Par exemple, cliquez avec le bouton droit de la souris sur **Mon ordinateur**.

2. Sélectionnez **Propriétés** dans le menu.
3. Cliquez sur l'onglet **Avancé** , puis sur **Variables d'environnement**.
4. Cliquez sur **Nouveau**.
5. Entrez le nom de la nouvelle variable.
6. Entrez la valeur de la nouvelle variable.

Gestionnaire des utilisateurs

Utilisez le gestionnaire d'utilisateurs pour créer des comptes d'utilisateur final.

Sur l'ordinateur serveur, connecté en tant qu'administrateur:

1. Dans le menu Démarrer de Windows, sélectionnez :

   Programmes > **Outils d'administration**

   - Sélectionnez **Gestion de l'ordinateur** , puis **Utilisateurs et groupes locaux**.
2. Créez les comptes utilisateur.

Panneau de configuration des services

Utilisez le panneau de configuration des services Windows pour:

- Arrêtez et démarrez le service.
- Modifiez les paramètres de démarrage du service.
- Vérifiez l'état du serveur.

Pour accéder au panneau de configuration des services et l'utiliser:

1. Dans le menu Démarrer de Windows, sélectionnez :

   Paramètres > **Panneau de configuration**
2. Sélectionnez **Outils d'administration** , puis **Services**.
3. Sélectionnez le service. Vous pouvez maintenant vérifier son statut, le démarrer ou l'arrêter et éditer les paramètres de démarrage.

Remarque: vous pouvez démarrer, arrêter et vérifier le statut du logiciel serveur avec l'application d'administration.

Gestionnaire de tâches

Utilisez le gestionnaire de tâches pour voir combien de processus liés au serveur sont en cours d'exécution.

1. Ouvrez le gestionnaire de tâches Windows en appuyant sur Ctrl-Alt-Suppr et en sélectionnant **Gestionnaire de tâches**.
2. Cliquez sur l'onglet **Processus** .
3. Cliquez sur **Nom de l'image** pour trier les processus par ordre alphabétique.
4. Recherchez le nom de fichier du processus serveur (*statisticssrvr.exe*).
5. Recherchez le nom de fichier du processus client (*statisticsproc.exe*). Il existe un processus pour chaque utilisateur final actuellement connecté au logiciel serveur.

Remarque: Vous pouvez surveiller les processus serveur et client à l'aide de l'application d'administration.

Administrateur ODBC

Utilisez ODBC Administrator pour configurer les sources de données système et utilisateur à utiliser avec le logiciel serveur.

La façon dont la source de données ODBC est créée affecte les personnes qui peuvent l'afficher et l'utiliser. Utilisez des DSN *système* lorsque vous souhaitez autoriser un accès général à la source de données. Utilisez les DSN *utilisateur* lorsque vous souhaitez restreindre l'accès aux informations sensibles ou lorsque vous souhaitez personnaliser le DSN pour un utilisateur spécifique.

Pour configurer un DSN système

Les DSN système peuvent être utilisés par toute personne connectée à l'ordinateur sur lequel ils sont définis. Les DSN système sont plus faciles à configurer et à administrer car vous ne le faites qu'une seule fois pour tous les utilisateurs.

Sur l'ordinateur sur lequel vous souhaitez que la source de données réside, connectez-vous en tant qu'administrateur:

1. Dans le menu Démarrer de Windows, sélectionnez :

   Paramètres > **Panneau de configuration**
2. Sélectionnez **Outils d'administration** , puis **Sources de données**.
3. Cliquez sur l'onglet **DSN du système**.
4. Cliquez sur **Ajouter**.
5. Sélectionnez un pilote dans la liste. Si vous configurez une source de données qui utilise la technologie d'accès aux données IBM Corp. , les noms de pilote Connect ODBC sont libellés avec le texte IBM Corp. OEM.
6. Cliquez sur **Terminer**.
7. Entrez les informations appropriées dans la boîte de dialogue **Configuration du pilote** .
8. Cliquez sur **OK**.

Pour configurer un DSN utilisateur

Les noms de fichier utilisateur ne peuvent être utilisés que par le compte de l'utilisateur qui les a créés. Configurez les DSN utilisateur lorsque vous souhaitez restreindre l'accès aux informations sensibles ou lorsque vous souhaitez personnaliser le DSN pour un utilisateur spécifique.

Connectez-vous en tant qu'utilisateur et suivez les étapes pour un DSN système, avec l'exception suivante:

- Cliquez sur l'onglet **Nom de fichier de l'utilisateur** à la place de l'onglet **Nom de fichier du système** .

Annexe D. Tâches du système d'exploitation UNIX

Vous pouvez effectuer la plupart des tâches d'administration avec l'application d'administration ; toutefois, quelques tâches peuvent être nécessaires avec le système d'exploitation UNIX. Utilisez les fonctions de système d'exploitation suivantes pour administrer les logiciels serveur s'exécutant sous UNIX:

- **chmod**. Permet de définir l'accès de l'utilisateur final aux fichiers de données.
- **env.** Utilisé pour vérifier les valeurs des variables d'environnement.
- **des scripts**. Permet de démarrer le logiciel serveur et de configurer son environnement.
- **ps** et **kill**. Permet de vérifier et d'arrêter les processus serveur.
- **odbc.ini**. Utilisé pour configurer les sources de données ODBC .

chmod

Utilisez la commande `chmod` (ou `chown`) pour modifier ou affecter le mode de droits d'accès aux répertoires et aux fichiers de données. Par exemple, pour définir le répertoire */usr/data* en lecture seule pour tout le monde:

1. Connectez-vous en tant que superutilisateur ou en tant que propriétaire du répertoire.
2. A l'invite UNIX, tapez :

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

env

Utilisez la commande `env` pour vérifier les valeurs en cours des variables d'environnement. Par exemple, pour utiliser `env` afin de vérifier les valeurs en cours des variables d'environnement pour le logiciel serveur:

1. Connectez-vous en tant que compte qui a démarré le démon, généralement *root*.
2. A l'invite UNIX, tapez :

   ```
   env
   ```
3. Vérifiez les paramètres de la ou des variables qui vous intéressent.

Scripts

Pour modifier la valeur des variables d'environnement, éditez le script de variable d'environnement appelé par le script qui démarre le logiciel serveur. Pour éditer le script de variable d'environnement:

1. Utilisez un éditeur de texte pour ouvrir le script *statsenv.sh* , qui est inclus dans le sous-répertoire */bin* du répertoire d'installation de IBM SPSS Statistiques Server. Par exemple, ouvrez */usr/local/myserverproduct/bin/statsenv.sh*.
2. Si nécessaire, supprimez la mise en commentaire de la ligne qui définit la variable, puis entrez la nouvelle valeur de la variable.
3. Sauvegardez le fichier.

statsenv.sh est appelé par le script *start_statistics_server* . Les variables d'environnement définies et exportées dans *statsenv.sh* affectent uniquement les processus démarrés avec le script *start_statistics_server* .

ps et kill

Utilisez la commande ps pour obtenir des informations sur les processus serveur en cours d'exécution et pour indiquer leur statut. Par exemple :

1. A l'invite UNIX, tapez :

   ```
   ps -efl.
   ```

2. Recherchez le nom de fichier du processus démon (par exemple, *statisticsd*). Ce processus possède l'**UID** de l'utilisateur qui a démarré le processus du démon du logiciel serveur (généralement *root*).
3. Recherchez le nom de fichier du processus client, *statisticsproc.exe*. Il existe un processus pour chaque utilisateur final actuellement connecté au logiciel serveur. La colonne *UID* affiche l'ID de connexion de l'utilisateur final propriétaire du processus client.

   Utilisez la commande `kill` pour arrêter un processus. Par exemple :
4. Connectez-vous en tant qu'utilisateur ayant démarré le démon.
5. A l'invite UNIX, tapez :

`kill -9 pid`

où *pid* est l'ID du processus.

Le démon du logiciel serveur crée également automatiquement un fichier contenant son ID de processus. Au lieu de rechercher manuellement le PID à l'aide de la commande ps , vous pouvez utiliser ce fichier avec la commande `kill` directement pour arrêter le processus démon directement:

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

Remarque: Si vous souhaitez utiliser l'application d'administration pour surveiller et arrêter des processus, vous devez démarrer le logiciel serveur avec le script de démarrage fourni par IBM Corp.. Pour plus d'informations, voir «Contrôle du démarrage du service», à la page 20.

odbc.ini

Vous devrez peut-être configurer les sources de données ODBC sur l'ordinateur serveur si:

- Vous utilisez IBM Corp. Data Access Pack

et

- Le logiciel serveur doit accéder aux bases de données

Aucun administrateur ODBC n'existe sous UNIX. Pour configurer une source de données ODBC sous UNIX, éditez un fichier texte d'informations système, *odbc.ini*. *Odbc.ini* est installé lorsque vous installez le module d'accès aux données pour UNIX. Les instructions d'installation figurent dans le document *IBM Corp. Data Access Pack Installation Instructions for Unix.pdf* (le document se trouve dans le répertoire */Documentation/<langue>/InstallationDocuments* sur le produit Fichier ISO). Veillez à installer la documentation supplémentaire afin d'avoir accès aux documents répertoriés ci-dessous.

Connect ODBC : Pour plus d'informations sur l'édition de votre fichier *odbc.ini* et la définition de variables d'environnement importantes, voir la section "Configuration des pilotes et des sources de données" dans le chapitre "Installation sous UNIX" du manuel *Connect ODBC Installation Instructions* pour des instructions détaillées.

La documentation du produit DataDirect pour Connect ODBC est incluse par défaut en tant que partie de l'installation de IBM SPSS Data Access Pack. Le programme d'installation crée l'entrée IBM SPSS OEM Connect et ConnectXE pour ODBC ainsi que les entrées de vos autres programmes dans le menu Démarrer. Vous pouvez accéder à la documentation du produit DataDirect à partir de cet élément du menu.

Vous trouverez la documentation du produit DataDirect pour Connect ODBC dans le répertoire où vous avez extrait les fichiers.

Remarque : Vous pouvez également accéder à la documentation depuis la page d'accueil DataDirect à l'adresse http://www.datadirect.com .

Remarques

Le présent document concerne des produits et des services disponibles dans différents pays. Il peut être mis à disposition par IBM dans d'autres langues. Toutefois, il peut être nécessaire de posséder une copie du produit ou de la version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Consultez votre représentant IBM local pour obtenir des informations sur les produits et services actuellement disponibles dans votre région. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout produit, programme ou service fonctionnellement équivalent qui ne porte pas atteinte à un droit de propriété intellectuelle IBM peut être utilisé à la place. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Pour toute demande d'informations relatives au jeu de caractères codé sur deux octets, contactez le service de propriété intellectuelle IBM ou envoyez vos questions par courrier à l'adresse suivante :

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

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et/ou programmes décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation

North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA (IBM Customer Agreement), des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances et les exemples de clients sont fournis à titre d'exemple uniquement. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces programmes exemples sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces programmes exemples n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "EN L'ETAT", sans garantie d'aucune sorte. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corporation dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Index

L

M

N

P

R

S

T

U

V