System i

Zabezpečení
SSL (Secure Sockets Layer)

verze 6 vydání 1

System i

Zabezpečení
SSL (Secure Sockets Layer)

verze 6 vydání 1

Poznámka

Před použitím těchto informací a odpovídajícího produktu si přečtěte informace v části “Upozornění”, na stránce 21.

Toto vydání se vztahuje k verzi 6, vydání 1, modifikaci 0 operačního systému i5/OS (5761–SS1) a všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

Obsah

SSL (Secure Sockets Layer)

Toto téma popisuje, jak na serveru používat SSL (Secure Sockets Layer).

iSeries SSL (Secure Sockets Layer) je v současné době odvětvovým standardem podporujícím aplikace pro zabezpečení komunikačních relací v nechráněné síti, jako je například Internet.

Co je nového ve verzi V6R1

Zde můžete zjistit, co jev kolekci témat SSL (Secure Sockets Layer) nového nebo co se změnilo.

Nové informace: System SSL

System SSL je sada generických služeb poskytovaných licenčním interním kódem systému i5/OS za účelem ochrany komunikací TCP/IP pomocí protokolu SSL/TLS. Produkt SSL je těsně spjatý s operačním systémem a kódem soketů a poskytuje dodatečný výkon a zabezpečení.

Byla přidána tato témata popisující System SSL:

- “System SSL” na stránce 15
- “Vlastnosti System SSL” na stránce 15

Nové hodnoty pro System SSL

Byly přidány tyto systémové hodnoty:

- Systémová hodnota SSL: QSSLPCL.
- Systémová hodnota SSL: QSSLCSLCTL.
- Systémová hodnota SSL: QSSLCSL.

Jak poznáte, co je nového nebo co se změnilo

Místa, kde byly provedeny technické změny, jsou označena následujícím způsobem:

- Ikona » označuje, kde nové nebo změněné informace začínají.
- Ikona « označuje, kde nové nebo změněné informace končí.

V souborech PDF můžete na levém okraji vidět revizní značky (|) označující nové nebo změněné informace.

Chcete-li najít další informace o tom, co je v tomto vydání nového nebo co se změnilo, přejděte na téma Sdělení pro uživatele.

Soubor PDF k tématu SSL

Tyto informace lze zobrazit a tisknout ve formátu PDF.

Chcete-li si zobrazit nebo vytisknout PDF verzi tohoto dokumentu, vyberte odkaz SSL (Secure Sockets Layer).

Ukládání souborů ve formátu PDF

Chcete-li soubory ve formátu PDF uložit na pracovní stanici za účelem prohlížení nebo tisku:

1. Klepněte pravým tlačítkem myši na odkaz PDF ve vašem prohlížeči.
2. Klepněte na volbu pro lokální uložení PDF.

3. Vyhledejte adresář, do něhož chcete soubor PDF uložit.
4. Klepněte na **Save** (Uložit).

Stažení produktu Adobe Reader

K prohlížení nebo tisku souborů ve formátu PDF potřebujete mít v systému instalován produkt Adobe Reader. Jeho kopii si můžete stáhnout z webových stránek Adobe (www.adobe.com/products/acrobat/readstep.html) .

Scénáře: SSL

Tyto scénáře byly navrženy za účelem co největšího využití výhod aktivace SSL na platformě systému System i.

Tyto scénáře obsahují příklady, které ilustrují možnosti použití SSL v systémech i5/OS. Po jejich prostudování lépe porozumíte tomu, jak SSL v systému funguje.

Související informace

Scénář: Zabezpečení Telnet pomocí SSL

Scénář: Ochrana soukromých klíčů pomocí šifrovacího hardwaru

Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL

Tento scénář popisuje, jak pomocí SSL zabezpečit spojení mezi vzdáleným klientem a modelem System i používajícím Centrální správu, která je součástí produktu System i Navigator, a funguje jako centrální systém.

Situace:

Firma provozuje lokální síť (LAN), která zahrnuje několik serverů i5/OS. Robert, systémový administrátor této firmy, určil jeden z těchto systémů i5/OS jako centrální systém sítě LAN (dále označovaný jako Systém A). Robert využívá server Centrální správy v Systému A ke správě všech ostatních koncových bodů v síti LAN.

Robert usiluje o připojení k serveru Centrální správy v Systému A pomocí připojení k síti, která je umístěna mimo síť LAN jeho firmy. Robert při práci mnoho cestuje, a když je mimo pracoviště, potřebuje zabezpečené spojení se serverem Centrální správy. V době, kdy není na pracovišti firmy, potřebuje zabezpečené spojení mezi svým počítačem (PC) a serverem Centrální správy. Robert se rozhodne aktivovat SSL na svém počítači a na serveru Centrální správy v Systému A. Takto aktivované SSL zajišťuje, aby se Robert mohl na cestách připojovat k serveru Centrální správy zabezpečeným spojením.

Cíle:

Robert chce zabezpečit spojení mezi svým počítačem a serverem Centrální správy. Nepožaduje další zabezpečení spojení mezi serverem Centrální správy v Systému A a koncovými systémy, které jsou v síti LAN. Ostatní zaměstnanci při práci na pracovišti firmy také nepotřebují další zabezpečení svých spojení se serverem Centrální správy. Robert chce nakonfigurovat svůj počítač a server Centrální správy v Systému A tak, aby jeho připojení používalo autentizaci serveru. Spojení ostatních počítačů a systémů i5/OS v síti LAN se serverem Centrální správy nebudou zabezpečení pomocí SSL používat.

Podrobnosti:

Používané typy autentizace na základě aktivace nebo zablokování SSL na klientském počítači jsou uvedeny v této tabulce:

Tabulka 1. Prvky požadované pro spojení mezi klientem a serverem Centrální správy zabezpečené pomocí SSL

Stav SSL na Robertově počítači	Zadaná úroveň autentizace pro server Centrální správy v Systému A	Spojení SSL aktivní?
SSL vypnutý	Libovolná	Ne
SSL zapnutý	Libovolná	Ano (autentizace serveru)

Autentizace serveru znamená, že Robertův počítač autentizuje certifikát serveru Centrální správy. Robertův počítač funguje při připojování k serveru Centrální správy jako klient SSL. Server Centrální správy funguje jako server SSL a musí prokázat svou totožnost tím, že poskytne certifikát vydaný vydavatelem certifikátů (CA), který je pro Robertův PC důvěryhodný.

Nezbytné podmínky a předpoklady

K zabezpečení spojení mezi svým počítačem a serverem Centrální správy v Systému A musí Robert provést tyto úkoly administrace a konfigurace:

1. Systém A musí splňovat nezbytné předpoklady pro SSL.
2. V systému A je provozován systém i5/OS verze V5R3 nebo novější.
3. Na PC klientu je provozován System i Navigator for System i Access for Windows verze V5R3 nebo vyšší verze.
4. Získání vydavatele certifikátu (CA) pro modely systémů i5/OS.
5. Vytvoření certifikátu pro Systém A podepsaného vydavatelem certifikátu (CA).
6. Odeslání vydavatele certifikátu (CA) a certifikátu do Systému A a jeho import do databáze klíčů.
7. Přiřazení certifikátů pomocí identifikace Centrální správy a identifikace systému pro všechny systémy i5/OS. K systémům i5/OS patří všechny tyto servery: centrální server TCP, databázový server, server datových front, souborový server, server síťového tisku, server vzdálených příkazů a přihlašovací server.
   a. V Systému A spustíte program IBM DCM (Digital Certificate Manager). Tímto způsobem Robert nyní může získat nebo vytvořit certifikáty, popř. jinak nastavit nebo změnit svůj systém certifikátů.
   b. Klepněte na volbu **Vybrat paměť certifikátů**.
   c. Vyberte ***SYSTEM** a klepněte na **Pokračovat**.
   d. Zadejte *Heslo paměti certifikátů* pro *SYSTEM a klepněte na **Pokračovat**. Jakmile se znovu načte nabídka, rozbalte volbu **Spravovat aplikace**.
   e. Klepněte na volbu **Aktualizace přiřazení certifikátu**.
   f. Vyberte **Server** a klepněte na **Pokračovat**.
   g. Vyberte **Server Centrální správy** a klepněte na **Aktualizace přiřazení certifikátu**. Tím přiřadíte certifikát k požadovanému serveru Centrální správy.
   h. Klepněte na volbu **Přiřazení nového certifikátu**. Produkt DCM se znovu zavede na stranu Aktualizace přiřazení certifikátu se zprávou o potvrzení.
   i. Klepněte na **Provedeno**.
   j. Přiřaďte tento certifikát všem serverům s přístupem klientů.
8. Stáhněte si vydavatele certifikátů (CA) do klientského počítače.

Aby mohl Robert aktivovat SSL na serveru Centrální správy, musí v systému nejprve nainstalovat programy nezbytné pro použití SSL a nastavit digitální certifikáty. Jakmile splní všechny nezbytné předpoklady, může pomocí následujících postupů aktivovat SSL na serveru Centrální správy.

Postup při konfiguraci

Při zabezpečování spojení klientského počítače se serverem Centrální správy v systému A pomocí SSL bude Robert postupovat takto:

1. “Krok 1: Deaktivace SSL pro klienta System i Navigator” na stránce 4

2. “Krok 2: Nastavení úrovně autentizace pro server Centrální správy”
3. “Krok 3: Restart systému Centrální správy v centrálním systému” na stránce 5
4. “Krok 4: Aktivace SSL pro klienta System i Navigator” na stránce 5
5. “Volitelný krok: Deaktivace SSL pro klienta System i Navigator” na stránce 5

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 18
Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

Související informace

Konfigurace DCM

Spuštění DCM (Digital Certificate Manager)

Podrobnosti konfigurace: Zabezpečení spojení klienta se systémem Centrální správy pomocí SSL

Toto téma uvádí postup při konfiguraci zabezpečení spojení klienta se serverem Centrální správy pomocí SSL.

Následující informace vycházejí z předpokladu, že jste si přečetli téma Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL.

V tomto scénáři je jako centrální systém v lokální síti (LAN) firmy určen model System i. Robert používá server Centrální správy v centrálním systému (který se zde nazývá Systém A) ke správě koncových bodů ve firemní síti. V následujících informacích je vysvětleno, jak provést jednotlivé kroky potřebné k zabezpečení připojení externího klienta k serveru Centrální správy. Společně s Robertem provádějte jednotlivé kroky konfigurace pro tento scénář.

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 18
Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

“Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL” na stránce 5
Tento scénář popisuje, jak pomocí SSL zabezpečit všechna spojení s modelem systému System i používajícím Centrální správu, která je součástí produktuSystem i Navigator, a funguje jako centrální systém.

Související informace

Prvotní nastavení certifikátů

Krok 1: Deaktivace SSL pro klienta System i Navigator:
Tento krok je nezbytný v případě, že máte již na klientovi produktu System i Navigator nastaven protokol SSL.

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na Systém A a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a zrušte výběr volby **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt System i Navigator a opět jej spusťte.

V sekci Centrální správa v prostředí produktu System i Navigator, zmizí zobrazený zámek, což indikuje nezabezpečené připojení. Robert tak pozná, že mezi jeho klientem a centrálním systémem jeho firmy nadále neexistuje spojení zabezpečené pomocí SSL.

Krok 2: Nastavení úrovně autentizace pro server Centrální správy:

1. V prostředí produktu System i Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte na kartu **Zabezpečení** a vyberte **Použít SSL (Secure Sockets Layer)**.
3. Pro úroveň autentizace vyberte volbu **Libovolná** (je k dispozici v produktu System i Access for Windows).
4. Klepněte na **OK** a nastavte tuto hodnotu v centrálním systému.

Krok 3: Restart systému Centrální správy v centrálním systému:

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. V systému A rozbalte **Síť-->Servery** a vyberte **TCP/IP**.
3. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**. Okno centrálního systému se zavře a zobrazí se zpráva, že nejste připojeni k serveru.
4. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

Krok 4: Aktivace SSL pro klienta System i Navigator:

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na Systém A a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a vyberte volbu **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt System i Navigator a opět jej spusťte.

V prostředí produktu System i Navigator se u serveru Centrální správy objeví zámek, což indikuje připojení zabezpečené pomocí SSL. Robert tak pozná, že úspěšně aktivoval spojení mezi svým klientem a centrálním systémem firmy.

Poznámka: Tento postup slouží k zabezpečení spojení pouze jednoho počítače se systémem Centrální správy. Ostatní spojení klientů se serverem Centrální správy a připojení z koncových bodů k serveru Centrální správy nebudou zabezpečení pomocí SSL používat. Chcete-li zabezpečit další klienty, zajistěte, aby u nich byly splněny nezbytné předpoklady, a opakujte “Krok 4: Aktivace SSL pro klienta System i Navigator”. Při zabezpečování dalších spojení se serverem Centrální správy použijte informace uvedené v tématu Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

Volitelný krok: Deaktivace SSL pro klienta System i Navigator:
Bude-li Robert chtít pracovat na pracovišti firmy a nebude potřebovat připojení SSL, které ovlivňuje výkon jeho počítače, může zabezpečení SSL snadno deaktivovat tímto postupem:

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na Systém A a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a zrušte výběr volby **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt System i Navigator a opět jej spusťte.

Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL

Tento scénář popisuje, jak pomocí SSL zabezpečit všechna spojení s modelem systému System i používajícím Centrální správu, která je součástí produktuSystem i Navigator, a funguje jako centrální systém.

Situace:

Firma právě nainstalovala síť WAN (wide area network), která zahrnuje několik modelů systému System i ve vzdálených systémech (koncových bodech). Koncové systémy jsou centrálně řízeny jedním systémem (centrálním systémem), který je umístěn v hlavním sídle firmy. Tomáš pracuje ve firmě jako odborník na zabezpečení. Tomáš chce pomocí SSL (Secure Sockets Layer) zabezpečit všechna spojení mezi serverem Centrální správy v centrálním systému firmy a všemi systémy a klienty i5/OS.

Podrobnosti:

Tomáš může řídit všechna připojení k serveru Centrální správy **zabezpečeným způsobem** - pomocí SSL. K tomu, aby mohl na serveru Centrální správy používat SSL, musí Tomáš zabezpečit produkt System i Navigator v počítači, který se bude používat při přístupu k centrálnímu systému.

Tomáš si může pro server Centrální správy vybrat jednu ze dvou úrovní autentizace:

Autentizace serveru

Zajišťuje autentizaci certifikátu serveru. Klient musí ověřit server, ať už je tímto klientem produkt System i Navigator na PC, nebo server Centrální správy v centrálním systému. Když se připojuje produkt System i Navigator z PC k centrálnímu systému, je tento PC klientem SSL a server Centrální správy v centrálním systému je serverem SSL. Centrální systém funguje jako klient SSL, když se připojuje ke koncovému systému. Koncový systém pak funguje jako server SSL. Tento server musí klientovi prokázat svou identitu pomocí certifikátu, který byl vydán vydavatelem certifikátu (CA), který je pro centrální systém důvěryhodný. Každý server SSL musí mít platný certifikát od důvěryhodného vydavatele certifikátů (CA).

Autentizace klienta a serveru

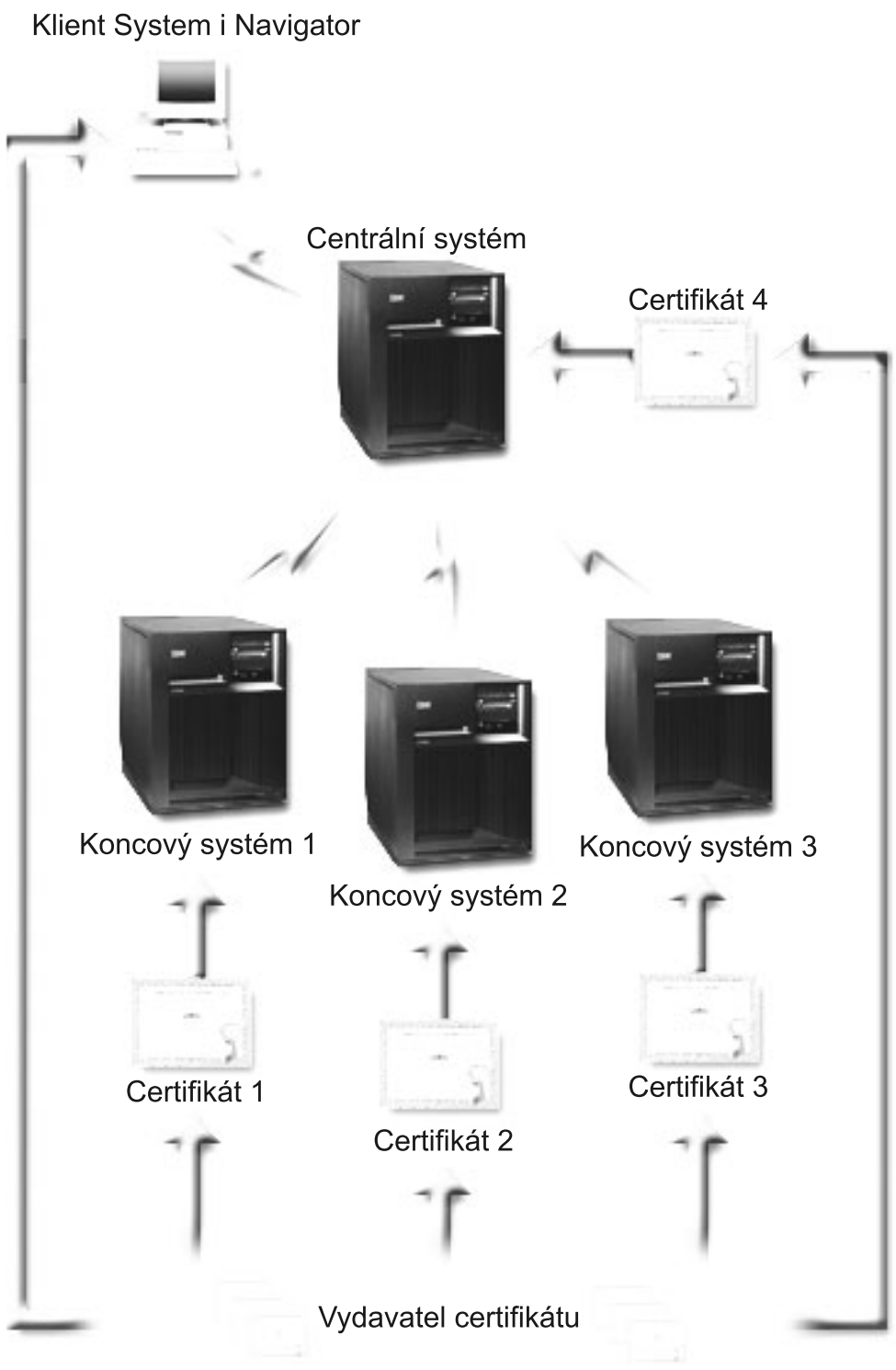
Umožňuje autentizaci jak certifikátu centrálního systému, tak certifikátu koncového systému. Toto je vyšší úroveň zabezpečení než úroveň autentizace serveru. V jiných aplikacích je tato autentizace známá jako autentizace klienta, kde klient musí poskytnout platný a důvěryhodný certifikát. Když se centrální systém (klient SSL) pokouší vytvořit spojení s koncovým systémem (server SSL), centrální systém a koncový systém si navzájem autentizují certifikáty kvůli pravosti vydavatele certifikátu (CA).

Poznámka: Autentizace klienta a serveru se provádí pouze mezi dvěma modely systémů System i. Autentizaci klienta server neprovádí, je-li tímto klientem některý PC.

Na rozdíl od jiných aplikací poskytuje produkt Centrální správa autentizaci také prostřednictvím ověřovacího seznamu, který se nazývá důvěryhodná skupina. Obecně se dá říci, že ověřovací seznam obsahuje informace identifikující uživatele, jako je identifikace uživatele, a informace o autentizaci, jako je heslo, osobní identifikační číslo nebo digitální certifikát. Tyto informace o autentizaci jsou zakódovány.

Ve většině aplikací obvykle není uvedeno, že aktivujete autentizaci serveru i klienta, protože k autentizaci serveru dochází téměř vždy při aktivaci relace SSL. Mnoho aplikací má volby pro konfiguraci autentizace klienta. Produkt Centrální správa používá namísto termínu autentizace klienta termín ″autentizace serveru a klienta″ kvůli dvojí úloze, kterou má centrální systém v síti. Když se uživatelé PC připojují k centrálnímu systému, funguje centrální systém jako server. Když se však centrální systém připojuje ke koncovému systému, funguje jako klient. Níže uvedený obrázek ukazuje, jak centrální systém funguje v síti jako server i jako klient.

Poznámka: V případě zobrazeném na tomto obrázku musí být certifikát asociovaný s vydavatelem certifikátu (CA) uložen v databázi klíčů v centrálním systému a ve všech koncových systémech. Vydavatel certifikátů (CA) musí být jak v centrálním systému, tak na všech koncových bodech i na PC.



Nezbytné podmínky a předpoklady:

K zabezpečení všech připojení k serveru Centrální správy musí Tomáš provést tyto úlohy administrace a konfigurace:

1. Systém A musí splňovat nezbytné předpoklady pro SSL.

2. Centrální systém a všechny koncové systémy jsou provozovány na serverech OS/400 verze V5R2 nebo novější, případně na serverech i5/OS V5R3 nebo novější.

   Poznámka: Připojení systému i5/OS verze V5R4 nebo novější k systému OS/400 verze V5R1 není povoleno.
3. Na PC klientu je provozován System i Navigator for System i Access for Windows verze V5R3 nebo novější.
4. Získání vydavatele certifikátu (CA) pro modely serverů System i.
5. Vytvoření certifikátu pro Systém A podepsaného vydavatelem certifikátu (CA).
6. Odeslání vydavatele certifikátu (CA) a certifikátu do Systému A a jeho import do databáze klíčů.
7. Přiřazení certifikátu pomocí identifikace Centrální správy a identifikace aplikací pro všechny systémy i5/OS. K systémům i5/OS patří všechny tyto servery: centrální server TCP, databázový server, server datových front, souborový server, server síťového tisku, server vzdálených příkazů a přihlašovací server.
   a. Spusťte program IBM DCM (Digital Certificate Manager) na serveru Centrální správy. Pokud chce Tomáš získat nebo vytvořit certifikáty, nebo nastavit nebo změnit certifikační systém, provede to nyní (informace o nastavení certifikačního systému najdete pod tématem Použití produktu DCM (Digital Certificate Manager)).
   b. Klepněte na volbu **Vybrat paměť certifikátů**.
   c. Vyberte ***SYSTEM** a klepněte na **Pokračovat**.
   d. Zadejte *Heslo paměti certifikátů* pro *SYSTEM a klepněte na **Pokračovat**. Jakmile se znovu načte nabídka, rozbalte volbu **Spravovat aplikace**.
   e. Klepněte na volbu **Aktualizace přiřazení certifikátu**.
   f. Vyberte **Server** a klepněte na **Pokračovat**.
   g. Vyberte server Centrální správy a klepněte na volbu **Aktualizace přiřazení certifikátu**. Tím přiřadíte certifikát k požadovanému systému Centrální správy.
   h. Vyberte certifikát, který chcete přiřadit aplikaci, a klepněte na volbu **Přiřadit nový certifikát**. Produkt DCM se znovu zavede na stranu **Aktualizace přiřazení certifikátu** se zprávou o potvrzení.
   i. Klepnutím na **Zrušit** se vraťte na seznam aplikací.
   j. Tuto proceduru opakujte pro všechny systémy i5/OS.
8. Stáhněte si vydavatele certifikátů (CA) do klientského počítače systému System i Navigator.

Postup při konfiguraci:

K tomu, aby mohl Tomáš aktivovat SSL na serveru Centrální správy, musí v centrálním systému nainstalovat nezbytné programy a nastavit digitální Certifikáty. Než budete pokračovat, prostudujte si téma Nezbytné podmínky a předpoklady pro tento scénář. Když Tomáš splní všechny nezbytné předpoklady, může pomocí následujících postupů zabezpečit všechna připojení k serveru Centrální správy:

Poznámka: Je-li aktivován SSL pro produkt System i Navigator, musí jej Tomáš nejdříve deaktivovat, aby mohl aktivovat SSL na serveru Centrální správy. Pokud byl SSL aktivován pro produkt System i Navigator, a nikoli pro server Centrální správy, pokusy produktu System i Navigator o připojení k centrálnímu systému selžou.

1. “Krok 1: Konfigurace centrálního systému pro autentizaci serveru” na stránce 9
2. “Krok 2: Konfigurace koncových systémů pro autentizaci serveru” na stránce 10
3. “Krok 3: Restart systému Centrální správy v centrálním systému” na stránce 10
4. “Krok 4: Restart systému Centrální správy ve všech koncových systémech” na stránce 10
5. “Krok 5: Aktivace SSL pro klienta System i Navigator” na stránce 11
6. “Krok 6: Konfigurace centrálního systému pro autentizaci klienta” na stránce 11
7. “Krok 7: Konfigurace koncových systémů pro autentizaci klienta” na stránce 11
8. “Krok 8: Kopírování ověřovacího seznamu do koncových systémů” na stránce 12
9. “Krok 9: Restart systému Centrální správy v centrálním systému” na stránce 12
10. “Krok 10: Restart systému Centrální správy ve všech koncových systémech” na stránce 12

Související pojmy

"Nezbytné předpoklady pro SSL" na stránce 18
Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

"Zabezpečení aplikací pomocí SSL" na stránce 18
Projděte si tento seznam, chcete-li vědět, které aplikace lze použít pro zabezpečení SSL na platformě systému System i.

Související úlohy

"Podrobnosti konfigurace: Zabezpečení spojení klienta se systémem Centrální správy pomocí SSL" na stránce 4
Toto téma uvádí postup při konfiguraci zabezpečení spojení klienta se serverem Centrální správy pomocí SSL.

"Podrobnosti konfigurace: Zabezpečení všech spojení se systémem Centrální správy pomocí SSL"
Toto téma uvádí podrobnosti zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

Související informace

Konfigurace DCM

Prvotní nastavení certifikátů

Podrobnosti konfigurace: Zabezpečení všech spojení se systémem Centrální správy pomocí SSL

Toto téma uvádí podrobnosti zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

Následující informace vycházejí z předpokladu, že jste si přečetli téma Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

Nyní byste se měli dozvědět, jak provést jednotlivé kroky potřebné k zabezpečení všech spojení se serverem Centrální správy. Ve scénáři postupujte společně s Tomášem.

K tomu, aby mohl Tomáš aktivovat SSL v systému Centrální správy, musí v centrálním systému nainstalovat nezbytné programy a nastavit digitální Certifikáty. Když splní všechny nezbytné předpoklady, může pomocí následujících postupů zabezpečit všechna připojení k serveru Centrální správy.

Poznámka: Je-li aktivován SSL pro produkt System i Navigator, musí jej Tomáš nejdříve deaktivovat, aby mohl aktivovat SSL na serveru Centrální správy. Pokud byl SSL aktivován pro produkt System i Navigator, a nikoli pro server Centrální správy, pokusy produktu System i Navigator o připojení k centrálnímu systému selžou.

SSL umožní Tomášovi zabezpečit ochranu přenosů mezi centrálním a koncovým systémem i mezi klientem System i Navigator a centrálním systémem. SSL umožňuje přenos a autentizaci certifikátů a kódování dat. Spojení SSL může nastat pouze mezi centrálním systémem podporujícím SSL a koncovým systémem podporujícím SSL. Než bude moci Tomáš nastavit autentizaci klienta, musí nastavit autentizaci serveru.

Související pojmy

"Nezbytné předpoklady pro SSL" na stránce 18
Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

"Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL" na stránce 5
Tento scénář popisuje, jak pomocí SSL zabezpečit všechna spojení s modelem systému System i používajícím Centrální správu, která je součástí produktuSystem i Navigator, a funguje jako centrální systém.

Související informace

Prvotní nastavení certifikátů

Krok 1: Konfigurace centrálního systému pro autentizaci serveru:

1. V prostředí produktu System i Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.

2. Klepněte na kartu **Zabezpečení** a vyberte **Použít SSL (Secure Sockets Layer)**.
3. Jako úroveň autentizace vyberte volbu **Server**.
4. Klepněte na **OK** a nastavte tuto hodnotu v centrálním systému.

   Poznámka: **NERESTARTUJTE** server Centrální správy, dokud k tomu nedostanete pokyn (později). Pokud byste nyní restartovali server, nemohli byste se připojit ke koncovým systémům. Před restartem serveru s aktivací SSL je třeba provést ještě další konfigurační kroky. Nejprve musíte přenést konfiguraci SSL na koncové systémy, a to pomocí úloh porovnání a aktualizace.

Krok 2: Konfigurace koncových systémů pro autentizaci serveru:
Když Tomáš nakonfiguruje centrální systém pro autentizaci serveru, musí pro autentizaci serveru nakonfigurovat i koncové systémy. Je třeba provést tyto úkoly:

1. Rozbalte okno **Centrální správa**.
2. Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:
   a. Pod hlavičkou **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis → Shromažďování**.
   b. V dialogu Shromažďování zaškrtněte volbu **Systémové hodnoty**, která shromáždí soupis systémových hodnot pro centrální systém. Zrušte případné zaškrtnutí všech ostatních voleb. Klepněte na OK a vyčkejte, až se úloha soupisu dokončí.
   c. Klepněte pravým tlačítkem myši na **Skupiny systémů → Nová skupina systémů**.
   d. Definujte novou skupinu systémů, která zahrnuje všechny koncové systémy, ke kterým se připojujete pomocí SSL. Tuto novou skupinu systémů pojmenujte 'Důvěryhodná skupina'.
   e. Jestliže chcete zobrazit novou 'Důvěryhodnou skupinu', rozbalte seznam skupin systémů.
   f. Je-li soupis dokončen, klepněte pravým tlačítkem myši na novou skupinu systémů a vyberte **Systémové hodnoty → Porovnání a aktualizace**.
   g. Ověřte, že se centrální systém zobrazil v poli **Modelový systém**.
   h. V poli **Kategorie** vyberte volbu **Centrální správa**.
   i. Ověřte, že volba **Použít pro připojení SSL** je nastavena na **Ano** a vyberte **Aktualizovat**. Tím se tato systémová hodnota přenese na 'Důvěryhodnou skupinu'.
   j. Ověřte, že volba **Úroveň autentizace přes SSL** je nastavena na **Server** a vyberte **Aktualizovat**. Tím se tato systémová hodnota přenese na 'Důvěryhodnou skupinu'.

      Poznámka: Jestliže tyto hodnoty nejsou nastaveny, proveďte Krok 1: Konfigurace centrálního systému pro autentizaci serveru.
   k. Klepněte na **OK**. Vyčkejte, až se dokončí proces **Porovnání a aktualizace**, a potom pokračujte dalším krokem.

Krok 3: Restart systému Centrální správy v centrálním systému:
1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Rozbalte centrální systém.
3. Rozbalte **Síť → Servery** a vyberte **TCP/IP**.
4. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**. Okno centrálního systému se zavře a zobrazí se zpráva, že nejste připojeni k serveru.
5. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

Krok 4: Restart systému Centrální správy ve všech koncových systémech:
1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Rozbalte koncový systém, který chcete restartovat.
3. Rozbalte **Síť → Servery** a vyberte **TCP/IP**.
4. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
5. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

6. Tuto proceduru opakujte pro všechny koncové systémy.

Krok 5: Aktivace SSL pro klienta System i Navigator:

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na centrální systém a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a vyberte volbu **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt System i Navigator a opět jej spusťte.

Poznámka: Když jsou všechny tyto kroky dokončeny, je v centrálním systému i koncových systémech nastavena autentizace serveru. Volitelně můžete v těchto systémech nastavit i autentizaci klienta. K nastavení autentizace klienta v centrálním systému i koncových systémech slouží kroky 6 až 10.

Krok 6: Konfigurace centrálního systému pro autentizaci klienta:

Nyní, když Tomáš dokončil konfiguraci autentizace serveru, může provést následující volitelné kroky pro nastavení autentizace klienta. Autentizace klienta umožňuje ověřit platnost vydavatele certifikátu (CA) a důvěryhodné skupiny pro koncové systémy i pro centrální systém. Když se centrální systém (klient SSL) pokouší použít SSL k připojení ke koncovému systému (serveru SSL), centrální systém a koncový systém si navzájem ověřují certifikáty prostřednictvím autentizace serveru i autentizace klienta. Hovoříme také o autentizaci vydavatele certifikátu a důvěryhodné skupiny.

Poznámka: Konfiguraci autentizace klienta lze provádět až po konfiguraci autentizace serveru. Pokud jste autentizaci serveru nenastavili, udělejte to.

1. V prostředí produktu System i Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte na kartu **Zabezpečení** a vyberte **Použít SSL (Secure Sockets Layer)**.
3. Pro úroveň autentizace vyberte volbu **Klient a server**.
4. Klepněte na **OK** a nastavte tuto hodnotu v centrálním systému.

   Poznámka: **NERESTARTUJTE** server Centrální správy, dokud k tomu nedostanete pokyn (později). Pokud byste nyní restartovali server, nemohli byste se připojit ke koncovým systémům. Před restartem serveru s aktivací SSL je třeba provést ještě další konfigurační kroky. Nejprve musíte přenést konfiguraci SSL na koncové systémy, a to pomocí úloh porovnání a aktualizace.

Krok 7: Konfigurace koncových systémů pro autentizaci klienta:
Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:

1. Rozbalte okno **Centrální správa**.
2. Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:
   a. Pod hlavičkou **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis → Shromažďování**.
   b. V dialogu Shromažďování zaškrtněte volbu **Systémové hodnoty**, která shromáždí soupis systémových hodnot pro centrální systém. Zrušte případné zaškrtnutí všech ostatních voleb. Klepněte na OK a vyčkejte, až se úloha soupisu dokončí.
   c. Je-li soupis dokončen, klepněte pravým tlačítkem myši na 'Důvěryhodnou skupinu' a vyberte **Systémové hodnoty → Porovnání a aktualizace**.
   d. Ověřte, že se centrální systém zobrazil v poli **Modelový systém**.
   e. V poli **Kategorie** vyberte volbu **Centrální správa**.
   f. Ověřte, že volba **Použít pro připojení SSL** je nastavena na **Ano** a vyberte **Aktualizovat**. Tím se tato systémová hodnota přenese na 'Důvěryhodnou skupinu'.
   g. Ověřte, že volba **Úroveň autentizace přes SSL** je nastavena na **Klient a Server** a vyberte **Aktualizovat**. Tím se tato systémová hodnota přenese na 'Důvěryhodnou skupinu'.

Poznámka: Jestliže tyto hodnoty nejsou nastaveny, proveďte Krok 6: Konfigurace centrálního systému pro autentizaci klienta.

h. Klepněte na **OK**. Vyčkejte, až se dokončí proces **Porovnání a aktualizace**, a potom pokračujte dalším krokem.

Krok 8: Kopírování ověřovacího seznamu do koncových systémů:

Tento postup předpokládá, že váš centrální systém má verzi systému i5/OS V5R3 nebo vyšší. V systémech i5/OS s verzí nižší než V5R3 byl soubor QYPSVLDL.VLDL umístěn v knihovně QUSRSYS.LIB, nikoliv v knihovně QMGTC2.LIB. V případě systémů nižší verze než V5R3 bude třeba odeslat ověřovací seznam pro tyto systémy a umístit jej do knihovny QUSRSYS.LIB, namísto QMGTC2.LIB. U systémů verze V5R3 nebo vyšší pokračujte následujícími kroky.

1. V prostředí produktu System i Navigator rozbalte volbu **Centrální správa → Definice**.
2. Klepněte pravým tlačítkem myši na **Sada programů** a vyberte **Nová definice**.
3. V okně **Nová definice** pracujte s těmito volbami:
   a. **Jméno:** Napište jméno definice.
   b. **Zdrojový systém:** Vyberte jméno centrálního systému.
   c. **Vybrané soubory a složky:** Klepněte na pole a napište /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL.
4. Klepněte na kartu **Volby** a vyberte **Nahradit existující soubor odesílaným souborem**.
5. Klepněte na **Rozšířené**.
6. V okně **Rozšířené volby** zadejte **Ano**, čímž povolíte rozdíly objektů při obnově, a změnu **Cílového vydání** na nejnižší úroveň vydání vašich koncových systémů.
7. Klepněte na **OK**, čímž obnovíte seznam definic a zobrazíte novou sadu.
8. Klepněte pravým tlačítkem myši na novou sadu a vyberte **Odeslat**.
9. V dialogovém okně **Odeslat** rozbalte volbu **Skupiny systémů->Důvěryhodná skupina**, která se nachází v seznamu **Dostupné systémy a skupiny**. Je to skupina, kterou jste nadefinovali v kroku “Krok 2: Konfigurace koncových systémů pro autentizaci serveru” na stránce 10.

   Poznámka: Úloha **Odeslat** v centrálním systému vždycky selže, protože centrální systém je vždy zdrojovým systémem. Úloha **Odeslat** by se měla úspěšně provést ve všech koncových systémech.
10. Máte-li nějaké systémy, na kterých je provozován system i5/OS verze V5R3 nebo nižší v **Důvěryhodné skupině**, je třeba v těchto systémech ručně přesunout objekt QYPSVLDL.VLDL z knihovny QMGTC2.LIB do QUSRSYS.LIB. Jestliže se v knihovně QUSRSYS.LIB objekt QYPSVLDL.VLDL již nachází, odstraňte jej a nahraďte jej novější verzí z knihovny QMGTC2.LIB.

Krok 9: Restart systému Centrální správy v centrálním systému:

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Rozbalte centrální systém.
3. Rozbalte **Síť → Servery** a vyberte **TCP/IP**.
4. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**. Okno centrálního systému se zavře a zobrazí se zpráva, že nejste připojeni k serveru.
5. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

Krok 10: Restart systému Centrální správy ve všech koncových systémech:

Poznámka: Tuto proceduru opakujte pro všechny koncové systémy.

1. V prostředí produktu System i Navigator rozbalte **Připojení**.
2. Rozbalte koncový systém, který chcete restartovat.
3. Rozbalte **Síť → Servery** a vyberte **TCP/IP**.
4. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
5. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

Koncepce SSL

Téma Koncepce SSL přináší doplňkové informace a poskytuje některé základní konstrukční bloky protokolů SSL (Secure Sockets Layer).

S protokolem SSL můžete mezi klientskými a serverovými aplikacemi vytvořit bezpečné spojení, které umožní autentizaci jednoho nebo obou koncových bodů komunikační relace. Protokol SSL také poskytuje soukromí a integritu dat vyměňovaných mezi klientskými a serverovými aplikacemi.

Jak SSL pracuje

SSL jsou vlastně dva protokoly. Je to záznamový protokol a protokol pro navazování spojení. Záznamový protokol řídí tok dat mezi dvěma koncovými body relace SSL.

Protokol pro navazování spojení autentizuje jeden nebo oba koncové body relace SSL a vytváří jedinečný symetrický klíč pro generování klíčů sloužících ke kódování a dekódování dat pro relaci SSL. SSL používá asymetrické šifrování, digitální certifikáty a toky navazování spojení SSL k autentizaci jednoho nebo obou koncových bodů relace SSL. SSL obvykle autentizuje server. Volitelně SSL autentizuje klienta. Digitální certifikát vydaný vydavatelem certifikátu (CA) může být přiřazen každému z koncových systémů nebo aplikacím používajícím SSL v každém koncovém bodě spojení.

Digitální certifikát obsahuje veřejný klíč a některé identifikační informace, které byly digitálně podepsány důvěryhodným vydavatelem certifikátu (CA). Každý veřejný klíč má asociovaný privátní klíč. Privátní klíč není uložen s certifikátem ani není jeho součástí. Při autentizaci serveru i klienta musí autentizovaný koncový bod prokázat, že má přístup k privátnímu klíči asociovanému s veřejným klíčem v digitálním certifikátu.

Navazování spojení SSL je časově náročná operace v důsledku šifrovacích operací pomocí veřejných a privátních klíčů. Po vytvoření počáteční relace SSL mezi dvěma koncovými body může být informace o relaci SSL pro tyto dva koncové body a aplikace uložena do bezpečné paměti kvůli urychlení aktivace následné relace SSL. Když relace SSL pokračuje, oba koncové systémy použijí zkrácený tok navazování spojení k autentizaci toho, zda má každý z nich přístup k jedinečným informacím bez použití veřejného nebo privátního klíče. Jestliže oba koncové body mohou prokázat, že mají přístup k těmto jedinečným informacím, vytvoří se nové symetrické klíče a relace SSL pokračuje. U relací TLS verze 1.0 a SSL verze 3.0 nezůstane uložená informace v bezpečné paměti déle než 24 hodin. V operačním systému OS/400 verze V5R2 a následujících vydáních nebo v systému i5/OS můžete vliv navazování spojení SSL na výkon hlavní CPU minimalizovat pomocí šifrovacího hardwaru.

Související informace

Koncepce digitálního certifikátu

Šifrovací hardware

Podporované protokoly SSL a TLS

Toto téma popisuje, kterou verzi protokolu SSL a TLS daná implementace i5/OS podporuje.

Existuje několik definovaných verzí protokolu SSL. Nejnovější verze TLS (Transport Layer Security) je založena na SSL 3.0 a je produktem společnosti IETF (Internet Engineering Task Force). Implementace i5/OS podporuje tyto verze protokolů SSL a TLS:

- TLS verze 1.0
- TLS verze 1.0 s kompatibilitou SSL verze 3.0

Poznámka:

1. Specifikace TLS verze 1.0 s kompatibilitou SSL verze 3.0 znamená, že o protokolu TLS se bude vyjednávat, zda je možný, a když možný nebude, bude se vyjednávat o protokolu SSL verze 3.0. Jestliže není možné vyjednat protokol SSL verze 3.0, navazování spojení SSL selže.
2. Systém System i rovněž podporuje TLS verze 1.0 s kompatibilitou SSL verze 3.0 a SSL verze 2.0. To je specifikováno hodnotou protokolu **ALL**, což znamená, že o protokolu TLS se bude vyjednávat, zda je možný, a když možný nebude, bude se vyjednávat o protokolu SSL verze 3.0.

Jestliže není možné vyjednávat o protokolu SSL verze 3.0, bude se vyjednávat o protokolu SSL verze 2.0. Jestliže není možné vyjednat protokol SSL verze 2.0, navazování spojení SSL selže. Protokol SSL verze 2.0 lze opětovně povolit prostřednictvím změny systémové hodnoty QSSLPCL. Systémovou hodnotu QSSLPCL lze použít pro vypnutí nebo zapnutí kteréhokoliv z těchto protokolů.

- SSL verze 3.0
- SSL verze 2.0
- SSL verze 3.0 s kompatibilitou SSL verze 2.0

SSL verze 3.0 versus SSL verze 2.0

Protokol SSL verze 3.0 je ve srovnání s protokolem SSL verze 2.0 téměř úplně jiným protokolem. Některé z hlavních rozdílů mezi oběma protokoly zahrnují tyto odlišnosti:

- Protokoly pro navazování spojení SSL verze 3.0 jsou jiné než protokoly pro navazování spojení SSL verze 2.0.
- SSL verze 3.0 používá implementaci BSAFE 3.0 od společnosti RSA Data Security, Incorporated. BSAFE 3.0 zahrnuje řadu oprav proti útokům souvisejícím s časováním a SHA-1 algoritmus přepočtu klíče. SHA-1 algoritmus přepočtu klíče je pokládán za bezpečnější než MD5 algoritmus přepočtu klíče. SHA-1 umožňuje protokolu SSL verze 3.0 podporovat další šifrovací sady, které používají SHA-1 namísto MD5.
- Protokol SSL verze 3.0 potlačuje výskyt útoků typu MITM (man-in-the-middle) během zpracování navazování spojení SSL. V protokolu SSL verze 2.0 bylo možné, i když nepravděpodobné, že útok MITM mohl oslabit specifikaci šifer. Oslabení šifrování mohlo umožnit neoprávněné osobě porušit klíč relace SSL.

TLS verze 1.0 versus SSL verze 3.0

Nejnovějším standardním protokolem SSL založeným na SSL verze 3.0 je TLS (Transport Layer Security) verze 1.0. Jeho specifikace jsou definovány organizací IETF (Internet Engineering Task Force) v dokumentu RFC 2246 *The TLS Protocol*.

Hlavním cílem TLS je učinit SSL bezpečnějším a současně učinit specifikaci protokolu přesnější a dokonalejší. TLS umožňuje tato zlepšení SSL verze 3:

- Bezpečnější algoritmus MAC.
- Přesnější výstrahy.
- Jasnější definici specifikací ″šedé oblasti″.

Všechny aplikace serveru System i, které jsou aktivovány pro SSL, získají automaticky podporu TTL. Výjimkou jsou případy, kdy aplikace výslovně žádala o použití pouze SSL verze 3.0 nebo SSL verze 2.0.

TLS poskytuje tato zlepšení zabezpečení ochrany dat:

- **HMAC (Key-Hashing for Message Authentication)**TLS používá kód HMAC (Key-Hashing for Message Authentication Code), který zajišťuje, že záznam nemůže být změněn během cesty v nechráněné síti, jako je Internet. SSL verze 3.0 umožňuje také autentizaci klíčované zprávy, ale kód HMAC je bezpečnější než funkce MAC (Message Authentication Code), kterou používá SSL verze 3.0.
- **PRF (Enhanced Pseudorandom Function)** PRF generuje data klíče. V TLS definuje funkce PRF kód HMAC. Funkce PRF používá dva algoritmy pro přepočet klíče takovým způsobem, který zaručuje její bezpečnost. Pokud je jeden z algoritmů nechráněný a druhý algoritmus není nechráněný, zůstanou data zabezpečena.
- **Rozšířená verifikace zprávy o dokončení** Jak TLS verze 1.0, tak SSL verze 3.0 odesílá zprávu o dokončení pro oba koncové systémy, která ověřuje, že vyměňované zprávy nebyly změněny. TLS však odvozuje tuto zprávu o ukončení od hodnot PRF a HMAC, což je opět bezpečnější, než SSL verze 3.0.
- **Konzistentní zacházení s certifikáty** Na rozdíl od SSL verze 3.0 se TLS pokouší specifikovat typ certifikátu, který si musejí implementace TLS vyměnit.
- **Specifické výstražné zprávy** TLS poskytuje specifičtější a nové výstražné zprávy pro indikaci problémů zjištěných některým z koncových bodů relace. TLS také dokumentuje, kdy by měly být odeslány určité varovné zprávy.

Související informace

Protokol TLS

System SSL

System SSL je sada generických služeb poskytovaných licenčním interním kódem systému i5/OS za účelem ochrany komunikací TCP/IP pomocí protokolu SSL/TLS. System SSL je těsně spjatý s operačním systémem a kódem soketů a poskytuje dodatečný výkon a zabezpečení.

System SSL je přístupný vývojářům aplikací z těchto programovacích rozhraní a implementací JSSE:

- Rozhraní API Global Secure Toolkit (GSKit)
  - Tato rozhraní API ILE C API jsou přístupná z ostatních jazyků ILE.
- Integrovaná rozhraní API SSL_ systému i5/OS
  - Tato rozhraní API ILE C API jsou přístupná z ostatních jazyků ILE.
  - Použití této sady API se nedoporučuje. Doporučeným rozhraním C je GSKit.
- Integrované implementace JSSE systému i5/OS
  - Předvolená implementace JSSE pro JDK 1.4.
  - Implementace i5/OS JSSE je dostupná pro JDK 1.5 a JDK, není to však přednastavená implementace.

Aplikace SSL od IBM nebo obchodních partnerů IBM či dodavatelů ISV nebo zákazníků, kteří používajíjedno ze tří výše uvedených rozhraní SSL, používají System SSL. Například FTP a Telnet jsou aplikace společnosti IBM, které využívají System SSL. Nikoliv všechny aplikace provozované v systému System i, které mají povoleny SSL, využívají SSL.

Vlastnosti System SSL

Vlastnosti System SSL určují, jaké funkce SSL jsou podporovány a jaké funkce SSL jsou použity při výchozím nastavení, pokud je požadováno chování systému podle výchozího nastavení.

Každá aplikace určuje, zda má být přednastavená funkčnost použita nebo přepsána kódovacím výběrem učiněným v rámci aplikace. Mnoho aplikací používá předvolby System SSL a umožňuje tak, aby byly využity nové schopnosti System SSL, aniž by bylo třeba implementovat změny kódu.

V systému i5/OS verze V6R1 nebo novější poskytuje System SSL systémovým administrátorům mechanizmus, pomocí kterého mohou přesně ovládat, jaké protokoly SSL a šifry doprovodu jsou v rámci System SSL podporovány. System SSL má dva koncepty, kterým budete muset porozumět předtím, než začnete System SSL používat. Prvním konceptem jsou podporované hodnoty. Podporované hodnoty jsou hodnoty, které má System SSL schopnost podporovat. Systém je dodáván tak, že část svých vlastních schopností má povolenou. Druhým konceptem jsou přednastavené hodnoty. Přednastavené hodnoty musí být částí podporovaných hodnot. Přednastavené hodnoty jsou použity, když aplikace požádá o přednastavenou podporu. Aby byla zajištěna ochrana aplikací IBM používajících předvolby System SSL před tím, aby byly nuceny podporovat nižší úroveň zabezpečení, je omezená možnost administrátorů ovládat přednastavené hodnoty. Nelze přidat funkčnostk přednastavené podpoře nad rámec předvoleb dodávaných se systémem. Administrátor může dále omezit, co je podporováno při výchozím nastavení tak, že zcela vypne podporu určité funkce.

Protokoly SSL

System SSL obsahuje infrastrukturu pro podporu těchto protokolů:

- Protokol SSLv2 (Secure Sockets Layer verze 2.0).
- Protokol SSLv3 (Secure Sockets Layer verze 3.0).
- Protokol TLSv1 (Transport Layer Security verze 1.0).

Dodávané protokoly podporující SSL

System SSL je dodáván s těmito podporovanými protokoly:

- Protokol SSLv3 (Secure Sockets Layer verze 3.0).
- Protokol TLSv1 (Transport Layer Security verze 1.0).

Poznámka: Protokol SSLv2 (Secure Sockets Layer verze 2.0) je dodáván v System SSL jako vypnutý. Protokol SSLv2 lze opětovně povolit prostřednictvím změny systémové hodnoty QSSLPCL. Systémovou hodnotu QSSLPCL lze použít pro vypnutí nebo zapnutí kteréhokoliv z těchto protokolů.

Přednastavené protokoly podporující SSL

Pokud jsou vyžádány aplikací, používá System SSL tyto přednastavené protokoly:

- Protokol SSLv3 (Secure Sockets Layer verze 3.0).
- Protokol TLSv1 (Transport Layer Security verze 1.0).

Poznámka: Pokud byl protokol SSLv2 přidán administrátorem zpět do seznamu podporovaných protokolů, není přidán mezi přednastavené protokoly. Pokud je přednastavený protokol odstraněn ze seznamu podporovaných protokolů, bude rovněž odstraněn ze seznamu přednastavených protokolů.

Šifry doprovodu SSL

System SSL obsahuje infrastrukturu pro podporu třinácti šifer doprovodů. Šifry doprovodů jsou specifikovány rozdílně pro každé programovací rozhraní. Níže jsou zobrazeny konvence pojmenování systémových hodnot.

Tyto šifry doprovodů mohou být podporovány v rámci System SSL:

- *RSA_NULL_MD5
- *RSA_NULL_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_RC4_128_MD5
- *RSA_RC4_128_SHA
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_DES_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_AES_256_CBC_SHA
- *RSA_RC2_CBC_128_MD5
- *RSA_DES_CBC_MD5
- *RSA_3DES_EDE_CBC_MD5

Seznam specifikací podporovaných dodávaných šifer SSL

Seznam specifikací šifer obsahuje seznam šifer doprovodů. System SSL je dodáván s deseti podporovanými šiframi doprovodů. Administrátoři mohou ovládat šifry podporované v rámci System SSL se systémovými hodnotami QSSLCSL a QSSLCSLCTL. Šifra doprovodu nemůže být podporována, pokud ji protokol SSL požaduje, ale nepodporuje.

Tyto šifry doprovodů jsou dodávány a podporovány v rámci System SSL:

- *RSA_AES_256_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA

| • *RSA_RC4_128_MD5
| • *RSA_3DES_EDE_CBC_SHA
| • *RSA_DES_CBC_SHA
| • *RSA_EXPORT_RC4_40_MD5
| • *RSA_EXPORT_RC2_CBC_40_MD5
| • *RSA_NULL_SHA
| • *RSA_NULL_MD5

| Seznam dodávaných specifikací podporovaných šifer je ovlivněn systémem podporovanými protokoly SSL, stejně jako
| změnami učiněnými v systémové hodnotě QSSLCSL. Hodnotu QSSLCSL můžete zobrazit a zjistit seznam specifikací
| šifer v systému.

| Seznam specifikací přednastavených dodávaných šifer SSL

| Tento seznam obsahuje pořadí Seznam dodávaných specifikací přednastavených šifer:
| • *RSA_AES_128_CBC_SHA
| • *RSA_RC4_128_SHA
| • *RSA_RC4_128_MD5
| • *RSA_AES_256_CBC_SHA
| • *RSA_3DES_EDE_CBC_SHA

| Seznam specifikací přednastavených dodávaných šifer lze zredukovat a změnit pořadí prostřednictvím změny
| systémové hodnoty QSSLCSL. Do seznamu nelze přidat další šifry doprovodu.

| **Související informace**

| systémová hodnota SSL: QSSLPCL

| systémová hodnota SSL: QSSLCSLCTL

| systémová hodnota SSL: QSSLCSL

Autentizace serveru

Při autentizaci serveru klient zajistí, že je certifikát serveru platný a že je podepsaný vydavatelem certifikátu (CA), který je pro klienta důvěryhodný.

SSL použije asymetrické šifrování a protokoly pro navazování spojení pro generování symetrického klíče, který se použije pouze pro tuto jedinečnou relaci SSL. Tento klíč se použije pro generování sady klíčů, jenž se použijí pro kódování a dekódování dat, která tečou v relaci SSL. Po dokončení navazování spojení SSL je autentizován jeden nebo oba konce komunikačního spoje. Dále je vygenerován jedinečný klíč k šifrování a dešifrování dat. Jakmile je ukončeno navazování spojení, tečou zakódovaná data aplikační vrstvy v relaci SSL.

Autentizace klienta

Mnoho aplikací umožňuje aktivovat autentizaci klienta. Při autentizaci klienta server zajistí, že je certifikát klienta platný a že je podepsaný vydavatelem certifikátu (CA), který je pro server důvěryhodný.

Autentizaci klienta podporují následující aplikace serveru System i:

- IBM HTTP Server for i5/OS
- server FTP
- server telnet
- koncový systém Centrální správy
- IBM Tivoli Directory Server for i5/OS

Související informace

SSL (Secure Sockets Layer) a TLS (Transport Layer Security) a server adresářů

Zabezpečení klientů FTP pomocí TLS (Transport Layer Security) nebo SSL (Secure Sockets Layer)

Zabezpečení Telnet pomocí SSL

Nastavení SSL pro pro server administrativy pro HTTP server

Nezbytné předpoklady pro SSL

Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

Ověřte, že máte před používáním SSL nainstalovány tyto volby:

- IBM Digital Certificate Manager (DCM) (5761-SS1 volba 34).

  Poznámka: Produkty IBM Java Secure Socket Extension (JSSE) a OpenSSL nevyžadují DCM.
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
- IBM HTTP Server for i5/OS (5761-DG1).
- Chcete-li kvůli používání produktu DCM použít HTTP server, ujistěte se, že je nainstalován produkt IBM Developer Kit for Java (5761–JV1). Jinak se HTTP Administration Server nespustí.
- Můžete také instalovat šifrovací hardware pro použití se SSL, abyste urychlili navazování spojení SSL. Chcete-li instalovat šifrovací hardware, je nutné nainstalovat také produkt Cryptographic Service Provider.

Poznámka: 5722 je kód produktu pro volby systému i5/OS a produktů předcházející verzi V6R1.

Související pojmy

"Odstraňování problémů se SSL" na stránce 19
Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, na které může platforma System i detekovat u SSL.

Související informace

Šifrovací hardware

Veřejné certifikáty versus soukromé certifikáty

Konfigurace DCM

Zabezpečení aplikací pomocí SSL

Projděte si tento seznam, chcete-li vědět, které aplikace lze použít pro zabezpečení SSL na platformě systému System i.

Pomocí SSL můžete zabezpečit ochranu těchto aplikací systému System i:

- EIM (Enterprise Identity Mapping)
- server FTP
- IBM HTTP Server for i5/OS
- System i Access for Windows
- IBM Tivoli Directory Server for i5/OS
- server DRDA (distributed relational database architecture) a DDM (distributed data management)
- Centrální správa
- server Telnet
- Websphere Application Server — Express
- aplikace napsané pro sadu rozhraní API (application programming interface) produktu System i Access for Windows
- aplikace vyvinuté pomocí rozhraní Secure Sockets API podporovaných na serveru System i (podporovaná API jsou Global Secure Toolkit (GSKit) a SSL_System i)

Související pojmy

"Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL" na stránce 5
Tento scénář popisuje, jak pomocí SSL zabezpečit všechna spojení s modelem systému System i používajícím Centrální správu, která je součástí produktuSystem i Navigator, a funguje jako centrální systém.

Související informace

EIM (Enterprise Identity Mapping)

Použití SSL k zabezpečení serveru FTP

HTTP server

Administrace SSL (Secure Sockets Layer) - téma iSeries Access for Windows

Scénář: Zabezpečení Telnet pomocí SSL

Rozhraní Secure Sockets API

Odstraňování problémů se SSL

Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, na které může platforma System i detekovat u SSL.

Je důležité si uvědomit, že toto není úplný zdroj informací pro odstraňování problémů, ale pouze průvodce, který vám pomůže s řešením běžných problémů.

Ověřte, že jsou splněny tyto podmínky:

- Splnili jste nezbytné předpoklady pro SSL na platformě systému System i.
- Váš vydavatel certifikátu (CA) i certifikáty jsou platné a nejsou prošlé.

Jestliže jste ověřili, že uvedené podmínky váš systém splňuje, a stále máte problém související se SSL, vyzkoušejte tyto možnosti:

- Chybový kód SSL v protokolu úloh serveru může mít křížový odkaz v tabulce chyb, kde lze najít více informací o chybě. Tato tabulka například mapuje chybový kód -93, který se může objevit v protokolu úloh serveru, na konstantu SSL_ERROR_SSL_NOT_AVAILABLE .
  - Negativní návratový kód (určený pomlčkou před číslem kódu) označuje, že používáte SSL_ API.
  - Pozitivní návratový kód označuje, že používáte GSKit API. Programátoři mohou ve svých programech použít gsk_strerror() nebo SSL_Strerror() API, aby získali stručný popis návratového kódu chyby. Některé aplikace využívají tato rozhraní API a vytisknou do protokolu úloh zprávu, která obsahuje tuto větu.

  Pokud potřebujete podrobnější informace, je možné na modelu System i zobrazit ID zprávy uvedené v tabulce za účelem zjištění možné příčiny chyby a možnosti jejího odstranění. Další dokumentaci vysvětlující tyto chybové kódy je možné najít v jednotlivých rozhraních Secure Sockets API, která vrátila chybu.
- Níže uvedené soubory záhlaví obsahují stejná jména konstant pro návratové kódy System SSL jako tabulka, ale bez křížové reference ID zprávy:
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.QSOSSL

  Pamatujte si, že přestože jména návratových kódů System SSL zůstávají v těchto dvou souborech konstantní, s každým návratovým kódem může být asociována více než jedna jedinečná chyba.

Související pojmy

"Nezbytné předpoklady pro SSL" na stránce 18
Toto téma popisuje nezbytné předpoklady pro nastavení System SSL na platformě systému System i a uvádí několik užitečných rad.

Související informace

Chybové zprávy rozhraní Secure socket API

Související informace k tématu SSL

V těchto tématech se dozvíte více o ostatních prostředcích a najdete zde další důležité informace o použití SSL (Secure Sockets Layer).

Webové stránky

- RFC 2246: ″The TLS Protocol Version 1.0 ″  (ftp://ftp.isi.edu/in-notes/rfc2246.txt)
  Podrobně vysvětluje protokol TLS.
- RFC2818: ″HTTP Over TLS″  (ftp://ftp.isi.edu/in-notes/rfc2818.txt)
  Popisuje, jak použít TLS k zabezpečení připojení HTTP na Internetu.

Další informace

- SSL a Java Secure Socket Extension
- IBM Toolbox for Java

Dodatek. Upozornění

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí nabízet produkty, služby a funkce popsané v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou momentálně dostupné ve vaší oblasti, můžete získat od obchodního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použít lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Vlastnictví tohoto dokumentu vám nedává k těmto patentům žádná práva. Písemné dotazy ohledně licencí můžete zaslat na adresu:

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

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve vaší zemi, nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Následující odstavec neplatí pro Velkou Británii a další země, ve kterých tato opatření nejsou v souladu s místními právními předpisy: IBM POSKYTUJE TUTO PUBLIKACI " JAK JE" (AS-IS), BEZ JAKÝCHKOLI ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNSOTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Právní řády některých zemí nepřipouštějí vyloučení záruk vyjádřených výslovně nebo vyplývajících z okolností v určitých transakcích, a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat anebo měnit produkt(y) anebo program(y) popsané v této publikaci.

Jakékoli 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 ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

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

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

IBM poskytuje licencovaný program popsaný v tomto dokumentu a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě pro programy, v Mezinárodní licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiném provozním prostředí se tudíž mohou výrazně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Všechna tvrzení o budoucím zaměření nebo úmyslech IBM mohou být bez upozornění změněna nebo zrušena a představují pouze hrubý nástin cílů a podmínek společnosti.

Tyto publikace obsahují příklady údajů a sestav, používaných v každodenních obchodních činnostech. Abyste si udělali co neúplnější představu, obsahují příklady názvy konkrétních podniků, firemních značek a produktů. Všechny tyto názvy jsou fiktivní a jakákoliv podobnost se jmény a adresami používanými ve skutečných obchodních podnicích je čistě náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyku, které ilustrují programovací metody na různých operačních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Každá kopie nebo část těchto vzorových programů nebo jakákoliv odvozená práce musí zahrnovat níže uvedenou copyrightovou výhradu:

© (jméno vaší společnosti) (rok). Části tohoto kódu byly odvozeny ze vzorových programů společnosti IBM Corp. © Copyright IBM Corp. _zadejte rok nebo roky_. Všechna práva vyhrazena.

Jestliže si prohlížíte tyto informace ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Následující výrazy jsou ochranné známky společnosti International Business Machines Corporation ve Spojených státech a případně v dalších jiných zemích:

DRDA
i5/OS
IBM

| OS/400
| System i
| Tivoli

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

Java a všechny ochranné známky obsahující slovo Java jsou ochranné známky společnosti Sun Microsystems, Inc. ve Spojených státech a případně dalších jiných zemích.

Další jména společností, produktů nebo služeb mohou být ochrannými známkami jiných společností.

Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoliv jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoliv informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ VČETNĚ, A TO ZEJMÉNA, ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN A VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ.

Vytištěno v Dánsku společností IBM Danmark A/S.