

IBM

@server

iSeries

SSL (Secure Sockets Layer)

verze 5, vydání 3





@server

iSeries

SSL (Secure Sockets Layer)

verze 5, vydání 3

Poznámka

Před použitím těchto informací a odpovídajícího produktu si přečtěte informace v tématu “Upozornění”, na stránce 19.

Páté vydání (srpen 2005)

Toto vydání se týká verze 5, vydání 3, modifikace 0 licenčního programu IBM Operating System/400 (5722–SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

© Copyright International Business Machines Corporation 2002, 2005. Všechna práva vyhrazena.

Obsah

| | |
|---|----------|
| SSL (Secure Sockets Layer) | 1 |
| Co je nového ve verzi V5R3 | 1 |
| Tisk tohoto tématu | 1 |
| Scénáře | 2 |
| Scénář: Zabezpečení spojení klienta se serverem | |
| Centrální správy pomocí SSL | 2 |
| Scénář: Zabezpečení všech spojení se serverem Centrální | |
| správy pomocí SSL | 5 |
| Koncepce | 12 |
| Historie SSL | 13 |
| Jak SSL pracuje | 13 |
| Podporované protokoly SSL a TLS (Transport Layer | |
| Security). | 13 |

| | |
|---|----|
| Autentizace serveru | 14 |
| Autentizace klienta | 15 |
| Plánování umožnění SSL. | 15 |
| Zabezpečení aplikací pomocí SSL | 16 |
| Odstraňování problémů se SSL | 16 |
| Související informace | 17 |

Dodatek. Upozornění. 19

| | |
|---|----|
| Ochranné známky | 20 |
| Ustanovení a podmínky pro stahování a tisk publikací. | 20 |

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. Více informací o SSL a aplikacích serveru iSeries najdete v těchto tématech:

- **Co je nového ve verzi V5R3**

Toto téma popisuje nové funkce a nové informace týkající se SSL.

- **Scénáře SSL**

Toto téma obsahuje nové dodatky k informacím o SSL a pomocí příkladů ilustrujících, jak funguje SSL, pomáhá lépe pochopit funkci SSL na serveru iSeries.

- **Koncepce SSL**

Toto téma obsahuje doplňkové informace a poskytuje určité základní stavební bloky protokolů SSL (Secure Sockets Layer).

- **Plánování umožnění SSL**

Toto téma popisuje nezbytné předpoklady pro umožnění SSL na serveru iSeries a uvádí několik užitečných rad.

- **Zabezpečení aplikací pomocí SSL**

Toto téma zahrnuje seznam aplikací, které můžete zabezpečit pomocí SSL na serveru iSeries.

- **Odstraňování problémů se SSL**

Toto téma nabízí základního průvodce procedurou odstraňování problémů se SSL na serveru iSeries.

- **Související informace pro SSL**

Toto téma zahrnuje odkazy na další zdroje informací.

Co je nového ve verzi V5R3

U tohoto vydání SSL (Secure Sockets Layer) stojí za povšimnutí dvě nové položky:

1. **Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL**

Tento nový scénář vysvětluje, jak pomocí SSL zabezpečit spojení mezi vzdáleným klientem a serverem Centrální správy na serveru iSeries, který je určeným centrálním systémem pro lokální síť (LAN).



2. **GSKit 6B verze rozhraní GSKit API**

Rozhraní GSKit API jsou počínaje verzí V5R3 založena na verzi GSKit 6B. V předchozím vydání byla založena na verzi GSKit 4D. Další informace o rozhraních GSKit API získáte klepnutím na tento odkaz.

Další informace o tom, co je nového nebo co se změnilo v tomto vydání, najdete ve Sdělení pro uživatele .

Jak zjistit, co je nového nebo co se změnilo:

K usnadnění přehledu o tom, kde byly provedeny technické změny, jsou použity tyto konvence:

- Symbol  označuje, kde začínají nové nebo změněné informace.
- Symbol  označuje, kde nové nebo změněné informace končí.

Tisk tohoto tématu

Můžete si prohlédnout nebo stáhnout tyto informace ve formátu PDF. Klepněte na odkaz SSL (Secure Sockets Layer) (přibližně 243 KB).

Další informace:

Můžete si také prohlédnout nebo vytisknout jakékoliv ze souvisejících informací vztahujících se k tomuto tématu.

Ukládání souborů PDF:

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

1. Klepněte v prohlížeči pravým tlačítkem myši na PDF.
2. Klepněte na **Save Target As** (Uložit jako).
3. Přejděte do adresáře, do kterého chcete ukládat soubory PDF.
4. Klepněte na **Save** (Uložit).

Stažení programu Adobe Acrobat Reader:

Jestliže potřebujete program Adobe Acrobat Reader, abyste si mohli prohlédnout nebo vytisknout tyto informace, můžete si jeho kopii stáhnout na webové stránce společnosti Adobe na adrese

www.adobe.com/products/acrobat/readstep.html. 

Scénáře

Pro maximalizaci výhod aktivace SSL na serveru iSeries byly navrženy tyto scénáře:

- **Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL**
Tento scénář vysvětluje, jak pomocí SSL zabezpečit spojení mezi vzdáleným klientem a serverem iSeries, který používá server Centrální správy (iSeries Navigator) a funguje jako centrální systém.
- **Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL**
Tento scénář vysvětluje, jak pomocí SSL zabezpečit **všechna** spojení se serverem iSeries, který používá server Centrální správy (iSeries Navigator) a funguje jako centrální systém.
- **Scénář: Zabezpečení FTP pomocí SSL.**
Tento scénář vysvětluje, jak umožnit SSL pro aplikaci FTP.
- **Scénář: Zabezpečení Telnet pomocí SSL.**
Tento scénář vysvětluje, jak umožnit SSL pro aplikaci Telnet.
- **Scénář: Zvýšení výkonu iSeries SSL.**
Tento scénář vysvětluje, jak pomocí šifrovacího hardwaru zvýšit výkonnost SSL na serveru iSeries.
- **Scénář: Ochrana privátních klíčů pomocí šifrovacího hardwaru.**
Tento scénář vysvětluje, jak pomocí šifrovacího hardwaru chránit soukromé klíče přidružené k transakcím na serveru iSeries.

Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL



Situace:

Firma provozuje na svém pracovišti lokální síť (LAN), která obsahuje několik serverů iSeries. Systémový administrátor této firmy (Robert) určil jeden ze serverů iSeries jako centrální systém sítě LAN (dále ho budeme označovat 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. Robert nepožaduje další zabezpečení spojení mezi serverem Centrální správy v Systému A a koncovými body, 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 klientské připojení využívalo autentizaci serveru. Spojení se serverem Centrální správy z ostatních počítačů a serverů iSeries v síti LAN nebudou zabezpečena pomocí SSL.

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. Server Centrální správy to provede tak, že poskytne certifikát vydaný vydavatelem certifikátu (CA), jemuž Robertův počítač důvěřuje.

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 (viz téma Nezbytné předpoklady SSL).
2. V Systému A musí být nainstalována verze V5R3 (nebo novější verze) operačního systému OS/400. Pokud Systém A používá verzi V5R1 operačního systému OS/400, nainstalujte tyto opravy (PTF) systému OS/400 (5722-SS1):
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. Na klientském počítači s produktem iSeries Navigator musí být spuštěna verze V5R3 nebo novější verze programu iSeries Access for Windows.
4. Získání vydavatele certifikátu (CA) pro servery iSeries.
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 serveru Centrální správy.
 - a. V systému A spusíte IBM DCM (Digital Certificate Manager). Robert nyní získá nebo vytvoří certifikáty, popř. jinak nastaví nebo změní svůj systém certifikátů. Postup nastavení systému certifikátů naleznete v tématu Použití produktu DCM (Digital Certificate Manager).
 - b. Klepněte myší na **Vybrat paměť certifikátů**.
 - c. Vyberte ***SYSTEM** a klepněte myší na **Pokračovat**.
 - d. Zadejte ***SYSTEM Heslo paměti certifikátů** a klepněte myší na **Pokračovat**. Jakmile se znovu načte menu, rozbalte volbu **Spravovat aplikace**.
 - e. Klepněte myší na volbu **Aktualizace přiřazení certifikátu**.

- f. Vyberte volbu **Server** a klepněte myší na **Pokračovat**.
 - g. Vyberte volbu **Server Centrální správy** a klepněte myší na volbu **Aktualizace přiřazení certifikátu**. Tím přiřadíte certifikát k požadovanému serveru Centrální správy, aby se vytvořila identita pro klienty iSeries Access for Windows.
 - h. Klepněte myší na volbu **Přiřazení nového certifikátu**. Produkt DCM se znovu zavede na stranu **Aktualizace přiřazení certifikátu** se zprávou o potvrzení.
 - i. Klepněte myší na **Provedeno**.
8. Nastavte produkt iSeries Navigator:
- a. Na klientský počítač selektivně nainstalujte komponentu SSL pro produkt iSeries.
 - b. Stáhněte vydavatele certifikátů (CA) do klientského počítače.

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 produktu iSeries Navigator.
2. Krok 2: Nastavení úrovně autentizace pro server Centrální správy.
3. Krok 3: Restartování serveru Centrální správy v Systému A.
4. Krok 4: Aktivace SSL pro klienta produktu iSeries Navigator.
5. Volitelný krok: Deaktivace SSL pro klienta produktu iSeries Navigator.

Podrobný popis postupu konfigurace naleznete v tématu Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL.

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

V následujících informacích se předpokládá, že jste si přečetli téma Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL. V tomto scénáři je server iSeries určen jako centrální systém v lokální síti (LAN) firmy. 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.

K tomu, aby mohl Robert aktivovat na serveru Centrální správy SSL, musí na serveru iSeries nejprve nainstalovat nezbytné programy a nastavit digitální certifikáty. Dříve než budete pokračovat, seznamte se s nezbytnými podmínkami a předpoklady pro tento scénář. Jakmile Robert splní všechny nezbytné předpoklady, může pomocí následujících postupů aktivovat SSL na serveru Centrální správy.

Krok 1: Deaktivace SSL pro klienta produktu iSeries Navigator.

1. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na Systém A a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a zrušte označení **Použit SSL (Secure Sockets Layer) pro připojení**.
4. Ukončete produkt iSeries Navigator a restartujte jej.

V zásobníku Centrální správy v prostředí produktu iSeries 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 iSeries Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte na kartu **Zabezpečení** a vyberte **Použit SSL (Secure Sockets Layer)**.

3. Pro úroveň autentizace vyberte volbu **Libovolná** (je k dispozici ve verzi V5R3 nebo novější verzi produktu iSeries Access for Windows).
4. Klepněte myši na **OK** a nastavte tuto hodnotu v centrálním systému.

Krok 3: Restartování serveru Centrální správy v centrálním systému.

1. V prostředí produktu iSeries 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. Jakmile se server Centrální správy zastaví, klepněte myši na **Spustit** a server restartujte.

Krok 4: Aktivace SSL pro klienta produktu iSeries Navigator.

1. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na **Systém A** a vyberte **Vlastnosti**.
3. Klepněte myši na kartu **Secure Sockets** a vyberte **Použit SSL (Secure Sockets Layer) pro připojení**.
4. Ukončete produkt iSeries Navigator a restartujte jej.

V prostředí produktu iSeries 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 serverem Centrální správy. Ostatní spojení klientů se serverem Centrální správy a připojení z koncových bodů k serveru Centrální správy nebudou zabezpečena. Chcete-li zabezpečit další klienty, zajistěte, aby u nich byly splněny nezbytné předpoklady a opakujte Krok 4. 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 produktu iSeries 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 iSeries Navigator rozbalte **Připojení**.
2. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
3. Klepněte na kartu **Secure Sockets** a zrušte označení **Použit SSL (Secure Sockets Layer) pro připojení**.
4. Ukončete produkt iSeries Navigator a restartujte jej.

V zásobníku Centrální správy v prostředí produktu iSeries Navigator zmizí zobrazený zámek, což indikuje nezabezpečené připojení. Robert tak pozná, že mezi jeho klientským počítačem a serverem Centrální správy v Systému A nadále neexistuje spojení zabezpečené pomocí SSL.

Odkazy na další scénáře SSL najdete v tématu Scénáře.

Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL

Situace:

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

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 produkty iSeries Access for Windows a iSeries Navigator v počítači, který bude používat k přístupu k centrálnímu systému.

Tomáš si může vybrat jednu ze dvou úrovní autentizace:

Autentizace serveru

Umožňuje autentizaci certifikátu serveru koncového systému. Při připojování ke koncovému systému pracuje centrální systém jako klient SSL. Koncový systém se chová jako server SSL a musí prokázat svou identitu pomocí certifikátu, který byl vydán vydavatelem certifikátu (CA), jemuž centrální systém věří. Pro každý koncový systém musí vydavatel certifikátu (CA) vydat platný certifikát.

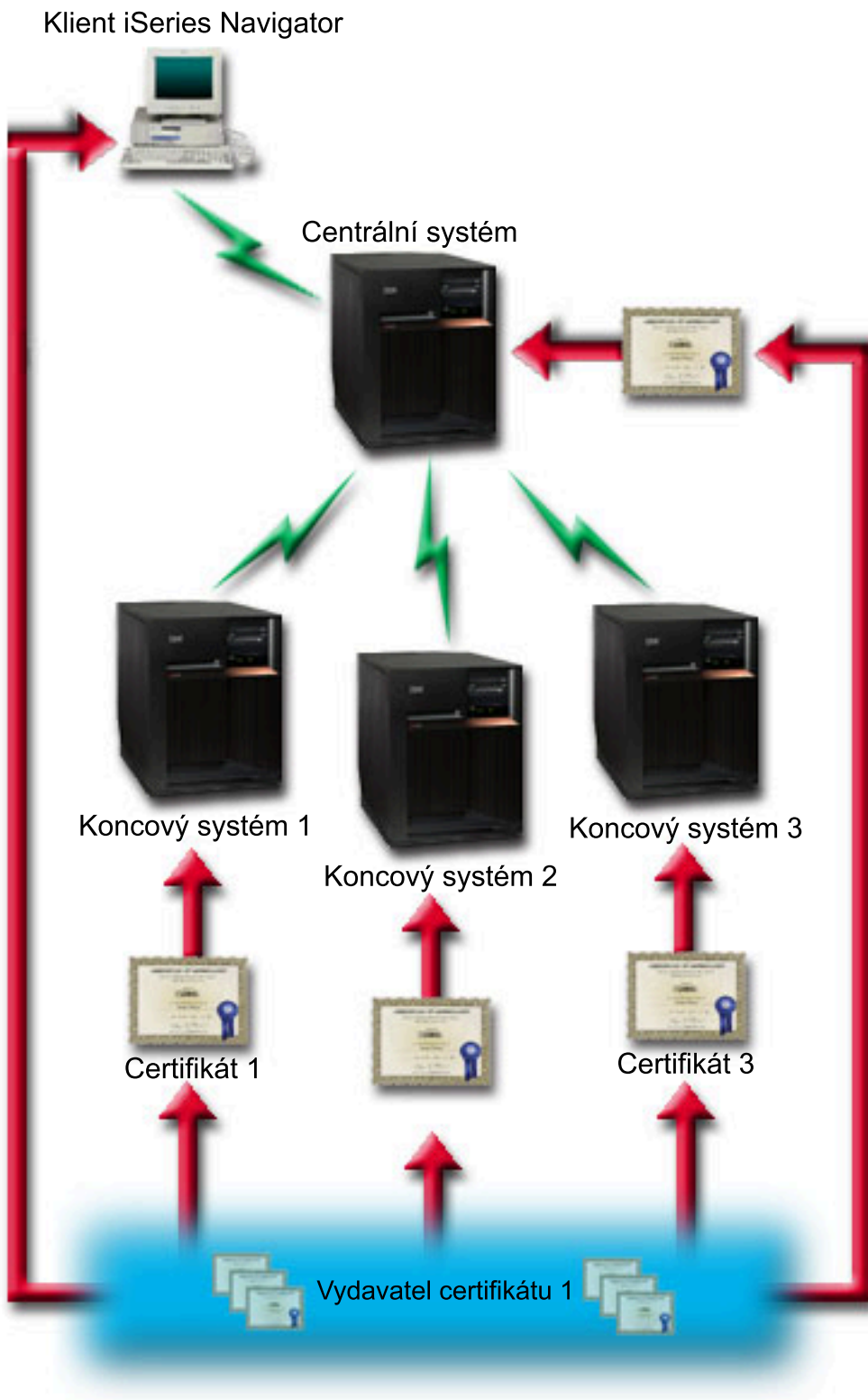
Autentizace klienta a serveru

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).

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 počítačů připojují k centrálnímu systému a je aktivován SSL, centrální systém pracuje 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.



Nezbytné podmínky a předpoklady:

K zabezpečení všech připojení k serveru Centrální správy musí Tomáš provést tyto úlohy administrace a konfigurace (viz obrázek Síť WAN Centrální správy zabezpečená pomocí SSL):

1. Centrální systém musí splňovat nezbytné předpoklady pro SSL (viz téma Nezbytné předpoklady SSL).
2. V centrálním systému a ve všech koncových serverech iSeries se musí používat verze V5R2 nebo novější verze operačního systému OS/400. Pokud se v centrálním systému a koncových bodech používá verze V5R1 operačního systému OS/400, nainstalujte tyto opravy (PTF) systému OS/400 (5722-SS1):
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. V klientském počítači s produktem iSeries Navigator musí být spuštěna verze V5R2 nebo novější verze programu iSeries Access for Windows. Používá-li klient verzi V5R1, nainstalujte servisní balík PTF SI01907 (nebo novější) pro verzi V5R1 iSeries Access for Windows (5722-XE1).
4. Získání vydavatele certifikátu (CA) pro servery iSeries.
5. Vytvoření certifikátu podepsaného vydavatelem certifikátu (CA) pro každý server iSeries, který bude spravován serverem Centrální správy podporujícím SSL.
6. Odeslání CA a certifikátu na každý server iSeries a jejich import do databáze klíčů.
7. Přiřazení certifikátů pomocí identifikace aplikací v rámci produktu Centrální správa a identifikace aplikací pro všechny koncové servery, které používá produkt iSeries Navigator:
 - a. Spusťte na centrálním serveru produkt IBM DCM (Digital Certificate Manager). Pokud chce Tomáš získat nebo vytvořit certifikáty či jinak nastavit nebo změnit certifikační systém, provede to nyní (informace o nastavení certifikačního systému najdete pod tématem Použití produktu DCM (Digital Certificate Manager)).
 - b. Klepněte myší na **Vybrat paměť certifikátů**.
 - c. Vyberte ***SYSTEM** a klepněte myší na **Pokračovat**.
 - d. Zadejte ***SYSTEM Heslo paměti certifikátů** a klepněte myší na **Pokračovat**. Jakmile se znovu načte menu, rozbalte volbu **Spravovat aplikace**.
 - e. Klepněte myší na volbu **Aktualizace přiřazení certifikátu**.
 - f. Vyberte volbu **Server** a klepněte myší na **Pokračovat**.
 - g. Vyberte volbu **Server Centrální správy** a klepněte myší na volbu **Aktualizace přiřazení certifikátu**. Tím přiřadíte certifikát k požadovanému serveru Centrální správy.
 - h. Klepněte myší na volbu **Přiřazení nového certifikátu**. Produkt DCM se znovu zavede na stranu **Aktualizace přiřazení certifikátu** se zprávou o potvrzení.
 - i. Klepněte myší na **Provedeno**.
 - j. Opakujte tuto proceduru pro všechny koncové servery, které používají produkt iSeries Navigator.
8. Nastavte produkt iSeries Navigator:
 - a. Na klientský počítač selektivně nainstalujte komponentu SSL pro produkt iSeries.
 - b. Stáhněte vydavatele certifikátů (CA) do klientského počítače.

Postup při konfiguraci:

K tomu, aby mohl Tomáš aktivovat na serveru Centrální správy SSL, musí v centrálním systému nainstalovat nezbytné programy a nastavit digitální Certifikáty. Dříve než budete pokračovat, seznamte se s nezbytnými podmínkami a předpoklady pro tento scénář. Jakmile Tomáš splní všechny nezbytné předpoklady, může pomocí následujících postupů zabezpečit všechna připojení k serveru Centrální správy:

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

- Krok 1: Konfigurace centrálního systému pro autentizaci serveru.

- Krok 2: Konfigurace koncových systémů pro autentizaci serveru.
- Krok 3: Restartování serveru Centrální správy v centrálním systému.
- Krok 4: Restartování serveru Centrální správy ve všech koncových systémech.
- Krok 5: Aktivace SSL pro klienta produktu iSeries Navigator.
- Krok 6: Konfigurace centrálního systému pro autentizaci klienta.
- Krok 7: Konfigurace koncových systémů pro autentizaci klienta.
- Krok 8: Kopírování ověřovacího seznamu do koncových systémů.
- Krok 9: Restartování serveru Centrální správy v centrálním systému.
- Krok 10: Restartování serveru Centrální správy ve všech koncových systémech.

Podrobný popis postupu konfigurace najdete v tématu Podrobnosti konfigurace: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

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

V následujících informacích se předpokládá, že jste si přečetli téma Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL. Nyní byste měli pochopit, jak provést jednotlivé kroky potřebné k zabezpečení všech spojení se serverem Centrální správy. Provádějte scénář společně s Tomášem.

K tomu, aby mohl Tomáš aktivovat na serveru Centrální správy SSL, musí na serveru iSeries nejprve nainstalovat nezbytné programy a nastavit digitální certifikáty. Dříve než budete pokračovat, seznamte se s nezbytnými podmínkami a předpoklady pro tento scénář. Jakmile Tomáš splní všechny nezbytné předpoklady, může pomocí následujících postupů zabezpečit všechna připojení k serveru Centrální správy.

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

Krok 1: Konfigurace centrálního systému pro autentizaci serveru.

SSL umožní Tomášovi zabezpečit ochranu přenosů mezi centrálním systémem a koncovým systémem i mezi klientem produktu iSeries 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. Dříve než může Tomáš konfigurovat autentizaci klienta, musí nakonfigurovat autentizaci serveru.

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Vlastnosti**.
2. Klepněte na kartu **Zabezpečení** a vyberte **Použit SSL (Secure Sockets Layer)**.
3. Jako úroveň autentizace vyberte volbu **Server**.
4. Klepněte myší na **OK** a nastavte tuto hodnotu v centrálním systému.

Poznámka: **NERESTARTUJTE** server Centrální správy, dokud nebude provedena konfigurace koncových systémů pro autentizaci serveru.

5. Konfigurace koncových systémů pro autentizaci serveru.

Krok 2: Konfigurace koncových systémů pro autentizaci serveru.

Jakmile Tomáš nakonfiguruje centrální systém pro autentizaci serveru, musí nakonfigurovat koncové systémy pro autentizaci serveru. Provede tyto úkoly:

1. Rozbalte okno **Centrální správa**.
2. Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:
 - a. Pod **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis**→**Shromažďování**.

- b. V dialogu Shromažďování zaškrtněte volbu **Systémové hodnoty**, abyste shromáždili soupis systémových hodnot pro centrální systém. Zrušte označení jakýchkoli ostatních voleb.
- 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 přes SSL.
- e. Jestliže chcete zobrazit novou skupinu, rozbalte seznam skupin systémů.
- f. Jakmile skončíte s výběrem, klepněte pravým tlačítkem myši na novou skupinu systémů a vyberte **Systémové hodnoty**—>**Porovnání a aktualizace**.
- g. Ověřte, že se centrální systém zobrazí v poli **Modelový systém**.
- h. Vyberte kategorii **Centrální správa** a ověřte tyto hodnoty (přitom zaškrtněte vedlejší políčko):
 - Pro **Použití SSL (Secure Sockets Layer)** vyberte volbu **Ano**.
 - Pro úroveň autentizace SSL vyberte volbu **Server**.

Tyto hodnoty se nastavují v centrálním systému během procedury konfigurace centrálního systému pro autentizaci serveru.
- i. Klepněte myši na **OK** a nastavte tyto hodnoty v koncových systémech v nové skupině systémů.
- j. Počkejte, až se dokončí proces **porovnání a aktualizace**, a potom restartujte server Centrální správy. To může trvat několik minut.

Krok 3: Restartování serveru Centrální správy v centrálním systému.

1. V prostředí produktu iSeries Navigator rozbalte **Připojení**.
2. Rozbalte okno centrálního systému.
3. Rozbalte volbu **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. Jakmile se server Centrální správy zastaví, klepněte myši na **Spustit** a server restartujte.

Krok 4: Restartování serveru Centrální správy ve všech koncových systémech.

1. Rozbalte koncový systém, který restartujete.
2. Rozbalte volbu **Síť**—> **Servery** a vyberte **TCP/IP**.
3. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
4. Jakmile se server Centrální správy zastaví, klepněte myši na **Spustit** a server restartujte.
5. Opakujte tuto proceduru pro všechny koncové systémy.

Krok 5: Aktivace SSL pro klienta produktu iSeries Navigator.

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

Krok 6: Konfigurace centrálního systému pro autentizaci klienta (volitelný krok).

Když Tomáš nyní dokončil konfiguraci autentizace serveru, může provést tyto volitelné procedury 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 autentizují certifikáty prostřednictvím autentizace klienta. Hovoříme také o autentizaci vydavatele certifikátu a důvěryhodné skupiny.

Poznámka: Konfiguraci autentizace klienta lze provádět až po nakonfigurování autentizace serveru.

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

2. Klepněte na kartu **Zabezpečení** a vyberte **Použití SSL (Secure Sockets Layer)**.
3. Pro úroveň autentizace vyberte volbu **Klient a server**.
4. Klepněte myši na **OK** a nastavte tuto hodnotu v centrálním systému.

Poznámka: NERESTARTUJTE server Centrální správy, dokud nenakonfigurujete všechny koncové systémy pro použití SSL při autentizaci serveru a klienta.

5. Nakonfigurujte koncové systémy pro autentizaci klienta.

Krok 7: Konfigurace koncových systémů pro autentizaci klienta (volitelný krok).

1. Porovnejte a aktualizujte systémové hodnoty pro koncové systémy:

Poznámka: Tato úloha nefunguje pro všechny koncové servery iSeries, na nichž je provozována verze V4R5.

- a. Pod **Koncové systémy** klepněte pravým tlačítkem myši na centrální systém a vyberte **Soupis—>Shromáždování**.
- b. V dialogu Shromáždování zaškrtněte volbu **Systémové hodnoty**, abyste shromáždili soupis systémových hodnot pro centrální systém. Zrušte označení jakýchkoli ostatních voleb.
- 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.
- e. Jestliže chcete zobrazit novou skupinu, rozbalte seznam skupin systémů.
- f. Jakmile skončíte s výběrem, klepněte pravým tlačítkem myši na novou skupinu systémů a vyberte **Systémové hodnoty—>Porovnání a aktualizace**.
- g. Ověřte, že se **centrální systém** zobrazí v poli **Modelový systém**.
- h. Vyberte kategorii **Centrální správa** a ověřte toto:
 - Pro **Použití SSL (Secure Sockets Layer)** vyberte volbu **Ano**.
 - Pro úroveň autentizace SSL vyberte volbu **Klient a server**.

Tyto hodnoty se nastavují v centrálním systému během procedury konfigurace centrálního systému pro autentizaci klienta. Zaškrtněte políčko **Aktualizace** vedle každé hodnoty.
- i. Klepněte myši na **OK** a nastavte tyto hodnoty v koncových systémech v nové skupině systémů.

Krok 8: Kopírování ověřovacího seznamu do koncových systémů.

1. V následujících krocích se předpokládá, že váš centrální systém je verze V5R3 nebo vyšší. V prostředí produktu iSeries Navigator rozbalte **Centrální správa—>Definice**.
2. Klepněte pravým tlačítkem myši na **Sada programů** a vyberte **Nová definice**.
3. V okně **Nová definice** pracujte s těmito volbami:
 - **Jméno:** Napište jméno definice.
 - **Zdrojový systém:** Vyberte jméno centrálního systému.
 - **Vybrané soubory a pořadače:** Klepněte myši na pole a napište /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL.
4. Klepněte myši na kartu **Volby** a vyberte **Nahradit existující soubor odesílaným souborem**.
5. Klepněte myši na **Rozšířené**.
6. V okně **Rozšířené volby** zadejte **Ano**, čímž povolíte rozdíly objektů při obnově.
7. Klepněte myši 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** umístěnou v seznamu **Dostupné systémy a skupiny**. Na seznam **Vybrané systémy a skupiny** přidejte postupně všechny systémy, které jsou verze V5R3 nebo vyšší. Odstraňte všechny ostatní systémy ze seznamu **Vybrané systémy a skupiny** a klepněte na **OK**. Důvěryhodná skupina je skupinou systémů, kterou jste definovali v kroku 1.c v rámci tématu Krok 7: Konfigurace koncových systémů pro autentizaci klienta.

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.

V systémech s verzí nižší než V5R3 byl soubor QYPSVLDL.VLDL umístěn v knihovně QUSRSYS.LIB, nikoliv v knihovně QMGTC2.LIB. Pokud jsou vaše systémy nižší verze, než je verze V5R3, budete muset zaslat ověřovací seznam do těchto systémů a budete muset tento seznam umístit do knihovny QUSRSYS.LIB (namísto do knihovny QMGTC2.LIB). To provedete takto:

- a. Klepněte pravým tlačítkem myši na definici sady programů, kterou jste vytvořili výše, a vyberte volbu **Nový podle**.
- b. Zadejte nové jméno definice, abyste ji odlišili od první definice.
- c. Na kartě **Obecné** k dané definici klepněte ve sloupci **Cesta k cílovému systému** na cestu /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL. To vám umožní cestu upravit. Změňte QMGTC2 na QUSRSYS.

Poznámka: Ujistěte se, že upravujete hodnotu **Cesta k cílovému systému**, nikoliv hodnotu **Cesta ke zdrojovému systému**.

- d. Klepněte na **OK** a uložte novou definici sady programů.
- e. Klepněte pravým tlačítkem myši na novou definici sady programů a vyberte volbu **Odeslat**.
- f. V dialogovém okně **Odeslat** postupujte následovně. Rozbalte volbu **Skupiny systémů->Důvěryhodná skupina** umístěnou v seznamu **Dostupné systémy a skupiny**. Do seznamu **Vybrané systémy a skupiny** přidejte postupně všechny systémy, které jsou nižší verze než V5R3. Odstraňte všechny ostatní systémy ze seznamu **Vybrané systémy a skupiny** a klepněte na **OK**. **Důvěryhodná skupina** je skupinou systémů, kterou jste definovali v kroku 1.c v rámci tématu Krok 7: Konfigurace koncových systémů pro autentizaci klienta.

Krok 9: Restartování serveru Centrální správy v centrálním systému.

1. V prostředí produktu iSeries 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. Jakmile se server Centrální správy zastaví, klepněte myši na **Spustit** a server restartujte.

Krok 10: Restartování serveru Centrální správy ve všech koncových systémech.

Poznámka: Opakujte tuto proceduru pro všechny koncové systémy.

1. Rozbalte koncový systém, který restartujete.
2. Rozbalte **Síť-> Servery** a vyberte **TCP/IP**.
3. Klepněte pravým tlačítkem myši na volbu **Centrální správa** a vyberte **Zastavit**.
4. Jakmile se server Centrální správy zastaví, klepněte myši na **Spustit** a server restartujte.

Odkazy na další scénáře SSL najdete v tématu Scénáře.

Koncepce

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.

Následující koncepční informace vám pomohou lépe pochopit vztah mezi SSL a serverem iSeries:

- Historie SSL.
- Jak SSL pracuje.
- Podporované protokoly SSL a TLS (Transport Layer Security).

- Autentizace serveru.
- Autentizace klienta.

Historie SSL

Protokol SSL (Secure Sockets Layer) vyvinula společnost Netscape v roce 1994 jako odpověď na rostoucí zájem o bezpečnost v síti Internet. Protokol SSL byl původně vyvinut k zabezpečení komunikace mezi webovým prohlížečem a serverem. Jeho specifikace byla navržena tak, aby ho mohly používat i další aplikace, například TELNET nebo FTP. Další informace o SSL a souvisejících protokolech najdete v tématu Podporované protokoly SSL a TLS (Transport Layer Security).

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. SSL volitelně autentizuje klienta. Digitální certifikát vydaný vydavatelem certifikátu (CA) může být přiřazen každému koncovému bodu nebo aplikacím používajícím SSL na každém koncovém bodu 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 body 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. Ve verzi V5R2M0 a následujících vydáních můžete vliv navazování spojení SSL na výkon hlavního CPU minimalizovat pomocí šifrovacího hardwaru.

Podporované protokoly SSL a TLS (Transport Layer Security).

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 OS/400 podporuje tyto verze protokolů SSL a TLS:

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

Poznámky:

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. Podporována je také 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 vyjednat 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.
- 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, aby útok MITM oslabil specifikaci šifrování. Oslabení šifrování by mohlo umožnit neoprávněně osobě odhalit 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 společností 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 iSeries, 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:

- **Kód 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.
- **Funkce PRF (Enhanced Pseudorandom Function)**
Funkce PRF generuje data klíče. V TLS definuje PFR 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.
- **Zdokonalené ověřování zprávy o dokončení**
Jak TLS verze 1.0, tak SSL verze 3.0 poskytuje zprávu o dokončení pro oba koncové body, která autentizuje, že vyměněné 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 zpracování certifikátů**
Na rozdíl od SSL verze 3.0 se TLS pokouší určit typ certifikátu, který si musejí vyměnit implementace TLS.
- **Specifické varovné zprávy**
TLS poskytuje konkrétnější a nové varovné zprávy pro označení problémů, které některý z koncových bodů relace detekuje. TLS také dokumentuje, kdy by měly být odeslány určité varovné zprávy.

Autentizace serveru

Při autentizaci serveru klient zjistí, že je platný certifikát serveru a že je tento certifikát podepsaný vydavatelem certifikátu (CA), kterému klient důvěřuje. 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 platný certifikát klienta a že je tento certifikát podepsán vydavatelem certifikátu (CA), kterému server důvěřuje. Následující aplikace serveru iSeries podporují autentizaci klienta:

- Server IBM HTTP Server (provozovaný na bázi Apache).
- Server FTP.
- Server Telnet.
- Koncový systém Centrální správy.
- LDAP (Directory Services).

Plánování umožnění SSL

Když plánujete umožnění SSL na serveru iSeries, musíte vzít v úvahu níže uvedené skutečnosti:

- Nezbytné předpoklady pro SSL.
- Jaký typ digitálních certifikátů chcete a kde je získáte.

Nezbytné předpoklady pro SSL:

- Produkt IBM DCM (Digital Certificate Manager), volba 34 operačního systému OS/400 (5722-SS1).
- TCP/IP Connectivity Utilities for iSeries (5722-TC1).
- IBM HTTP Server for iSeries (5722-DG1).
- Chcete-li kvůli používání produktu DCM použít HTTP server, ujistěte se, že je nainstalován produkt IBM Developer Kit for Java (5722-JV1). Jinak se server HTTP Administration Server nespustí.
- Produkt IBM Cryptographic Access Provider, 5722-AC3 (128bitový). Počet bitů pro tento produkt označuje maximální velikost utajovaného materiálu v symetrických klíčích, který může být použit v šifrovacích operacích. Velikost povolená pro symetrický klíč se řídí exportními a importními zákony každé země. Vyšší počet bitů má za následek bezpečnější spojení.
- Můžete také instalovat šifrovací hardware pro použití se SSL, abyste urychlili navazování spojení SSL. Dostupné volby naleznete v informacích o šifrovacím hardwaru. Chcete-li instalovat šifrovací koprocessor 4758 IBM Cryptographic Coprocessor nebo 4764 IBM Cryptographic Coprocessor, musíte nainstalovat také volbu 35 Cryptographic Service Provider.

Jestliže chcete používat SSL s komponentami produktu iSeries Access for Windows, musíte nainstalovat také produkt iSeries Client Encryption, 5722-CE3 (128bitový). Produkt iSeries Access for Windows vyžaduje tento produkt, aby vytvořil zabezpečené spojení.

Poznámka: Produkt Client Encryption nemusíte instalovat, abyste mohli používat emulátor PC5250, který se dodává s produktem Personal Communications. Produkt Personal Communications má svůj vestavěný šifrovací kód.

Digitální certifikáty

Přečtěte si téma Použití veřejných certifikátů versus použití privátních certifikátů, abyste lépe pochopili rozdíly mezi veřejnými a privátními digitálními certifikáty a dověděli se o možnostech jejich získání.

Produkt IBM DCM (Digital Certificate Manager) je řešení serveru iSeries pro správu digitálních certifikátů. Více informací o produktu DCM najdete v rámci aplikace Information Center pod tématem Digital Certificate Manager.

Zabezpečení aplikací pomocí SSL

Pomocí SSL můžete zabezpečit ochranu těchto aplikací serveru iSeries:

- EIM (Enterprise Identity Mapping).
- Server FTP.
- HTTP server (provozovaný na bázi Apache).
- iSeries Access for Windows.
- LDAP (Directory Services Server).
- Server DRDA (distributed relational database architecture) a DDM (distributed data management).
- Server Centrální správy.
- Server Telnet.
- Aplikační server Websphere Application Server - Express.
- Aplikace napsané pro sadu rozhraní API produktu iSeries Access for Windows.
- Aplikace vyvinuté pomocí rozhraní Secure Sockets API podporovaných na serveru iSeries. Podporovaná rozhraní API jsou GSKit (Global Secure Toolkit) a nativní rozhraní API SSL_ iSeries. Informace o GSKit a SSL_API najdete pod tématem Secure Sockets APIs.

Odstraňování problémů se SSL

Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, které může server iSeries detekovat u SSL. Je důležité, abyste pochopili, že toto není vyčerpávající zdroj informací pro odstraňování problémů, ale pouze průvodce.

Ověřte, že jsou pravdivá tato tvrzení:

- Splnili jste nezbytné předpoklady pro SSL na serveru iSeries (viz téma Nezbytné předpoklady pro SSL).
- Používáte-li komponentu Centrální správa produktu iSeries Navigator se systémem V5R1, nainstalovali jste v systému tato PTF:
 - si01375
 - si01376
 - si01377
 - si01378
 - si01838
- Váš vydavatel certifikátu (CA) a certifikáty jsou platné a nemají prošlé datum.

Jestliže jste ověřili, že předcházející tvrzení jsou pro váš systém pravdivá, a stále máte problém související se SSL, vyzkoušejte tyto možnosti:

- Chybový kód SSL v protokolu úloh serveru může mít křížovou referenci v tabulce chyb, kde můžete najít více informací o chybě. Informace o chybových zprávách rozhraní Secure Sockets API najdete na stránce Chybové zprávy o kódech rozhraní Secure Sockets API. 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 naprogramovat `gsk_strerror()` nebo `SSL_strerror()` API v programech, aby získali stručný popis návratového kódu chyby. Některé aplikace využijí tato rozhraní API a vytisknou do protokolu úloh zprávu, která obsahuje tuto větu.

Pokud požadujete podrobnější informace, je možné na serveru iSeries zobrazit ID zprávy uvedené v tabulce kvůli 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 systémového SSL jako tabulka, ale bez křížové reference ID zprávy:
 - QSYSINC/H.GSKSSL
 -



QSYSINC/H.QSOSSL

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

Další informace o odstraňování problémů se serverem iSeries server najdete v tématu nazvaném Troubleshooting and service, které se zabývá odstraňováním problémů a servisem.


Související informace

Další informace o SSL můžete najít v těchto zdrojích:

Zdroje IBM

- Téma SSL and Java Secure Socket Extension (JSSE) obsahuje stručný popis JSSE a jejího použití.
- Téma IBM Toolbox for Java obsahuje stručný popis dostupných tříd Java a jejich použití.

RFC (Request for Comments)

- RFC 2246: "The TLS Protocol Version 1.0"  vysvětluje podrobně protokol TLS.
- RFC2818: "HTTP Over TLS"  popisuje, jak použít TLS pro zabezpečení připojení HTTP na Internetu.

Jiné zdroje

- Dokument The SSL Protocol Version 3.0  vysvětluje podrobně protokol SSL verze 3.0.

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. Použití 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
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

S dotazy ohledně licencí týkajícími se informací v dvoubajtové znakové sadě (DBCS) se obraťte na IBM Intellectual Property Department ve své zemi nebo zašlete písemně dotaz na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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 NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řady některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk 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 nebo měnit produkty a programy 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 jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoli 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 49XA
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 popsany v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, ve smlouvě IBM International Program License nebo v jiné ekvivalentní smlouvě.

Všechny informace o provozu byly určeny v řízeném prostředí. Výsledky získané v jiném provozním prostředí se tudíž mohou výrazně lišit. Některá měření byla provedena v systémech s vývojovým prostředím a neexistuje žádná záruka, že tato měření budou stejná v obecně dostupných systémech. Některá měření byla odhadnuta extrapolací. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit vhodnost dat pro svá specifická prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže potvrdit přesnost údajů o výkonu, kompatibilitě nebo jiná tvrzení, která se k těmto produktům vztahují. 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.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA a případně v dalších jiných zemích:

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows NT

Lotus, Freelance a WordPro jsou ochrannými známkami společností IBM a Lotus Development Corporation v USA a případně v dalších jiných zemích.

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

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

Ustanovení a podmínky pro stahování a tisk publikací

Oprávnění k používání publikací, které jste se rozhodli stáhnout, závisí na níže uvedených ustanoveních a podmínkách a na vašem potvrzení, že je akceptujete.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoli 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, šířit a prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace a veškeré 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 udělená tímto dokumentem, kdykoli usoudí, že používání publikací poškozuje její 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. PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI "JAK JSOU" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL.

Autorská práva na veškeré materiály náleží společnosti IBM Corporation.

Stážením nebo vytištěním publikace z tohoto serveru vyjadřujete svůj souhlas s těmito ustanoveními a podmínkami.



Vytištěno v Dánsku společností IBM Danmark A/S.