Systemy IBM - iSeries

Ochrona
Protokół SSL (Secure Sockets Layer)

Wersja 5 Wydanie 4

Systemy IBM - iSeries

Ochrona
Protokół SSL (Secure Sockets Layer)

Wersja 5 Wydanie 4

Uwaga

Przed korzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje znajdujące się w dodatku “Uwagi”, na stronie 19.

Wydanie szóste (luty 2006)

To wydanie dotyczy wersji 5, wydania 4, modyfikacji 0 systemu operacyjnego i5/OS (5722–SS1 oraz wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie określono inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Protokół SSL (Secure Sockets Layer)

W tym temacie znajdują się informacje dotyczące używania protokołu SSL na serwerze

Protokół SSL jest standardem przemysłowym umożliwiającym aplikacjom nawiązywanie chronionych sesji komunikacyjnych poprzez niezabezpieczoną sieć, taką jak Internet.

Co nowego w wersji V5R4

W temacie opisano zmiany wprowadzone w bieżącej wersji protokołu SSL

Wycofano produkt: IBM Cryptographic Access Provider, 5722-AC3 (128-bitowy)

Produkt IBM Cryptographic Access Provider, 5722-AC3 (128-bitowy) nie jest już wymagany. Jest to zmiana wprowadzona w wersji V5R4 systemu i5/OS. Wszystkie systemy w wersji V5R4 są wyposażone w funkcje poprzednio udostępniane przez produkt 5722-AC3.

Jak uzyskać informacje o nowościach lub zmianach

Aby ułatwić odnalezienie miejsc, w których wprowadzono zmiany techniczne, użyto następujących symboli:

- symbolu » wskazującego miejsce, gdzie się one rozpoczynają,
- symbolu « wskazującego, gdzie się kończą.

Drukowanie plików PDF

W tym temacie opisano przeglądanie i drukowanie pliku PDF z tymi informacjami.

Aby wyświetlić lub pobrać wersję PDF tego dokumentu, wybierz temat Protokół SSL (Secure Sockets Layer).

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu dalszego wykorzystania:

1. Prawym przyciskiem myszy kliknij plik PDF w przeglądarce (prawym przyciskiem myszy kliknij odsyłacz powyżej).
2. Kliknij opcję zapisania pliku PDF na komputerze lokalnym.
3. Przejdź do katalogu, w którym ma być zapisany plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Jego bezpłatną kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Scenariusze

Poniższe scenariusze SSL mają na celu pomoc w maksymalizacji korzyści wynikających z włączenia protokołu SSL na serwerze iSeries:

Przedstawione w scenariuszach SSL przykładowe zastosowania pozwalają lepiej zrozumieć działanie protokołu SSL na serwerze iSeries.

Informacje pokrewne

Scenariusz: Ochrona aplikacji Telnet za pomocą SSL

Scenariusz: Zwiększenie wydajności protokołu SSL systemu iSeries

Scenariusz: Wykorzystanie sprzętu szyfrującego do zabezpieczania prywatnych kluczy

Scenariusz: Ochrona połączenia klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL

Informacje zawarte w tym rozdziale będą przydatne podczas konfigurowania ochrony połączenia między klientem zdalnym a serwerem za pomocą protokołu SSL.

Scenariusz wyjaśnia sposób używania protokołu SSL do ochrony połączenia między klientem zdalnym a serwerem iSeries działającym jako serwer centralny, poprzez użycie serwera Centrum Zarządzania w programie iSeries Navigator.

Sytuacja:

Firma dysponuje siecią LAN zawierającą wiele serwerów iSeries w biurze. Administrator systemu w tej firmie, Robert, określił jeden z serwerów iSeries jako system centralny (nazywany Systemem A) w sieci LAN. Robert używa serwera Centrum Zarządzania w Systemie A do zarządzania wszystkimi pozostałymi systemami końcowymi w tej sieci LAN.

Robert chce się połączyć z serwerem Centrum Zarządzania w Systemie A z sieci lokalnej znajdującej się poza jego firmą. Robert wiele podróżuje i podczas podróży potrzebuje bezpiecznego połączenia z serwerem Centrum Zarządzania. Chce mieć bezpieczne połączenie między komputerem PC i serwerem Centrum Zarządzania, gdy znajduje się poza biurem. Robert decyduje się na włączenie protokołu SSL na swoim komputerze PC oraz na serwerze Centrum Zarządzania w Systemie A. W przypadku protokołu SSL włączonego w ten sposób Robert może być pewien, że podczas podróży jego połączenie z serwerem Centrum Zarządzania jest bezpieczne.

Cele:

Robert chce chronić połączenie między swoim komputerem PC i serwerem Centrum Zarządzania. Robert nie wymaga dodatkowej ochrony połączenia między serwerem Centrum Zarządzania w Systemie A i systemami końcowymi w sieci LAN. Pozostali pracownicy biura nie potrzebują dodatkowej ochrony połączeń z serwerem Centrum Zarządzania. Robert planuje skonfigurować swój komputer PC i serwer Centrum Zarządzania w Systemie A tak, aby połączenie używało uwierzytelniania serwera. Połączenia z serwerem Centrum Zarządzania z komputerów PC lub serwerów iSeries w sieci LAN nie są chronione przez protokół SSL.

Szczegóły:

Poniższa tabela przedstawia typy używanego uwierzytelniania na podstawie włączania i wyłączania protokołu SSL w kliencie PC:

Tabela 1. Wymagane elementy dla połączenia między klientem i serwerem Centrum Zarządzania chronionego za pomocą protokołu SSL

Status SSL na komputerze PC Roberta	Określony poziom uwierzytelniania dla serwera Centrum Zarządzania w Systemie A	Czy włączono połączenie SSL?
Protokół SSL wyłączony	Dowolny	Nie
Protokół SSL jest włączony	Dowolny	Tak (uwierzytelnianie serwera)

Uwierzytelnianie serwera oznacza, że komputer PC Roberta uwierzytelnia certyfikat serwera Centrum Zarządzania. Komputer PC Roberta podczas łączenia się z serwerem Centrum Zarządzania działa jako klient SSL. Serwer Centrum Zarządzania działa jako serwer SSL i musi udowodnić swoją tożsamość. Serwer Centrum Zarządzania czyni to, udostępniając certyfikat wystawiony przez ośrodek certyfikacji (CA), któremu ufa komputer PC Roberta.

Wymagania wstępne i założenia:

Robert musi wykonać poniższe zadania administrowania i konfiguracji, aby chronić połączenie między swoim komputerem PC a serwerem Centrum Zarządzania w systemie A:

1. Sprawdzić, czy System A spełnia wymagania wstępne dla protokołu SSL.
2. Upewnić się, że w Systemie A jest zainstalowany system OS/400 w wersji V5R3 lub nowsza wersja systemu i5/OS.
3. Upewnić się, że klient PC iSeries Navigator ma zainstalowaną wersję V5R3 lub nowszą programu iSeries Access for Windows.
4. Znaleźć ośrodek wydający certyfikaty (CA) dla serwerów iSeries.
5. Utworzyć certyfikat podpisany przez ośrodek certyfikacji dla systemu A.
6. Wysłać ośrodek certyfikacji i certyfikat do Systemu A oraz zaimportować go do bazy danych kluczy.
7. Przypisać certyfikat z identyfikacją serwera Centrum Zarządzania i identyfikacjami aplikacji dla wszystkich serwerów iSeries Access. Serwerami dostępu iSeries są: serwer centralny TCP, serwer bazy danych, serwer kolejek danych, serwer plików, sieciowy serwer wydruków, serwer komend zdalnych i serwer wpisywania się do systemu.
   a. W Systemie A uruchom program IBM Digital Certificate Manager. Robert uzyskuje lub tworzy certyfikaty albo konfiguruje lub zmienia system certyfikacji.
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz hasło bazy certyfikatów *SYSTEM i kliknij przycisk **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.
   e. Kliknij **Aktualizacja przypisania certyfikatów**.
   f. Wybierz **Serwer** i kliknij **Kontynuuj**.
   g. Wybierz pozycję **Serwer Centrum Zarządzania** i kliknij przycisk **Aktualizacja przypisania certyfikatów**. Powoduje to przypisanie certyfikatu do serwera Centrum Zarządzania.
   h. Kliknij **Przypisanie nowego certyfikatu**. Program DCM zostanie przeładowany do strony Aktualizacja przypisania certyfikatów z komunikatem potwierdzającym.
   i. Kliknij **Gotowe**.
   j. Przypisz certyfikat do wszystkich serwerów dostępu klienta.
8. Pobrać ośrodek certyfikacji (CA) do klienta PC.

Zanim Robert będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy oraz skonfigurować certyfikaty cyfrowe na serwerze iSeries. Po spełnieniu wymagań wstępnych Robert może wykonać poniższe procedury w celu włączenia protokołu SSL dla serwera Centrum Zarządzania.

Pojęcia pokrewne

“Wymagania wstępne protokołu SSL” na stronie 16

Informacje pokrewne

Konfigurowanie programu DCM

Uruchamianie programu Digital Certificate Manager

Etapy konfiguracji

Robert musi wykonać poniższe czynności, aby zabezpieczyć połączenie swojego komputera PC z serwerem Centrum Zarządzania w Systemie A za pomocą protokołu SSL:

1. “Punkt 1: Deaktywuj protokół SSL dla klienta iSeries Navigator.” na stronie 4
2. “Punkt 2: Ustaw poziom uwierzytelniania dla serwera Centrum Zarządzania” na stronie 4
3. “Punkt 3: Zrestartuj serwer Centrum Zarządzania w systemie centralnym” na stronie 4
4. “Punkt 4: Aktywuj protokół SSL dla klienta iSeries Navigator.” na stronie 4

5. **Opcjonalne:** “Etap opcjonalny: Deaktywuj SSL dla klienta iSeries Navigator” na stronie 5

Szczegóły konfiguracji: Ochrona połączenia klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL

W temacie przedstawiono w rozwinięciu etapy konfigurowania ochrony połączeń klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

W poniższym opisie przyjęto, że użytkownik zapoznał się z sekcją Scenariusz: Ochrona połączenia klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

W tym scenariuszu serwer iSeries jest systemem centralnym w firmowej sieci LAN. Robert używa serwera Centrum Zarządzania w systemie centralnym (nazywanym tutaj Systemem A) do zarządzania systemami końcowymi w firmowej sieci. Poniższe informacje wyjaśniają sposób wykonywania czynności wymaganych do ochrony połączenia klienta zewnętrznego z serwerem Centrum Zarządzania. Należy śledzić sposób wykonywania przez Roberta czynności konfiguracyjnych w tym scenariuszu.

Pojęcia pokrewne

“Wymagania wstępne protokołu SSL” na stronie 16

Zadania pokrewne

“Wymagania wstępne i założenia:” na stronie 7

Informacje pokrewne

Pierwsze konfigurowanie certyfikatów

Punkt 1: Deaktywuj protokół SSL dla klienta iSeries Navigator.:

Ten etap jest konieczny tylko wtedy, gdy wcześniej protokół SSL dla klienta iSeries Navigator został włączony.

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Prawym przyciskiem myszy kliknij System A i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i usuń zaznaczenie z pola wyboru **Podczas połączenia używaj protokołu SSL**.
4. Zakończ program iSeries Navigator i uruchom go ponownie.

Znika kłódka z pojemnika Centrum Zarządzania w programie iSeries Navigator, co oznacza, że połączenie jest niechronione. Informuje to Roberta o tym, że nie ma już chronionego przez SSL połączenia między klientem i systemem centralnym w swojej firmie.

Punkt 2: Ustaw poziom uwierzytelniania dla serwera Centrum Zarządzania:

1. W programie iSeries Navigator, kliknij prawym przyciskiem myszy **Centrum Zarządzania**, a następnie wybierz **Właściwości**.
2. Kliknij zakładkę **Ochrona**, a następnie zaznacz opcję **Używaj protokołu SSL**.
3. Wybierz opcję **Dowolny** dla poziomu uwierzytelniania (dostępna w wersji V5R3 lub nowszej programu iSeries Access for Windows).
4. Kliknij **OK**, aby ustawić tę wartość w systemie centralnym.

Punkt 3: Zrestartuj serwer Centrum Zarządzania w systemie centralnym:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. W Systemie A rozwiń pozycję **Sieć-->Serwery** i wybierz **TCP/IP**.
3. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**. Widok systemu centralnego zostaje zwinięty i wyświetlany jest komunikat wyjaśniający, że użytkownik nie jest połączony z serwerem.
4. Po zatrzymaniu serwera Centrum Zarządzania kliknij przycisk **Uruchom**, aby go zrestartować.

Punkt 4: Aktywuj protokół SSL dla klienta iSeries Navigator.:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.

2. Prawym przyciskiem myszy kliknij System A i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i wybierz opcję **Podczas połączenia używaj protokołu SSL**.
4. Zakończ program iSeries Navigator i uruchom go ponownie.

Obok serwera Centrum Zarządzania w programie iSeries Navigator pojawia się kłódka wskazująca, że połączenie jest chronione za pomocą protokołu SSL. Informuje ona Roberta o tym, że połączenie między jego klientem i systemem centralnym w jego firmie jest chroniona przez protokół SSL.

Uwaga: Ta procedura chroni tylko połączenie między jednym komputerem PC i serwerem Centrum Zarządzania. Pozostałe połączenia klientów z serwerem Centrum Zarządzania, jak również połączenia systemów końcowych z serwerem Centrum Zarządzania nie będą chronione. Aby chronić innych klientów, należy sprawdzić, czy spełniają oni wymagania wstępne i powtórzyć “Punkt 4: Aktywuj protokół SSL dla klienta iSeries Navigator.” na stronie 4. Informacje na temat ochrony innych połączeń z serwerem Centrum Zarządzania zawiera sekcja Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL.

Etap opcjonalny: Deaktywuj SSL dla klienta iSeries Navigator:

Jeśli Robert chce pracować w biurze firmy i nie chce używać połączenia chronionego za pomocą protokołu SSL wpływającego na wydajność komputera PC, może je w prosty sposób deaktywować, wykonując następujące czynności:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Prawym przyciskiem myszy kliknij System A i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i usuń zaznaczenie z pola wyboru **Podczas połączenia używaj protokołu SSL**.
4. Zakończ program iSeries Navigator i uruchom go ponownie.

Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą SSL

Ten scenariusz wyjaśnia, jak używać protokołu SSL do ochrony wszystkich połączeń z serwerem iSeries.

Scenariusz wyjaśnia sposób używania protokołu SSL do ochrony wszystkich połączeń z serwerem iSeries działającym jako system centralny, przy użyciu serwera Centrum Zarządzania w programie iSeries Navigator.

Pojęcia pokrewne

“Ochrona aplikacji za pomocą protokołu SSL” na stronie 16
Temat zawiera spis aplikacji serwera iSeries, które można chronić za pomocą protokołu SSL.

Sytuacja:

W firmie skonfigurowano sieć WAN zawierającą wiele serwerów iSeries w miejscach zdalnych (systemy końcowe). System końcowe są centralnie zarządzane przez jeden serwer iSeries (system centralny), znajdujący się w głównym biurze. Tomek jest specjalistą do spraw ochrony w firmie. Chce używać protokołu SSL (Secure Sockets Layer) do ochrony wszystkich połączeń między serwerem Centrum Zarządzania zainstalowanym w systemie centralnym firmy a wszystkimi serwerami dostępu i klientami iSeries.

Szczegóły:

Tomek może **bezpiecznie**, za pomocą protokołu SSL, zarządzać wszystkimi połączeniami z serwerem Centrum Zarządzania. Aby używać protokołu SSL dla serwera Centrum Zarządzania, Tomek musi chronić program iSeries Navigator na komputerze PC używanym w celu uzyskania dostępu do systemu centralnego.

Może wybrać jeden z dwóch poziomów uwierzytelniania serwera Centrum Zarządzania:

Uwierzytelnianie serwera
Uwierzytelnianie certyfikatu serwera. Klient musi sprawdzić poprawność serwera bez względu na to, czy tym klientem jest program iSeries Navigator na komputerze PC, czy serwer Centrum Zarządzania w systemie centralnym. Gdy program iSeries Navigator nawiązuje połączenie z systemem centralnym,komputer PC jest

klientem SSL, a Centrum Zarządzania uruchomione w systemie centralnym jest serwerem SSL. System centralny podczas łączenia się z systemem końcowym działa jako klient SSL. System końcowy działa jako serwer SSL. Serwer musi udowodnić swoją tożsamość klientowi, dostarczając certyfikat wydany przez ośrodek certyfikacji, któremu ufa klient. Każdy serwer SSL musi mieć poprawny certyfikat wydany przez zaufany ośrodek certyfikacji (CA).

Uwierzytelnianie klienta i serwera

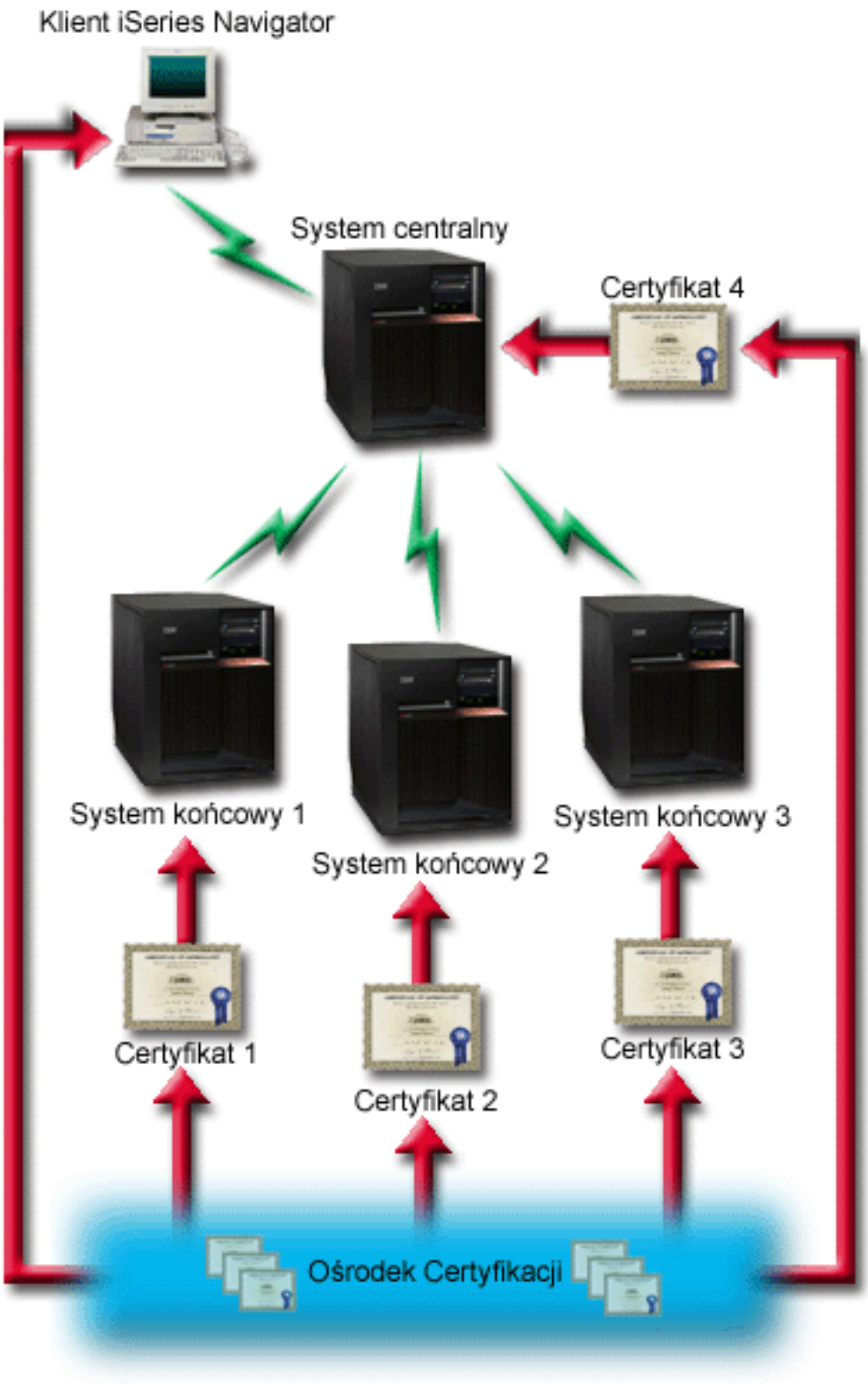
Uwierzytelnianie certyfikatów systemu centralnego i końcowego. Jest to wyższy poziom ochrony niż poziom uwierzytelniania serwera. W innych aplikacjach nazywane jest ono uwierzytelnianiem klienta, ponieważ klient musi dostarczyć poprawny zaufany certyfikat. Gdy system centralny (klient SSL) próbuje nawiązać połączenie z systemem końcowym (serwer SSL), obydwa systemy uwierzytelniają wzajemnie swoje certyfikaty pod kątem autentyczności ośrodka certyfikacji.

Uwaga: Uwierzytelnianie klienta i serwera odbywa się wyłącznie między dwoma systemami iSeries. Serwer nie wykonuje uwierzytelniania klienta, gdy klientem jest komputer PC.

W przeciwieństwie do innych aplikacji, Centrum Zarządzania umożliwia także uwierzytelnianie przez listę weryfikacji, nazywaną listą weryfikacji zaufanych grup. Zazwyczaj lista weryfikacji przechowuje informacje identyfikujące użytkownika, takie jak identyfikator użytkownika, oraz informacje uwierzytelniające, takie jak hasło, osobisty numer identyfikacyjny lub certyfikat cyfrowy. Informacje uwierzytelniające są zaszyfrowane.

Większość aplikacji nie informuje o włączeniu uwierzytelniania serwera i klienta, ponieważ uwierzytelnianie serwera prawie zawsze ma miejsce podczas włączania sesji SSL. Wiele aplikacji ma opcje konfiguracyjne uwierzytelniania klienta. Centrum Zarządzania używa terminu ″uwierzytelnianie serwera i klienta″ zamiast ″uwierzytelnianie klienta″ z uwagi na podwójną rolę systemu centralnego w sieci. Gdy komputer PC używa połączenia z systemem centralnym, system centralny działa jako serwer. Jeśli jednak system centralny łączy się z systemem końcowym, działa jako klient. Rysunek ilustruje, jak system centralny funkcjonuje w sieci jako serwer i jako klient.

Uwaga: Na tej ilustracji certyfikat powiązany z ośrodkiem certyfikacji musi być zapisany w bazie danych kluczy w systemie centralnym i we wszystkich systemach końcowych. Ośrodek certyfikacji musi być zapisany w systemie centralnym, systemach końcowych, a także na komputerze PC.



Wymagania wstępne i założenia:

Tomek musi wykonać następujące zadania administrowania i konfiguracji, aby zapewnić ochronę wszystkich połączeń z serwerem Centrum Zarządzania:

1. Sprawdzić, czy System A spełnia wymagania wstępne dla protokołu SSL.
2. Upewnić się, że system centralny i wszystkie serwery końcowe iSeries mają zainstalowaną wersję V5R2 lub nowszą systemu OS/400 lub i5/OS. Połączenia systemu i5/OS w wersji V5R4 z systemami OS/400 w wersji V5R1 są niedozwolone.
3. Upewnić się, że klient PC iSeries Navigator ma zainstalowaną wersję V5R2 lub nowszą programu iSeries Access for Windows.
4. Znaleźć ośrodek wydający certyfikaty (CA) dla serwerów iSeries.
5. Utworzyć certyfikat podpisany przez ośrodek certyfikacji dla systemu A.
6. Wysłać ośrodek certyfikacji i certyfikat do Systemu A oraz zaimportować go do bazy danych kluczy.
7. Przypisać certyfikaty z identyfikacją aplikacji Centrum Zarządzania i identyfikacjami aplikacji dla wszystkich serwerów dostępu iSeries. Serwerami dostępu iSeries są: serwer centralny TCP, serwer bazy danych, serwer kolejek danych, serwer plików, sieciowy serwer wydruków, serwer komend zdalnych i serwer wpisywania się do systemu.
   a. Na serwerze Centrum Zarządzania uruchom programIBM Digital Certificate Manager. Jeśli chcesz uzyskać lub utworzyć certyfikaty, zmienić lub skonfigurować system certyfikatów, zrób to w tym momencie.
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz hasło bazy certyfikatów *SYSTEM i kliknij przycisk **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.
   e. Kliknij **Aktualizacja przypisania certyfikatów**.
   f. Wybierz **Serwer** i kliknij **Kontynuuj**.
   g. Wybierz pozycję Serwer Centrum Zarządzania i kliknij przycisk **Aktualizacja przypisania certyfikatów**. Powoduje to przypisanie certyfikatu do serwera Centrum Zarządzania.
   h. Wybierz certyfikat, który ma być przypisany do aplikacji i kliknij polecenie **Przypisz nowy certyfikat**. Program DCM zostanie przeładowany do strony **Aktualizacja przypisania certyfikatów** z komunikatem potwierdzającym.
   i. Kliknij przycisk **Anuluj**, aby powrócić do listy aplikacji.
   j. Powtórz te procedurę dla wszystkich serwerów dostępuiSeries.
8. Pobierz ośrodek certyfikacji do klienta PC iSeries Navigator.

Pojęcia pokrewne

“Wymagania wstępne protokołu SSL” na stronie 16

Zadania pokrewne

“Szczegóły konfiguracji: Ochrona połączenia klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL” na stronie 4
W temacie przedstawiono w rozwinięciu etapy konfigurowania ochrony połączeń klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

“Szczegóły konfiguracji: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL” na stronie 9
W temacie przedstawiono szczegóły używania protokołu SSL do ochrony wszystkich połączeń z serwerem Centrum Zarządzania.

Informacje pokrewne

Centrum informacyjne V5R1, ″Securing Management Central″

Używanie programu Digital Certificate Manager

Etapy konfiguracji:

Zanim Tomek będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy oraz skonfigurować certyfikaty cyfrowe w systemie centralnym. Przed przystąpieniem do kolejnych

czynności należy zapoznać się z informacjami dotyczącymi tego scenariusza w sekcji “Wymagania wstępne i założenia:” na stronie 7. Po spełnieniu wymagań wstępnych może wykonać poniższe procedury, aby włączyć ochronę wszystkich połączeń z serwerem Centrum Zarządzania:

Uwaga: Jeśli protokół SSL włączono dla programu iSeries Navigator, Tomek musi go wyłączyć przed włączeniem protokołu SSL dla serwera Centrum Zarządzania. Jeśli protokół SSL włączono dla programu iSeries Navigator, a nie włączono dla serwera Centrum Zarządzania, próby nawiązania połączenia programu iSeries Navigator z systemem centralnym zakończą się niepowodzeniem.

1. “Punkt 1: Skonfiguruj system centralny pod kątem uwierzytelniania serwera” na stronie 10
2. “Punkt 2: Skonfiguruj systemy końcowe pod kątem uwierzytelniania serwera” na stronie 10
3. “Punkt 3: Zrestartuj serwer Centrum Zarządzania w systemie centralnym” na stronie 10
4. “Punkt 4: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych” na stronie 11
5. “Punkt 5: Aktywuj protokół SSL dla klienta iSeries Navigator” na stronie 11
6. “Punkt 6: Skonfiguruj system centralny pod kątem uwierzytelniania klientów” na stronie 11
7. “Punkt 7: Skonfiguruj systemy końcowe pod kątem uwierzytelniania klientów” na stronie 11
8. “Punkt 8: Skopiuj listę sprawdzania do systemów końcowych” na stronie 12
9. “Punkt 9: Zrestartuj serwer Centrum Zarządzania w systemie centralnym” na stronie 12
10. “Punkt 10: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych” na stronie 13

Pojęcia pokrewne

“Wymagania wstępne protokołu SSL” na stronie 16

Informacje pokrewne

Pierwsze konfigurowanie certyfikatów

Szczegóły konfiguracji: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL

W temacie przedstawiono szczegóły używania protokołu SSL do ochrony wszystkich połączeń z serwerem Centrum Zarządzania.

W poniższych informacjach przyjęto, że użytkownik zapoznał się z następującym tematem: Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL.

Użytkownik chce zrozumieć sposób wykonywania czynności wymaganych do ochrony wszystkich połączeń z serwerem Centrum Zarządzania. Należy śledzić sposób wykonywania operacji przez Tomka w tym scenariuszu.

Zanim Tomek będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy oraz skonfigurować certyfikaty cyfrowe na serwerze iSeries. Po spełnieniu wymagań wstępnych może wykonać poniższe procedury, aby chronić wszystkie połączenia z serwerem Centrum Zarządzania.

Uwaga: Jeśli protokół SSL włączono dla programu iSeries Navigator, Tomek musi go wyłączyć przed włączeniem protokołu SSL dla serwera Centrum Zarządzania. Jeśli protokół SSL włączono dla programu iSeries Navigator, a nie włączono dla serwera Centrum Zarządzania, próby nawiązania połączenia programu iSeries Navigator z systemem centralnym zakończą się niepowodzeniem.

Protokół SSL umożliwia ochronę transmisji zarówno pomiędzy systemem centralnym a systemem końcowym, jak i pomiędzy klientem iSeries Navigator a systemem centralnym. Protokół SSL umożliwia transport i uwierzytelnianie certyfikatów oraz szyfrowanie danych. Połączenie SSL może zostać nawiązane jedynie pomiędzy systemem centralnym z włączonym SSL i systemem końcowym z włączonym SSL. Tomek musi skonfigurować uwierzytelnianie serwera, zanim skonfiguruje uwierzytelnianie klienta.

Pojęcia pokrewne

“Wymagania wstępne protokołu SSL” na stronie 16

Zadania pokrewne

“Wymagania wstępne i założenia:” na stronie 7

Informacje pokrewne

Pierwsze konfigurowanie certyfikatów

Punkt 1: Skonfiguruj system centralny pod kątem uwierzytelniania serwera:

1. W programie iSeries Navigator kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Właściwości**.
2. Kliknij zakładkę **Ochrona**, a następnie zaznacz opcję **Używaj protokołu SSL**.
3. Jako poziom uwierzytelniania wybierz **Serwer**.
4. Kliknij **OK**, aby ustawić tę wartość w systemie centralnym.

Uwaga: **NIE** restartuj serwera Centrum Zarządzania, zanim zostaniesz o to poproszony. Jeśli serwer zostanie zrestartowany w tej chwili, nie będzie można się połączyć z serwerami końcowymi. Aby zrestartować serwer w celu włączenia SSL, konieczne jest wcześniejsze wykonanie określonych zadań konfiguracyjnych. W pierwszej kolejności należy wykonać zadania porównania i aktualizacji, aby skonfigurować systemy końcowe pod kątem SSL.

Punkt 2: Skonfiguruj systemy końcowe pod kątem uwierzytelniania serwera:

Po skonfigurowaniu systemu centralnego pod kątem uwierzytelniania serwera Tomek musi skonfigurować w tym celu również systemy końcowe. Należy wykonać następujące zadania:

1. Rozwiń pozycję **Centrum Zarządzania**.
2. Porównaj i zaktualizuj wartości systemowe dla systemów końcowych:
   a. W oknie **Systemy końcowe** kliknij prawym przyciskiem myszy system centralny i wybierz polecenie **Zasoby → Kolekcjonuj**.
   b. Zaznacz opcję **Wartości systemowe** w oknie dialogowym kolekcjonowania, aby gromadzić ustawienia wartości systemowych w systemie centralnym. Usuń zaznaczenie wszystkich pozostałych opcji.Kliknij przycisk OK i czekaj na zakończenie spisywania zasobów.
   c. Kliknij prawym przyciskiem myszy opcję **Grupy systemów → >Nowa grupa systemów**.
   d. Zdefiniuj nową grupę systemową zawierającą wszystkie systemy końcowe, z którymi będziesz się łączyć, korzystając z SSL. Nadaj tej grupie nazwę Zaufana grupa.
   e. Aby wyświetlić nową grupę (Zaufaną grupę), rozwiń grupy systemów.
   f. Po zakończeniu zbierania informacji kliknij prawym przyciskiem myszy nową grupę systemów i wybierz polecenie **Wartości systemowe → Porównaj i zaktualizuj**.
   g. Sprawdź, czy system centralny jest wyświetlany w polu **System modelowy**.
   h. W polu **Kategoria** zaznacz pozycję **Centrum Zarządzania**.
   i. Sprawdź, czy dla opcji **Użyj protokołu SSL** ustawiona jest wartość **Tak** i wybierz polecenie **Aktualizuj**, aby przesłać tę wartość do Zaufanej grupy.
   j. Sprawdź, czy dla opcji **Poziom uwierzytelniania SSL** ustawiona jest wartość **Serwer** i wybierz polecenie **Aktualizuj**, aby przesłać tę wartość do Zaufanej grupy.

      Uwaga: Jeśli te wartości nie są ustawione, wykonaj Punkt 1: Skonfiguruj system centralny pod kątem uwierzytelniania serwera .

   k. Kliknij przycisk **OK**. Zanim przejdziesz do kolejnego etapu, poczekaj na zakończenie przetwarzania polecenia **Porównaj i zaktualizuj**.

Punkt 3: Zrestartuj serwer Centrum Zarządzania w systemie centralnym:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń system centralny.
3. Rozwiń opcje **Sieć → Serwery** i wybierz pozycję **TCP/IP**.
4. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**. Widok systemu centralnego zostaje zwinięty i wyświetlany jest komunikat wyjaśniający, że użytkownik nie jest połączony z serwerem.

5. Po zatrzymaniu serwera Centrum Zarządzania kliknij przycisk **Uruchom**, aby go zrestartować.

Punkt 4: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń system końcowy, który chcesz zrestartować.
3. Rozwiń opcje **Sieć → Serwery** i wybierz pozycję **TCP/IP**.
4. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
5. Po zatrzymaniu serwera Centrum Zarządzania kliknij przycisk **Uruchom**, aby go zrestartować.
6. Powtórz procedurę dla każdego systemu końcowego.

Punkt 5: Aktywuj protokół SSL dla klienta iSeries Navigator:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Kliknij prawym przyciskiem myszy system centralny i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i wybierz opcję **Podczas połączenia używaj protokołu SSL**.
4. Zakończ program iSeries Navigator i uruchom go ponownie.

Uwaga: Po wykonaniu wszystkich czynności opisanych powyżej uwierzytelnianie serwera jest skonfigurowane dla systemu centralnego i systemów końcowych. Opcjonalnie można także skonfigurować system centralny i systemy końcowe pod kątem uwierzytelniania klientów. Aby umożliwić uwierzytelnianie klientów w systemie centralnym i systemach końcowych, należy kolejno wykonać zadania opisane w punktach 6 - 10.

Punkt 6: Skonfiguruj system centralny pod kątem uwierzytelniania klientów:

Po zakończeniu konfiguracji pod kątem uwierzytelniania serwera Tomek może wykonać następujące opcjonalne procedury uwierzytelniania klienta. Uwierzytelnianie klienta umożliwia sprawdzenie ośrodka certyfikacji i zaufanej grupy dla systemów końcowych i systemu centralnego. Gdy system centralny (klient SSL) próbuje użyć SSL w celu połączenia się z systemem końcowym (serwerem SSL), system centralny i system końcowy wzajemnie uwierzytelniają swoje certyfikaty poprzez uwierzytelnianie serwera i uwierzytelnianie klienta. Taka operacja jest czasem nazywana uwierzytelnianiem ośrodka certyfikacji i zaufanej grupy.

Uwaga: Konfiguracji uwierzytelniania klienta nie można zakończyć do momentu skonfigurowania uwierzytelniania serwera. Jeśli jeszcze nie skonfigurowano uwierzytelniania serwera, należy to zrobić teraz.

1. W programie iSeries Navigator kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Właściwości**.
2. Kliknij zakładkę **Ochrona** i wybierz **Używaj protokołu SSL**.
3. Wybierz **Klient i serwer** w celu wybrania poziomu uwierzytelniania.
4. Kliknij **OK**, aby ustawić tę wartość w systemie centralnym.

   Uwaga: **NIE** restartuj serwera Centrum Zarządzania, zanim zostaniesz o to poproszony. Jeśli serwer zostanie zrestartowany w tej chwili, nie będzie można się połączyć z serwerami końcowymi. Aby zrestartować serwer w celu włączenia SSL, konieczne jest wcześniejsze wykonanie określonych zadań konfiguracyjnych. W pierwszej kolejności należy wykonać zadania porównania i aktualizacji, aby skonfigurować systemy końcowe pod kątem SSL.

Punkt 7: Skonfiguruj systemy końcowe pod kątem uwierzytelniania klientów:

Porównaj i zaktualizuj wartości systemowe dla systemów końcowych:

1. Rozwiń pozycję **Centrum Zarządzania**.
2. Porównaj i zaktualizuj wartości systemowe dla systemów końcowych:
   a. W oknie **Systemy końcowe** kliknij prawym przyciskiem myszy system centralny i wybierz polecenie **Zasoby → Kolekcjonuj**.

b. Zaznacz opcję **Wartości systemowe** w oknie dialogowym kolekcjonowania, aby gromadzić ustawienia wartości systemowych w systemie centralnym. Usuń zaznaczenie wszystkich pozostałych opcji.Kliknij przycisk OK i czekaj na zakończenie spisywania zasobów.

c. Po zakończeniu zbierania informacji kliknij prawym przyciskiem myszy Zaufaną grupę i wybierz polecenie **Wartości systemowe → Porównaj i zaktualizuj**.

d. Sprawdź, czy system centralny jest wyświetlany w polu **System modelowy**.

e. W polu **Kategoria** zaznacz pozycję **Centrum Zarządzania**.

f. Sprawdź, czy dla opcji **Użyj protokołu SSL** ustawiona jest wartość **Tak** i wybierz polecenie **Aktualizuj**, aby przesłać tę wartość do Zaufanej grupy.

g. Sprawdź, czy dla opcji **Poziom uwierzytelniania SSL** ustawiona jest wartość **Klient i Serwer** i wybierz polecenie **Aktualizuj** aby przesłać tę wartość do Zaufanej grupy.

Uwaga: Jeśli te wartości nie są ustawione, wykonaj Punkt 6: Skonfiguruj system centralny pod kątem uwierzytelniania klientów.

h. Kliknij przycisk **OK**. Zanim przejdziesz do kolejnego etapu, poczekaj na zakończenie przetwarzania polecenia **Porównaj i zaktualizuj**.

Punkt 8: Skopiuj listę sprawdzania do systemów końcowych:

W poniższej procedurze przyjęto założenie, że systemem centralnym użytkownika jest system V5R3 lub nowszy. W wersjach systemu starszych niż V5R3, lista QYPSVLDL.VLDL znajdowała się w bibliotece QUSRSYS.LIB, a nie w QMGTC2.LIB. Dlatego w wersjach systemu starszych niż V5R3 konieczne będzie wysłanie listy sprawdzania do tych systemów i umieszczenie jej w bibliotece QUSRSYS.LIB, zamiast w bibliotece QMGTC2.LIB. Jeśli korzystasz z systemu w wersji V5R3 lub nowszej, przejdź do wykonywania następujących czynności:

1. W programie iSeries Navigator rozwiń pozycję **Centrum Zarządzania → Definicje**.
2. Kliknij prawym przyciskiem myszy **Pakiety** i wybierz **Nowa definicja**.
3. W oknie **Nowa definicja** wypełnij następujące pola:
   a. **Nazwa:** wpisz nazwę definicji.
   b. **System źródłowy:** wybierz nazwę systemu centralnego.
   c. **Wybrane pliki i foldery:** kliknij pole i wpisz /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL.
4. Kliknij zakładkę **Opcje** i wybierz **Zastępuj istniejące zbiory przysłanymi**.
5. Kliknij **Zaawansowane**.
6. W oknie **Opcje zaawansowane** wybierz opcję **Tak**, aby zezwolić na różnice w obiektach podczas odtwarzania i zmień wartość pozycji **Wersja docelowa** na najwcześniejszą wersję systemów końcowych.
7. Kliknij **OK**, aby odświeżyć spis definicji i wyświetlić nowy pakiet.
8. Kliknij prawym przyciskiem myszy nowy pakiet i wybierz **Wyślij**.
9. W oknie dialogowym **Wyślij** rozwiń pozycję **Grupy systemów->Zaufana grupa**, znajdującą się na liście **Dostępne systemy i grupy**. Jest to jedna z grup, które zdefiniowano, wykonując “Punkt 2: Skonfiguruj systemy końcowe pod kątem uwierzytelniania serwera” na stronie 10.

   Uwaga: Zadanie **Wyślij** nigdy nie powiedzie się w systemie centralnym, gdyż jest on zawsze systemem źródłowym. Zadanie **Wyślij** powinno zakończyć się pomyślnie we wszystkich systemach końcowych.
10. Jeśli w **Zaufanej grupie** znajdują się systemy starsze niż V5R3, musisz ręcznie przejść do tych systemów i przenieść obiektQYPSVLDL.VLDL z bibliotekiQMGTC2.LIB do biblioteki QUSRSYS.LIB. Jeśli w bibliotece QUSRSYS.LIB znajduje się już jedna wersja obiektu QYPSVLDL.VLDL, usuń ją i zastąp nowszą wersją z biblioteki QMGTC2.LIB

Punkt 9: Zrestartuj serwer Centrum Zarządzania w systemie centralnym:

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń system centralny.
3. Rozwiń opcje **Sieć → Serwery** i wybierz pozycję **TCP/IP**.

4. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**. Widok systemu centralnego zostaje zwinięty i wyświetlany jest komunikat wyjaśniający, że użytkownik nie jest połączony z serwerem.
5. Po zatrzymaniu serwera Centrum Zarządzania kliknij przycisk **Uruchom**, aby go zrestartować.

Punkt 10: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych:

Uwaga: Powtórz procedurę dla każdego systemu końcowego.

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń system końcowy, który chcesz zrestartować.
3. Rozwiń opcje **Sieć → Serwery** i wybierz pozycję **TCP/IP**.
4. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
5. Po zatrzymaniu serwera Centrum Zarządzania kliknij przycisk **Uruchom**, aby go zrestartować.

Pojęcia

Temat zawiera informacje uzupełniające dotyczące protokołów Secure Sockets Layer (SSL).

Dzięki protokołowi SSL można nawiązywać chronione połączenia pomiędzy aplikacjami serwera i klienta, uwierzytelniając jeden lub dwa punkty końcowe sesji komunikacyjnej. SSL zapewnia także prywatność i integralność danych wymienianych pomiędzy aplikacjami serwera i klienta.

Historia SSL

Firma Netscape opracowała protokół SSL (Secure Sockets Layer) w roku 1994, jako odpowiedź na rosnące zainteresowanie ochroną w Internecie.

Protokół SSL został początkowo opracowany do ochrony komunikacji między przeglądarką WWW i serwerem. Specyfikacja została opracowana w taki sposób, aby inne aplikacje, takie jak TELNET i FTP, mogły używać SSL.

Pojęcia pokrewne

“Obsługiwane protokoły SSL i TLS (Transport Layer Security” na stronie 14
Ten temat zawiera informacje o tym, z które wersje protokołów SSL i TLS obsługuje implementacja i5/OS.

Jak działa SSL

SSL składa się obecnie z dwóch protokołów: rekordów i uzgadniania. Protokół rekordów steruje przepływem danych pomiędzy dwoma punktami końcowymi sesji SSL.

Protokół uzgadniania uwierzytelnia jeden lub oba punkty końcowe sesji SSL i ustanawia unikalny symetryczny klucz używany do generowania kluczy służących do szyfrowania i deszyfrowania danych w sesji SSL. Protokół SSL używa asymetrycznego szyfrowania, certyfikatów cyfrowych i przepływu uzgadniania SSL do uwierzytelniania jednego lub obu systemów końcowych sesji SSL. Zwykle protokół SSL wymaga uwierzytelnienia serwera. Opcjonalnie protokół SSL wymaga uwierzytelnienia klienta. Certyfikat cyfrowy wydawany przez ośrodek certyfikacji może zostać przypisany każdemu z punktów końcowych lub każdej z aplikacji korzystającej z SSL we wszystkich punktach końcowych połączenia.

Certyfikat cyfrowy składa się z klucza publicznego i informacji identyfikacyjnych podpisanych cyfrowo przez zaufany ośrodek certyfikacji. Każdemu kluczowi publicznemu przypisany jest klucz prywatny, którego nie przechowuje się ani jako jednej z części certyfikatu, ani z samym certyfikatem. Zarówno podczas uwierzytelniania serwera, jak i klienta, uwierzytelniany punkt końcowy musi udowadniać, że ma dostęp do klucza prywatnego przypisanego kluczowi publicznemu, zawartemu w certyfikacie cyfrowym.

Uzgadnianie SSL, ze względu na operacje szyfrujące z użyciem kluczy publicznych i prywatnych, jest działaniem wymagającym dużej wydajności. Po nawiązaniu pomiędzy dwoma punktami końcowymi początkowej sesji SSL, informacje o sesji SSL przeznaczone dla nich i dla aplikacji mogą być przechowywane w pamięci chronionej, dzięki czemu kolejne aktywacje sesji SSL będą szybsze. Punkty końcowe korzystają ze skróconego przepływu uzgodnień do

uwierzytelnienia, że każdy z nich ma dostęp do unikalnych danych bez korzystania z kluczy publicznych lub prywatnych, gdy sesja SSL jest wznawiana. Jeśli oba mogą udowodnić, że mają dostęp do tych unikalnych informacji, ustanawiane są nowe klucze symetryczne i wznawiana jest sesja SSL. W sesjach wersji 1.0 protokołu TLS i 3.0 protokołu SSL informacje nie są buforowane w pamięci chronionej dłużej niż 24 godziny. W wersji V5R2 systemu OS/400 i kolejnych wydaniach lub w systemie i5/OS można zminimalizować wpływ wydajności uzgadniania SSL na procesor główny poprzez używanie sprzętu szyfrującego.

Informacje pokrewne

Koncepcje dotyczące certyfikatów cyfrowych

Sprzęt szyfrujący

Obsługiwane protokoły SSL i TLS (Transport Layer Security

Ten temat zawiera informacje o tym, z które wersje protokołów SSL i TLS obsługuje implementacja i5/OS.

Istnieje kilka zdefiniowanych wersji protokołu SSL. Najnowsza, nazywana Transport Layer Security Protocol (TLS), jest produktem grupy wykonawczej IETF wykorzystującym wersję 3.0 protokołu SSL. Implementacja w systemie i5/OS obsługuje następujące wersje protokołów SSL i TLS:

- protokół TLS w wersji 1.0
- protokół TLS w wersji 1.0 zgodny z protokołem SSL w wersji 3.0

  Uwaga:

  1. Określenie protokół TLS w wersji 1.0 zgodny z protokołem SSL w wersji 3.0 oznacza, że negocjowane będzie użycie protokołu TLS, a jeśli nie będzie to możliwe, negocjowana będzie użycie protokołu SSL w wersji 3.0. Jeśli protokół SSL wersja 3.0 nie może być negocjowany, uzgadnianie SSL zakończy się niepowodzeniem.
  2. System iSeries obsługuje również wersję 1.0 protokołu TLS zgodną z protokołem SSL w wersjach 3.0 i 2.0. Określa się to, podając wartość protokołu **ALL**, co oznacza, że negocjowane będzie użycie protokołu TLS, a jeśli nie jest to możliwe, to wersji 3.0 protokołu SSL. Następnie, jeśli nie zostanie wynegocjowana wersja 3.0 SSL, podjęta zostanie próba negocjacji wersji 2.0 protokołu SSL. Jeśli protokół SSL wersja 2.0 nie może być negocjowany, uzgadnianie SSL zakończy się niepowodzeniem.
- protokół SSL w wersji 3.0
- protokół SSL w wersji 2.0
- protokół SSL w wersji 3.0 zgodny z protokołem SSL w wersji 2.0

Protokół SSL wersja 3.0 a protokół SSL wersja 2.0

W porównaniu z wersją 2.0 protokół SSL wersja 3.0 jest niemal całkiem innym protokołem. Niektóre z ważniejszych różnic pomiędzy tymi dwoma protokołami to:

- Różnice w przepływie protokołu uzgadniania.
- Protokół SSL w wersji 3.0 używa implementacji BSAFE 3.0 z RSA Data Security, zawierającej poprawki analizy czasowej i algorytm kodowania mieszającego SHA-1. Algorytm kodowania mieszającego SHA-1 uważa się za bardziej bezpieczny niż algorytm kodowania mieszającego MD5. SHA-1 umożliwia SSL w wersji 3.0 obsługę dodatkowych zestawów algorytmów szyfrowania używających SHA-1 zamiast MD5.
- Wersja 3.0 protokołu SSL redukuje możliwość wystąpienia ataku typu przechwycenie połączenia (man-in-the-middle) podczas przetwarzania uzgadniania SSL. W wersji 2.0 było możliwe, chociaż mało prawdopodobne, że taki typ ataku mógł spowodować osłabienie specyfikacji szyfru. Osłabienie szyfru może umożliwić osobie nie posiadającej uprawnień złamanie klucza sesji SSL.

Protokół TLS wersja 1.0 a protokół SSL wersja 3.0

Najnowszym standardem przemysłowym protokołu SSL opartym na SSL w wersji 3.0 jest protokół TLS (Transport Layer Security) w wersji 1.0. Jego specyfikacje są zdefiniowane w dokumentach RFC 2246 zespołu IETF (Internet Engineering Task Force), *protokół TLS*.

Głównym celem protokołu TLS jest uczynienie protokołu SSL bardziej bezpiecznym, a jego specyfikacji pełniejszą i bardziej precyzyjną. TLS, w porównaniu do wersji 3.0 SSL, zapewnia następujące udoskonalenia:

- bezpieczniejszy algorytm MAC,
- dokładniejsze alerty,
- prostsze definicje specyfikacji ″szarej strefy″.

Aplikacja serwera iSeries z włączonym protokołem SSL będzie korzystać z obsługi TLS automatycznie, chyba że otrzyma żądanie użycia wyłącznie wersji 3.0 lub 2.0 protokołu SSL.

TLS zapewnia następujące sposoby zwiększenia ochrony:

- **Key-Hashing for Message Authentication** Protokół TLS korzysta z metody HMAC gwarantującej, że rekord nie zostanie zmodyfikowany w trakcie przejścia przez otwartą sieć, taką jak Internet. SSL wersja 3.0 zapewnia uwierzytelnianie wiadomości zabezpieczonych kluczem, ale funkcja HMAC jest bardziej bezpieczna niż funkcja MAC (Message Authentication Code) używana przez protokół SSL w wersji 3.0.
- **Rozszerzony pseudolosowy generator funkcji (PRF)** PRF generuje dane klucza. W TLS funkcja HMAC definiuje generator PRF. Generator PRF korzysta z dwóch algorytmów mieszających, które gwarantują jego ochronę. Jeśli używany jest jeden z algorytmów, dane będą nadal chronione tak długo, jak długo drugi algorytm nie będzie używany.
- **Udoskonalona weryfikacja końcowa komunikatów** Zarówno wersja 1.0 protokołu TLS, jak i wersja 3.0 protokołu SSL wysyłają do obu punktów końcowych komunikat uwierzytelniający brak zmian w wymienianych komunikatach. Protokół TLS wykorzystuje do utworzenia komunikatu końcowego wartości PRF i HMAC, co również jest bezpieczniejsze niż w wersji 3.0 protokołu SSL.
- **Spójna obsługa certyfikatów** W przeciwieństwie do protokołu SSL wersja 3.0, protokół TLS próbuje określić typ certyfikatu, który musi być wymieniany między implementacjami protokołu TLS.
- **Dokładniejsze komunikaty alertów** TLS udostępnia dodatkowe i dokładniejsze alerty, wskazując problemy wykryte przez punkt końcowy sesji. Dokumentuje także, kiedy określone alerty powinny zostać wysłane.

  Pojęcia pokrewne

  “Historia SSL” na stronie 13
  Firma Netscape opracowała protokół SSL (Secure Sockets Layer) w roku 1994, jako odpowiedź na rosnące zainteresowanie ochroną w Internecie.

  Informacje pokrewne

  Protokół TLS

Uwierzytelnianie serwera

Dzięki uwierzytelnieniu serwera klient upewnia się, że certyfikat serwera jest poprawny i że podpisał go zaufany ośrodek wydający certyfikaty.

Protokół SSL korzysta z szyfrowania asymetrycznego i przepływu protokołu uzgadniania do wygenerowania klucza symetrycznego, którego używa się tylko podczas jednej sesji SSL. Klucz ten zostaje użyty do wygenerowania zestawu kluczy, które z kolei zostaną wykorzystane do szyfrowania i deszyfrowania danych przesyłanych podczas sesji SSL. Następnie po zakończeniu uzgadniania SSL jeden lub oba końce łącza komunikacyjnego zostaną uwierzytelnione. Dodatkowo wygenerowany zostanie unikalny klucz do szyfrowania i deszyfrowania danych. Zaszyfrowane dane na poziomie warstwy aplikacji będą przesłane w ramach sesji SSL.

Uwierzytelnianie klienta

Wiele aplikacji ma opcję włączania uwierzytelniania klienta. Korzystając z możliwości uwierzytelniania klienta serwer upewnia się, że certyfikat klienta jest poprawny i że podpisał go zaufany ośrodek wydający certyfikaty.

Funkcję uwierzytelniania klienta obsługują następujące aplikacje serwera iSeries

- serwer HTTP IBM (oparty na Apache),
- serwer FTP,

- serwer Telnet,
- system końcowy Centrum Zarządzania,
- Serwer katalogów (LDAP)

Planowanie włączenia SSL

W tym rozdziale przedstawiono wymagania wstępne związane z włączeniem protokołu SSL na serwerze iSeries oraz kilka pożytecznych wskazówek.

Pojęcia pokrewne

"Rozwiązywanie problemów z protokołem SSL" na stronie 17
Podane w tym rozdziale informacje będą użyteczne jako pomoc w rozwiązywaniu jedynie podstawowych problemów, na jakie może napotkać serwer iSeries w związku z protokołem SSL.

Wymagania wstępne protokołu SSL

- Program IBM Digital Certificate Manager (DCM), opcja 34 systemu i5/OS (5722-SS1)
- Program TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- Serwer IBM HTTP Server for iSeries (5722-DG1)
- Jeśli próbujesz użyć serwera HTTP, aby korzystać z DCM, sprawdź, czy zainstalowano pakiet IBM Developer Kit for Java (5722–JV1). W przeciwnym razie serwer administratora HTTP nie zostanie uruchomiony.
- Aby przyspieszyć przetwarzanie uzgadniania SSL, można zainstalować sprzęt szyfrujący do obsługi protokołu SSL. Jeśli ma zostać zainstalowany sprzęt szyfrujący, należy również zainstalować opcję 35, Cryptographic Service Provider.

Informacje pokrewne

Sprzęt szyfrujący

Certyfikaty cyfrowe

Rozwiązaniem służącym do zarządzania certyfikatami cyfrowymi jest program IBM Digital Certificate Manager (DCM).

Informacje pokrewne

Certyfikaty publiczne a certyfikaty prywatne

Konfigurowanie programu DCM

Ochrona aplikacji za pomocą protokołu SSL

Temat zawiera spis aplikacji serwera iSeries, które można chronić za pomocą protokołu SSL.

Protokołem SSL można chronić następujące aplikacje serwera iSeries:

- Odwzorowanie tożsamości dla przedsiębiorstwa (EIM)
- serwer FTP,
- serwer HTTP (oparty na serwerze Apache)
- program iSeries Access for Windows
- serwer katalogów (LDAP)
- Distributed Relational Database Architecture (DRDA) i serwer Distributed Data Management (DDM),
- serwer Centrum Zarządzania
- serwer Telnet,
- Websphere Application Server — Express
- Aplikacje napisane dla zestawu funkcji API (aplikacyjny interfejs programowy) iSeries Access for Windows,
- aplikacje tworzone z wykorzystaniem funkcji API SSL obsługiwanych przez serwer iSeries, Obsługiwanymi aplikacjami API są Global Secure Toolkit (GSKit) oraz aplikacje API SSL_ iSeries.

Pojęcia pokrewne

“Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą SSL” na stronie 5
Ten scenariusz wyjaśnia, jak używać protokołu SSL do ochrony wszystkich połączeń z serwerem iSeries.

Informacje pokrewne

Odwzorowanie tożsamości dla przedsiębiorstwa (EIM)

Używanie protokołu SSL do ochrony serwera FTP

Serwer HTTP

Administrowanie protokołem SSL (temat dotyczący programu iSeries Access for Windows)

Scenariusz Telnet: Ochrona aplikacji Telnet za pomocą SSL

Interfejs API protokołu SSL

Rozwiązywanie problemów z protokołem SSL

Podane w tym rozdziale informacje będą użyteczne jako pomoc w rozwiązywaniu jedynie podstawowych problemów, na jakie może napotkać serwer iSeries w związku z protokołem SSL.

Należy pamiętać, że w dział ten nie stanowi obszernego źródła informacji, gdyż jego zadaniem jest tylko pomoc w rozwiązywaniu typowych problemów.

Sprawdź, czy zostały spełnione następujące warunki:

- spełniono wymagania wstępne dla protokołu SSL na serwerze iSeries.
- ośrodek certyfikacji i certyfikaty są poprawne i nie wygasły.

Jeśli poprzednie stwierdzenia są prawdziwe w danym systemie i nadal występują problemy związane z protokołem SSL, należy skorzystać z poniższych opcji:

- Kod błędu SSL w protokole zadania serwera może być odniesieniem w tabeli błędów umożliwiającym odnalezienie dalszych informacji na temat błędu. Na przykład ta tabela przypisuje kod -93, który może znajdować się w protokole zadania serwera, do stałej SSL_ERROR_SSL_NOT_AVAILABLE.
  - Ujemny kod powrotu (kreska przed numerem kodu) wskazuje, że używane są funkcje API SSL_.
  - Dodatni kod powrotu wskazuje na użycie funkcji API GSKit. Programiści mogą wykorzystywać w swoich programach funkcje API gsk_strerror() lub SSL_Strerror(), aby otrzymać krótki opis kodu powrotu dla błędu. Niektóre aplikacje używają funkcji API i zapisują w protokole zadania komunikat zawierający to zdanie.

  Jeśli potrzebny jest dokładniejszy opis, to serwer iSeries może wyświetlić identyfikator komunikatu, pokazując prawdopodobną przyczynę i sposób usunięcia tego błędu. Dodatkowa dokumentacja wyjaśniająca kody błędów może znajdować się w zwracających ten błąd konkretnych funkcjach API SSL.
- Następujące pliki nagłówkowe zawierają takie same nazwy stałych dla kodów powrotu SSL jak tabela, ale bez odniesienia do identyfikatora komunikatu:
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.QSOSSL

  Należy pamiętać, że wprawdzie nazwy kodów powrotu SSL pozostają stałe w obu plikach nagłówkowych, jednak każdemu z tych kodów może być przypisany więcej niż jeden unikalny kod powrotu.

Pojęcia pokrewne

“Planowanie włączenia SSL” na stronie 16
W tym rozdziale przedstawiono wymagania wstępne związane z włączeniem protokołu SSL na serwerze iSeries oraz kilka pożytecznych wskazówek.

Informacje pokrewne

Serwis i wsparcie

Komunikaty kodów błędu funkcji API SSL

Informacje pokrewne dotyczące protokołu SSL

Serwisy WWW

- RFC 2246: ″The TLS Protocol Version 1.0 ″ (ftp://ftp.isi.edu/in-notes/rfc2246.txt)
  Zawiera szczegółowe informacje na temat protokołu TLS.
- RFC2818: ″HTTP Over TLS″ (ftp://ftp.isi.edu/in-notes/rfc2818.txt)
  Opisuje, jak korzystać z protokołu TLS do ochrony połączeń HTTP w Internecie.
- Dokument The SSL Protocol Version 3.0 (http://home.netscape.com/eng/ssl3/ssl-toc.html)
  Zawiera wiele szczegółowych informacji na temat protokołu TLS.
- Serwis WWW SSL Encryption explained (http://www.digicert.com/ssl)
  Omawia szyfrowanie SSL ze szczególnym uwzględnieniem certyfikatów.

Inne informacje

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

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu dalszego wykorzystania:

1. Prawym przyciskiem myszy kliknij plik PDF w przeglądarce (prawym przyciskiem myszy kliknij odsyłacz powyżej).
2. Kliknij opcję zapisania pliku PDF na komputerze lokalnym.
3. Przejdź do katalogu, w którym ma być zapisany plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Jego bezpłatną kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html) .

Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

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

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

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

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ ZNAJDUJE (“AS IS”) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Kody te nie zostały kompleksowo przetestowane we wszelkich możliwych warunkach. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakikolwiek jego fragment, jak też jakiekolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

DRDA
i5/OS
IBM
iSeries
OS/400

Intel, logo Intel Inside, MMX oraz Pentium są znakami towarowymi Intel Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java oraz wszystkie znaki towarowe dotyczące języka Java są znakami towarowymi Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub w innych krajach.

Linux jest znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i/lub w innych krajach.

UNIX jest zastrzeżonym znakiem towarowym Open Group w Stanach Zjednoczonych i w innych krajach.

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ (″AS IS″) BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.