



Systemy IBM - iSeries

Zabezpečení

Secure Sockets Layer (SSL)

Verze 5, vydání 4





Systemy IBM - iSeries

Zabezpečení

Secure Sockets Layer (SSL)

Verze 5, vydání 4

Poznámka

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

Šesté vydání (únor 2006)

Toto vydání se vztahuje k verzi 5, vydání 4, modifikaci 0 operačního systému i5/OS (5722–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.

© Copyright International Business Machines Corporation 2002, 2006. Všechna práva vyhrazena.

Obsah

SSL (Secure Sockets Layer)	1
Co je nového ve verzi V5R4	1
Tisk souborů ve formátu PDF	1
Scénáře	1
Scénář: Zabezpečení spojení klienta se serverem	
Centrální správy pomocí SSL	2
Situace	2
Cíle:	2
Podrobnosti:	2
Nezbytné podmínky a předpoklady	2
Postup při konfiguraci	3
Scénář: Zabezpečení všech spojení se serverem Centrální	
správy pomocí SSL	5
Situace:	5
Podrobnosti:	5
Nezbytné podmínky a předpoklady:	7
Postup při konfiguraci:	8
Koncepce	13

Historie SSL	13
Jak SSL pracuje	13
Podporované protokoly SSL a TLS (Transport Layer	
Security)	13
Autentizace serveru	15
Autentizace klienta	15
Plánování použití SSL	15
Nezbytné předpoklady pro SSL	15
Digitální certifikáty	16
Zabezpečení aplikací pomocí SSL	16
Odstraňování problémů SSL	16
Související informace k tématu SSL (Secure Sockets	
Layer)	17

Dodatek. Upozornění.	19
Ochranné známky	20
Ustanovení a podmínky	21

SSL (Secure Sockets Layer)

Toto téma popisuje, jak používat SSL na serveru.

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 V5R4



Toto téma popisuje, co je v tomto vydání nového v oblasti SSL (Secure Sockets Layer).

Ukončený produkt: IBM Cryptographic Access Provider, 5722-AC3 (128-bit)

Produkt IBM Cryptographic Access Provider, 5722-AC3 (128-bit) není již třeba. Namísto toho je zde nová verze V5R4 operačního systému i5/OS. Všechny systémy verze V5R4 poskytují stejné funkce, které poskytoval produkt 5722-AC3.

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.

Tisk souborů ve formátu PDF

Tyto informace si lze zobrazit a vytisknout 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. V prohlížeči klepněte pravým tlačítkem myši na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na volbu pro lokální uložení PDF.
3. Vyhledejte adresář, do něhož chcete soubor PDF uložit.
4. Klepněte na **Save** (Uložit).

Stážení 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

Tyto scénáře byly navrženy za účelem co největšího využití výhod aktivace SSL na serveru iSeries.

Tyto scénáře obsahují příklady, které ilustrují možnosti použití SSL. Po jejich prostudování lépe porozumíte, jak SSL na serveru iSeries funguje.

Související informace

Scénář: Zabezpečení Telnet pomocí SSL

Scénář: Zvýšení výkonu SSL na serveru iSeries

Scénář: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL

Informace uvedené v tomto scénáři slouží k zabezpečení spojení vzdáleného klienta s vaším serverem.

Tento scénář popisuje, jak pomocí SSL zabezpečit spojení mezi vzdáleným klientem a serverem iSeries, který používá server Centrální správy (iSeries Navigator) a funguje jako centrální systém.

Situace

Firma provozuje lokální síť (LAN), která obsahuje několik serverů iSeries. Systémový administrátor této firmy (Robert) určil jeden z těchto serverů 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 serverů iSeries v síti LAN se serverem Centrální správy nebudou zabezpečeny 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 musí být nainstalována verze V5R3 operačního systému OS/400 nebo vyšší verze operačního systému i5/OS.

3. Na klientském počítači s produktem iSeries Navigator musí být spuštěna verze V5R3 vyšší verze produktu 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 identifikace aplikací pro všechny servery iSeries Access. K serverům produktu iSeries Access 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 na server iSeries 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.

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 15

Související informace

Konfigurace DCM

Spuštění DCM (Digital Certificate Manager)

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

Podrobnosti konfigurace: Zabezpečení spojení klienta se serverem 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 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.

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 15

Související úlohy

“Nezbytné podmínky a předpoklady:” na stránce 7

Související informace

Prvotní nastavení certifikátů

Krok 1: Deaktivace SSL pro klienta produktu iSeries Navigator:

Tento krok je nezbytný v případě, že máte již na klientovi produktu iSeries Navigator nastaven protokol SSL.

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 výběr volby **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt iSeries Navigator a opět jej spusťte.

V sekci Centrální správa 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 **Použít SSL (Secure Sockets Layer)**.
3. Pro úroveň autentizace vyberte volbu **Libovolná** (je k dispozici v produktu iSeries Access for Windows verze V5R3 nebo vyšší).
4. Klepněte na **OK** a nastavte tuto hodnotu v centrálním systému.

Krok 3: Restart 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. Když se server Centrální správy zastaví, klepněte myší na **Spustit** a server opět spusťte.

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 na kartu **Secure Sockets** a vyberte volbu **Použít pro připojení SSL (Secure Sockets Layer)**.
4. Ukončete produkt iSeries Navigator a opět jej spusťte.

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 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 produktu iSeries Navigator” na stránce 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 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 iSeries Navigator a opět jej spusťte.

Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL

Tento scénář popisuje, jak zabezpečit všechna spojení se serverem iSeries pomocí SSL.

Tento scénář popisuje, jak pomocí SSL zabezpečit všechna spojení se serverem iSeries, který používá server Centrální správy (iSeries Navigator) a funguje jako centrální systém.

Související pojmy

“Zabezpečení aplikací pomocí SSL” na stránce 16

Toto téma obsahuje přehled aplikací, které můžete na serveru iSeries zabezpečit pomocí SSL.

Situace:

Firma právě nainstalovala síť WAN (wide area network), která zahrnuje několik serverů iSeries ve vzdálených systémech (koncových bodech). Koncové systémy 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 pomocí SSL (Secure Sockets Layer) zabezpečit všechna spojení mezi serverem Centrální správy v centrálním systému firmy a všemi servery a klienty iSeries Access.

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 iSeries 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 iSeries Navigator na PC, nebo server Centrální správy v centrálním systému. Když se připojuje produkt iSeries 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

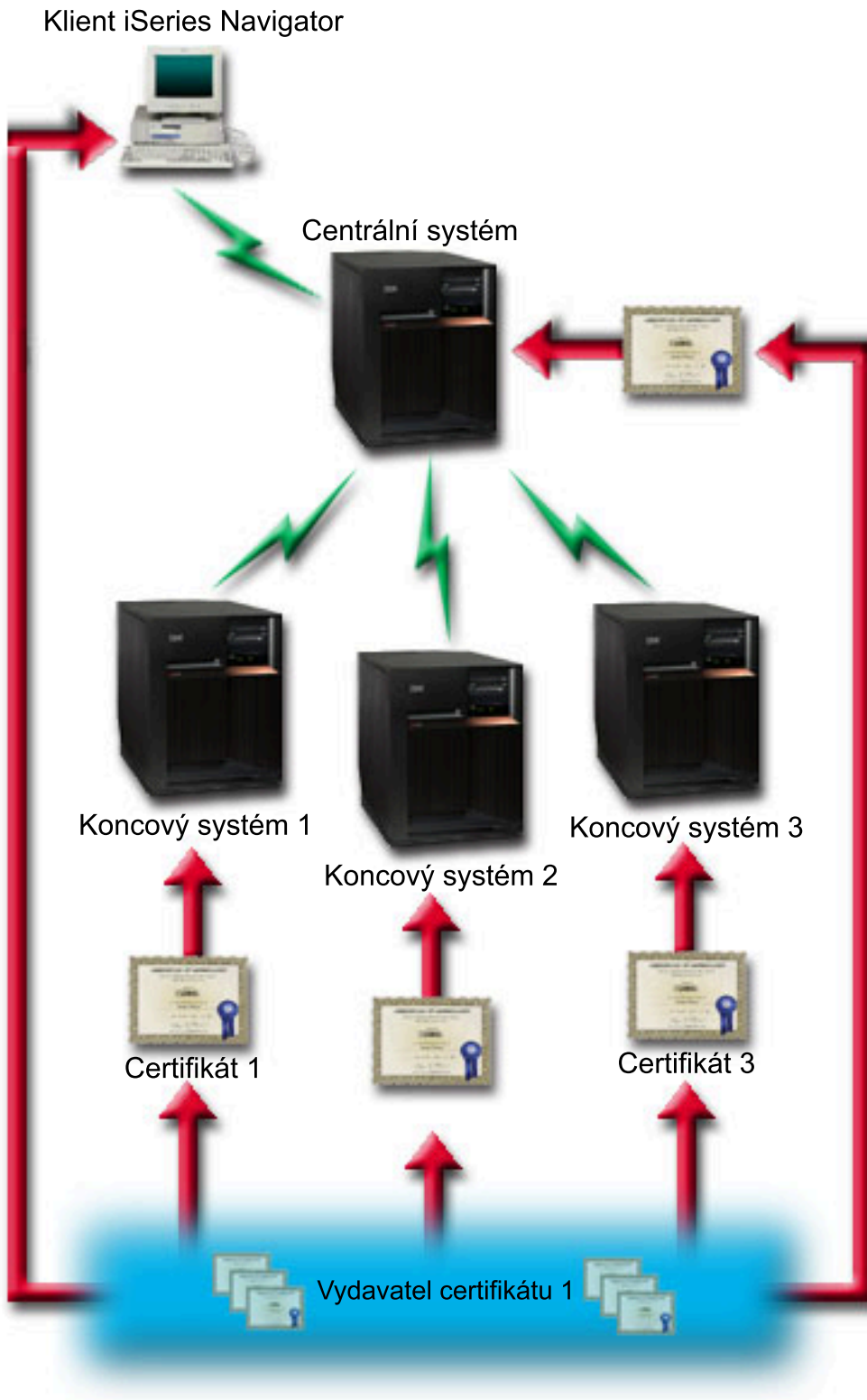
(klient SSL) pokouší vytvořit spojení s koncovým systémem (server SSL), centrální systém a koncový systém si navzájem autentizují certifikáty kvůli pravosti vydavatele certifikátu (CA).

Poznámka: Autentizace klienta a serveru se provádí pouze mezi dvěma systémy iSeries. 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. V centrálním systému a na všech koncových serverech iSeries se musí používat verze V5R2 nebo novější operačního systému OS/400 nebo i5/OS. Připojení operačního systému i5/OS verze V5R4 k operačním systémům OS/400 není povoleno.
3. Na klientském počítači s produktem iSeries Navigator musí být spuštěna verze V5R2 nebo novější produktu 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 Centrální správy a identifikace aplikací pro všechny servery iSeries Access. K serverům produktu iSeries Access 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 serveru 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 servery iSeries Access.
8. Stáhněte si vydavatele certifikátů (CA) na klientský PC produktu iSeries Navigator.

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 15

Související úlohy

“Podrobnosti konfigurace: Zabezpečení spojení klienta se serverem Centrální správy pomocí SSL” na stránce 3
Toto téma uvádí postup při konfiguraci zabezpečení spojení klienta se serverem Centrální správy pomocí SSL.

“Podrobnosti konfigurace: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL” na stránce 9
Toto téma uvádí podrobnosti zabezpečení všech spojení se serverem Centrální správy pomocí SSL.

Související informace

V5R1 Information Center, “Zabezpečení Centrální správy”

Použití DCM (Digital Certificate Manager)

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, podívejte se na tento scénář v tématu “Nezbytné podmínky a předpoklady:” na stránce 7. Když 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 jej 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.

1. “Krok 1: Konfigurace centrálního systému pro autentizaci serveru”
2. “Krok 2: Konfigurace koncových systémů pro autentizaci serveru” na stránce 10
3. “Krok 3: Restart serveru Centrální správy v centrálním systému” na stránce 10
4. “Krok 4: Restart serveru Centrální správy ve všech koncových systémech” na stránce 10
5. “Krok 5: Aktivace SSL pro klienta iSeries 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 serveru Centrální správy v centrálním systému” na stránce 12
10. “Krok 10: Restart serveru Centrální správy ve všech koncových systémech” na stránce 12

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 15

Související informace

Prvotní nastavení certifikátů

Podrobnosti konfigurace: Zabezpečení všech spojení se serverem 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.

Aby mohl Tomáš aktivovat SSL na serveru Centrální správy, musí na server iSeries nejprve 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 iSeries Navigator, musí jej Tomáš nejdříve deaktivovat, aby mohl aktivovat SSL na serveru Centrální správy. Jestliže byl SSL aktivován pro produkt iSeries Navigator, a nikoli pro server Centrální správy, pokusy produktu iSeries Navigator o připojení k centrálnímu systému selžou.

SSL umožní Tomášovi zabezpečit ochranu přenosů mezi centrálním a koncovým systémem i mezi klientem 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. Než bude moci Tomáš nastavit autentizaci klienta, musí nastavit autentizaci serveru.

Související pojmy

“Nezbytné předpoklady pro SSL” na stránce 15

Související úlohy

“Nezbytné podmínky a předpoklady:” na stránce 7

Související informace

Prvotní nastavení certifikátů

Krok 1: Konfigurace centrálního systému pro 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 **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 **Použit 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 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. Když se server Centrální správy zastaví, klepněte myši na **Spustit** a server opět spusťte.

Krok 4: Restart serveru Centrální správy ve všech koncových systémech:

1. V prostředí produktu iSeries 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 myši na **Spustit** a server opět spusťte.
6. Tuto proceduru opakujte pro všechny koncové systémy.

Krok 5: Aktivace SSL pro klienta iSeries Navigator:

1. V prostředí produktu iSeries 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 iSeries 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 iSeries 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 přenesou 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 přenesou 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 V5R3 nebo vyšší. V systémech 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 iSeries 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 **Rozšíření**.
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 v **Důvěryhodné skupině** nějaké systémy verze nižší než V5R3, 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 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. Když se server Centrální správy zastaví, klepněte myši na **Spustit** a server opět spusťte.

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

Poznámka: Tuto proceduru opakujte pro všechny koncové systémy.

1. V prostředí produktu iSeries 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 myši na **Spustit** a server opět spusťte.

Koncepce

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.

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 jej mohly používat i další aplikace, například TELNET nebo FTP.

Související pojmy

“Podporované protokoly SSL a TLS (Transport Layer Security)”

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

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 dekodování 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 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 (Transport Layer Security)

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 iSeries 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.

- 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 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:

- **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 pojmy

“Historie SSL” na stránce 13

Protokol SSL (Secure Sockets Layer) vyvinula společnost Netscape v roce 1994 jako odpověď na rostoucí zájem o bezpečnost v síti Internet.

Související informace

Protokol TLS

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 iSeries:

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

Plánování použití SSL

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

Související pojmy

“Odstraňování problémů SSL” na stránce 16

Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, které může server iSeries detekovat u SSL.

Nezbytné předpoklady pro SSL

- Produkt IBM DCM (Digital Certificate Manager), volba 34 operačního systému i5/OS (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 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 volbu 35 Cryptographic Service Provider.

Související informace

Šifrovací hardware

Digitální certifikáty

Systémovým řešením pro správu digitálních certifikátů je produkt IBM DCM (Digital Certificate Manager).

Související informace

Veřejné certifikáty versus soukromé certifikáty

Konfigurace DCM

Zabezpečení aplikací pomocí SSL

Toto téma obsahuje přehled aplikací, které můžete na serveru iSeries zabezpečit pomocí SSL.

Pomocí SSL můžete zabezpečit ochranu těchto aplikací serveru iSeries:

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

Související pojmy

“Scénář: Zabezpečení všech spojení se serverem Centrální správy pomocí SSL” na stránce 5

Tento scénář popisuje, jak zabezpečit všechna spojení se serverem iSeries pomocí SSL.

Související informace

EIM (Enterprise Identity Mapping)

Použití SSL k zabezpečení FTP serveru

HTTP server

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

Scénář: Zabezpečení Telnet pomocí SSL

Rozhraní Secure Sockets API

Odstraňování problémů SSL

Tyto základní informace o odstraňování problémů vám mají pomoci zredukovat seznam možných problémů, které může server iSeries 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 serveru iSeries.

- 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 serveru iSeries 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 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.

Související pojmy

“Plánování použití SSL” na stránce 15

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





Související informace

Služby a podpora

Chybové zprávy rozhraní Secure socket API

Související informace k tématu 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.
- The SSL Protocol Version 3.0 document  (<http://home.netscape.com/eng/ssl3/ssl-toc.html>)
Velmi podrobně vysvětluje protokol SSL verze 3.0.
- The SSL Encryption explained 3.0 information  (<http://www.digicert.com/ssl>)
Pojednává o šifrování SSL s důrazem na certifikáty.

Další informace

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


Ukládání souborů ve formátu PDF

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

1. V prohlížeči klepněte pravým tlačítkem myši na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).

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)  .

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. Použit 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 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 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 popsany v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě na programy, v Mezinárodní licenční smlouvě IBM na strojový kód 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 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.

Všechny uváděné ceny IBM jsou doporučené maloobchodní ceny IBM, které platí v současné době a mohou být změněny bez předchozího upozornění. Ceny u jednotlivých prodejců se mohou lišit.

Informace zde uvedené slouží pouze pro účely plánování. Mohou být změněny ještě před uvedením produktu na trh.

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 jsou odvozeny ze vzorových programů společnosti IBM Corporation. © 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 ochrannými známkami IBM v USA a případně v dalších jiných zemích:

DRDA
i5/OS
IBM
iSeries
OS/400

Intel, Intel Inside (loga), MMX a Pentium jsou ochranné známky společnosti Intel Corporation ve Spojených státech a případně v dalších jiných zemích.

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

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

Linux je ochranná známka, jejímž majitelem je Linus Torvalds, ve Spojených státech a případně v dalších jiných zemích.

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

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 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, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoli 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 NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.



Vytištěno v Dánsku společností IBM Danmark A/S.