

*IBM SPSS Statistics Server -Příručka
administrátora*



Poznámka

Před použitím těchto informací a produktu, který podporují, si přečtěte informace v tématu [“Upozornění” na stránce 57](#).

Informace o produktu

Toto vydání se vztahuje k verzi 29, vydání 0, modifikaci 1 produktu Server IBM® SPSS Statistics a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

© Copyright International Business Machines Corporation .

Obsah

Kapitola 1. Přehled.....	1
Produkty a operační systémy.....	1
Architektura.....	1
Softwarové komponenty.....	3
Použití distribuovaného režimu.....	4
Správa softwaru serveru.....	4
Použití tohoto dokumentu.....	5
Kapitola 2. Instalace.....	7
Instalace softwaru serveru.....	7
Instalace aplikace klienta.....	7
Kapitola 3. Přístup k datům.....	9
Pohled na data.....	9
Technologie přístupu k datům.....	9
Připojení ODBC.....	9
Přístup k datům.....	10
Odkazující data.....	10
Řízení přístupu k datům.....	10
Zdroje dat.....	11
Konfigurace prostředí UNIX pro přístup k datům.....	11
Kapitola 4. Konfigurace, monitorování využití a údržba.....	13
Správa účetních řetězců a souborů koncových uživatelů.....	13
Účty.....	13
Přístup k datům.....	13
Soubory.....	13
Profily.....	14
Konfigurace zdrojů dat ODBC.....	14
Zdroje dat ODBC a IBM SPSS Data Access Pack.....	14
Použití třídícího stroje třetích stran.....	14
IBM SPSS Statistics Administrace serveru.....	14
Konfigurace Xtense.....	15
Konfigurace rozhraní příkazového řádku produkčního zařízení k odeslání úloh.....	15
Konfigurace více instancí.....	16
Řízení spouštění služby.....	17
Parametry příkazového řádku spouštěcího skriptu.....	18
Jiná údržba.....	18
Spuštění a zastavení softwaru serveru.....	19
Spuštění služby nebo démona.....	19
Zastavení služby nebo démona.....	19
Konfigurace pro zlepšení výkonu.....	19
Kapitola 5. Podpora koncových uživatelů.....	21
Ověření.....	21
Konfigurace ověření na úrovni operačního systému.....	21
Konfigurace PAM.....	21
Konfigurace interního ověřování.....	22
Konfigurace ověření unix2.....	23
Konfigurace jednotného přihlášení (SSO).....	24

Oprávnění.....	28
Oprávnění na úrovni administrátora.....	29
Autorizace skupiny.....	29
Profily.....	30
Verze klienta a serveru.....	30
Připojení uživatelů přes bránu firewall.....	30
Konfigurace připojení přes bránu firewall.....	30
Připojování uživatelů s PPTP.....	32
Použití SSL k zabezpečení přenosu dat.....	33
Jak SSL funguje.....	33
Povolení zabezpečení SSL pomocí sady GSKit.....	33
Povolení SSL pomocí OpenSSL.....	37
Nastavení národního prostředí.....	40
Připojení k serverovým softwaru.....	41
Přístup k datům a souborům.....	42
Ukládání dat a souborů.....	42
Kapitola 6. Analýza a zlepšení výkonu.....	43
Získávání informací o výkonu.....	43
Zlepšení využití disku.....	44
Zlepšení využití CPU.....	45
Zlepšení využití paměti.....	45
Zlepšení využití sítě.....	45
Použití produktu IBM SPSS Statistics Efficiently.....	45
Dodatek A. Odstraňování problémů.....	47
Serverový software.....	47
Software klienta.....	47
Dodatek B. Dávkové zařízení IBM SPSS Statistics.....	49
Co potřebujete vědět.....	49
Dodatek C. Úlohy operačního systému Windows.....	51
Vlastnosti souboru.....	51
Vlastnosti systému.....	51
Správce uživatelů.....	52
Ovládací panel služeb.....	52
Správce úloh.....	52
Administrátor ODBC.....	52
Chcete-li konfigurovat systémový název DSN.....	53
Chcete-li konfigurovat uživatelské DSN.....	53
Dodatek D. Úlohy operačního systému UNIX.....	55
chmod.....	55
prostředí.....	55
Skripty.....	55
ps a kill.....	55
odbc.ini.....	56
Upozornění.....	57
Ochranné známky.....	58
Rejstřík.....	61

Kapitola 1. Přehled

Technologie serveru IBM SPSS Statistics je **distribuovaná architektura** společně s klíčovými optimalizacemi správy dat podporuje rozšiřitelnou analýzu. Technologie je založena na klientu/serveru. Distribuuje požadavky klientů na operace náročné na prostředky na výkonný serverový software. Když se klient a server vzájemně spolupracují, nazývá se **distribuovaným režimem analýzy**. Distribuovaná analýza umožňuje koncovým uživatelům provádět analýzy, které jejich stolní počítače nemohou podporovat.

Pro maximální flexibilitu mohou být klientské aplikace, které používají serverovou technologii, konfigurovány tak, aby se spouštěly výhradně na stolním počítači koncového uživatele-to se nazývá **lokální režim analýzy**. Koncoví uživatelé mohou snadno přepínat režimy.

Produkty a operační systémy

Serverová technologie podporuje klientskou aplikaci IBM SPSS Statistics a serverový software běží na několika operačních systémech (viz pokyny k instalaci pro specifika). Na svém serveru můžete instalovat více verzí serverového softwaru, na stejném serverovém počítači nebo na různých serverových počítačích.

Architektura

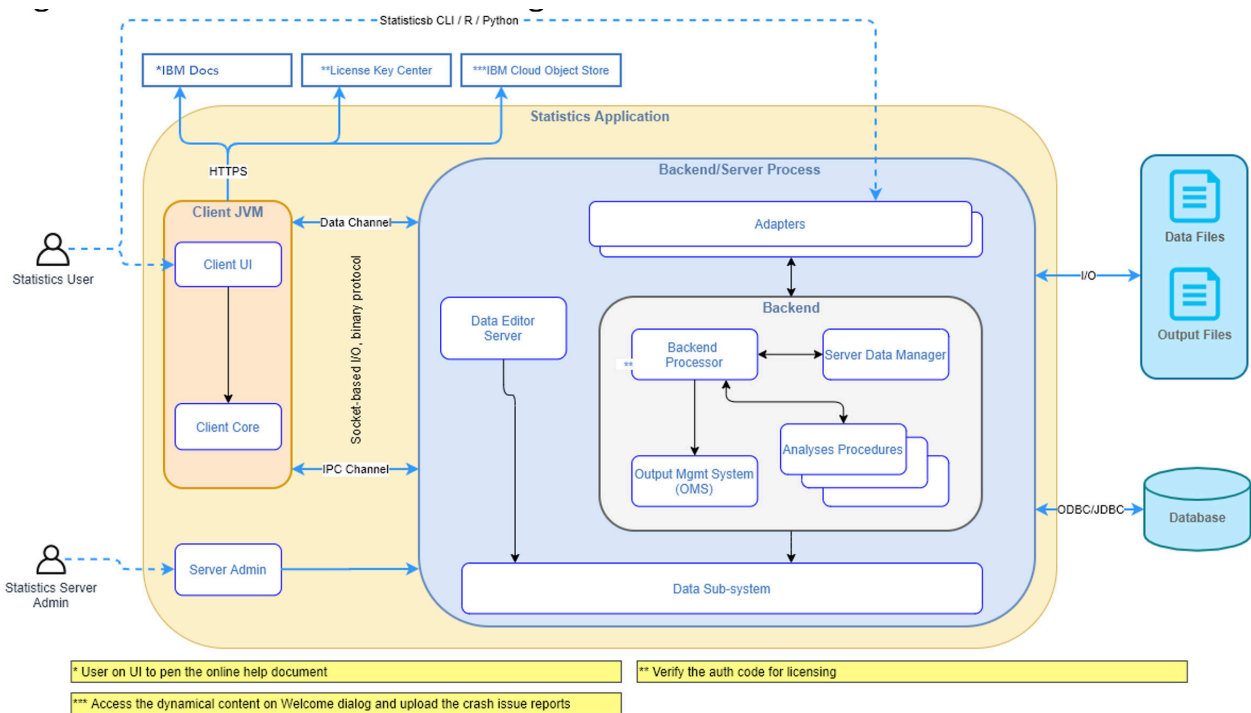
Serverová verze softwaru má dvouvrstvou distribuovanou architekturu. Distribuuje softwarové operace mezi klientem a serverovými počítači. Operace náročné na paměť, jako je například přístup k rozsáhlé databázi nebo analýza velkého datového souboru, jsou prováděny na serverovém počítači bez stahování dat na klientský počítač.

Vrstva klienta

Aplikace **client** . Je nainstalován a běží na stolním počítači koncového uživatele. Klientská aplikace poskytuje grafické uživatelské rozhraní pro přístup k datům a analýzu. Prezентuje výsledky analýz koncového uživatele.

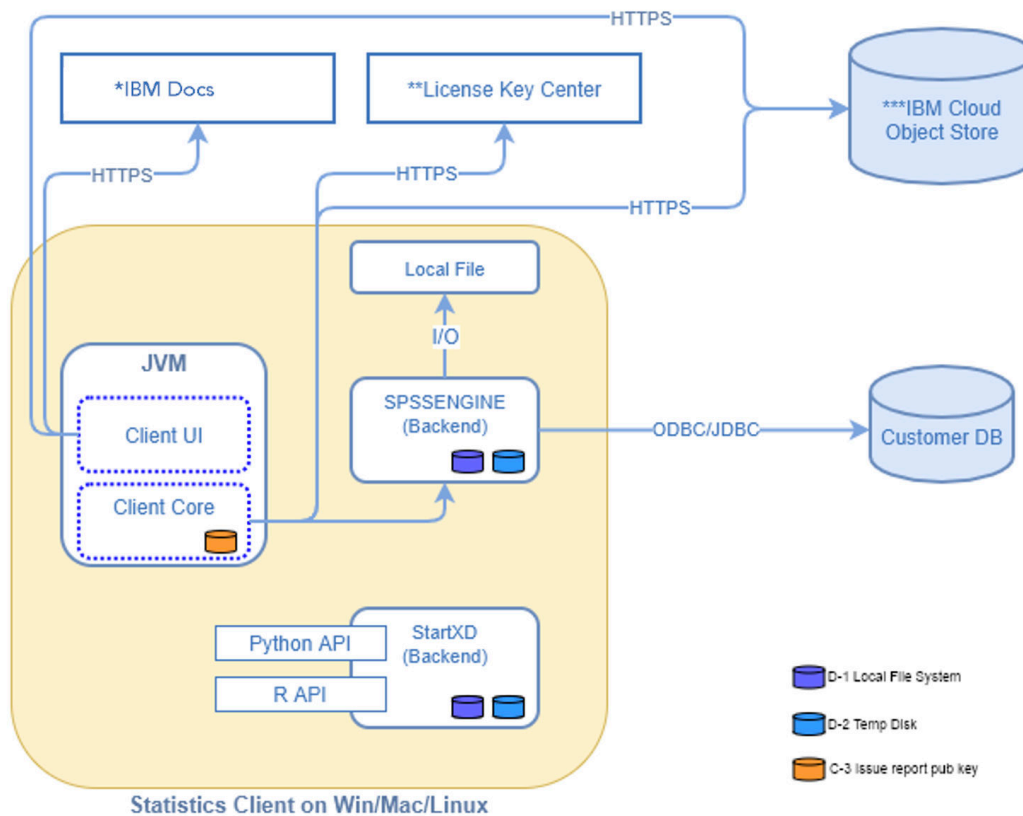
Vrstva serveru

Software **server** . Je instalován a spuštěn na počítači se síťovým serverem. Serverové software poskytuje rámec nezbytný k obsluze více klientů, algoritmů použitých ve statistické analýze a přístupu k datům.



Obrázek 1. Rozdělený režim analýzy

U analýz, které nevyžadují intenzivní přístup k datům nebo numerické zpracování, lze klientský software použít jako standardní samostatnou aplikaci pro stolní počítače. Je-li v režimu lokální analýzy veškerý přístup k datům a statistické zpracování zacházeno na stolním počítači koncového uživatele.



* User on UI to pen the online help document

** Verify the auth code for licensing

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

Obrázek 2. Režim lokální analýzy

Softwarové komponenty

Jak je znázorněno na obrázku "Distribuovaný režim analýzy", komponenty technologie serveru jsou následující. (Viz Obrázek 1 na stránce 2.)

Software klienta. Klientská aplikace je úplná instalace produktu IBM Corp. koncového uživatele (např. IBM SPSS Statistics). Je-li použit pro distribuovanou analýzu, použije se pouze grafické uživatelské rozhraní a možnosti úprav. Když se používá pro lokální analýzu, použijí se také jeho přístup k datům a schopnosti statistického zpracování.

Software serveru. Serverový software je tvořen podkomponentami: framework, který spravuje komunikaci mezi klientem a serverem, klientskými procesy, které spravují požadavky klientů, a moduly, které přistupují k datům a provádějí analýzy.

- **Rámec.** Rámec serverového softwaru je služba (na systému Windows) nebo démon (v systému UNIX). Podporuje veškerou komunikaci mezi klientskou aplikací a moduly. Rámec se neustále spouští na serverovém počítači a čeká na připojení klienta. Když se klient připojí, rámec spustí proces, který obslouží požadavky pro tohoto klienta.
- **Proces klienta.** Klientský proces je pro klienta efektivně relací. Pro každého klienta existuje jeden proces. Proces se spustí, když se klient připojí, a je ukončen, když se klient odpojí. Proces spravuje požadavky klientů na data a analýzy. Načte moduly, které jsou potřebné pro přístup k datům a jejich analýzu. Vynuje moduly, když již nejsou zapotřebí.
- **Moduly.** Modul je spustitelný soubor DLL nebo sdílená knihovna, která přistupuje k datům a spouští analytické procedury. Server analytického serveru má několik modulů. Moduly jsou načítány na vyžádání. Moduly mohou načítat jiné moduly.

Použití distribuovaného režimu

Pokud koncový uživatel spustí produkt v režimu distribuované analýzy, dojde k následujícím krokům:

1. **Spustíte klientskou aplikaci.** Koncový uživatel spustí software klienta na svém stolním počítači. Klientská aplikace představuje kompletní uživatelské rozhraní.
2. **Připojíte se k serveru.** Koncový uživatel se připojuje k softwaru serveru přihlášením z aplikace klienta. Služba nebo démon struktury serveru je vždy spuštěn a čeká na požadavky na připojení. Když je vytvořeno připojení, software serveru spustí proces ke zpracování koncového uživatele.
3. **Přístupová data.** Koncový uživatel přistupuje k datům jako obvykle z aplikace klienta, kromě toho, že jeho pohled na ovladače databáze, datové soubory, adresáře a jednotky představuje počítač vzdáleného serveru, nikoli stolní počítač. Proces serveru načítá příslušné moduly pro přístup k datům a načítá data. Do klientské aplikace se odešle malý segment dat, takže koncový uživatel se může při výběru analýzy odkazovat na tento segment. Většina dat zůstane na serveru. Software serveru můžete také nakonfigurovat tak, aby zabránil odeslání dat do klientské aplikace. Můžete použít aplikaci administrace (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager), a zabránit tak odesílání dat všem klientům. Další informace naleznete v tématu Uživatelé v příručce *Deployment Manager User's Guide* (zahrnuté v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Můžete také konfigurovat přístup pro každého uživatele nebo skupinu. Další informace naleznete v tématu IBM SPSS Statistics Server User Profiles and Groups (Uživatelské profily a skupiny uživatelů IBM SPSS Statistics Server) v příručce *Deployment Manager User's Guide*.
4. **Analyzujete data.** Pomocí uživatelského rozhraní klientské aplikace vybere koncový uživatel data a vyžádá si typ analýzy, kterou chce. Požadavek se odešle na proces serveru, který načte odpovídající balíky analýzy dat a zpracuje analýzu. Všechny úlohy související s daty, jako je čtení dat, transformace dat, výpočet nových proměnných a výpočet statistik, jsou prováděny na serverovém počítači.
5. **Přezkoumejte výsledky.** Serverový software odešle výstup z požadavku klienta zpět do klientské aplikace. Jsou odeslány pouze výsledky, data zůstanou na serveru. Koncový uživatel pak může použít aplikaci klienta k upřesnění a úpravě výsledků.

Správa softwaru serveru

Tato příručka je určena především pro administrátory systému, kteří jsou odpovědní za integraci technologie serveru do síťového prostředí, v němž jsou klientské aplikace spouštěny v režimu distribuované analýzy. Administrativní úlohy zahrnují:

Instalace. Software serveru je navržen tak, aby nepřetržitě běžel a odpovídal na přihlašovací údaje a požadavky od stolních počítačů koncových uživatelů. Vyberte vhodný serverový počítač pro serverový software-takový, který má malý prostor, je nakonfigurován pro přístup koncových uživatelů a je připojen k příslušným stolním počítačům. Čím více paměti a výpočetního výkonu má počítač serveru, tím rychleji se s požadavky klientů zachází. Aplikace klienta musí být nainstalována na stolním počítači koncového uživatele. Instalaci klienta lze provést ze síťového umístění. Produkt [Kapitola 2, "Instalace"](#), na stránce [7](#) poskytuje přehled o tom, jak instalovat software serveru a klientskou aplikaci. Podrobné pokyny k instalaci jsou obsaženy v produktu DVD.

Přístup k datům. Potřebujete-li poskytnout koncovým uživatelům přístup k datům na vzdáleném serveru v době, kdy pracují v distribuovaném režimu, je třeba, aby byl serverový software schopen přistupovat k datům. Produkty IBM Corp. mohou přistupovat k datům z různých typů datových souborů, včetně databází. Pro usnadnění práce se produkty IBM Corp. distribuují s produktem DataDirect Connect ODBC pro přístup k datům z databáze. Produkt [Kapitola 3, "Přístup k datům"](#), na stránce [9](#) zavádí přístup k datům pro produkty IBM Corp. . Další dokumentace je k dispozici na produktu DVD.

Konfigurace a údržba. Protože je software serveru určen pro nepřetržitý provoz, měl by být monitorován v pravidelných intervalech administrátorem systému. Existuje několik voleb konfigurace, které vám poskytují kontrolu nad tím, jak pracuje serverový software. [Kapitola 4, "Konfigurace, monitorování využití a údržba"](#), na stránce [13](#) popisuje konfiguraci a monitorování softwaru serveru.

Podpora koncových uživatelů. Koncoví uživatelé vyžadují informace o názvech serverů, uživatelských účtech a o tom, kde mají být nalezena data. Může být také třeba pomoci jim při řešení problémů. Část

Kapitola 5, “Podpora koncových uživatelů”, na stránce 21 pojednává o druhu podpory, kterou potřebují koncoví uživatelé.

Výkon. Produkt Kapitola 6, “Analýza a zlepšení výkonu”, na stránce 43 poskytuje strategie pro zlepšení výkonu serverového softwaru.

Odstraňování problémů. Produkt “Serverový software” na stránce 47 poskytuje tipy pro odstraňování problémů.

IBM SPSS Statistics Dávkové zařízení (pouze IBM SPSS Statistics Server). Produkt IBM SPSS Statistics Server obsahuje produkt IBM SPSS Statistics Batch Facility, který je určen pro automatizovanou produkci statistických sestav. Pokud provozujete server IBM SPSS Statistics na svém webu, přečtěte si téma Dodatek B, “Dávkové zařízení IBM SPSS Statistics”, na stránce 49, které popisuje nástroj IBM SPSS Statistics Batch Facility a úlohy, které byste měli provést, abyste ji mohli podporovat.

Použití tohoto dokumentu

Tato příručka je primárně určena pro administrátory systému, kteří jsou odpovědní za instalaci a údržbu softwaru serveru v síťovém prostředí, v němž jsou klientské aplikace spouštěny v režimu distribuované analýzy.

Kapitola 2. Instalace

Produkty, které používají serverovou technologii, jsou zabaleny na více médiích-jeden DVD pro serverový software a jeden produkt DVD pro klientskou aplikaci.

Chcete-li implementovat serverovou technologii, postupujte takto:

- Instalujte software serveru na počítač síťového serveru.
- Instalace nebo dohled nad instalací aplikace klienta tak, aby byla přístupná z stolních počítačů koncového uživatele.

Tato kapitola poskytuje přehled instalačního procesu. Podrobné pokyny k instalaci jsou k dispozici na vašem produktu DVD v adresáři */Documentation/ < language>/InstallationDocuments* .

Úplný seznam serverových produktů a jejich přidružených klientských aplikací naleznete v tématu “Produkty a operační systémy” na stránce 1 .

Instalace softwaru serveru

Instalujte software serveru na počítač síťového serveru. Na počítači serveru musí být spuštěna odpovídající verze operačního systému. Je-li to možné, použijte serverový počítač nakonfigurovaný pro rychlé numerické zpracování a přístup k datům, které jsou k dispozici. Další výkon zpracování a paměť zvyšují výkon softwaru serveru. Podrobné požadavky na hardware a software, včetně požadavků na operační systém, se zobrazí v pokynech k instalaci.

Instalace technologie serveru nainstaluje software, který spravuje přístup k datům, a provádí výpočty nezbytné pro statistickou analýzu. Nainstaluje také službu (v systému Windows) nebo démona (v systému UNIX), která naslouchá příchozím požadavkům na přihlášení koncových uživatelů a spouští proces ke zpracování jednotlivých koncových uživatelů.

Chcete-li instalovat serverový software, postupujte podle pokynů v adresáři */Documentation/ < language>/InstallationDocuments* na serveru DVD.

Instalace aplikace klienta

Instalace klientské aplikace nainstaluje software, který zpracovává uživatelské rozhraní, a prezentaci výsledků. Musíte nainstalovat nebo dohlížet na instalaci klientské aplikace na stolním počítači každého koncového uživatele. Na stolním počítači musí být spuštěn systém Windows a musí splňovat minimální požadavky na hardware a operační systém. Podrobné požadavky se zobrazí v pokynech k instalaci, které se nacházejí v adresáři */Documentation/ < language>/InstallationDocuments* na klientovi DVD.

Před čtením jakýchkoliv jiných instalačních dokumentů si přečtěte téma *Getting Started with Installation and Licensing.pdf*.

Kapitola 3. Přístup k datům

Pokud chcete, aby koncoví uživatelé měli přístup k datům na vzdálených serverech, včetně dat z databází, musíte naplánovat, instalovat a konfigurovat přístup k datům. Chcete-li tak učinit, musíte porozumět tomu, jak aplikace rozhodne, kde hledat data. Musíte se také rozhodnout, zda chcete používat technologii přístupu k datům, která nabízí produkt DataDirect Connect ODBC. Také můžete použít zdroje dat OLE DB.

Pohled na data

Než začnete s plánováním přístupu k datům pro koncové uživatele, je důležité porozumět tomu, jak aplikace rozhoduje o tom, jaká data jsou k dispozici koncovému uživateli. Zobrazení dat, která jsou prezentována koncovým uživatelům, závisí na tom, jak tento program běží lokálně nebo v distribuovaném režimu.

Režim lokální analýzy. V režimu lokální analýzy, kdy ke všem datům přístup a zpracování dochází na stolním počítači koncového uživatele, zobrazení datových souborů, zdrojů dat ODBC, adresářů a jednotek, je z pohledu počítače se stolním počítačem-to znamená, že když se koncový uživatel pokusí otevřít datový soubor, vidí datové soubory, adresáře a síťové jednotky na svém stolním počítači.

Distribuovaný režim analýzy. V distribuovaném režimu analýzy, kdy dochází k přístupu a zpracování dat na vzdáleném serveru, zobrazení datových souborů, zdrojů dat ODBC, adresářů a jednotek, je z pohledu serverového počítače-to znamená, že když se koncový uživatel pokusí otevřít datový soubor, vidí datové soubory, adresáře a připojené jednotky na serverovém počítači.

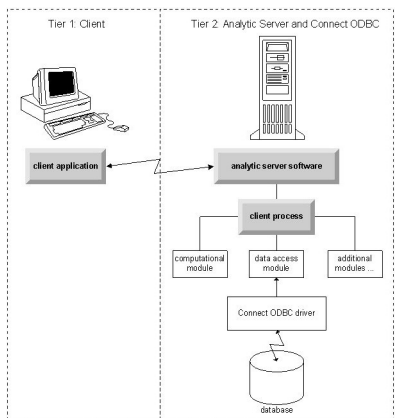
Vaším úkolem je konfigurovat přístup k datům buď v režimu lokální analýzy, nebo v distribuovaném režimu analýzy, jak to vyžaduje koncový uživatel.

Technologie přístupu k datům

Následuje stručný popis připojení ODBC. Další informace o tom, jak technologie pro přístup k datům pracuje s produkty IBM Corp. a pro odkazy na podrobnou dokumentaci pro specifické databáze, viz *Instalační pokyny produktu IBM SPSS Data Access Pack* v adresáři /Documentation/ <language>/ InstallationDocuments na produktu DVD.

Připojení ODBC

Připojení ODBC je komplexní sada individuálních, databázových ovladačů, které používají rozhraní ODBC k poskytování konektivity ke všem důležitým datovým úložištím, z relačních databází po data nestruturovaných souborů.



Obrázek 3. Připojit ODBC v režimu distribuované analýzy

Přístup k datům

Při nastavení přístupu k datům vezměte v úvahu následující skutečnosti:

Technologie přístupu k datům. Rozhodněte se, zda chcete použít některou z technologií přístupu k datům distribuovaných s produktem IBM Corp. . Další informace naleznete v tématu “[Technologie přístupu k datům](#)” na stránce 9 . Podrobnější diskuse o tom, jak vybrat technologii, se objeví v příručce *IBM SPSS Data Access Pack Installation Instructions*(v */Documentation/ < language>/ InstallationDocuments* na produktu DVD).

Režim analýzy. Režim analýzy koncového uživatele určuje, jaká data má k datům on nebo ona. Další informace naleznete v tématu “[Pohled na data](#)” na stránce 9 .

Výkon systému souborů (pouze Windows). Pokud je většina dat v proprietárním formátu od IBM Corp. (například .sav souborů) raději než v databázi, doporučujeme ukládat data na síťový systém Windows NTFS, abyste dosáhli nejlepšího výkonu.

Formát souboru. Software zpracovává otevírání a čtení souborů ve formátu UNIX automaticky-vy a vaši koncoví uživatelé nemusíte provádět žádné akce, aby sdělili softwaru, že soubor je ve formátu UNIX.

Odkazující data

Některý klientský software umožňuje koncovému uživateli ukládat odkazy na data a jiné soubory. Tyto odkazy musí být napsány z pohledu počítače, který bude přistupovat k datům. Je-li například koncový uživatel spuštěn v lokálním režimu analýzy, odkaz na `C:\mydata\mydata.sav` způsobí, že se software pokusí o přístup k souboru na lokální jednotce C na *stolním počítači*. Je-li koncový uživatel spuštěn v režimu distribuované analýzy, stejný odkaz na `C:\mydata\mydata.sav` způsobí, že se software pokusí o přístup k souboru na lokální jednotce C na *serveru*, což může vést k chybě.

Okna. Pokud spravujete systém Windows, můžete se rozhodnout uložit data na stejném počítači jako serverový software. Pokud tak učiníte, doporučujeme, aby uživatelé odkazovali na umístění dat z pohledu na počítač serveru (například `C:\ServerData\mydata.sav`). Výkon je rychlejší, protože síť se nepoužívá k vyhledání souboru. Pokud jsou vaše data na jiném síťovém počítači, doporučujeme, aby vaši uživatelé používali odkazy souboru UNC (například `\\mydataserver\ServerData\mydata\mydata.sav`). Všimněte si, že názvy UNC lze použít pouze v případě, že odkazovaná umístění obsahují název *sdíleného prostředku* v síti. Koncoví uživatelé, kteří často přejdou z distribuované do lokální analýzy, se vyzývají, aby používali odkazy na soubor UNC, protože pracují bez ohledu na režim.

UNIX. Pokud spravujete verzi softwaru serveru UNIX, můžete se rozhodnout umístit soubory na server UNIX. Koncoví uživatelé mohou odkazovat na soubory na serveru UNIX-říkají jim, že mají použít úplnou specifikaci souboru a dopředná lomítka (například `/FILE = '/public/datadatadata.txt'`.) Vyvarovat se použití znaku zpětného lomítka v adresáři UNIX a v názvech souborů použitých serverovým softwarem.

Řízení přístupu k datům

Přístup k datům můžete řídit pomocí operačního systému pro nastavení oprávnění podle ID uživatelů a skupin. Koncový uživatel se připojuje k softwaru serveru přihlášením z aplikace klienta. Serverový software používá operační systém k vynucení oprávnění pro tohoto uživatele.

Poznámka: Další zabezpečení dat může být vynutitelné s vaším databázovým softwarem-výzvu k přístupu k datům softwaru serveru pro ID a hesla, když je databáze vyžaduje.

Okna. Způsob nastavení přístupových oprávnění v systému Windows závisí na tom, kde jsou data uložena.

- Pokud se soubory nacházejí na síťovém počítači jiném než na počítači, na kterém běží serverový software, přiřadte oprávnění ke sdíleným prostředkům.
- Pokud se soubory nacházejí na serverovém počítači a na jednotce NTFS, použijte nastavení zabezpečení. Nemůžete řídit přístup k souboru pro data na počítači serveru na jednotce FAT.

Informace o nastavení sdílení a oprávnění zabezpečení na systému Windows viz “[Vlastnosti souboru](#)” na stránce 51 .

UNIX. Když se koncový uživatel připojí k serverovému softwaru přihlášením z aplikace klienta, serverový software předá ID uživatele a heslo uživatele do operačního systému a spustí proces pro uživatele. Tento spuštěný proces má přístupová práva k souboru na přihlašovací účet koncového uživatele.

Zdroje dat

ODBC

Software serveru IBM SPSS Statistics používá ODBC k přístupu většiny dat, která nejsou ve vlastním formátu, včetně dat uložených v databázích. ODBC vyžaduje zdroj dat ODBC. Zdroj dat ODBC je kombinací následujících možností:

- Popisný název
- Specifický ovladač
- Odkaz na databázi nebo jiný typ datového souboru

Chcete-li získat přístup k většině dat, musíte nakonfigurovat nebo pomoci koncovým uživatelům nakonfigurovat zdroje dat ODBC, které potřebují.

Umístění nakonfigurovaného zdroje dat je kritické. Musí být konfigurován na počítači, který přistupuje k datům a zpracovává data, a nakonfigurujte tak zdroj dat ODBC na *počítači serveru* pro distribuovanou analýzu a na *stolním počítači* pro lokální analýzu. Například porovnejte umístění ovladačů ODBC v obrazcích zobrazených v části [“Připojení ODBC”](#) na stránce 9.

Pokud právě začínáš používat technologii přístupu k datům (zavedenou v produktu [“Technologie přístupu k datům”](#) na stránce 9), je třeba před konfigurací zdroje dat provést některé další úlohy. Další informace naleznete v příručce *IBM SPSS Data Access Pack Installation Instructions* (v příručce /Documentation/ <language>/InstallationDocuments na produktu DVD). Konfigurace zdroje dat je znovu projednána v produktu [Kapitola 4, “Konfigurace, monitorování využití a údržba”](#), na stránce 13 této příručky.

Konfigurace prostředí UNIX pro přístup k datům

Aby mohla technologie pro přístup k datům pracovat na systémech UNIX, musí být nakonfigurovaný spouštěcí skript softwaru serveru.

Otevřít spouštěcí skript

1. Přejděte do podadresáře `/bin` instalačního adresáře softwaru serveru. Na příkazový řádek UNIX například zadejte:

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

kde `/usr/local/serverproduct/bin` je podadresář `/bin` adresáře, ve kterém je nainstalován software serveru.

2. Otevřete soubor `statsenv.sh` pomocí textového editoru.

Určete skript DataDirect

1. Vyhledejte první komentář, který obsahuje text:

```
MERANT_ENVIRONMENT_SCRIPT
```

2. Najděte řádek, který definuje umístění souboru **odbc.sh**.
3. Upravte řádek tak, aby obsahoval správnou cestu k produktu *Connect ODBC instalace klienta*, a odeberte znak komentáře, pokud jej nějaký má. Změňte například:

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

komu:

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

Přidat proměnnou prostředí `odbc.ini`

1. Přidejte následující řádky za výše uvedenými řádky a vytvořte proměnnou prostředí `ODBCINI`, která umožní serveru IBM SPSS Statistics najít soubor `odbc.ini` :

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

kde `ODBCDIR` je nahrazena cestou k instalačnímu adresáři Connect ODBC .

Přidat cesty ke knihovnám databáze

1. Přidejte řádky vhodné pro vaši databázi, obvykle *domovský adresář databáze* a, pokud *nepoužíváte* ovladače protokolu Data Direct Wire Protocol, *cestu ke knihovnám databáze*. Používáte-li například databázi Oracle v systému Linux, přidejte následující řádky:

```
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
```

kde `/bigdisk/oracle/product/8.1.6` je nahrazen cestou do instalačního adresáře Oracle a `LD_LIBRARY_PATH` je proměnná cesty ke knihovně pro váš operační systém.

Všimněte si, že ovladače protokolu Data Direct Wire Protocol nevyžadují instalaci knihoven klienta databáze. Další ovladače Data Direct však tyto knihovny vyžadují.

Uložit spouštěcí skript

1. Uložte soubor `statsenv.sh`.

Upravit `odbc.ini`

1. Upravte soubor `odbc.ini`, konfigurační soubor ODBC , aby bylo možné přistupovat ke zdrojům dat ODBC z produktu IBM SPSS Statistics Server. Viz příloha "The UNIX Environment" v produktu DataDirect's *Odkaz na produkt DataDirect Connect ODBC* (k dispozici, pokud jste nainstalovali další dokumentaci DataDirect při instalaci Connect ODBC) a kapitoly pro specifické ovladače v adresáři `odbchel.pdf` v podadresáři `doc` instalačního adresáře Connect ODBC .

Změna se projeví při příštím spuštění softwaru serveru.

Poznámka: Pokud plánujete použít ODBC s produktem IBM SPSS Statistics Batch Facility, budete muset stejným způsobem upravit spouštěcí skript *Dávková služba IBM SPSS Statistics* .

Kapitola 4. Konfigurace, monitorování využití a údržba

Po instalaci softwaru serveru nakonfigurujte jeho prostředí o:

- Správa účtů a souborů koncových uživatelů
- Konfigurace zdrojů dat ODBC
- Použití administrační aplikace (IBM SPSS Statistics Administration Console) ke konfiguraci a monitorování serverového softwaru
- Řízení spuštění služby

Tyto úlohy jsou popsány v následujících sekcích.

Správa účetních řetězců a souborů koncových uživatelů

Tento oddíl poskytuje přehled o tom, co je třeba udělat pro podporu koncových uživatelů na vašem webu. Další informace naleznete v tématu [Kapitola 5, “Podpora koncových uživatelů”](#), na stránce 21 .

Účty

Koncoví uživatelé potřebují účty, aby se mohli přihlásit k softwaru serveru a přistupovat k datům. Tyto účty musí být ověřeny a musí být schopné číst, zapisovat a/nebo provádět ve specifických složkách na počítači serveru. Další informace o oprávněních k souboru naleznete v tématu [“Oprávnění”](#) na stránce 28. Další informace o ověření naleznete v tématu [“Ověření”](#) na stránce 21.

Oprávnění k databázi jsou vynucována databázovým softwarem. Ke správě těchto účtů použijte běžné nástroje pro administraci databází. Je-li databáze omezena, moduly přístupu k datům softwaru serveru vyzývají uživatele k přihlášení a předání těchto informací zpět do databáze pro ověření před přístupem k datům.

Přístup k datům

Standardně může každý koncový uživatel vidět všechna data při otevření souboru při připojení k serverovému softwaru. Zobrazení všech dat může negativně ovlivnit výkon a zvýšit síťový provoz. Můžete se rozhodnout, že zabráníte tomu, aby klientské počítače koncového uživatele zobrazovaly data změnou globálního nastavení pomocí administrativní aplikace (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager). Další informace naleznete v tématu [Uživatelé](#) v příručce *Deployment Manager User's Guide* (zahrnuté v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Také můžete upravit nastavení uživatelského profilu a skupiny, abyste určili přístup k datům pro jednotlivé uživatele nebo skupiny. Další informace naleznete v tématu [IBM SPSS Statistics Server User Profiles and Groups](#) (Uživatelské profily a skupiny uživatelů IBM SPSS Statistics Server) v příručce *Deployment Manager User's Guide*.

Soubory

Většina souborů, které potřebují koncoví uživatelé uložit, by měla být uložena na stolním počítači; nicméně můžete chtít uživatelům umožnit ukládání datových souborů na síťový počítač. Když se koncový uživatel přihlásí k softwaru analytického serveru poprvé, výchozí adresář pro otevírání a ukládání souborů je instalačním adresářem serverového softwaru. Je zřejmé, že toto není umístění, kde chcete, aby uživatelé zapsali soubory, takže nastavte adresář s oprávněním k zápisu a distribuujte toto umístění koncovým uživatelům. Jakmile budou mít přístup k tomuto umístění z uživatelského rozhraní, aplikace klienta ji uloží a stane se výchozím umístěním pro uložené soubory.

Profily

Serverový software také umožňuje vytvářet profily pro uživatele. Profil může určovat dočasný adresář, nastavení systému UNIX `umask`, prioritu procesu CPU, nastavení přístupu k datům klienta a maximální počet podprocesů pro každého uživatele nebo skupinu uživatelů.

Konfigurace zdrojů dat ODBC

Pokud koncoví uživatelé přistupují k datům z databází, zatímco pracují v distribuovaném režimu analýzy, musíte nakonfigurovat zdroje dat ODBC na počítači, na kterém je nainstalován serverový software.

Zdroje dat ODBC a IBM SPSS Data Access Pack

Používáte-li technologii přístupu k datům produktu IBM Corp., přečtěte si téma [Kapitola 3, “Přístup k datům”](#), na stránce 9 v tomto dokumentu. Přečtěte si příslušné *Pokyny k instalaci* pro přehled konfigurace přístupu k databázi a odkazy na podrobnou dokumentaci o přístupu k datům pro konkrétní databáze (dokument se nachází v adresáři `/Documentation/ < language > /InstallationDocuments` na produktu DVD).

Windows. Konfigurace zdrojů dat ODBC pomocí modulu ODBC Administrator. Další informace naleznete v tématu [“Administrátor ODBC”](#) na stránce 52.

UNIX. Upravte skript spouštěcího prostředí pro serverový software podle popisu v tématu [“Konfigurace prostředí UNIX pro přístup k datům”](#) na stránce 11 a konfigurujte zdroje dat ODBC pomocí souboru `odbc.ini`. Další informace naleznete v tématu [“odbc.ini”](#) na stránce 56.

Použití třídícího stroje třetích stran

Při výchozím nastavení se software serveru pokouší použít externí stroj jiného dodavatele pro řazení. Chcete-li použít správný stroj řazení, proveďte následující kroky:

1. Není-li generátor řazení třetí strany nainstalován na počítači serveru, nainstalujte jej. Produkt IBM Corp. neposkytuje stroje. Jste povinni zakoupit a licencovat stroj od dodavatele třetí strany.
2. Ujistěte se, že knihovna třídícího stroje je v proměnné provedení systému nebo v proměnné cestě ke knihovně. V systému Windows se jedná o proměnnou prostředí `PATH`; v systému UNIX se jedná o `LD_LIBRARY_PATH` nebo `LIBPATH`, v závislosti na dodavateli systému UNIX. Tento krok je nutný k tomu, aby mohl software serveru načíst knihovnu řazení jiného dodavatele.
3. Při použití administrační aplikace (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager) nastavte volbu řazení na příslušný stroj jiného dodavatele. Další informace naleznete v tématu [Uživatelé v příručce *Deployment Manager User's Guide*](#) (zahrnuté v nápovědě k produktu IBM SPSS Collaboration and Deployment Services).

Všechny procedury, které vyžadují řazení (např. SORT), budou následně používat třídící stroj třetí strany. Vydáním příkazu syntaxe `SET SORT=INTERNAL` se vynutí, aby software serveru používal interní algoritmus pro třídění. Koncový uživatel může také explicitně určit řazení jiných dodavatelů zadáním příkazu `SET SORT=EXTERNAL`. To však není nutné, protože řazení třetí strany je výchozí.

Kontrola aktuální volby řazení

Chcete-li zkontrolovat, která volba řazení se používá, můžete zadat příkaz syntaxe `SET MESSAGES ON` a spustit úlohu SORT. Také můžete použít příkaz syntaxe `SHOW SORT`.

IBM SPSS Statistics Administrace serveru

Produkt IBM SPSS Statistics Administration Console poskytuje uživatelské rozhraní pro monitorování a konfiguraci instalací serveru IBM SPSS Statistics Server. Produkt IBM SPSS Statistics Administration Console se instaluje jako součást produktu IBM SPSS Deployment Manager. Úplná dokumentace pro IBM SPSS Statistics Administration Console je zahrnuta v *Sekce Konzoly pro administraci v Uživatelská*

Konfigurace Xtense

Administrátor serveru IBM SPSS Statistics musí provést kroky k dispozici pro spuštění procedur Xtension (krr, lenr, lrr a lrr) pro spuštění v serveru **statsb** a SPSS Statistics Server. Mezi procedury Xtense patří:

- Regrese jádra jádra (KRR)
- Lineární regrese na elastické elastické regrese (LENR)
- Lineární laso Regrese (LLR)
- Regrese lineárního hřebenu (LRR)

Instalace prostředí Xtensions na serveru SPSS Statistics

1. Na straně klienta IBM SPSS Statistics nainstalujte prostředí Xtensions (v lokálním režimu) z produktu Extension Hub.
2. Ujistěte se, že je knihovna **sklearn** nainstalována na serveru IBM SPSS Statistics .

SYSTEM UNIX®

Spusťte následující příkaz jako uživatel, který nainstaloval server SPSS Statistics .

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

Poznámka: Položka **statisticspython3** se nachází v adresáři bin instalace serveru SPSS Statistics .

Windows®

Spusťte následující příkaz.

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

Poznámka: Soubor **statisticspython3.bat** je umístěn v instalačním adresáři serveru SPSS Statistics .

3. Zkopírujte adresář `xtensions` a jeho obsah z klienta SPSS Statistics (`%APPDATA%\IBM\SPSS Statistics\one\xtensions\` na systému Windows, `$HOME/Library/Application Support/IBM/SPSS Statistics/one/xtensions` na systému macOS) do instalačního adresáře serveru SPSS Statistics .

Server SPSS Statistics je nyní připraven ke spuštění procedur Xtension, které jsou instalovány v adresáři `xtensions` .

Konfigurace rozhraní příkazového řádku produkčního zařízení k odeslání úloh

Počínaje produktem IBM SPSS Statistics verze 26 můžete k odeslání úloh na server SPSS Statistics použít rozhraní příkazového řádku produktu Production Facility. Když se rozhraní příkazového řádku Production Facility používá ve spojení s Plánovačem úloh Microsoft Windows Task Scheduler/MacOS Automator pro plánování úloh, můžete efektivně nahradit IBM SPSS Collaboration and Deployment Services pro zpracování úloh SPSS Statistics .

Příkaz SPSS Statistics **INSERT HIDDEN** může provádět úlohy, které generují výstup. Je-li příkaz použit, uživatelé nemohou přistupovat ke zdrojové syntaxi SPSS Statistics nebo je prohlížet.

Poznámka: Příkaz **INSERT HIDDEN** vyžaduje server SPSS Statistics . Příkaz nebude pracovat na samostatném klientském počítači SPSS Statistics .

Funkce INSERT HIDDEN

Administrátoři mohou povolit funkci **INSERT HIDDEN** pomocí administrativní konzoly serveru SPSS Statistics nebo úpravou souboru <install_path>/config/statisticsd.conf (**INSERT HIDDEN = Enabled**). Pole **INSERT HIDDEN Feature** je umístěno na kartě Konfigurace serveru SPSS Statistics Administrace serveru SPSS Statistics (pod sekci **Uživatelé**).

1. Vyberte **Povoleno** jako hodnotu **VLOŽIT funkci HIDDEN**. Všimněte si, že na kartě Konfigurace serveru SPSS Statistics se objeví hvězdička (*).
2. Uložte změnu. Buď klepněte na ikonu **Uložit** na panelu nástrojů, Control.-S, nebo vyberte **Soubor > Uložit**.
3. Restartujte server SPSS Statistics.
4. Jakmile se server restartuje na serverech Windows, zobrazí se dialogové okno s výzvou administrátora, aby zadal heslo **INSERT HIDDEN Feature**. Na serverech se systémem Linux musí administrátor ručně spustit server SPSS Statistics. Když se server restartuje, vyzve administrátora k zadání hesla.

Heslo je uloženo v systémovém registru (podobné jako heslo SSL) a všechny skryté soubory syntaxe jsou šifrovány stejným heslem.

Volitelně může administrátor odepřít uživateli přístup k souborům **INSERT HIDDEN** prostřednictvím řízení přístupu k systému souborů.

Proces démona serveru SPSS Statistics vyžaduje přístup pro čtení k souborům **INSERT HIDDEN**. Příkaz OMS lze použít k zalamování syntaxe, aby se zajistilo, že výstup nebude odeslán do Prohlížeče výstupu.

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

Syntaxe **INSERT HIDDEN** je podobná syntaxi **INSERT FILE**. Příklad:

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

Autor souboru **INSERT HIDDEN** poskytuje skryté cesty k souborům pro uživatele klienta produktu SPSS Statistics. Během běhu provádí uživatelé klienta syntaxi **INSERT HIDDEN SOURCE= "<file_path>"**.

Podrobnější informace naleznete v příručce *IBM SPSS Statistics Command Syntax Guide*.

Proces klienta na serveru SPSS Statistics odesílá cestu **SOURCE** k procesu démona serveru. Proces démona dešifruje soubor a vrátí jej do procesu klienta k provedení.

Proces klienta zakazuje protokoly a žurnály, provádí dešifrovaný soubor a poté znovu povolí protokoly a žurnály. Výsledkem je, že Prohlížeč výstupu produktu SPSS Statistics neobsahuje žádné zdrojové protokolování syntaxe (obsahuje výstup). Žurnál také neobsahuje žádnou zdrojovou syntaxi.

Konfigurace více instancí

Můžete vytvořit více instancí serverového softwaru, každý se svým vlastním číslem portu. To se často používá ve spojení s autorizací skupiny pro přiřazení skupiny uživatelů k určité instanci. Nicméně více instancí může být používáno nezávisle na autorizaci skupiny. Další informace o autorizaci skupiny viz [“Autorizace skupiny”](#) na stránce 29.

Vytvoření nové instance

Chcete-li vytvořit instanci skupiny softwaru serveru, musíte spustit skript.

V systému Windows spusťte následující skript z instalačního adresáře serveru.

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

V systémech UNIX a Linux spusťte následující skript z podadresáře bin instalačního adresáře.

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

< group_name> je jedinečný název instance a < číslo_portu> je dostupné číslo portu, které bude instance používat.

Po spuštění skriptu bude existovat konfigurační složka, která je specifická pro danou instanci. Podívejte se na `config_<groupname>` v pořadí instalace serveru. Složka obsahuje několik konfiguračních souborů, jako např. `statisticsd.conf` a `UserSettings.xml`. Pokud chcete aktualizovat konfiguraci určité instance, ujistěte se, že jste aktualizovali konfigurační soubor ve správném umístění.

Spouštění instance serveru

V systému Windows je instance samostatnou službou s názvem *IBM SPSS Statistics NN.m*, kde *NN* je číslo hlavní verze a *m* je číslo vedlejší verze. Tuto službu můžete spustit a zastavit jako jakékoli jiné služby systému Windows.

V systému Linux a UNIX je třeba při spuštění spouštěcího skriptu uvést název skupiny:

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

kde < group_name> je název skupiny instancí.

Odstranění instance serveru

1. Na systému Windows odeberte položku služby:
 - a. Otevřete příkazový řádek jako administrátor.
 - b. Spusťte následující příkaz:

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

kde *NN* je číslo hlavní verze, *m* je vedlejší číslo verze a < group_name> je skupina instancí.

2. Odstraňte podadresář `config_<groupname>` v instalačním adresáři serveru.

Řízení spouštění služby

Serverová verze softwaru má komponentu struktury, která zpracovává veškerou komunikaci mezi klientskou aplikací a moduly. V systému Windows je komponenta rámce službou. V systému UNIX je komponenta rámce aplikací, která se obvykle spouští jako démon.

Windows

Standardně je služba konfigurována pro automatické spuštění, což znamená, že se restartuje automaticky po restartu počítače. Když je tento způsob spuštěn, služba běží bez obsluhy a počítač serveru může být odhlášen, aniž by to mělo vliv na službu. Ke změně parametrů spuštění služby můžete použít Ovládací panel služeb systému Windows. Další informace naleznete v tématu [“Ovládací panel služeb”](#) na stránce 52 . Pokud provozujete více instancí, bude panel služeb obsahovat položku pro každou instanci serveru.

Poznámka: Pokud počítač serveru nepodporuje adresu IP lokálního hostitele (127.0.0.1::: 1), musíte vytvořit systémovou proměnnou prostředí s názvem `STATS_LH_OVERRIDE` a nastavit její hodnotu na `YES` před spuštěním serveru. Informace o spuštění a zastavení serveru viz [“Spuštění a zastavení softwaru serveru”](#) na stránce 19.

UNIX

Spouštěcí skript, `start_statistics_server`, je obsažen v podadresáři `/bin` instalačního adresáře. Skript zavolá skript `statsenv.sh`, který nakonfiguruje prostředí pro software serveru, a pak spustí aplikaci. Musíte spustit serverový software s tímto skriptem. Spouštěcí skript musí být spuštěn z podadresáře `/bin`. Chcete-li ji provést, musíte být přihlášení jako uživatel **root**, používáte-li výchozí ověření systému Unix nebo modul PAM (Pluggable Authentication Module). Jinak musíte být přihlášení jako uživatel, který vlastní serverovou softwarovou démona. Další informace o ověření naleznete v tématu [“Ověření”](#) na stránce 21. Příkaz:

```
./start_statistics_server -d
```

spustí serverový software jako proces démona, což je doporučený způsob, jak spustit serverový software.

Pokud provozujete více instancí serverového softwaru, tento příkaz spustí výchozí instanci. Chcete-li spustit jinou instanci, uveďte skupinu instancí s přepínačem `-g`:

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

kde `< groupname>` je název skupiny instancí.

Poznámka: Pokud počítač serveru nepodporuje adresu IP lokálního hostitele (127.0.0.1/: 1), musíte před spuštěním serveru nastavit proměnnou prostředí `STATS_LH_OVERRIDE` na `YES`. `STATS_LH_OVERRIDE` je nastaven z `statsenv.sh`, který je obsažen v podadresáři `/bin` instalačního adresáře. Informace o spuštění a zastavení serveru viz [“Spuštění a zastavení softwaru serveru”](#) na stránce 19.

Parametry příkazového řádku spouštěcího skriptu

Skript `start_statistics_server` přijímá následující parametry příkazového řádku (v libovolném pořadí):

- **Démon.** Spustíte serverový software jako proces démona pomocí volitelného zadání `-d`. Vynecháte-li `-d`, server se spustí jako proces na popředí. Chcete-li například spustit serverový software jako démon, použijte příkaz:

```
./start_statistics_server -d
```

- **Skupina.** Pokud provozujete více instancí serverového softwaru, uveďte skupinu, která je přidružená k instanci:

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

kde:

`< groupname>` je příslušný název skupiny.

- **Port.** Číslo portu lze volitelně zadat na příkazovém řádku spouštěcího skriptu. Chcete-li například zadat číslo portu, použijte příkaz:

```
start_statistics_server -p nnnn
```

kde:

`nnnn` je požadované číslo portu.

Zadejte číslo portu pouze v případě, že potřebujete vyřešit konflikt čísel portů. Předvolba bude fungovat, pokud jiná aplikace na počítači nepoužívá stejné číslo. Toto nastavení příkazového řádku přepíše hodnotu nastavenou v aplikaci administrace.

Jiná údržba

Odeberte nepotřebné soubory. Pravidelně kontrolujte umístění dočasných souborů a umístění souboru protokolu kvůli nepotřebným souborům a odeberte je. Lokality jsou definovány v aplikaci administrace.

Zkontrolujte spuštěné procesy. Pokud pravidelně nerestartujete počítač serveru, pravidelně kontrolujte procesy spuštěné na počítači a ukončete všechny procesy, které se nepoužívají. Názvy procesů jsou uvedeny v části [“Spuštění a zastavení softwaru serveru”](#) na stránce 19 .

Spuštění a zastavení softwaru serveru

Administrativní aplikace restartuje software serveru, aby mohly být potvrzeny změny konfigurace; v některých případech však může být nutné spustit nebo zastavit serverový software z operačního systému. Postupujte podle níže uvedených kroků pro váš operační systém a použijte název procesu vašeho serverového produktu. V systému Windows je výchozí název služby *IBM SPSS Statistics NN.m*, kde *NN* je číslo hlavní verze a *m* je číslo vedlejší verze. Pokud spouštíte více instancí, název služby je *IBM SPSS Statistics NN.m <groupname>*, kde *NN* je číslo hlavní verze, *m* je vedlejší číslo verze a *<groupname>* je skupina instancí. V systémech UNIX a Linux je název démona *statisticsd*.

Poznámka k plánování: Zastavení služby nebo démona odpojí koncové uživatele a ukončí své procesy, takže se pokuste naplánovat úlohy konfigurace a údržby po dobu, kdy očekáváte přístup k systému (například brzy ráno nebo pozdě večer) jen málo uživatelů).

Spuštění služby nebo démona

Windows. Pro spuštění služby použijte Ovládací panel služeb Windows. Další informace naleznete v tématu [“Ovládací panel služeb”](#) na stránce 52 .

UNIX. Spusťte server se spouštěcím skriptem, *start_statistics_server*, který je zahrnut v podadresáři */bin* instalačního adresáře. Spouštěcí skript musí být spuštěn z podadresáře */bin* . Chcete-li ji provést, musíte být přihlášení jako uživatel **root** , používáte-li výchozí ověření systému Unix nebo modul PAM (Pluggable Authentication Module). Jinak musíte být přihlášení jako uživatel, který vlastní serverovou softwarovou démona. Další informace o ověření naleznete v tématu [“Ověření”](#) na stránce 21.

Zastavení služby nebo démona

Windows. K zastavení služby použijte Ovládací panel služeb Windows. Další informace naleznete v tématu [“Ovládací panel služeb”](#) na stránce 52 .

UNIX. Ukončete proces serveru. (Příklad viz [“ps a kill”](#) na stránce 55 .) Démon automaticky vytvoří soubor (*statisticsd.pid*), který obsahuje ID procesu pro démona. Tento soubor můžete použít ve spojení s příkazem `kill` tak, že spustíte následující příkaz z podadresáře `config` instalačního adresáře nebo `config_<group_name>` pro další instanci softwaru serveru:

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

Nezávislá platforma. Použijte administrační aplikaci (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager). Další informace naleznete v tématu Řízení serveru IBM SPSS Statistics Server v příručce *Deployment Manager User's Guide* (je obsažena v nápovědě k produktu IBM SPSS Collaboration and Deployment Services).

Konfigurace pro zlepšení výkonu

Informace o úpravách konfigurace softwaru serveru za účelem zvýšení výkonu naleznete v tématu [Kapitola 6, “Analýza a zlepšení výkonu”](#), na stránce 43 .

Kapitola 5. Podpora koncových uživatelů

Podpora koncových uživatelů znamená zajistit, aby měli informace, které potřebují ke spuštění svého produktu IBM Corp. v režimu distribuované analýzy. Chcete-li použít software serveru, koncoví uživatelé musí vědět:

- Jak se připojit k softwaru serveru.
- Jak přistupovat k datům a souborům.
- Kam uložit data a soubory.

Ověření

Pro ověření uživatelů máte několik možností. Některé volby vyžadují, aby byl server spuštěn s oprávněními uživatele root.

Metoda	Dostupnost OS	Server musí být spuštěn jako systém/kořen?
Standardní ověření na úrovni operačního systému (účet Windows nebo UNIX)	<ul style="list-style-type: none">• Windows• UNIX	Ano
Modul PAM (Pluggable Authentication Module)	<ul style="list-style-type: none">• UNIX	Ano
Interní ověření	<ul style="list-style-type: none">• Windows• UNIX	NO
unix2	<ul style="list-style-type: none">• UNIX	NO
jednotné přihlášení	<ul style="list-style-type: none">• Windows• UNIX	NO

Konfigurace ověření na úrovni operačního systému

Ověření na úrovni operačního systému je výchozí metoda ověření. Použijte běžné nástroje pro administraci systému k vytvoření a správě standardních účtů koncových uživatelů na úrovni operačního systému (viz "Správce uživatelů" na stránce 52, kde získáte informace o tom, jak přistupovat k programu Windows User Manager).

Pokud zkusíte jinou metodu ověření a chcete se vrátit k ověření na úrovni operačního systému, je třeba aktualizovat prvek *userauth* v souboru *statisticsd.conf* a změnit parametr *value* na *unix* nebo *win32*.

Konfigurace PAM

Software serveru v systému UNIX může pro ověření uživatelů použít modul PAM (Pluggable Authentication Module). Nejprve musíte nakonfigurovat serverový software, aby používal modul PAM. Poté nakonfigurujte modul PAM podle pokynů, které jsou specifické pro vašeho dodavatele systému UNIX. Následují kroky v systému Linux. Ty se mohou lišit v závislosti na verzi a dodavateli.

Poznámka: Je-li serverový software spuštěný, musíte jej restartovat po dokončení všech kroků.

Konfigurace softwaru serveru pro použití modulu PAM

1. Přihlaste se k počítači se systémem UNIX jako *root*.
2. V podadresáři *config* instalačního adresáře softwaru serveru otevřete konfigurační soubor (např. *statisticsd.conf*) v textovém editoru.
3. Vyhledejte prvek *userauth* a změňte parametr *value* z *unix* na *pam*.
4. Uložte soubor.

Konfigurace modulu PAM v systému Linux

1. Přejděte do konfiguračního adresáře PAM (např. */etc/pam.d*).
2. Použijte textový editor k vytvoření souboru s názvem *statisticsd*.
3. Přidejte informace o konfiguraci PAM, které chcete použít. Příklad:

```
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
```

Poznámka: Tyto řádky se mohou lišit v závislosti na konkrétní konfiguraci. Další informace naleznete v dokumentaci k operačnímu systému Linux .

4. Uložte soubor.

Konfigurace interního ověřování

Interní ověření umožňuje, aby software serveru byl spuštěn bez oprávnění uživatele *root*. Omezuje však připojení klienta ke stejnému disku-přístup. Každý uživatel, který se připojuje k softwaru serveru, má stejnou úroveň zabezpečení přístupu k disku. Proto může jeden uživatel odstranit soubor jiného uživatele. Je-li to problém, doporučuje se místo toho použít metodu ověření *unix2* . Tato metoda neomezuje připojení klienta, protože používá soubor *passwd* systému UNIX pro ověření. Další informace naleznete v tématu “Konfigurace ověření *unix2*” na stránce 23 .



Upozornění: Při spuštění démona/služby jako *root*/SYSTEM nepoužívejte interní ověření. Tato akce je stejná jako volba *root*/SYSTEM access to your server to any user that connects.

Konfigurace interního ověřování v systému UNIX

1. Vytvořte skupinu pro uživatele, kteří se připojí k softwaru serveru. Doporučujeme pojmenování této skupiny **statistiky**.
2. Člen této skupiny musí instalovat serverový software. Tento uživatel bude vlastníkem démona serverového softwaru.
3. Jiný člen této skupiny (liší se od vlastníka démona a obvykle uživatel, který spravuje uživatele softwaru serveru), vytvoří soubor *statisticksusers* v adresáři *config* v instalačním adresáři softwaru serveru. Tento soubor by měl mít přístup pro čtení a zápis pro uživatele, který jej vytvořil. Měl by mít přístup pro čtení pro skupinu uživatelů. Žádní jiní uživatelé by k ní neměli mít přístup. Pokud tento soubor nevytvoříte ručně, je automaticky vytvořen při prvním spuštění nástroje příkazového řádku *statisticsuser* (viz další krok). Nástroj příkazového řádku nastavuje příslušná oprávnění.
4. V adresáři *config* použijte nástroj příkazového řádku *statisticsuser* k přidání uživatelů. Jako uživatel, který vytvořil soubor *statistickyusers* , zadejte příkaz *statisticsuser <username>* a vytvořte běžného uživatele (např. *statisticsuser jdoe*). Pomocí volby *-a* vytvořte uživatele s oprávněním administrátora (např. *statisticsuser -a jdoe*). Nástroj příkazového řádku *statisticsuser* vás vyzve k zadání hesla. Koncový uživatel zadá jméno uživatele a heslo pro připojení k serverovému softwaru. Ujistěte se, že jste řádně distribuovali jméno uživatele a hesla. Chcete-li odstranit uživatele, použijte volbu *-d* (např. *statisticsuser -d jdoe*).
5. Přihlaste se jako vlastník démona serverového softwaru, otevřete konfigurační soubor (např. *statisticsd.conf*) v textovém editoru.

6. Najděte prvek *userauth* a změňte parametr *value* z *unix* na *internal*.
7. Přihlaste se jako vlastník démona serverového softwaru, spusťte server.

Konfigurace vnitřního ověření v systému Windows

1. Upravte položku IBM SPSS Statistics Server tak, aby se spouštěla jako specifický uživatel:
 - a. Otevřete panel služeb systému Windows a poklepejte na položku *IBM SPSS Statistics NN.m*, kde *NN* je číslo hlavní verze a *m* je číslo vedlejší verze.
 - b. Klepněte na kartu **Přihlášení**.
 - c. Pod položkou **Přihlásit se jako** vyberte volbu **Tento účet**.
 - d. Zadejte doména\jméno uživatele a heslo uživatele, který bude vlastnit serverový proces. Tento uživatel bude potřebovat oprávnění *Logon as a service*.
2. Stejný uživatel musí vytvořit soubor *statisticsusers* v adresáři *config* v instalačním adresáři softwaru serveru. Tento soubor by měl mít přístup pro čtení a zápis pro uživatele, který jej vytvořil. Žádní jiní uživatelé by neměli mít přístup pro zápis. Pokud tento soubor nevytvoříte ručně, je automaticky vytvořen při prvním spuštění nástroje příkazového řádku *statisticsuser* (viz další krok).
3. V adresáři *config* použijte nástroj příkazového řádku *statisticsuser* k přidání uživatelů. Jako uživatel, který vytvořil soubor *statisticsusers*, zadejte *statisticsuser <username>* pro vytvoření běžného uživatele (např. *statisticsuser jdoe*). Použijte volbu *-a* k vytvoření uživatele s oprávněním administrátora (např. *statisticsuser -a jdoe*). Nástroj příkazového řádku *statisticsuser* vás vyzve k zadání hesla. Koncový uživatel zadá jméno uživatele a heslo pro připojení k serverovému softwaru. Ujistěte se, že jste řádně distribuovali jméno uživatele a hesla. Chcete-li odstranit uživatele, použijte volbu *-d* (např. *statisticsuser -d jdoe*).
4. Přihlaste se jako vlastník démona serverového softwaru, otevřete konfigurační soubor (např. *statisticsd.conf*) v textovém editoru.
5. Najděte prvek *userauth* a změňte parametr *value* z *win32* na *internal*.
6. Přejděte na panel Služby systému Windows a spusťte službu.

Konfigurace ověření unix2

Ověřování *unix2* umožňuje softwaru serveru běžet bez oprávnění uživatele *root* a ověřuje se vůči souboru *passwd* systému UNIX se standardními uživatelskými účty. Spustitelný soubor (*suauth*) nainstalovaný se softwarem serveru provádí ověření. Má-li pracovat správně, musíte nastavit nezbytná oprávnění.

Chcete-li nakonfigurovat ověření *unix2*, proveďte následující kroky:

1. Pomocí nastavení *setuid* a *setgid* nebo řízení přístupu založeného na rolích (RBAC) změňte oprávnění spustitelného souboru *suauth* tak, aby uživatel, který bude spouštět serverový démon, měl potřebná oprávnění uživatele *root*. Tento uživatel musí být schopen ověřit uživatele proti souboru *passwd* a změnit ID uživatele a ID skupiny procesu vytvořeného serveru pro každého koncového uživatele. Následují podrobnosti o nastavení oprávnění. Všimněte si, že použijete *buď* *setuid/setgid* *nebo* RBAC. Nepoužívejte obě metody.
2. Otevřete konfigurační soubor (např. *statisticsd.conf*) v textovém editoru.
3. Najděte prvek *userauth* a změňte parametr *value* z *unix* na *unix2*.
4. Přihlaste se jako vlastník démona serverového softwaru, spusťte server.

Nastavení oprávnění s nastavením *setuid* a *setgid*

1. Vytvořte skupinu pro uživatele, který bude spouštět serverový software. Doporučujeme pojmenování této skupiny **statistiky**. Také doporučujeme omezit členství ve skupině pouze na uživatele, který bude spouštět serverový softwarový démon.
2. Člen této skupiny musí instalovat serverový software. Tento uživatel bude vlastníkem démona serverového softwaru.

3. Spusťte relaci terminálu jako *root*.
4. Přejděte do adresáře *bin* v instalačním adresáři softwaru serveru.
5. Změňte vlastníka souboru *suauth* na hodnotu *root*.

```
chown root suauth
```

6. Přidejte hodnoty *setuid* a *setgid* bitů na *suauth*. Tyto bity umožňují uživateli ve skupině instalačního programu provést soubor a běžet dočasně jako *root*. Oprávnění uživatele *root* jsou vyžadována z důvodů uvedených výše v tomto tématu.

```
chmod 6550 suauth
```

7. Ukončete činnost jako *root* a přihlaste se jako vlastník serverového softwaru.

Nastavení oprávnění pro řízení přístupu dle rolí

Měli byste být také schopni používat řízení přístupu dle rolí (RBAC) k nastavení nezbytných oprávnění. Informace naleznete v dokumentaci k RBACu. Budete muset provést následující:

1. Vytvořte autorizaci pro spustitelný soubor *suauth*.
2. Vytvořte roli pro tuto autorizaci.
3. Přiřaďte roli démona serverového softwaru k roli.
4. Konfigurujte autorizace tak, aby povolovala následující oprávnění:
 - Přečtěte si soubor *passwd*.
 - Změňte ID uživatele.
 - Změňte ID skupiny.

Konfigurace jednotného přihlášení (SSO)

Můžete použít jednotné přihlášení pro připojení k serveru, který je spuštěn na jakékoli podporované platformě. Nejprve je třeba konfigurovat server IBM SPSS Statistics, klienta IBM SPSS Statistics a počítače IBM SPSS Collaboration and Deployment Services. Interní ověření umožňuje, aby software serveru byl spuštěn bez oprávnění uživatele *root*.

Používáte-li jednotné přihlášení pro připojení k produktu Server IBM SPSS Statistics i k produktu IBM SPSS Collaboration and Deployment Services, musíte se před připojením k produktu Server IBM SPSS Statistics připojit k produktu IBM SPSS Collaboration and Deployment Services.

Chcete-li spolupracovat s nejmodernějšími, zabezpečenými instalacemi Active Directory, musíte instalovat šifrovací balík vysoké odolnosti pro Java, protože požadované šifrovací algoritmy nejsou ve výchozím nastavení podporovány. Je třeba instalovat balík pro klienta i server. Když selže připojení k serveru, protože připojení k serveru není nainstalováno, zobrazí se v klientu chybová zpráva, jako například `Illegal key size`. Viz [“Instalace neomezené síly šifrování”](#) na stránce 37.

Poznámka: Před konfigurací serveru SPSS Statistics, klienta SPSS Statistics a počítače IBM SPSS Collaboration and Deployment Services pro jednotné přihlášení se musíte ujistit, že počítače mají přístup k serveru řadiče domény.

Informace o konfiguraci produktu IBM SPSS Collaboration and Deployment Services pro jednotné přihlášení naleznete v tématu [Přehled služeb jednotného přihlášení produktu IBM SPSS Collaboration and Deployment Services](#).

Konfigurace serveru pro jednotné přihlášení

Konfigurace serveru v systému Windows

1. Ujistěte se, že počítač serveru Windows je členem domény Active Directory (AD).
2. V umístění instalace produktu Server IBM SPSS Statistics vyhledejte složku s názvem `config`.

3. Ve složce config vytvořte podsložku s názvem sso.
4. Ve složce sso vytvořte soubor krb5.conf. Pokyny pro vytvoření souboru krb5.conf lze najít na adrese http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html. Níže je uveden příklad souboru 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
```

Konfigurace serveru v systému UNIX

Chcete-li konfigurovat jednotné přihlášení pro serverové počítače se systémem UNIX, můžete přidat počítač UNIX do domény Windows AD a pak postupovat podle pokynů pro konfiguraci jednotného přihlášení (SSO) na systému Windows. Alternativně můžete provést následující kroky:

1. Vytvořte uživatelský účet domény pro počítač UNIX.
2. Změňte název hostitele. Používáte-li systém RedHat Linux, otevřete soubor /etc/sysconfig/network a upravte HOSTNAME na formulář <name>.<realm>. To umožňuje službě AD najít pověření serveru.
3. Chcete-li povolit, aby server DNS našel počítač UNIX, proveďte jeden z následujících kroků:
 - Otevřete soubor %windows%/system32/drivers/etc/hosts a přidejte adresu IP/host mapování, například:

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

Nebo

- Přidejte novou položku zóny zpětného vyhledání. Tím se přidá IP/mapování hostitele na server DNS.

Pokud položka DNS pro počítač UNIX není správná, můžete ručně přidat položku zpětného vyhledávání na server DNS.

Konfigurace klienta pro jednotné přihlášení

Kroky jsou společné pro všechny klienty kromě kroků, které jsou výslovně uvedeny pro systém Windows.

1. Ujistěte se, že lokální počítač se systémem Windows, který provozuje produkt IBM SPSS Statistics, je členem domény Active Directory (AD).
2. Přidejte uživatele domény jako administrátora na lokální počítač.
3. Povolit systému Windows přístup k klíči relace TGT:
 - a. V nabídce **Start** klepněte na **Spustit**.
 - b. Zadejte příkaz `regedit` a klepnutím na tlačítko **OK** otevřete **Editor registru**.
 - c. Přejděte do následujícího umístění registru:

```
My
Computer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
```
 - d. Klepněte pravým tlačítkem myši na složku a vyberte volbu **Nový** > **DWORD**. Název nové hodnoty by měl být `allowtgtsessionkey`.
 - e. Nastavte hodnotu `allowtgtsessionkey` na hexadecimální hodnotu 1, tj. `0x0000001`.

- f. Zavřete **Editor registru**.
 - g. Spusťte příkaz `kinit.exe`, který lze nalézt v `<IBM SPSS Statistics installation location>\jre\bin`.
4. Ve složce `config` v umístění instalace produktu IBM SPSS Statistics vytvořte složku s názvem `sso`.
 5. Zkopírujte soubor `krb5.conf` ze serveru do složky `sso`.
 6. Restartujte počítač klienta a počítač serveru.

Registrace názvu SPN (Service Principle Name)

Každá instance serveru musí registrovat jedinečný *název SPN (Service principal name)* pro vlastní identitu a klient musí při připojení k serveru uvést stejnou SPN.

SPN pro instanci softwaru serveru má tento tvar:

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

Příklad:

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

Všimněte si, že název hostitele musí být kvalifikován jeho doménou DNS (`ibm.com` v tomto příkladu) a doména musí být mapována na sféru Kerberos.

Kombinace názvu hostitele a čísla portu činí SPN jedinečný (protože každá instance na daném hostiteli musí naslouchat na jiném portu). A klient i server již mají název hostitele a číslo portu, a tak mohou zkonstruovat odpovídající SPN pro instanci. Dodatečný krok konfigurace je nutný pro registraci SPN v databázi Kerberos.

Registrace názvu SPN v systému Windows

Pokud používáte Active Directory jako vaši implementaci Kerberos, použijte příkaz `setspn` k registraci SPN. Chcete-li spustit tento příkaz, musí být splněny následující podmínky:

- Musíte být přihlášení k řadiči domény
- Příkazový řádek je třeba spustit se zvýšenými oprávněními (spuštění jako administrátor)
- Musíte být členem skupiny administrátorů domény (nebo jste měli odpovídající oprávnění delegované administrátorem domény)

Další informace naleznete v následujících článcích:

- [Příkaz Setspn-Odkaz na řádek](#)
- [Delegování oprávnění pro úpravu SPN](#)

Pro výchozí instanci, poslechu na standardním portu (například 3023 pro verzi 23) a běžící pod účtem lokálního systému, musíte registrovat SPN proti názvu počítače serveru. Příklad:

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

Pro každou následnou instanci serveru, naslouchající na vlastním portu (například 3099) a spuštěnou pod libovolným uživatelským účtem (například `johndoe`) s volbou `userauth` nastavenou na `internal` (tj. pomocí interního ověření), musíte registrovat SPN na jméno uživatelského účtu služby:

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

Všimněte si, že v tomto případě (je-li servisní účet jiný než místní systém), registrace SPN není dostatečná, aby se klient mohl připojit. Další kroky konfigurace jsou popsány v následující sekci.

Chcete-li zjistit, které SPN jsou registrovány na účet jdoe, postupujte takto:

```
setspn -l jdoe
```

Registrace názvu SPN v systému UNIX

Pokud používáte Active Directory jako vaši implementaci Kerberos , použijte příkaz setspn , jak je popsáno v předchozí sekci systému Windows. To předpokládá, že jste již vytvořili počítač nebo uživatelský účet v adresáři. Případně můžete experimentovat s produktem ktpass, je-li to žádoucí (viz [Ktpass Command-Line Reference](#)).

Používáte-li jinou implementaci Kerberos , pak pomocí svého oblíbeného administračního nástroje Kerberos přidejte činitele služby do databáze Kerberos . Chcete-li převést hodnotu SPN na činitele Kerberos , je třeba přidat název sféry Kerberos . Příklad:

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

Přidejte stejného činitele a heslo do tabulky klíčů serveru. Tabulka klíčů musí obsahovat položku pro každou instanci spuštěnou na hostiteli.

Konfigurace jednotného přihlášení, pokud je spuštěn jako jiný než kořenový/ systém

Je-li démon/démon serveru spuštěn jako libovolný uživatel (ne uživatel root na systému UNIX a ne v systému Windows), je třeba registrovat účet služby/démona. Potřebujete SPN, který jste vytvořili dříve.

1. Vytvořte adresář <STATISTICSSERVER>\config\sso.
2. Zkopírujte soubor krb5.conf z adresáře SSO klienta do adresáře SSO serveru, který jste vytvořili v kroku 1.
3. K vytvoření souboru krb5.keytab v adresáři SSO na serveru použijte tento příkaz:

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

Příklad:

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

Zobrazí se výzva k zadání hesla. Heslo, které zadáte, musí být heslo účtu služby. Je-li servisní účet například jdoe, musíte zadat heslo pro uživatele jdoe.

Samotný servisní účet není uveden v tabulce klíčů, ale dříve jste zaregistrovali SPN na tento účet pomocí produktu setspn. To znamená, že heslo pro činitele služby a heslo pro servisní účet jsou jedno a stejné heslo.

Pro každou novou instanci serveru, kterou vytvoříte, musíte registrovat SPN pro tuto instanci (pomocí produktu setspn) a vytvořit soubor tabulky klíčů. Soubor keytab by měl být zkopírován do podadresáře config_<group_name>/sso v instalačním adresáři serveru. Výchozí instance nepotřebuje soubor tabulky klíčů.

Chcete-li ověřit, že je instance zahrnuta v tabulce klíčů, postupujte takto:

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

Pro každého činitele můžete vidět více položek s různými typy šifrování, ale to je normální.

Konfigurace členství ve skupinách

Pokud používáte autorizaci skupiny, můžete produkt IBM SPSS Collaboration and Deployment Services nakonfigurovat tak, aby se dotazoval na poskytovatele LDAP, aby určil skupinu, do které ověřený uživatel patří. Další informace o autorizaci skupiny naleznete v tématu [“Autorizace skupiny”](#) na stránce 29.

Pak musíte nejprve nakonfigurovat úložiště pro správné fungování skupiny, abyste přidali protokol LDAP nebo poskytovatele Active Directory , a poté povolit jednotné přihlášení pomocí tohoto poskytovatele:

1. Spusťte klienta produktu IBM SPSS Deployment Manager a vyberte volbu **Soubor > Nový > Spravované připojení k serveru ...** chcete-li vytvořit připojení spravovaného serveru pro úložiště (pokud dosud nemáte).
2. Přihlaste se ke správě spravovaného serveru a rozbalte složku **Konfigurace** .
3. Klepněte pravým tlačítkem myši na volbu **Poskytovatelé zabezpečení** vyberte volbu **Nový > Definice poskytovatele zabezpečení ...**, a zadejte příslušné hodnoty. Další informace získáte klepnutím na tlačítko **Nápověda** v dialogovém okně.
4. Rozbalte složku **Poskytovatelé jednotného přihlášení** , klepněte pravým tlačítkem myši na **Poskytovatel SSO Kerberosa** vyberte **Otevřít**.
5. Klepněte na volbu **Povolit**, vyberte svého poskytovatele zabezpečení a poté klepněte na tlačítko **Uložit**. Nemusíte vyplňovat žádné jiné podrobnosti, pokud nechcete použít jednotné přihlášení (jednoduše mít povolenu poskytovatele je dostatečné k umožnění vyhledání skupiny).

Důležité: Chcete-li, aby skupinové vyhledávání fungovalo správně, musí být vámi konfigurovaný poskytovatel Kerberos stejný jako poskytovatel, který jste nakonfigurovali pro produkt Server IBM SPSS Statistics. Zejména musí pracovat ve stejné sféře Kerberos . Takže pokud se uživatel přihlásí k serveru pomocí jednotného přihlášení a identifikuje ho jako `jdoe@ibm.com` (kde `ibm.com` je sféra), bude očekávat, že poskytovatel zabezpečení v produktu IBM SPSS Collaboration and Deployment Services rozpozná jméno uživatele a vrátí odpovídající členství ve skupině z adresáře LDAP.

Konfigurace jednotného přihlášení pro zdroje dat

K databázím se můžete připojit z produktu IBM SPSS Statistics pomocí jednotného přihlášení. Chcete-li vytvořit připojení k databázi pomocí jednotného přihlášení, musíte nejprve použít software pro správu ODBC , abyste mohli správně konfigurovat zdroj dat a token jednotného přihlášení. Při připojení k databázi v produktu IBM SPSS Statistics bude produkt IBM SPSS Statistics používat stejný token jednotného přihlášení a uživatel nebude vyzván k přihlášení ke zdroji dat.

Pokud však nebyl zdroj dat správně nakonfigurován pro jednotné přihlášení, produkt IBM SPSS Statistics vyzve uživatele, aby se přihlásil ke zdroji dat. Uživatel bude i nadále moci přistupovat ke zdroji dat po poskytnutí platných pověření.

Úplné podrobnosti o konfiguraci zdrojů dat ODBC ve vašem systému s povoleným jednotným přihlášením naleznete v dokumentaci od dodavatele databáze. Dále je uveden příklad obecných kroků, které se mohou zapojit:

1. Nakonfigurujte svou databázi tak, aby mohla podporovat jednotné přihlášení Kerberos .
2. Na počítači serveru vytvořte zdroj dat ODBC a otestujte jej. Připojení DSN by nemělo vyžadovat ID uživatele a heslo.
3. Připojte se k serveru pomocí jednotného přihlášení a začněte používat zdroj dat ODBC , který byl vytvořen a ověřen v kroku 2.

Oprávnění

Pokud nepoužíváte interní ověření nebo autorizaci skupin s jednotným přihlášením, server spustí proces pro koncového uživatele a předá ID uživatele a heslo operačnímu systému. Tento spuštěný proces má přístupová práva k souboru na účtu koncového uživatele. Uživatel připojující se k serverovým softwaru se musí přihlásit s účtem, který má následující oprávnění:

- Číst a provádět oprávnění k instalačnímu adresáři serveru a jeho podadresářům

- Číst, provádět a zapisovat oprávnění do umístění adresáře pro dočasné soubory

Pro vnitřní ověření a jednotné přihlášení má uživatel připojovaného klienta oprávnění, která jsou přiřazena uživateli, který spustil službu/démona.

Chcete-li změnit výchozí umístění dočasných souborů, můžete použít administrativní aplikaci (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager). Další informace naleznete v tématu Umístění souborů v příručce *Deployment Manager User's Guide* (zahrnuté v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Také můžete změnit umístění pro jednotlivé uživatele nebo skupiny. Další informace naleznete v tématu IBM SPSS Statistics Server User Profiles and Groups (Uživatelské profily a skupiny uživatelů IBM SPSS Statistics Server) v příručce *Deployment Manager User's Guide*.

Oprávnění na úrovni administrátora

Předvoleně je skupina administrátorů pro software serveru skupina administrátorů pro počítač, na kterém je spuštěn software serveru. Skupinu administrátorů pro software serveru můžete změnit tak, že ji uvedete v textovém poli Skupina administrátorů v administrativní aplikaci (IBM SPSS Statistics Administration Console, která se instaluje jako součást produktu IBM SPSS Deployment Manager). Další informace naleznete v tématu Uživatelé v příručce *Deployment Manager User's Guide* (zahrnuté v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Používáte-li interní ověřování v systému UNIX, můžete vytvořit administrátory přímo. Další informace naleznete v tématu [“Konfigurace interního ověřování”](#) na stránce 22 .

Autorizace skupiny

Software serveru můžete nakonfigurovat tak, aby podporoval autorizaci skupiny. Samostatná instance služby/démona se spouští pro každou autorizovanou skupinu uživatelů.

Konfigurace autorizace skupiny

1. Vytvořte instanci serveru pro každou skupinu. Další informace o vytváření instancí serveru viz [“Konfigurace více instancí”](#) na stránce 16.
2. Vytvořte skupiny v produktu IBM SPSS Collaboration and Deployment Services a přiřadte uživatele do skupin.
3. Otevřete administrativní aplikaci a aktualizujte hodnotu **Adresa URL služby autorizace skupiny** na adresu URL pro produkt IBM SPSS Collaboration and Deployment Services. Ujistěte se, že jste zahrnuli číslo portu (například `http://myserver.mydomain.com:9080`).

Řízení přístupu DSN podle skupin

Vícefaktorové ověření (MFA) vyžaduje, aby uživatelé mohli být omezeni v sadě názvů zdrojů dat ODBC (DSN), kterým mohou uživatelé přistupovat v souladu se svým členstvím ve skupině.

1. Otevřete administrativní aplikaci a nastavte volbu **Omezit databázový přístup** na Ano.
2. Do pole **Povolené zdroje databáze** zadejte seznam názvů DSN oddělených středníky (;), které jsou povoleny pro přístup (například `Analýza podvodného jednání; podvody-V provozu`).

Je-li toto omezení povoleno, má následující výsledky:

- Když uživatel prohlíží zdroje dat v průvodci databází místo toho, aby se prezentoval se všemi názvy DSN definovanými v systému serveru, uživatel uvidí pouze podmnožinu DSN, která je definována aplikací administrace. Všimněte si, že cesta může obsahovat názvy DSN, které nejsou definovány na serveru. Tyto jsou ignorovány a uživatel tyto názvy nevidí.
- Pokud uživatel upraví syntaxi `GET DATA /TYPE=ODBC`, která určuje název DSN, který není určen aplikací administrace, syntaxe se nespustí a uživatel bude prezentován s chybou podobnou chybě **Přístup k datovému zdroji: < X>**.

Profily

Serverová software poskytuje schopnost vytvářet profily individuálních uživatelů a skupin uživatelů. Tyto uživatelské profily a skupiny vám umožňují definovat nastavení pro specifické uživatele.

Verze klienta a serveru

Počínaje verzí 20.0.1 nemusí být klientský software na stejné úrovni vydání jako software serveru, ke kterému se připojuje. Například, klient 20.0.1 se může připojit k softwaru serveru 21 a 21 klient se může připojit k serveru 20.0.1. Všimněte si, že můžete také spustit více verzí serverového softwaru na serverovém počítači.

Mísení úrovní verzí je povoleno pouze pro zjednodušení aktualizací. Úrovně vydání mohou být rozloženy během období upgradu, a klienti nemusí být upgradováni současně. Nedoporučuje se však udržovat tuto konfiguraci po delší dobu. Je-li server novější než klient, server může vytvořit výstup, který nemůže klient číst. Je-li klient novější než server, syntaxe odeslaná klientem nemusí být serverem rozpoznána. Proto byste měli co nejdříve přejít na vyšší verzi softwaru klienta nebo serveru, v závislosti na tom, která z nich je druhou.

Pokud distribuujete informace o připojení koncovým uživatelům, mějte na paměti, jakou verzi softwaru klienta jsou spuštěny, a ujistěte se, že mají informace o připojení pro odpovídající verzi serveru.

Připojení uživatelů přes bránu firewall

Používáte-li **bránu firewall** k zajištění zabezpečení vaší sítě před vetřelci, můžete nakonfigurovat bránu firewall a serverový software tak, aby koncoví uživatelé mimo bránu firewall mohli připojit klienta k serverovému softwaru. Brána firewall může použít **NAT** (Network Address Translation), ale není to povinné.

Typický scénář pro připojení koncových uživatelů přes bránu firewall, který používá NAT, je následující:

1. Koncový uživatel připojí klientskou aplikaci k serverovému softwaru s použitím **maskované adresy IP** (IP adresa, kterou NAT představuje pro vnější svět) a číslo portu serveru. Koncový uživatel se například připojí k IP 10.10.10.2 a číslu portu 3016.
2. Brána firewall umožňuje připojení, protože byla nakonfigurována pro přijetí připojení od maskované adresy IP.
3. Brána firewall přeměrovává maskovanou adresu IP na skutečnou interní adresu IP serveru. Umožňuje připojení, protože je na bráně firewall povolen port (například 3016).
4. Server vytvoří proces pro připojení klienta koncového uživatele a přiřadí mu číslo portu ze seznamu v proměnné prostředí systému STATISTICS_CLIENT_PORTS. Tento proces například komunikuje prostřednictvím portu 3287.
5. Brána firewall umožňuje komunikaci přes tento port (např. 3287), protože je zapnutý na bráně firewall.

Konfigurace připojení přes bránu firewall

Úvod

IBM SPSS Statistics Server znovu použije stejné číslo portu pro připojení klienta. To znamená, že je třeba otevřít pouze dva porty přes bránu firewall: démon SPSS Statistics nebo naslouchací port (standardně se používá 3028, ačkoli jej lze v případě potřeby změnit) a port odezvy, přes který klienti produktu SPSS Statistics promluví s podřízenými procesy serveru SPSS Statistics.

Poznámka: Opětné použití portu je svázáno se schopností opětného připojení klienta. Při výchozím nastavení je klient-reconnect povolen po dobu 100 sekund. Je-li povoleno připojení klienta, server SPSS Statistics Server má poměr připojených klientů k otevření portů 1: 1 poměru k poměru otevřených odpovědí. Chcete-li povolit opakované použití portu, musíte nejprve zakázat připojení klienta znovu. To lze

provést úpravou nastavení **reconnect-timeout** v produktu <Statistics Install Path>/config/statisticsd.conf. Příklad:

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

V prostředí s mnoha možnými připojeními typu klient-server můžete chtít nakonfigurovat více než jeden port odezvy klienta. Je-li klient produktu SPSS Statistics v procesu připojování k serveru SPSS Statistics, je port klienta v podstatě uzamčen a může jej používat pouze jeden klient, dokud se proces připojení neukončí. Doba k připojení je v rozsahu 1-3 sekund (tento čas se může lišit v závislosti na zatížení systému). Když se druhý nebo třetí klient SPSS Statistics pokusí o připojení během této doby, jsou klienti blokováni, dokud nebude k dispozici port klienta. Otevření více portů klienta zkracuje dobu čekání při připojování v prostředí, ve kterém mnoho uživatelů souběžně spouští relace SPSS Statistics.

Příklad

Předpokládejme, že jsou v systémové proměnné prostředí **STATISTICS_CLIENT_PORTS** uvedeny pět portů klienta (porty 40001-40005) a existuje čtyři možná klient. Uživatel iniciuje připojení k serveru SPSS Statistics a první kontakt se provádí přes naslouchací port (3028). Server vytvoří podřízený proces a pokračuje v komunikaci prostřednictvím prvního dostupného portu klienta (4001). Není-li port 40001 uzamknut (protože komunikace s jiným klientem právě začala), port bude znovu použit. Je-li port 40001 zamčený, komunikace se přesune na další port (4002), za předpokladu, že není zamčený, a tak dále.

Po připojení všech čtyř klientů budou pravděpodobně všichni používat stejné číslo portu (40001). Existuje malá šance, že jeden nebo více klientů použije port 40002, menší pravděpodobnost, že klient použije port 40003, a ještě menší šanci, že jeden nebo více klientů bude používat port 40004. Není pravděpodobné, že by klient používal port 40005, protože existují pouze čtyři klienti, a algoritmus začíná na prvním dostupném čísle portu, které je uvedeno v systémové proměnné prostředí **STATISTICS_CLIENT_PORTS**.

Pro konfiguraci připojení k serveru SPSS Statistics prostřednictvím brány firewall existují dvě doporučené metody.

Konfigurace brány firewall pro povolení procesů

Pomocí softwaru brány firewall se ujistěte, že následující procesy jsou povoleny pro přijetí síťových připojení.

statisticsproc.exe

Proces `statisticsproc.exe` se otevře, zavře a znovu použije porty odezvy (nebo porty, které jsou definovány v produktu **STATISTICS_CLIENT_PORTS**).

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

Proces je hlavní služba systému Windows, nebo démon UNIX/Linux a spravuje naslouchající port.

Zajištění přístupu k procesům účinně umožňuje jakýkoli port, který bude proces používat.

Poznámka: Když je hodnota časového limitu opětovného připojení větší než 0 a `statisticsproc.exe` je povoleno přijímat síťová připojení, platí následující podmínky:

- **STATISTICS_CLIENT_PORTS** je irelevantní, kromě diagnostiky. Lze použít libovolný port.
- Neexistuje žádné omezení počtu připojení, pokud nejsou porty definovány v parametru **STATISTICS_CLIENT_PORTS**. Počet definovaných portů **STATISTICS_CLIENT_PORTS** efektivně omezuje porty, které bude server SPSS Statistics používat.

Konfigurace brány firewall ručním otevřením portů

Chcete-li ručně nakonfigurovat software serveru a bránu firewall, postupujte takto:

1. Nainstalujte software serveru jako obvykle. Musíte znát IP adresu počítače, na kterém je server instalován, a číslo portu, které server používá pro komunikaci. Například, nainstalujte server na 202.123.456.78 na naslouchajícím portu 3028.

2. Konfigurujte systémovou proměnnou prostředí `STATISTICS_CLIENT_PORTS` tak, že zadáte alespoň jedno číslo portu. Proměnná prostředí uvádí seznam portů, které se používají k pokračování připojení klienta se serverem (porty **RESPONSE**). V případě potřeby můžete zadat seznam hodnot oddělených čárkami a rozsah portů (například 4001, 4002, 4003-4005).

Důležité:

- Při nastavování časového limitu automatického opětovného připojení na hodnotu větší než 0, `STATISTICS_CLIENT_PORTS` definuje maximální počet povolených souběžných připojení klienta a serveru.
- Nepište seznam portů **LISTEN** (3028) v proměnné prostředí `STATISTICS_CLIENT_PORTS`.

Microsoft® Windows™

Pomocí vlastností systému Windows vytvořte a nakonfigurujte proměnnou prostředí. Pokyny naleznete v příručce [“Vlastnosti systému”](#) na stránce 51.

UNIX

Upravte skript prostředí serverového softwaru `statsenv.sh`, který je obsažen v podadresáři `/bin` instalačního adresáře. Definujte port, který může používat klientské procesy, které server spouští. Přidejte například následující řádky:

```
STATISTICS_CLIENT_PORTS=4001  
  
export STATISTICS_CLIENT_PORTS
```

3. Používáte-li NAT (Network Address Translation), vytvořte a mapujte adresy IP. Pomocí softwaru brány firewall vytvořte maskovanou adresu IP pro externí použití a namapujte ji na interní adresu IP serveru. Vytvořte například masquerade IP `10.10.10.2` a namapujte ji na `202.123.456.78`.
4. Pomocí softwaru brány firewall povolte čísla portů na bráně firewall:
 - Číslo portu **LISTEN** serveru. Povolte například port 3028.
 - Čísla portů, která jste zadali v proměnné prostředí `STATISTICS_CLIENT_PORTS`. Povolte například port 4001.
5. Distribuujte informace o připojení uživatelům, kteří se připojují k serverovým softwaru z prostředí mimo bránu firewall.
 - Je-li použita, maskovaná adresa IP počítače, na kterém je nainstalován serverový software (nedistribuuje interní adresu IP serveru). Například, distribuujte `10.10.10.2` jako adresu IP serveru.
 - Distribuujte číslo portu softwaru serveru jako obvykle. Například, distribuujte 3028 jako číslo portu **LISTEN** serveru.

Připojování uživatelů s PPTP

Koncoví uživatelé mohou připojit vzdálený klientský počítač k softwaru analytického serveru pomocí protokolu PPTP (**Point-to-Point Tunneling Protocol**). Protokol PPTP je síťový protokol, který podporuje multiprotokolové virtuální privátní sítě (VPNs). Umožňuje vzdáleným koncovým uživatelům přistupovat k vaší síti bezpečně přes Internet.

Chcete-li použít připojení PPTP:

1. **Konfigurace serveru pro vzdálený přístup pro PPTP.** Ujistěte se, že jste vytvořili dostatečný počet IP adres pro klienty, protože serverový software podporuje více klientských připojení. Každé připojení klienta vyžaduje vlastní adresu IP.
2. **Konfigurujte pracovní počítač klienta.** Použijte ovládací panel Síť Windows k přidání připojení do privátní sítě pomocí PPTP. Zadejte adresu IP, kterou vzdálený přístupový server rozpozná jako připojení PPTP.
3. **Povolte připojení PPTP na stolním počítači klienta.** Pokud se koncoví uživatelé chtějí připojit k serverovému softwaru ze vzdáleného umístění, povolí připojení PPTP a pak tento klientský software použije pro připojení k serveru jako obvykle.

Použití SSL k zabezpečení přenosu dat

Produkt Secure Sockets Layer (SSL) je protokol pro šifrování dat přenášených mezi dvěma počítači. SSL zajišťuje, že komunikace mezi počítači je zabezpečená. SSL může zašifrovat ověření jména uživatele/hesla a obsah výměny mezi serverem a klientem.

Jak SSL funguje

SSL spoléhá na veřejné a soukromé klíče serveru, navíc k certifikátu veřejného klíče, který spojuje identitu serveru s jeho veřejným klíčem.

1. Když se klient připojuje k serveru, ověřuje klient server s certifikátem veřejného klíče.
2. Klient pak vygeneruje náhodné číslo, zašifruje číslo pomocí veřejného klíče serveru a odešle šifrovanou zprávu zpět na server.
3. Server dešifruje náhodné číslo se svým soukromým klíčem.
4. Z náhodného čísla vytvoří server i klient klíče relace použité pro šifrování a dešifrování následných informací.

Certifikát veřejného klíče je obvykle podepsán certifikační autoritou. Vydavatele certifikátů, jako je VeriSign a Thawte, jsou organizace, které vydávají, ověřují a spravují bezpečnostní pověření obsažené v certifikátech veřejného klíče. Certifikační autorita v podstatě potvrzuje identitu serveru. Certifikační autorita obvykle účtuje za certifikát peněžní poplatek, ale certifikáty podepsané sebou samým mohou být také generovány.

Povolení zabezpečení SSL pomocí sady GSKit

Zabezpečení komunikace typu klient/server a serveru s produktem GSKit

Hlavní kroky při zabezpečení komunikace mezi klientem a serverem a serverovou serverem se zabezpečením SSL jsou:

1. Získejte a nainstalujte certifikát SSL a klíče.
2. Povolte a nakonfigurujte uvedený konfigurační soubor umístěný v instalačním adresáři serveru IBM SPSS Statistics .

Poznámka: Produkt IBM SPSS Statistics Server podporuje protokol TLSv1.2 . Sada GSKit v současné době nepodporuje žádné jiné verze.

3. Pokud používáte šifrovací certifikáty o síle větší než 2048 bitů, nainstalujte na klientské počítače neomezené šifrování síly.
4. Instruuje uživatele k povolení zabezpečení SSL při připojování k serveru.

Poznámka: Někdy se serverový produkt chová jako klient. Příkladem je server IBM SPSS Statistics , který se připojuje k Produkt IBM SPSS Collaboration and Deployment Services Repository. V tomto případě je server IBM SPSS Statistics serverem *client*.

Získání a instalace certifikátu SSL a klíčů

První kroky, které je třeba provést při konfiguraci podpory zabezpečení SSL, jsou:

1. Získejte certifikát SSL a soubor s klíči. Existuje několik způsobů, jak to můžete provést:
 - Zakoupte je od veřejné certifikační autority (jako je VeriSign, Thawte nebo Entrust). Veřejný certifikační autorita (CA) podepisuje certifikát, aby ověřil server, který jej používá.
 - Získejte soubory s klíči a certifikáty od certifikační autority jiného dodavatele. If this approach is taken, the third-party CA's * . pfx root certificate must be imported into the server's keystore file (explained below).
 - Generujte soubory s klíči a certifikáty s interním certifikačního autorit s vlastním podpisem. Kroky k provedení tohoto postupu:

- a. Připravte databázi klíčů. Další informace naleznete v tématu [“Vytvoření databáze klíčů SSL”](#) na stránce 35 .
 - b. Vytvořte certifikát podepsaný (svým) držitelem. Další informace naleznete v tématu [“Vytvoření certifikátu SSL s automatickým podpisem”](#) na stránce 35 .
2. V případě certifikátů certifikačních autorit (CA) nebo certifikátů s automatickým podpisem zkopírujte soubory .kdb a .sth z kroku 1 do adresáře, k němuž má produkt Server IBM SPSS Statistics přístup, a zadejte cestu k tomuto adresáři v souboru statisticsd.conf . Soubor statisticsd.conf se nachází v <Statistics Server installation directory>/config/; pro certifikáty třetích stran zkopírujte soubory .pfx a .sth z kroku 1.
 3. Nastavte následující parametry v souboru statisticsd.conf :

Pro certifikační autoritu (CA) nebo certifikáty s automatickým podpisem:

- <gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>, kde <value> je buď 0 nebo 1 , které udává, zda má být sada GSKit povolena.
- <gsk-keystore desc="GSKSSL Key store database filename." value="<filename>.kdb"/>, kde <filename> je název souboru databáze klíčů.
- <gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>, kde <filename> je název souboru pro uložení hesla databáze klíčů.
- <gsk-cert-label desc="GSKSSL certificate label." value=""/>, kde <label> je označení vašeho certifikátu.

Pro certifikáty třetích stran:

- <gsk desc="0=GSKSSL Disabled; 1=GSKSSL Enabled" value="<value>"/>, kde <value> je buď 0 nebo 1 , které udává, zda má být sada GSKit povolena.
- <gsk-keystore = "<*.pfx_file_location>", kde <*.pfx_file_location> je umístění a název kořenového souboru certifikátu produktu *.pfx .
- <gsk-keystore-stash desc="GSKSSL Key store stash filename." value="<filename>.sth"/>, kde <filename> je název souboru pro uložení hesla databáze klíčů.
- <gsk-cert-label desc="GSKSSL certificate label." value=""/>, kde <label> je označení vašeho certifikátu.

4. Pro certifikáty třetích stran:

- a. Extrahujte soubor root.pem ze souboru *.pfx , pomocí následujícího příkazu GSK jako příklad:

```
gsk8capi64.exe -cert -extract -db C:\SSL\<certificate_name>.pfx -stashed -label
<cert-certificate_issuing_server.com> -target C:\SSL\root.pem
```

- b. Zkopírujte root.pem do složky C:\ProgramData\IBM\SPSS\certificates (Windows) nebo /Library/Application Support/IBM/SPSS/certificates (macOS) na klientovi.
 - c. Na straně klienta nastavte připojení pomocí plně kvalifikovaného názvu domény (například cert-certificate_issuing_server.com) " v poli **Název serveru** a povolte volbu **SSL** .
5. U certifikátů podepsaných sebou samým nainstalujte certifikát na klientských systémech. U zakoupených veřejných CA nebo certifikátů třetích stran se tento krok nepožaduje. Ujistěte se, že přístupová oprávnění zakazují příležitostné procházení adresáře, který obsahuje daný certifikát. Další informace naleznete v tématu [“Instalace certifikátu SSL s automatickým podpisem”](#) na stránce 36 .

Konfigurace prostředí pro spuštění sady GSKit

GSKCapiCmd je nástroj příkazového řádku, který není založený na jazyku Java, a prostředí Java™ není třeba instalovat do systému pro použití tohoto nástroje; je umístěn ve složce <Statistics Server installation directory>/bin . Proces konfigurace vašeho prostředí ke spuštění produktu IBM Global Security Kit (GSKit) se liší v závislosti na používané platformě.

Chcete-li konfigurovat systém Linux/Unix, přidejte do svého prostředí adresář sdílených knihoven <Statistics Server installation directory>/lib:

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

Název proměnné cesty ke sdílené knihovně závisí na použité platformě:

- Systém Linux používá název proměnné: LD_LIBRARY_PATH

Chcete-li například nastavit prostředí na systému Linux, použijte:

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

Přístup účtu k souborům

Ujistěte se, že udělíte správná oprávnění pro účty, které budou přistupovat k souborům SSL:

1. Pro všechny účty, které používá produkt IBM SPSS Statistics pro připojení, udělte přístup pro čtení k souborům SSL.

Poznámka: To platí také pro uživatele *Přihlášení jako*, který je definován ve službě serveru IBM SPSS Statistics. Na systému UNIX nebo Linuxse používá pro uživatele, na kterém spouštíte server.

2. Pro systém Windows není dostatečné, aby účty byly ve skupině administrátorů a aby bylo skupině administrátorů uděleno oprávnění, je-li povoleno řízení přístupu uživatele (UAC). Kromě toho je třeba provést jednu z následujících akcí:

- Poskytněte oprávnění účtu odděleně.
- Vytvořte novou skupinu, přidejte účty do nové skupiny a udělte skupině oprávnění pro přístup k souborům SSL.
- Vypněte UAC.

Vytvoření databáze klíčů SSL

K vytvoření databáze klíčů použijte nástroj GSKCapiCmd. Před použitím tohoto nástroje je třeba nakonfigurovat prostředí; další informace naleznete v tématu [“Konfigurace prostředí pro spuštění sady GSKit” na stránce 34](#).

Chcete-li vytvořit databázi klíčů, spusťte sadu GSKit a zadejte následující příkaz:

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

kde <ver> je číslo verze sady GSKit, <filename> je název, který chcete použít pro soubor databáze klíčů, a <password> je heslo pro databázi klíčů.

Volba -stash vytvoří soubor pro dočasné ukládání ve stejné cestě jako databáze klíčů s příponou souboru .sth. Sada GSKit používá soubor pro uložení k získání hesla k databázi klíčů, takže nemusí být pokaždé zadávána na příkazovém řádku.

Poznámka: Měli byste použít silnou ochranu systému souborů v souboru .sth.

Vytvoření certifikátu SSL s automatickým podpisem

Chcete-li vygenerovat certifikát podepsaný svým držitelem a uložit jej do databáze klíčů, použijte tento příkaz:

```
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>
```


kde <ver> je číslo verze sady GSKit, <filename> je název souboru databáze klíčů, <Number of days certificate is valid> je fyzický počet dní, po které je certifikát platný, a <label> je popisný štítek, který vám pomůže s identifikací souboru (například můžete použít popisek, jako je: myselfsigned).

Instalace certifikátu SSL s automatickým podpisem

U klientských počítačů, které se připojují k serveru pomocí protokolu SSL, je třeba distribuovat veřejnou část certifikátu klientům tak, aby mohla být uložena ve svých klíčových databázích. Chcete-li to provést, proveďte následující kroky:

Poznámka: Přeskočte tento krok, pokud používáte certifikát podepsaný certifikační autoritou. Pokud používáte certifikát podepsaný držitelem, musíte zkopírovat důvěryhodnou certifikační autoritu na počítače klienta. Mějte na paměti, že počítač serveru může vystupovat také jako klient. Příklad: IBM SPSS Statistics Server se připojuje k Produktu IBM SPSS Collaboration and Deployment Services Repository. V tomto případě je server IBM SPSS Statistics klientem, a proto musíte zkopírovat certifikát pro server Produktu IBM SPSS Collaboration and Deployment Services Repository na server IBM SPSS Statistics Server.

1. Extrahujte veřejnou část do souboru pomocí následujícího příkazu:

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

2. Distribuujte root . pem klientům. Máte-li více důvěryhodných certifikačních autorit, zkopírujte je do jediného souboru root . pem . Oprávnění důvěryhodných certifikátů jsou textové soubory, takže můžete zkopírovat a vložit certifikát nebo certifikáty. Zkopírujte root . pem do následujícího umístění na klientských počítačích. Pokud jste již zkopírovali soubor root . pem do klienta jiného produktu IBM , připojte informace o důvěryhodné kořenové certifikační autoritě od svého oprávnění k existujícímu souboru root . pem . Všechny klientské produkty společnosti IBM se standardně v tomto umístění hledají pro důvěryhodné soubory s certifikátem podepsaným držitelem. Chcete-li použít jiné umístění, vytvořte proměnnou prostředí SSL_CERT_DIR a nastavte hodnotu proměnné na její umístění.
 - Systém Windows 7 a vyšší: C:\ProgramData\IBM\SPSS\certificates
 - Mac: /Library/Application Support/IBM/SPSS/certificates
 - UNIX a Linux: /opt/IBM/SPSS/certificates

Konfigurace klientských certifikátů

Je-li produkt SPSS Statistický server nakonfigurován tak, aby používal připojení SSL a používáte-li certifikát podepsaný držitelem, musíte zkopírovat a nakonfigurovat oprávnění důvěryhodného certifikátu ke všem pracovním stanicím klienta.

Příklad by měl být, když IBM SPSS Collaboration and Deployment Services zadá úlohu do SPSS Statistický server (což je povoleno SSL). V této situaci je klient IBM SPSS Collaboration and Deployment Services klientem. Důvěryhodná certifikační autorita (root . pem na serveru SPSS Statistický server) by měla být kopírována do a nakonfigurována na všech počítačích IBM SPSS Collaboration and Deployment Services .

Konfigurace souborů certifikátů pro produkt IBM SPSS Collaboration and Deployment Services

Podpora produktu IBM SPSS Collaboration and Deployment Services může být implementována na webovém aplikačním serveru (například IBM WebSphere a RedHat JBoss EAP).

Prvním krokem v konfiguraci souborů certifikátů pro podporu produktu IBM SPSS Collaboration and Deployment Services je načtení souboru SPSS Statistický server root . pem od administrátora.

Proces konfigurace certifikátu SSL závisí na tom, který webový aplikační server je použit.

IBM WebSphere a RedHat JBoss EAP

Následující pokyny platí pro produkty IBM WebSphere a RedHat JBoss EAP.

Poznámka RedHat JBoss EAP: Když produkt SPSS Statistický server používá zabezpečení SSL IBM GSKit, musíte při konfiguraci produktu IBM SPSS Collaboration and Deployment Services na JBoss EAP použít sadu IBM JDK.

1. Distribuujte soubor `root.pem` na počítač serveru IBM SPSS Collaboration and Deployment Services. Máte-li více důvěryhodných certifikačních autorit, zkopírujte je do jednoho souboru `root.pem` (důvěryhodné certifikační autority jsou textové soubory, takže můžete zkopírovat a vložit certifikáty) Kopírovat `root.pem` do následujícího umístění na serveru IBM SPSS Collaboration and Deployment Services.

Pokud jste již zkopírovali soubor `root.pem` do klienta jiného produktu IBM, připojte informace o důvěryhodném kořenovém certifikační autoritě z vašeho oprávnění k existujícímu souboru `root.pem`. Vytvořte proměnnou prostředí `SSL_CERT_DIR` a nastavte hodnotu proměnné na požadované umístění serveru, které obsahuje soubor `root.pem`.

2. Ověřte, že uživatel serveru IBM SPSS Collaboration and Deployment Services přidá proměnnou prostředí `SSL_CERT_DIR`.

Poznámka: Server IBM SPSS Collaboration and Deployment Services musí být restartován po přidání proměnné prostředí.

Instalace neomezené síly šifrování

V prostředí Java Runtime Environment dodaném s produktem je povoleno šifrování exportu s exportováním v USA. Pro lepší zabezpečení dat doporučujeme upgrade na neomezené šifrování dat.

1. Extrahujte soubory zásad s neomezenou jurisdikcí, které jsou zabaleny v komprimovaném souboru. Komprimovaný soubor obsahuje soubor `US_export_policy.jar` a soubor `local_policy.jar`.
2. Nahraďte existující kopie souborů `US_export_policy.jar` a `local_policy.jar` dvěma soubory, které jste stáhli a extrahovali.

Instruování uživatelů k povolení zabezpečení SSL

Když se uživatelé připojí k serveru prostřednictvím klientského produktu, musí aktivovat SSL v dialogovém okně pro připojení k serveru. Ujistěte se, že jste označili vašim uživatelům, aby vybrali odpovídající zaškrtnávací políčko.

Povolení SSL pomocí OpenSSL

Zabezpečení komunikací typu klient/server a server-server s OpenSSL

Hlavní kroky při zabezpečení komunikace mezi klientem a serverem a serverovou serverem se zabezpečením SSL jsou:

1. Nainstalujte OpenSSL na serverovém počítači.
2. Získejte a nainstalujte certifikát SSL a klíče.
3. Povolte a nakonfigurujte zabezpečení SSL v aplikaci administrace serveru (IBM SPSS Deployment Manager).

Poznámka: Produkt IBM SPSS Statistics Server podporuje protokol TLSv1. SSLv3 se osvědčil jako bezpečnostní zranitelnost a neměl by se používat.

4. Pokud používáte šifrovací certifikáty s pevností větší než 2048 bitů, nainstalujte na počítačích klienta neomezené šifrování síly.
5. Pokud používáte certifikát podepsaný sebou samým, zkopírujte certifikát na klientském počítači.
6. Instruuje uživatele k povolení zabezpečení SSL při připojování k serveru.

Poznámka: Někdy se serverový produkt chová jako klient. Příkladem je server IBM SPSS Statistics, který se připojuje k serveru Produkt IBM SPSS Collaboration and Deployment Services Repository. V tomto případě je server IBM SPSS Statistics serverem *client*.

Instalovat OpenSSL

Není-li na serveru k dispozici OpenSSL, musíte jej nainstalovat.

1. Stáhněte OpenSSL z <http://www.openssl.org/>. Dbejte na to, abyste použili verzi OpenSSL odpovídající verzi serveru:

Tabulka 2. OpenSSL verze	
Serverový produkt	Kompatibilita verze OpenSSL
IBM SPSS Statistics 29	1.1.1f nebo novější
IBM SPSS Statistics 28	1.1.1f nebo novější
IBM SPSS Statistics 27.0.1	1.1.1f nebo novější Poznámka: Podpora pro nezabezpečený protokol SSLv3 byla zamítnuta.
IBM SPSS Statistics 26-27	1.0.2 nebo novější
IBM SPSS Statistics 24-25	1.0.1f nebo novější
IBM SPSS Statistics 20-23	1.0.0
IBM SPSS Statistics 17-19 (ne Linux® on System z®)	0.9.8 a její podverze (0.9.8a, 0.9.8batd.)
IBM SPSS Statistics 19 (Linux® on System z®)	1.0.0

2. Postupujte podle pokynů pro instalaci a konfiguraci softwaru. Doporučuje se vytvořit OpenSSL sami, s následujícími pokyny:

Okna. OpenSSL by měl být sestaven s DLL (které jsou ve výchozím nastavení multithreaded).

UNIX. OpenSSL by mělo podporovat více vláken (což není vždy standardně) a sdílených knihoven.

3. Ujistěte se, že jsou moduly OpenSSL zahrnuty na systémové cestě.

Poznámka: Pokud na serverovém počítači existuje více než jedna verze modulů OpenSSL, zkopírujte moduly OpenSSL pro server IBM SPSS Statistics do adresáře, kde je nainstalován produkt IBM SPSS Statistics Server.

Získání a instalace certifikátu SSL a klíčů

1. Získejte certifikát SSL a soubor s klíči. Existují dva způsoby, jak to lze provést:

- Zakoupte je od veřejné certifikační autority (například Comodo, Symantec nebo GoDaddy). Obecné certifikační autorita podepisuje certifikát, aby ověřil server, který jej používá. Toto je doporučená metoda.
- Generujte soubory s klíči a certifikáty s interním vydavatelem certifikátů s vlastním podpisem. OpenSSL poskytuje nástroj pro správu certifikátů pro tento účel, nebo můžete vyhledávat instrukce na vytvoření certifikátu SSL s automatickým podpisem.

2. Zkopírujte certifikát a soubor klíčů nebo soubory do místního adresáře nebo adresářů na serveru. Veřejné a soukromé klíče mohou být uloženy v samostatných adresářích. Mohou být také uloženy v jednom souboru. Ujistěte se, že soukromý klíč není umístěn v umístění, které by mohlo být rozpoznáno během příležitostného procházení systému souborů.

3. Zkopírujte důvěryhodné certifikační autority s názvem *root.pem* do následujícího umístění na počítači serveru. Chcete-li použít jiné umístění, vytvořte proměnnou prostředí `SSL_CERT_DIR` a nastavte hodnotu proměnné na umístění.

System Windows 7 a vyšší: `C:\ProgramData\IBM\SPSS\certificates`

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

UNIX a Linux: /opt/IBM/SPSS/certificates

Povolit a konfigurovat SSL v produktu IBM SPSS Deployment Manager

1. Spusťte aplikaci pro administraci serveru (IBM SPSS Statistics Administration Console, která je nainstalována jako část produktu IBM SPSS Deployment Manager) a připojte se k serveru.
2. Na stránce konfigurace nastavte volbu **SSL (Secure Sockets Layer)** na hodnotu **Ano**.
3. Do pole **Soubor s veřejnými klíči SSL** zadejte úplnou cestu k souboru s veřejnými klíči.
4. Do pole **Soubor soukromého klíče zabezpečení SSL** zadejte úplnou cestu k souboru se soukromými klíči.

Poznámka: Pokud jsou veřejné a soukromé klíče uloženy v jednom souboru, uveďte stejný soubor v **Soubor s veřejnými klíči SSL** a **Soubor soukromého klíče SSL**.

5. Z nabídky vyberte:

Soubor > Uložit

6. Restartujte službu serveru nebo démona. Když restartujete, budete vyzváni k zadání hesla SSL. Na systému Windows můžete vybrat volbu **Zapamatovat toto heslo**, abyste heslo uložili bezpečně. Tato volba eliminuje nutnost zadávat heslo pokaždé, když je server spuštěn.

Instalace neomezené síly šifrování

V prostředí Java Runtime Environment dodaném s produktem je povoleno šifrování exportu s exportováním v USA. Pro lepší zabezpečení dat doporučujeme upgrade na neomezené šifrování dat.

1. Extrahujte soubory zásad s neomezenou jurisdikcí, které jsou zabaleny v komprimovaném souboru. Komprimovaný soubor obsahuje soubor `US_export_policy.jar` a soubor `local_policy.jar`.
2. Nahraďte existující kopie souborů `US_export_policy.jar` a `local_policy.jar` dvěma soubory, které jste stáhli a extrahovali.

Kopírování souboru s certifikátem do klientských počítačů

Poznámka: Přeskočte tento krok, pokud používáte certifikát podepsaný certifikační autoritou.

Používáte-li certifikát podepsaný držitelem, musíte zkopírovat důvěryhodnou certifikační autoritu na počítače *klienta*. Mějte na paměti, že počítač serveru může vystupovat také jako klient. Příkladem je server IBM SPSS Statistics, který se připojuje k Produktu IBM SPSS Collaboration and Deployment Services Repository. V tomto případě je server IBM SPSS Statistics serverem *client*, a proto musíte zkopírovat certifikát pro server Produktu IBM SPSS Collaboration and Deployment Services Repository na server IBM SPSS Statistics.

1. Vytvořte důvěryhodnou certifikační autoritu s názvem `root.pem`. Pokud jste například vytvářeli důvěryhodnou certifikační autoritu s OpenSSL, použijte přepínač `-out` k určení výstupního souboru jako `root.pem`. Máte-li více důvěryhodných certifikačních autorit, zkopírujte je do jednoho souboru `root.pem`. Oprávnění důvěryhodných certifikátů jsou textové soubory, takže můžete zkopírovat a vložit certifikát nebo certifikáty.
2. Zkopírujte soubor `root.pem` do následujícího umístění na klientských počítačích. Pokud jste již zkopírovali soubor `root.pem` do klienta pro jiný produkt IBM Corp., připojte informace o důvěryhodném kořenovém certifikační autoritě od svého oprávnění k existujícímu souboru `root.pem`. Ve výchozím nastavení se všechny klientské produkty IBM Corp. v tomto umístění hledají pro důvěryhodné soubory s certifikátem podepsaným sebou samým. Chcete-li použít jiné umístění, vytvořte proměnnou prostředí `SSL_CERT_DIR` a nastavte hodnotu proměnné na umístění.

Systém Windows 7 a vyšší: `C:\ProgramData\IBM\SPSS\certificates`

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

Instruování uživatelů k povolení zabezpečení SSL

Když se uživatelé připojí k serveru prostřednictvím klientského produktu, musí aktivovat SSL v dialogovém okně pro připojení k serveru. Ujistěte se, že jste označili vašim uživatelům, aby vybrali odpovídající zaškrtnuté políčko.

Nastavení národního prostředí

Serverová software a klient, který se k němu připojuje, musí být spuštěny ve stejné znakové sadě, kódování a národním prostředí. Software serveru získává národní prostředí od klienta. Při výchozím nastavení se jedná o národní prostředí *systému* klienta. Klient však může přepsat výchozí nastavení pro zpracování datových souborů v jiných národních prostředích. Při potlačení výchozího nastavení uživatel instruuje software serveru, aby se spouštěl v určeném národním prostředí, aniž by změnil národní prostředí klienta.

Syntaxe

Uživatel přepíše výchozí nastavení pomocí příkazu syntaxe SET LOCALE :

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

localeid je řetězec, který identifikuje národní prostředí, v němž bude software serveru spuštěn. Produkt SET LOCALE zapíše položku registru na klientský počítač. Tento záznam trvá, takže se příště IBM SPSS Statistics spustí na klientském počítači, IBM SPSS Statistics se spustí v tomto národním prostředí.

Konvence pojmenování pro ID národního prostředí se může lišit mezi platformami a dodavateli. Proto existuje soubor XML nainstalovaný se serverem, který mapuje národní prostředí klienta na národní prostředí serveru. Tento soubor, *loclmap.xml*, je umístěn v instalačním adresáři serveru v systému Windows a v podadresáři */bin* v systému UNIX.

loclmap.xml

Kořenový prvek v souboru *loclmap.xml* je následující. Kořenový prvek také identifikuje umístění schématu.

```
<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">
```

Kořenový prvek obsahuje prvky produktu `<client-locale>` s atributem `name`, který identifikuje národní prostředí klienta. Prvky `<client-locale>` obsahují jeden nebo více prvků `<server-locale>`. Každý prvek `<server-locale>` má atribut `name` identifikující národní prostředí serveru, které odpovídá národnímu prostředí klienta. Software serveru přeloží ID národního prostředí klienta na takový, který lze použít na serverovém počítači. Kontroluje každé národní prostředí serveru v pořadí, dokud nenajde jednu, která je platná na počítači serveru.

Žádné z výchozích národních prostředí serveru v souboru *loclmap.xml* nejsou národními prostředím Windows. Národní prostředí systému Windows nejsou obecně potřeba, protože software serveru se nejprve pokusí použít stejné národní prostředí jako národní prostředí systému klienta. Server Windows by měl mít národní prostředí, které odpovídá národnímu prostředí klienta. Nicméně můžete přidat národní prostředí serveru Windows do souboru *loclmap.xml*, pokud potřebujete nahradit jiné než podobné národní prostředí systému Windows.

Soubor *loclmap.xml* můžete upravit podle potřeby. Je třeba si uvědomit, že vaše prvky XML musí být ověřeny proti schématu.

Příklad

Následující text je příkladem použití obsahu souboru *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.IS08859-15"></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.IS08859-1"></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="fr_FR.UTF-8"></server-locale>
</client-locale>
```

V tomto případě, v případě problémů uživatele SET LOCALE="French", software serveru nejprve zkontroluje fr_FR.cp1252. Zvažte případ serveru AIX. Národní prostředí fr_FR.cp1252 nefunguje na systému AIX, takže software serveru pokračuje v kontrole, dokud nedosáhne fr_FR.windows-1252, což funguje na systému AIX.

Použití národního prostředí serveru

Pokud uživatel zadá příkaz SET LOCALE s použitím ID národního prostředí serveru, které není rozpoznáno na klientském počítači, použije počítač klienta soubor *loclmap.xml* k vyhledání ID národního prostředí klienta přidruženého k národnímu prostředí serveru. Tento identifikátor národního prostředí zapisuje do registru. Například, pokud uživatel zadá SET LOCALE="fr_FR.windows-1252", French se zapíše do registru. Chcete-li zjistit, která položka v souboru *loclmap.xml* se vztahuje na klienta, můžete spustit příkaz SHOW LOCALE v lokálním režimu.

Potenciální problémy

Mějte na paměti, že použití příkazu SET LOCALE může v některých případech způsobit funkční problémy:

- Aktuální názvy proměnných nemusí být v nové kódové stránce přípustné.
- Shody názvu nerozlišující velikost písmen mohou selhat. K selhání může dojít kvůli tomu, že řetězce jsou převedeny na znaky upper-case v názvech bez rozlišení velkých a malých písmen (například při porovnávání názvů proměnných). Je-li národní prostředí nesprávné, tento převod by změnil znak (například na stránce středoevropského kódu 1250).
- Některé bajty by mohly být nesprávně interpretovány jako olovené bajty a problém se může vyskytnout kvůli neočekávanému bajtovému bajtu.
- Produkt SET LOCALE nemění národní prostředí systému klienta. Proto je-li národní prostředí produktu IBM SPSS Statistics přidružené k produktu SET LOCALE odlišné od národního prostředí klientského systému, budou v různých místech zobrazeny problémy s obrazovkou. V této situaci uživatel také nemůže použít Editor IME (Input Method Editor) k zadání národních znaků.
- Musí být kompatibilní národní prostředí produktu IBM SPSS Statistics, nastavení OLANG a kódování použité pro data. Jinak může být výstup nepoužitelný a nečitelný.

Připojení k serverovým softwaru

Koncový uživatel se připojuje k softwaru serveru přihlášením z aplikace klienta. Pro přihlášení koncového uživatele potřebuje od vás následující informace:

- **Název počítače nebo adresa IP.** Když se koncoví uživatelé připojí k softwaru serveru, přihlašují se z klientské aplikace. Chcete-li tak učinit, musí správně určovat název počítače, na kterém je spuštěn serverový software. Počítač serveru může být identifikován pomocí alfanumerického názvu (například `myserver`) nebo adresy IP přiřazené k počítači serveru (například 202.123.456.78)-podle toho, co dáváte přednost. Pokud nakonfigurujete server a počítače klientských počítačů tak, aby používaly

zabezpečení SSL (Secure Sockets Layer), musí koncový uživatel používat úplný název domény (např. `myserver.mycompany.com`).

- **Číslo portu.** Koncoví uživatelé musí správně uvádět port, na kterém software serveru naslouchá připojení. Číslo portu je výchozí pro server nebo cokoli, co jste zadali při konfiguraci softwaru serveru.
- **Název domény (pouze Windows).** Koncoví uživatelé mohou také vyžadovat uvedení jména domény. Název domény je požadován pouze tehdy, je-li počítač serveru v jiné doméně než stolní počítače koncového uživatele.
- **ID uživatele a heslo.** Koncoví uživatelé jsou povinni se přihlásit k počítači serveru. K tomu potřebují uživatelé platný účet s příslušnými oprávněními pro počítač, na kterém je spuštěn software serveru.
- **Secure Socket Layer (SSL).** Pokud používáte SSL k šifrování komunikací, které se vyskytnou, když se koncoví uživatelé připojí k serverovému softwaru, sdělíte uživatelům, aby aktivovali SSL, když nastaví připojení k serveru. Klienti nepotřebují vědět, který protokol zabezpečení SSL je serverem používán. Klientský software vyzkouší obojí a použije ten, který pracuje.

Přístup k datům a souborům

Když se koncoví uživatelé připojují k softwaru analytického serveru, jejich zobrazení zdrojů dat a souborů pochází z perspektivy počítače serveru, nikoli na stolních počítačích.

- **Zdroje dat ODBC .** Pokud vaši koncoví uživatelé potřebují přístup ke zdrojům dat ODBC definovaným na počítači serveru, distribuujte tyto názvy, popisy a přihlašovací informace pro tyto zdroje dat. Informace o přístupu k databázi ze softwaru serveru najdete v tématu [Kapitola 3, “Přístup k datům”](#), na stránce 9 .
- **Přístup k souboru.** Rozdělte názvy a umístění souborů na serverovém počítači, ke kterému chcete koncovým uživatelům přistupovat. Další informace naleznete v tématu [“Odkazující data”](#) na stránce 10 .

Ukládání dat a souborů

Když koncoví uživatelé ukládají soubory, zatímco jsou připojeni k serverovému softwaru, výchozím umístěním pro uložení je adresář, ze kterého byl soubor otevřen. V mnoha případech se jedná o lokální stolní počítač, avšak pro datové soubory bude v počítači serveru často na počítači serveru chráněné místo zápisu. Informujte uživatele o tom, kam mají být uloženy datové soubory. V typickém případě se jedná o domovský adresář uživatele, který je někde na vaší síti.

Poznámka k systému UNIX: Sdělte koncovým uživatelům použití úplné specifikace souboru a dopředných lomítek při ukládání souborů (například `/public/myhome/myserverdata/data/data/data.sav`). Vyvarujte se použití znaku zpětného lomítka v adresáři systému UNIX a názvů souborů použitých se serverovým softwarem.

Kapitola 6. Analýza a zlepšení výkonu

Potřebujete-li zlepšit výkon softwaru serveru, prostudujte si tuto kapitolu pro různé strategie, od konfiguračních změn až po přechod na vyšší verzi hardwaru. Před provedením těchto změn získajte informace o výkonu, abyste věděli, které oblasti jsou problematické.

Poskytlí jsme také dokument White paper, který obsahuje další informace o zlepšení výkonu. Přejděte na adresu <http://www.ibm.com/developerworks/spssdevcentral> a vyhledejte odkaz na "Knihy a články."

Získávání informací o výkonu

Chcete-li zkontrolovat výkon, porovnejte využití v následujících oblastech, když se server nepoužívá, když je intenzivně využíván.

- Využití disku
- Využití CPU
- Využití paměti
- Využití sítě

Protokolování

Aplikace administrace (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager) vám umožňuje konfigurovat serverový software tak, aby protokoloval informace o výkonu. Pomocí uzlu **Interval protokolu výkonu** můžete uvést, jak často software serveru zapisuje informace o výkonu do protokolu. Další informace naleznete v tématu Protokolování v příručce *Deployment Manager User's Guide* (je obsažena v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Informace o výkonu můžete také získat přímo z operačního systému.

Získávání informací o výkonu v systému Windows

V systému Windows můžete získat informace o výkonu pomocí nástroje Sledování výkonu.

Oblast	Objekt monitoru výkonu systému Windows	Užitečný čítač
Využití disku	Fyzický disk	Doba nečinnosti v%
Využití CPU	Procesor	Čas procesoru v procentech
Využití paměti	Paměť	Potvrzené bajty
Využití sítě	Síťové rozhraní	Celkem bajtů/sek pro každou instanci fyzického rozhraní (nikoli se smyčkovým rozhraním MS TSP)

Získání informací o výkonu na systému UNIX

V systému UNIX jsou k dispozici různé příkazy pro získání informací o výkonu, v závislosti na dodavateli.

Tabulka 4. Informace o výkonu UNIX

Oblast	Dodavatel	Příkaz	Poznámka
Využití disku	Linux	iostat -x	Zkontrolujte sloupec %util .
Využití disku	AIX	iostat -d	Zkontrolujte sloupec %tm_actl .
Využití CPU	Linux	top	Použijte interaktivní příkaz P k řazení podle využití CPU.
Využití CPU	AIX	ps aux	Chcete-li řadit podle sloupce %CPU , příkaz sort seřadí příkaz do řazení do roury.
Využití CPU	ALL	Doba provozu	Zkontrolujte průměr zatížení.
Využití paměti	Linux	top	Použijte interaktivní příkaz M k řazení podle využití CPU.
Využití paměti	AIX	ps aux	Chcete-li provést řazení podle sloupce RSS , použijte příkaz sort .
Využití sítě	ALL	netsat	Chcete-li získat informace, použijte přepínače -i a -s .

Další krok

Po shromáždění těchto informací byste měli být schopni identifikovat oblast nebo oblasti, které jsou problematické. Následující oddíly popisují možná řešení a doporučení pro každou oblast.

Zlepšení využití disku

Zvažte následující možnosti zlepšení využití disku.

Prostor. Povolte dostatek místa na disku. Každý uživatel obvykle potřebuje dočasný prostor na disku, který se rovná dvojnásobku velikosti použitého souboru dat (SAV) (požadovaný prostor je v rozsahu od 1 do 2.5 krát). Třídění uživatele může vyžadovat dočasný prostor o více než trojnásobek velikosti souboru. Například, pokud šest souběžných uživatelů přistupuje k souboru a dva najednou to třídí, mohou potřebovat až sedmnáctinásobku velikosti souboru. V praxi nebudou současně ve špičce, takže by stačilo tak 12krát větší než velikost souboru.

Hardware. Použijte disky SCSI pro nejrychlejší výkon. Nepoužívejte IDE.

Konfigurace systému. Ponechte dočasné soubory na samostatném vřetenu. Pomocí administrativní aplikace můžete také definovat více umístění dočasných souborů. Ujistěte se, že každé umístění je na samostatném vřetenu. Používáte-li pole RAID, použijte pro dočasné vřetene souboru hodnotu RAID0 . Rychlost pracovních souborů získaná z RAID0 se upřednostňuje před redundancí získanou z RAID1. Pokud váš CPU není problém a serverový počítač spouští systém Windows, můžete také komprimovat datový adresář nebo datové soubory na disku. Nepřidělujte více virtuální paměti.

Konfigurace produktu IBM SPSS Statistics . Pokud paměť není problém, ale využití disku je, zvyšte pracovní prostor v produktu IBM SPSS Statistics kvůli rychlejšímu výkonu. Pokuste se jej nastavit vydělením množství paměti RAM na počítači serveru očekávaným počtem souběžných uživatelů. Například, pokud má počítač serveru 1 GB paměti RAM, nastavte pracovní prostor na 0,25 GB RAM.

Adresář dočasných souborů. Upravte nastavení profilu uživatele nebo skupiny tak, aby se adresáře dočasných souborů pro každého uživatele nacházeli na různých fyzických discích.

Komprese mezipaměti. Pokud uživatelé trvale pracují s velkými datovými soubory (zejména pokud je velikost souborů větší než polovina paměti RAM serveru), zkuste povolit komprimaci mezipaměti v aplikaci administrace.

Zlepšení využití CPU

Zvažte následující možnosti zlepšení využití procesoru:

Číslo. Přidejte více procesorů. Chcete-li přistupovat k rychlosti, kterou by uživatel setoval při lokálním spuštění produktu IBM SPSS Statistics, pokuste se mít jeden procesor pro každý dva souběžné uživatele. Také použijte procesory, které jsou stejně rychlé jako procesor na stolním počítači nebo rychlejší než procesor. Očekáváte-li například průměr čtyř souběžných uživatelů, nakonfigurujte počítač serveru se dvěma procesory typu fast.

Hardware. Používejte rychlé procesory. Přidání několika opravdu rychlých procesorů je lepší než přidání mnoha pomalých procesorů. Je-li využití procesoru stále problém s rychlými procesory, zvažte přidání více serverových počítačů do systému.

Umístění souborů SAV a přístup. Jsou-li určité soubory často používány mnoha souběžnými uživateli, zvažte přesunutí souborů mezi více serverů, abyste vyrovnali zatížení uživatelů. Pokud jsou například *TestScores.sav* a *GPA.sav* intenzivně používány, umístěte je na samostatné servery. Řízení přístupu k souborům s oprávněními operačního systému (pro skupinu nebo pro uživatele) namísto řízení přístupu prostřednictvím účtů serveru.

Priorita CPU. Pokud určití uživatelé potřebují vyšší prioritu CPU než ostatní uživatelé (například uživatelé, kteří spouštějí rychlé úlohy oproti těm, kteří spouštějí dlouhé úlohy), upravte nastavení profilu uživatele nebo skupiny.

Komprese mezipaměti. Komprese mezipaměti má určité zatížení procesoru pro kompresi a dekompresi pracovních souborů. Pokud vaši uživatelé nepracují s velkými datovými soubory, možná budete chtít tuto operaci vypnout.

Zlepšení využití paměti

Při zvyšování využití paměti vezměte v úvahu následující skutečnosti:

Počet. Přidejte co nejvíce paměti RAM. Zkuste mít 128 MB paměti RAM pro každého souběžného uživatele. Takže, pokud existují čtyři souběžné uživatele, nakonfigurujte server s 512 MB paměti RAM.

Konfigurace produktu IBM SPSS Statistics. Snižte pracovní prostor v produktu IBM SPSS Statistics.

Zlepšení využití sítě

Při zvyšování využití sítě vezměte v úvahu následující skutečnosti:

Konfigurace systému. Plánování operací náročných na síť pro dobu, kdy se software serveru nepoužívá (například, spusťte zálohování systému přes noc). Pokud identifikujete problém se síťovým provozem na počítači, na kterém je server spuštěný, produkt IBM Corp. s vámi bude pracovat k diagnostice problému dále.

Použití produktu IBM SPSS Statistics Efficiently

Kromě zaměření se na specifické problematické oblasti můžete také zlepšit výkon tím, že dodržíte níže uvedené pokyny pro efektivní použití produktu IBM SPSS Statistics.

Správa dat. Máte-li velké datové soubory, které vyžadují pravidelnou aktualizaci a jsou sdíleny uživateli, zvažte provedení aktualizací jednou a potom tyto soubory uvolníte uživatelům k analýze. Pokud například pravidelně přidáváte měsíční data do souboru, třídíte ji a provádíte transformace, označte jednu osobu,

která spustí úlohu na daném souboru. Ostatní uživatelé mohou získat data, která potřebují, aniž by museli opakovat sloučení, třídění a transformace.

Interaktivní vs. dávkové zpracování. Pokud máte pravidelné a časově náročné operace, které provádíte s produktem IBM SPSS Statistics, zvažte jejich spuštění z produktu IBM SPSS Statistics Batch Facility, spíše než z klienta připojeného k serveru. Použijte klienta pro sestavení sestav a spusťte je z produktu IBM SPSS Statistics Batch Facility poté, co jsou sestavy připraveny.

Dodatek A. Odstraňování problémů

Serverový software

Konflikt čísel portů. Dojde-li ke konfliktu číslo portu, může se stát, že se software serveru nespustí. Opravte problém pomocí administrativní aplikace (IBM SPSS Statistics Administration Console, která je nainstalována jako součást produktu IBM SPSS Deployment Manager), a změňte tak číslo portu. Další informace naleznete v tématu Connections v příručce *Deployment Manager User's Guide* (je obsažena v nápovědě k produktu IBM SPSS Collaboration and Deployment Services). Ujistěte se, že jste distribuovali nové číslo portu koncovým uživatelům.

Vyzpytatelné chování. Software serveru se může chovat neskutečně, je-li jeho konfigurační soubor (například *statisticsd.conf*) poškozen nebo chybí. Chcete-li opravit tento problém, obnovte konfigurační soubor ze záložní kopie. Zkopírujte jej do umístění určeného v aplikaci administrace nebo do proměnné prostředí konfiguračního souboru a restartujte software serveru. Informace o restartování naleznete v tématu [“Spuštění a zastavení softwaru serveru”](#) na stránce 19 .

Aplikace administrace nefunguje (pouze systém UNIX). Pokud k řízení nebo konfiguraci softwaru serveru používáte administrativní aplikaci a nefunguje (například nemůžete server zastavit), může to být proto, že jste nespustili software serveru se spouštěcím skriptem poskytovaného produktem IBM Corp.. Opravte problém spuštěním softwaru serveru se spouštěcím skriptem *start_statistics_server* . Další informace naleznete v tématu [“Zastavení služby nebo démona”](#) na stránce 19 . Obdržíte-li chybovou zprávu při pokusu o řízení nebo konfiguraci softwaru serveru, může to být způsobeno tím, že jste se připojili k účtu, který nemá oprávnění administrátora.

Nelze změnit umístění dočasných souborů (pouze UNIX). Pokud použijete aplikaci pro správu ke změně umístění dočasných souborů a změna není účinná, může to být způsobeno tím, že nové umístění nemá dostatečná oprávnění k souboru pro koncové uživatele. Vyberte umístění, které má přístup **read**, **write** a **execute** pro všechny uživatele, kteří se budou připojovat k softwaru serveru.

Server se nespustí (pouze UNIX). Pokud se software serveru nespustí, může to být způsobeno tím, že nemáte požadované opravy operačního systému. Chcete-li opravit tento problém, stáhněte a nainstalujte odpovídající opravu. Požadované opravy jsou uvedeny v pokynech k instalaci systému UNIX pro váš serverový produkt.

Software klienta

Koncový uživatel se nemůže připojit k serveru. Je možné, že uživatel nemá odpovídající oprávnění, nebo že brána firewall blokuje serverový software. Další informace o uživatelských oprávněních naleznete v tématu [“Oprávnění”](#) na stránce 28 . Informace o konfiguraci brány firewall naleznete v tématu [“Konfigurace připojení přes bránu firewall”](#) na stránce 30 .

Přihlášení koncového uživatele se nezdařilo se zprávou "zadaný počítač vzdáleného serveru nebyl nalezen". Je možné, že služba nebo démon nejsou spuštěny. Potvrdíte to tak, že zkontrolujete stav serverového softwaru. Chcete-li opravit tento problém, restartujte službu nebo démona. Další informace naleznete v tématu [“Spuštění a zastavení softwaru serveru”](#) na stránce 19 .

Přihlášení koncového uživatele se nezdaří a zobrazí se zpráva "chyba připojující se k balíku". Koncový uživatel zadal název nebo adresu IP počítače serveru, který není v síti. Chcete-li opravit tento problém, požádejte koncového uživatele o zadání platného názvu serveru.

Zdroj dat produktu DataDirect ODBC selže se zprávou "není licencováno". Technologie pro přístup k datům DataDirect se distribuuje s produkty IBM Corp. . Pracuje pouze s novějšími produkty IBM Corp. -nefunguje s dřívějšími verzemi, ani nefunguje s aplikacemi jiného typu než IBM Corp. . Pokud se koncoví uživatelé pokusí použít zdroje dat DataDirect se starším nebo nelicencovaným produktem, obdrží zprávu obsahující text **Nejste licencováni k použití ovladače DataDirect ODBC Driver**. Chcete-li opravit problém s produktem IBM Corp. , upgradujte své uživatele na aktuální verzi. Chcete-li opravit

problém s nelicencovanými produkty, proveďte upgrade licencí s produktem DataDirect nebo se dotázejte koncových uživatelů, aby se nepokoušely použít zdroje dat, které jste definovali pro produkty IBM Corp. s nelicencovanými aplikacemi.

Koncový uživatel nemůže najít datový soubor nebo zdroj dat ODBC . Když jsou koncoví uživatelé spuštěni v distribuovaném režimu analýzy, budou mít přístup pouze k datovým souborům a zdrojům dat ODBC na počítači, na kterém běží serverový software. Když jsou koncoví uživatelé spuštěni v režimu lokální analýzy, budou mít přístup pouze k datovým souborům a zdrojům dat ODBC na svých stolních počítačích. Chcete-li opravit tento problém, požádejte koncového uživatele o spuštění aplikace klienta v odpovídajícím režimu.

Koncový uživatel nemůže spustit statistickou proceduru (pouze IBM SPSS Statistics Server). Jsou-li koncoví uživatelé připojeni k softwaru serveru, mají přístup pouze k volbám produktu IBM SPSS Statistics , které byly nainstalovány během instalace serveru IBM SPSS Statistics . Chcete-li opravit tento problém, požádejte koncového uživatele, aby spustil proceduru v režimu lokální analýzy, nebo nainstalujte požadovanou proceduru na počítač serveru.

Dodatek B. Dávkové zařízení IBM SPSS Statistics

Poznámka: Produkt IBM SPSS Statistics Batch Facility je obslužný program dávkového zpracování zahrnutý se serverem **IBM SPSS Statistics Server**.

Klient pro produkt IBM SPSS Statistics Server je zpravidla IBM SPSS Statistics spuštěný na stolním počítači. Produkt IBM SPSS Statistics Batch Facility je však alternativním způsobem použití moci serveru IBM SPSS Statistics a jeho spuštění na počítači serveru. Produkt IBM SPSS Statistics Batch Facility je určen pro **automatizovanou produkci** statistických sestav. Automatizovaná produkce poskytuje možnost provádět analýzy bez zásahu uživatele. Automatizovaná produkce je výhodná, pokud uživatelé na vašem místě pravidelně vyžadují soubor časově náročných rozborů, jako jsou týdenní zprávy.

Dávkový prostředek IBM SPSS Statistics bere jako svůj vstup požadavek na sestavu obsažený v souboru **syntaxe příkazu** . Produkt IBM SPSS Statistics Batch Facility pak automaticky vytvoří statistické sestavy určené syntaxí.

Co potřebujete vědět

Operační systémy. Produkt IBM SPSS Statistics Batch Facility je v současné době dostupný se všemi servery IBM SPSS Statistics , systémy UNIX a Windows.

Instalace. Produkt IBM SPSS Statistics Batch Facility je automaticky nainstalován v instalačním adresáři serveru IBM SPSS Statistics v systému Windows a v podadresáři */bin* instalačního adresáře v systému UNIX.

Vyvolání. Nástroj IBM SPSS Statistics Batch Facility se spouští z příkazového řádku pomocí spustitelného souboru *statisticcsb* . Běží nezávisle na produktu IBM SPSS Statistics Server-IBM SPSS Statistics Server nemusí být spuštěn, aby mohl být spuštěn. Lze ji také spustit souběžně s produktem IBM SPSS Statistics Server.

Režimy provozu. Příkazy jsou odeslány do zařízení IBM SPSS Statistics Batch Facility buď v **batch** , nebo v **interactive mode** . V dávkovém režimu analytiků nebo profesionální IT odešle soubor se syntaxí příkazu do IBM SPSS Statistics Batch Facility pro provedení-příkazy v souboru jsou čteny a zpracovávány jako dávková dávka a výstup je směřován do souboru. Produkt IBM SPSS Statistics Batch Facility je spuštěn bez obsluhy a po provedení posledního příkazu je ukončen. Jedná se o typický způsob použití nástroje IBM SPSS Statistics Batch Facility. V interaktivním režimu se v příkazovém řádku na příkazovém řádku zadává příkaz jeden po druhém. Příkazy se provedou okamžitě a výstup se zobrazí v okně. Produkt IBM SPSS Statistics Batch Facility čeká na další příkaz.

Dokumentace. Uživatelská příručka, určená analytikům a profesionálům v oblasti IT na organizační jednotce, která bude používat produkt IBM SPSS Statistics Batch Facility, je na serveru IBM SPSS Statistics DVD v */Documentation/ < language>/manuals* . Referenční příručka syntaxe příkazů, kterou analytici potřebují, aby mohli vytvořit soubory syntaxe příkazu pro produkt IBM SPSS Statistics Batch Facility, je na serveru IBM SPSS Statistics DVD v */Documentation/ < language>/manuals* . Produkt IBM SPSS Statistics Batch Facility for UNIX je také distribuován s ruční stránkou *statisticcsb.1* , která se nachází v podadresáři */bin* v instalačním adresáři serveru IBM SPSS Statistics . Pokud provádíte administraci systému UNIX, zkopírujte jej do umístění, do kterého chcete uchovávat své manuálové stránky.

Další dokumentace. Uživatelská příručka produktu IBM SPSS Statistics Batch Facility obsahuje dostatečné informace pro analytika, který má zkušenosti s jazykem syntaxe příkazu IBM SPSS Statistics k sestavení souborů syntaxe příkazu pro produkt IBM SPSS Statistics Batch Facility. Jsou-li analytici na vašem webu nové pro produkt IBM SPSS Statistics, mohou vyžadovat další dokumentaci. Pokud ano, nasměrovat je na naše webové stránky na adrese <http://www.ibm.com/software/analytics/spss/> nebo je požádat, aby se obrátili na obchodního zástupce.

Dodatek C. Úlohy operačního systému Windows

Můžete provádět většinu administrativních úloh pomocí administrativní aplikace ; je však možné, že bude třeba provést několik úloh s operačním systémem Windows. Použijte následující funkce operačního systému k administraci serverového softwaru spuštěného na systému Windows:

- **Vlastnosti souboru.** Používá se k nastavení přístupu koncových uživatelů k instalačnímu adresáři softwaru serveru, k dočasnému umístění souboru a k datovým souborům.
- **Systémové vlastnosti.** Používá se k vytvoření proměnných prostředí.
- **Správce uživatelů.** Používá se k vytvoření účtů koncového uživatele.
- **Ovládací panel služeb.** Používá se ke spuštění, zastavení a konfiguraci služby.
- **ODBC Administrator.** Používá se ke konfiguraci zdrojů dat.

Vlastnosti souboru

Chcete-li nastavit oprávnění pro soubory, použijte Vlastnosti souboru. Způsob použití datových souborů závisí na tom, kde jsou data uložena. Když ukládáte data na stejném počítači jako serverový software, můžete řídit přístup k datovému adresáři nastavením oprávnění k adresáři na jednotce NTFS.

Na serverovém počítači se přihlašte jako administrátor:

1. Použijte Průzkumníka Windows pro přechod do datového adresáře.
2. Klepněte na adresář, klepněte pravým tlačítkem myši a v kontextové nabídce klepněte na volbu **Sdílení**.
3. Klepněte na kartu **Zabezpečení** a nakonfigurujte oprávnění.

Poznámka: Karta Zabezpečení je k dispozici pouze na jednotkách NTFS. Pokud si nejste jisti, jaký typ systému souborů váš hardware používá, proveďte následující kroky:

4. K přechodu na jednotku použijte Průzkumníka Windows.
5. Klepněte na jednotku, pravým tlačítkem myši a poté klepněte na volbu **Vlastnosti** v kontextové nabídce.
6. Klepněte na kartu **Obecné** a podívejte se na hodnotu v systému souborů.

Když ukládáte data na počítač ve vaší síti, můžete řídit přístup k datovému adresáři vytvořením sdíleného prostředku a nastavením příslušných oprávnění.

Na síťovém počítači se přihlašte jako administrátor:

7. Použijte Průzkumníka Windows pro přechod do datového adresáře.
8. Klepněte na adresář, klepněte pravým tlačítkem myši a v kontextové nabídce klepněte na volbu **Sdílení**.
9. Klepněte na kartu **Sdílení** v dialogovém okně, klepněte na volbu **Sdílené jako**, zadejte název sdílené položky a nastavte příslušný přístup.

Vlastnosti systému

K vytvoření proměnných prostředí použijte systémové vlastnosti.

Na serverovém počítači se přihlašte jako administrátor:

1. Na pracovní ploše Windows klepněte pravým tlačítkem myši na ikonu počítače. Klepněte například pravým tlačítkem myši na **Můj počítač**.
2. Z nabídky vyberte volbu **Vlastnosti**.
3. Klepněte na kartu **Rozšířené** a poté klepněte na volbu **Proměnné prostředí**.

4. Klepněte na volbu **Nový**.
5. Zadejte název nové proměnné.
6. Zadejte hodnotu nové proměnné.

Správce uživatelů

K vytvoření účtů koncového uživatele použijte správce User Manager.

Na serverovém počítači se přihlašte jako administrátor:

1. V nabídce Start systému Windows vyberte:

Programy > Administrativní nástroje

- Vyberte volbu **Správa počítače** a poté **Lokální uživatelé a skupiny**.

2. Vytvořte uživatelské účty.

Ovládací panel služeb

Použijte ovládací panel služeb systému Windows, abyste:

- Zastavte a spusťte službu.
- Změňte parametry spuštění služby.
- Zkontrolujte stav serveru.

Přístup k ovládacímu panelu služeb a jeho použití:

1. V nabídce Start systému Windows vyberte:

Nastavení > Ovládací panely

2. Vyberte volbu **Administrativní nástroje** a poté **Služby**.
3. Vyberte službu. Nyní můžete zkontrolovat jeho stav, spustit nebo zastavit jej a upravit parametry spuštění.

Poznámka: Můžete spustit, zastavit a zkontrolovat stav serverového softwaru s aplikací administrace.

Správce úloh

Použijte Správce úloh k zobrazení, kolik procesů souvisejících se serverem je spuštěno.

1. Otevřete správce úloh systému Windows stisknutím kombinace kláves Ctrl-Alt-Delete a výběrem volby **Správce úloh**.
2. Klepněte na kartu **Procesy**.
3. Klepnutím na **Název obrazu** seřadíte procesy podle abecedy.
4. Vyhledejte název souboru procesu serveru (*statisticsrvr.exe*).
5. Vyhledejte název souboru procesu klienta (*statisticproc.exe*). Pro každého koncového uživatele, který je momentálně připojen k serverovým softwaru, je jeden proces.

Pozn.: Server a klientské procesy můžete monitorovat pomocí administrativní aplikace.

Administrátor ODBC

Pomocí administrátora ODBC můžete konfigurovat systémové a uživatelské zdroje dat pro použití se serverovým softwarem.

Jak se zdroj dat ODBC vytváří, ovlivní, kdo jej může zobrazit a použít. Pokud chcete povolit obecný přístup ke zdroji dat, použijte *systémové* DSN. Chcete-li omezit přístup k citlivým informacím nebo chcete-li upravit DSN pro určitého uživatele, použijte názvy DSN *uživatele*.

Chcete-li konfigurovat systémový název DSN

Systémové názvy DSN mohou být používány uživatelem, který je přihlášen k počítači, na kterém jsou definovány. Systémové DSN jsou pro vás jednodušší konfigurovat a spravovat, protože to pro všechny uživatele provádíte pouze jednou.

Na počítači, na kterém se má zdroj dat nacházet, se přihlašte jako administrátor:

1. V nabídce Start systému Windows vyberte:

Nastavení > Ovládací panely

2. Vyberte volbu **Administrativní nástroje** a poté **Zdroje dat**.

3. Klepněte na kartu **Systémové DSN**.

4. Klepněte na tlačítko **Přidat**.

5. Vyberte ovladač ze seznamu. Pokud konfigurujete zdroj dat, který používá technologii přístupu k datům produktu IBM Corp. , názvy ovladačů ODBC Connect jsou označeny popiskem s textem IBM Corp. OEM.

6. Klepněte na tlačítko **Dokončit**.

7. Zadejte příslušné informace do dialogového okna **Nastavení ovladače** .

8. Klepněte na tlačítko **OK**.

Chcete-li konfigurovat uživatelské DSN

Uživatelské názvy DSN lze použít pouze v účtu uživatele, který je vytvořil. Chcete-li omezit přístup k citlivým informacím nebo chcete-li upravit DSN pro určitého uživatele, konfigurujte uživatelské DSN.

Přihlaste se jako uživatel a postupujte podle kroků pro systémový název DSN, s touto výjimkou:

- Klepněte na kartu **Uživatel DSN** místo na kartě **Systémové DSN** .

Dodatek D. Úlohy operačního systému UNIX

Můžete provádět většinu administrativních úloh pomocí administrativní aplikace ; je však možné, že bude třeba provést několik úloh s operačním systémem UNIX. Použijte následující funkce operačního systému k administraci softwaru serveru spuštěného na systému UNIX:

- **chmod**. Používá se k nastavení přístupu koncových uživatelů k datovým souborům.
- **env**. Používá se ke kontrole hodnot proměnných prostředí.
- **skripty**. Používá se ke spuštění softwaru serveru a ke konfiguraci jeho prostředí.
- **ps a kill**. Používá se ke kontrole a zastavení procesů serveru.
- **odbc.ini**. Používá se ke konfiguraci zdrojů dat ODBC .

chmod

Pomocí příkazu chmod (nebo chown) můžete změnit nebo přiřadit režim oprávnění pro adresáře a datové soubory. Chcete-li například nastavit adresář `/usr/data` pouze pro čtení pro všechny, postupujte takto:

1. Přihlaste se jako super-uživatel nebo jako vlastník adresáře.
2. Na příkazový řádek UNIX zadejte:

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

prostředí

Chcete-li zkontrolovat aktuální hodnoty proměnných prostředí, použijte příkaz `env` . Chcete-li například použít produkt `env` ke kontrole aktuálních hodnot proměnných prostředí pro software serveru, postupujte takto:

1. Přihlaste se jako účet, který spustil démona, obvykle `root`.
2. Na příkazový řádek UNIX zadejte:
`prostředí`
3. Zkontrolujte nastavení pro požadovanou proměnnou (proměnné).

Skripty

Chcete-li změnit hodnotu proměnných prostředí, upravte skript proměnné prostředí, který je volán skriptem, který spouští software serveru. Chcete-li upravit skript proměnné prostředí:

1. V textovém editoru otevřete skript `statsenv.sh` , který je obsažen v podadresáři `/bin` v instalačním adresáři serveru IBM SPSS Statistics . Například otevřete soubor `/usr/local/myserverproduct/bin/statsenv.sh`.
2. Je-li to nutné, zrušte komentář řádku, který definuje proměnnou, a pak zadejte novou hodnotu proměnné.
3. Uložte soubor.

Příkaz `statsenv.sh` je volán skriptem `start_statistics_server` . Proměnné prostředí nastavené a exportované v souboru `statsenv.sh` mají vliv pouze na procesy spuštěné se skriptem `start_statistics_server` .

ps a kill

Příkaz `ps` se používá k získání informací o tom, které procesy serveru jsou spuštěny, a o hlášení stavu procesu. Příklad:

1. Na příkazový řádek UNIX zadejte:

```
ps -efl.
```

2. Vyhleďte název souboru procesu démona (například *statisticsd*). Tento proces má **UID** uživatele, který spustil proces démona softwaru serveru (obvykle *root*).
3. Vyhleďte název souboru procesu klienta, *statisticcsproc.exe*. Pro každého koncového uživatele, který je momentálně připojen k serverovým softwaru, je jeden proces. Sloupec *UID* zobrazuje ID pro přihlášení koncového uživatele, který vlastní proces klienta.

Chcete-li proces ukončit, použijte příkaz `kill`. Příklad:

4. Přihlaste se jako uživatel, který spustil démona.

5. Na příkazový řádek UNIX zadejte:

```
kill -9 pid
```

kde *pid* je ID procesu daného procesu.

Serverovým softwarovým daemon také automaticky vytvoří soubor, který obsahuje jeho ID procesu. Místo ručního vyhledávání identifikátoru PID pomocí příkazu `ps` můžete tento soubor použít spolu s příkazem `kill` přímo k přímému ukončení procesu démona:

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

Poznámka: Chcete-li použít administrativní aplikaci k monitorování a ukončení procesů, musíte spustit serverový software se spouštěcím skriptem poskytovaného produktem IBM Corp.. Další informace naleznete v tématu [“Řízení spouštění služby”](#) na stránce 17 .

odbc.ini

Je možné, že budete muset konfigurovat zdroje dat ODBC na počítači serveru, pokud:

- Používáte balík IBM Corp. Data Access Pack

a

- Software serveru potřebuje přístup k databázím

V systému UNIX neexistuje žádný administrátor ODBC . Chcete-li konfigurovat zdroj dat ODBC v systému UNIX, můžete upravit textový soubor s informacemi o systému *odbc.ini*. Obslužný program *ODdbc.ini* je instalován při instalaci balíku pro přístup k datům pro systém UNIX. Pokyny k instalaci se zobrazí v příručce *IBM Corp. Data Access Pack Installation Instructions for Unix.pdf* (dokument je umístěn v adresáři */Documentation/ < language>/InstallationDocuments* na produktu DVD). Nezapomeňte nainstalovat další dokumentaci, abyste měli přístup k dokumentům uvedeným níže.

Připojte ODBC. Informace o úpravě souboru *odbc.ini* a nastavení důležitých proměnných prostředí naleznete v části "Configuring Drivers and Data Sources" v kapitole "Installation on UNIX" v kapitole *Connect ODBC Installation Instructions* , kde naleznete podrobné pokyny.

Dokumentace produktu DataDirect pro připojení ODBC je standardně zahrnuta jako součást instalace produktu IBM SPSS Data Access Pack . Instalační program vytvoří položku IBM SPSS OEM Connect a ConnectXE for ODBC spolu s položkami pro ostatní programy v nabídce Start. K dokumentaci k produktu DataDirect získáte přístup z této položky nabídky.

Dokumentaci k produktu DataDirect pro připojení ODBC lze nalézt v adresáři, do kterého jste extrahovali soubory.

Pozn.: K dokumentaci lze také přistoupit z domovské stránky DataDirect na <http://www.datadirect.com> .

Upozornění

Tyto informace byly vytvořeny pro produkty a služby poskytované v USA. Tento materiál může být dostupný od IBM v jiných jazycích. K povolení přístupu však může být vyžadováno vlastnictví kopie produktu nebo verze produktu v tomto jazyce.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou aktuálně k dispozici ve vaší oblasti, získáte od lokálního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM neuvádí ani neimplikují, že lze použít pouze daný produkt, program nebo službu společnosti IBM. Lze použít libovolný funkčně ekvivalentní produkt, program nebo službu neporušující práva duševního vlastnictví společnosti IBM. Vyhodnocení a ověření funkčnosti produktů, programů nebo služeb, které nepatří společnosti IBM, je však zodpovědností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy na licence můžete písemně odeslat na následující adresu:

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

S dotazy na licence týkající se dvoubajtových informací (DBCS) se obraťte na oddělení intelektuálního vlastnictví společnosti IBM v dané zemi, nebo je odešlete písemně na následující adresu:

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

SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION POSKYTUJE TUTO PUBLIKACI "TAKOVOU, JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, MIMO JINÉ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás výše uvedené omezení nemusí vztahovat, a proto se vás toto prohlášení nemusí týkat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek. Materiály uvedené na těchto webových stránkách nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoli informace, které jí poskytnete, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

*IBM Director of Licensing
IBM Corporation*

North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

Licencovaný program popsáný v tomto dokumentu a veškerý licencovaný materiál k němu dostupný jsou společností IBM poskytovány na základě podmínek uvedených ve smlouvách IBM Customer Agreement, IBM International Program License Agreement nebo v jiné ekvivalentní smlouvě.

Citovaná data o výkonu a příklady klienta jsou uvedeny pouze pro názornost. Skutečné výsledky výkonu se mohou lišit v závislosti na specifických konfiguracích a provozních podmínkách.

Informace týkající se produktů jiných společností než IBM byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže potvrdit přesnost údajů o výkonu, kompatibilitě nebo jiná tvrzení týkající se produktů jiných společností než IBM. Otázky týkající se možností produktů jiných společností než IBM by měly být adresovány dodavatelům těchto produktů.

Prohlášení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou změnit nebo mohou být zrušena bez předchozího upozornění a představují pouze cíle a záměry.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob, společností, značek a produktů. Všechna tato jména jsou fiktivní a jakákoliv podobnost se skutečnými lidmi nebo obchodními podniky je čistě náhodná.

COPYRIGHT - LICENCE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyku a ilustrují různé programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly důkladně testovány ve všech podmínkách. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů. Ukázkové programy jsou poskytovány "JAK JSOU", bez záruky jakéhokoli druhu. IBM nenes odpovědnost za žádné škody vzniklé ve spojení s Vaším užíváním ukázkových programů.

Jakákoli kopie nebo část těchto ukázkových programů nebo jakékoli odvozené dílo musí obsahovat následující poznámku o autorských právech:

© Copyright IBM Corp. 2021. Části tohoto kódu jsou odvozeny ze vzorových programů společnosti IBM Corp. Vzorové programy.

© Copyright IBM Corp. 1989-2021. Všechna práva vyhrazena.

Ochranné známky

IBM, logo IBM a ibm.com jsou ochranné známky nebo registrované ochranné známky společnosti International Business Machines Corp., registrované v mnoha jurisdikcích po celém světě. Ostatní názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webu na stránce "Copyright and trademark information" na adrese www.ibm.com/legal/copytrade.shtml.

Adobe, logo Adobe, PostScript a logo PostScript jsou buď registrované ochranné známky, nebo ochranné známky společnosti Adobe Systems Incorporated ve Spojených státech anebo v dalších zemích.

Intel, logo Intel, Intel Inside, logo Intel Inside, Intel Centrino, logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium a Pentium jsou ochranné známky nebo registrované ochranné známky společnosti Intel Corporation nebo jejich dceřiných společností ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka společnosti The Open Group ve Spojených státech a případně v dalších jiných zemích.

Java a všechny ochranné známky a loga založené na jazyce Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

Rejstřík

A

administrace [14](#)
administrační aplikace [14](#)
administrátoři systémů
 co musí koncoví uživatelé vědět [21](#)
 přehled administrativních úloh [4](#)
Aplikace klienta
 instalace [7](#)
 odstraňování problémů [47](#)
automatizovaná produkce se serverem IBM SPSS Statistics Server [49](#)
autorizace skupiny [16](#), [29](#)

B

brána firewall [30](#)

C

Certifikáty
 konfigurace [36](#)

Č

číslo portu
 co musí koncoví uživatelé vědět [41](#)
 odstraňování problémů [47](#)

D

distribuovaná architektura [1](#)
distribuovaný režim analýzy
 definované [1](#)
 kroky k použití [1](#)
 zobrazení dat [9](#)

I

IBM SPSS Collaboration and Deployment Services
 náhrada [15](#)
IBM SPSS Statistics Administration Console [14](#)
IBM SPSS Statistics Batch Facility
 to, co potřebujete vědět [49](#)
 úvod do [49](#)
ID uživatele a heslo
 co musí koncoví uživatelé vědět [41](#)
IDE [44](#)
informace o výkonu [43](#)
instalace
 Aplikace klienta [7](#)
 serverový software [7](#)

J

jednotné přihlášení

jednotné přihlášení (*pokračování*)

 Členství ve skupinách [28](#)
 konfigurace klienta [25](#)
 konfigurace serveru [24](#)
 název zásady služby [26](#), [27](#)
 zdroje dat [28](#)

K

koncoví uživatelé
 číslo portu [41](#)
 ID uživatele a heslo [41](#)
 Název domény [41](#)
 název počítače [41](#)
 podpora [21](#)
 přístup k datovému souboru [42](#)
 seznam toho, co potřebují vědět [21](#)
 zdroje dat ODBC [42](#)
konfigurace
 Certifikáty [36](#)
 xtensions [15](#)
konfigurace softwaru serveru [13](#)
Konfigurační soubor
 odstraňování problémů [47](#)

L

lokální režim analýzy
 definované [1](#)
 zobrazení dat [9](#)

N

národní prostředí [40](#)
NAT [30](#)
Název domény
 co musí koncoví uživatelé vědět [41](#)
název počítače
 co musí koncoví uživatelé vědět [41](#)
název zásady služby [26](#), [27](#)
názvy procesů podle produktu [19](#)

O

Odkazy na datový soubor UNC [42](#)
odstraňování problémů
 Aplikace klienta [47](#)
 číslo portu [47](#)
 Konfigurační soubor [47](#)
 přihlášení klienta [47](#)
 serverový software [47](#)
 zdroje dat ODBC [47](#)
oprávnění [28](#)
oprávnění na úrovni administrátora [29](#)
oprávnění uživatele root [22–24](#)
ověření

ověření (*pokračování*)
jednotné přihlášení [24](#)
Operační systém [21](#)
pam [21](#)
unix2 [23](#)
vnitřní [22](#)

P

pam [21](#)
PPTP. [32](#)
pracovní prostor [44](#), [45](#)
Pracovní prostor IBM SPSS Statistics [44](#), [45](#)
procesory [45](#)
produkty a operační systémy [1](#)
profily [30](#)
profily uživatele [30](#)
prostor na disku [44](#)
Prostředí UNIX a přístup k datům [11](#)
protokol tunelového propojení [32](#)
Přídavný ověřovací modul [21](#)
Připojení ODBC
architektura [9](#)
nastavení prostředí systému UNIX pro [11](#)
přehled [9](#)
přístup k datovému souboru
co musí koncoví uživatelé vědět [42](#)
přístup k datům
faktory k posouzení [10](#)
konfigurace zdrojů dat ODBC pro [14](#)
odkazování na data z klientského softwaru [10](#)
ovládání [10](#)
Připojení ODBC [9](#)
v systému UNIX [11](#)
Zdroje dat ODBC pro [10](#)
Přístup k DSN [29](#)

R

RAID [44](#)
RAM [45](#)
RBACANA [23](#)

Ř

řazení [14](#)
řazení jiného dodavatele [14](#)
řízení přístupu dle rolí [23](#)

S

scsi [44](#)
serverový software
administrátoři [29](#)
architektura [1](#)
definované [1](#)
instalace [7](#)
konfigurace [13](#)
konfigurace zdrojů dat ODBC [14](#)
názvy procesů podle produktu [19](#)
odstraňování problémů [47](#)
použití spouštěcího skriptu systému UNIX [17](#)
Products [1](#)

serverový software (*pokračování*)
rutinní údržba [18](#)
řízení spouštění [17](#)
součásti [1](#)
správa účtů a souborů koncových uživatelů [13](#)
spuštění a zastavení [19](#)
více instancí [16](#)
spuštění bez oprávnění uživatele root [22–24](#)
SSO [24](#)
start_statistics_server [17](#)
statistickýb [49](#)
Synchronizovat řazení [14](#)

Š

šifrování
zabezpečení SSL [33](#)

T

technologie přístupu k datům [9](#)

U

Účty [13](#)
úlohy operačního systému, UNIX
použití příkazu env ke kontrole proměnných prostředí [55](#)
použití příkazu chmod k nastavení oprávnění k souboru [55](#)
použití příkazu kill k zastavení procesů serveru [55](#)
použití příkazu ps ke kontrole procesů serveru [55](#)
použití skriptů k nastavení proměnných prostředí [55](#)
použití souboru odbc.ini ke konfiguraci zdrojů dat [56](#)
úlohy operačního systému, Windows
nastavení vlastností souboru [51](#)
pomocí administrátora ODBC [52](#)
použití ovládacího panelu Služby [52](#)
použití správce úloh [52](#)
použití správce User Manager [52](#)
vytvoření proměnných prostředí [51](#)
UNIX
kontrola procesů serveru [55](#)
kontrola proměnných prostředí [55](#)
nastavení oprávnění k souboru [55](#)
Nastavení proměnných prostředí [55](#)
vytvoření a konfigurace zdrojů dat ODBC [56](#)
zastavení procesů serveru [55](#)

V

verze [30](#)
VLOŽIT SKRYTÉ
Výrobní zařízení [15](#)
výkon
zlepšení [43](#)
Výrobní zařízení
VLOŽIT SKRYTÉ [15](#)
Využití CPU
zlepšení [45](#)
využití disku
zlepšení [44](#)
využití paměti
zlepšení [45](#)

využití sítě
zlepšení [45](#)

W

Windows

kontrola procesů serveru [52](#)
kontrola stavu služby [52](#)
nastavení oprávnění k souboru [51](#)
spuštění a zastavení služeb [52](#)
vytvoření a konfigurace zdrojů dat ODBC [52](#)
vytvoření proměnných prostředí [51](#)
vytvoření účtů koncového uživatele [52](#)
změna parametrů spuštění služby [52](#)

X

xtensions

konfigurace [15](#)

Z

zabezpečení

zabezpečení SSL [33](#)

zabezpečení SSL

přehled [33](#)

zabezpečení komunikací [33](#), [37](#)

Zabezpečení SSL [33](#)

zdroje dat

jednotné přihlášení [28](#)

zdroje dat ODBC

a serverový software [11](#)

co musí koncoví uživatelé vědět [42](#)

konfigurace [14](#)

odstraňování problémů [47](#)

zdroje dat ODBC , UNIX

definované v souboru odbc.ini [56](#)

zdroje dat ODBC , Windows

DSN uživatele [52](#)

Systémové DSN [52](#)

zlepšení výkonu [43](#)

Zobrazení dat [13](#)

zobrazovat data [13](#)

