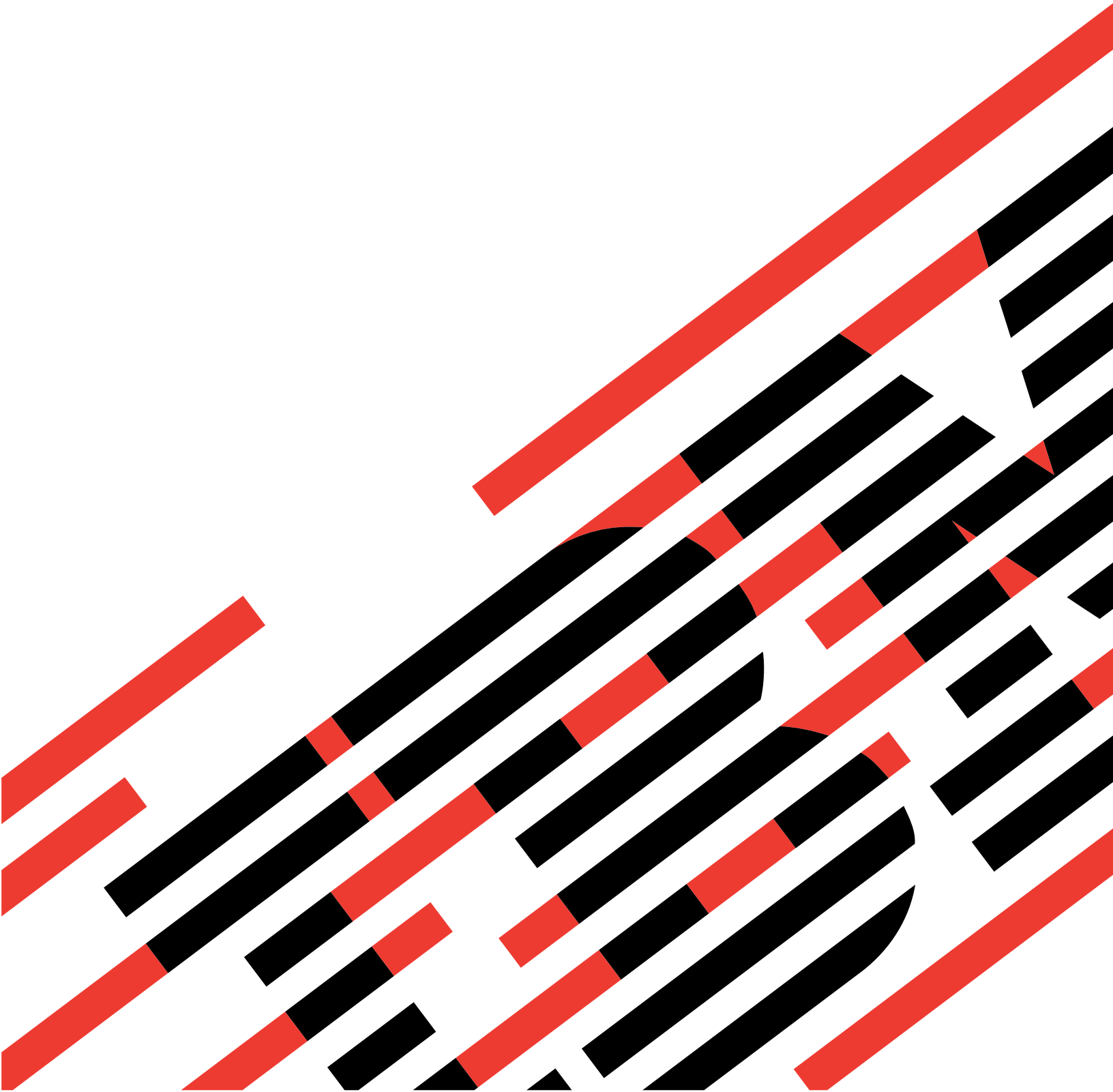
IBM

eserver

System iSeries

Protokół SSL

Wersja 5 Wydanie 3



IBM

@server

System iSeries

Protokół SSL

Wersja 5 Wydanie 3

Uwaga

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

Wydanie piąte (sierpień 2005)

Niniejsze wydanie dotyczy wersji 5, wydania 3, modyfikacji 0 systemu IBM Operating System/400 (numer produktu 5722–SS1) oraz wszelkich kolejnych wersji i modyfikacji tego produktu, o ile nowe wydania nie wskazują inaczej. Niniejsza wersja nie działa we wszystkich modelach komputerów RISC ani CISC.

Spis treści

Protokół SSL

Protokół SSL jest standardem przemysłowym umożliwiającym aplikacjom nawiązywanie chronionych sesji komunikacyjnych poprzez niezabezpieczoną sieć, taką jak Internet. Więcej informacji o protokole SSL i aplikacjach serwera iSeries można znaleźć w następujących sekcjach:

- **Co nowego w wersji V5R3**
  Uwagi na temat nowych funkcji lub nowych informacji dotyczących protokołu SSL.
- **Scenariusze SSL**
  Dodatkowe informacje dotyczące protokołu SSL na serwerze iSeries pomagające w jego przyswojeniu dzięki przedstawionym przykładom możliwych zastosowań.
- **Pojęcia dotyczące protokołu SSL**
  zawiera informacje uzupełniające składające się z kilku podstawowych bloków dla protokołów Secure Sockets Layer (SSL).
- **Planowanie uruchomienia protokołu SSL**
  Wymagania wstępne związane z uruchomieniem protokołu SSL na serwerze iSeries oraz kilka pożytecznych wskazówek.
- **Aplikacje chronione protokołem SSL**
  Spis aplikacji serwera iSeries, które można chronić korzystając z protokołu SSL.
- **Rozwiązywanie problemów związanych z protokołem SSL**
  Podstawowe informacje dotyczące rozwiązywania problemów związanych z SSL na serwerze iSeries.
- **Informacje pokrewne**
  Odsyłacze do dodatkowych zasobów informacji.

Co nowego w wersji V5R3

Do sekcji Uwagi dodano dwie nowe pozycje dotyczące protokołu Secure Sockets Layer (SSL) w tej wersji:

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

   Jest to nowy scenariusz wyjaśniający sposób używania protokołu SSL do ochrony połączenia między klientem zdalnym a serwerem Centrum Zarządzania na serwerze iSeries, który jest systemem centralnym określonym dla sieci LAN.
2. Pakiet GSKit w wersji 6B funkcji API GSKit

   Począwszy od wersji V5R3, funkcje API GSKit są oparte na pakiecie GSKit w wersji 6B. W poprzedniej wersji były one oparte na pakiecie GSKit w wersji 4D. Kliknij tutaj, aby uzyskać więcej informacji na temat funkcji API pakietu GSKit.

Więcej informacji na temat nowości lub zmian w tej wersji zawiera publikacja Informacje dla użytkowników 

Jak sprawdzić nowości i zmiany:

Aby pomóc w określeniu, gdzie wprowadzone zostały zmiany techniczne, w informacjach używa się:

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

Drukowanie tego dokumentu

Wymienione informacje można przeglądać lub pobrać w wersji PDF. Aby to zrobić, należy wybrać Protokół SSL (Secure Sockets Layer) (około 243 kB).

Inne informacje:

Można także przejrzeć lub wydrukować dowolne informacje pokrewne.

Zapisz pliki PDF:

Aby zapisać plik PDF na stacji roboczej w celu dalszego wykorzystania:
1. W przeglądarce kliknij prawym przyciskiem myszy plik PDF.
2. Kliknij **Zapisz jako**.
3. Wybierz katalog, w którym ma zostać zachowany plik PDF.
4. Kliknij **Zapisz**.

Pobierz program Adobe Acrobat Reader:

Jeśli do przeglądania lub drukowania informacji potrzebny jest program Adobe Acrobat Reader, jego kopię można pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html). 

Scenariusze

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

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

  Ten 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.
- Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL

  Ten 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.
- Scenariusz: Ochrona aplikacji FTP za pomocą SSL

  Ten scenariusz wyjaśnia sposób włączania protokołu SSL dla aplikacji FTP.
- Scenariusz: Ochrona aplikacji Telnet za pomocą SSL

  Ten scenariusz wyjaśnia sposób włączania protokołu SSL dla aplikacji Telnet.
- Scenariusz: Zwiększenie wydajności protokołu SSL systemu iSeries

  Ten scenariusz wyjaśnia sposób wykorzystania sprzętu szyfrującego w celu zwiększenia wydajności SSL na serwerze iSeries.
- Scenariusz: Wykorzystanie sprzętu szyfrującego do zabezpieczania prywatnych kluczy

  Ten scenariusz wyjaśnia sposób używania sprzętu szyfrującego do ochrony kluczy prywatnych powiązanych z transakcjami SSL na serwerze iSeries.

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

Sytuacja:

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

Bob chce się połączyć z serwerem Centrum Zarządzania w Systemie A z sieci lokalnej znajdującej się poza jego firmą. Bob 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. Bob 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 Bob może być pewien, że podczas podróży jego połączenie z serwerem Centrum Zarządzania jest bezpieczne.

Cele:

Bob chce chronić połączenie między swoim komputerem PC i serwerem Centrum Zarządzania. Bob 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. Bob planuje skonfigurować swój komputer PC i serwer Centrum Zarządzania w Systemie A, tak aby połączenie klienta 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 Boba	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 Boba uwierzytelnia certyfikat serwera Centrum Zarządzania. Komputer PC Boba 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 Boba.

Wymagania wstępne i założenia:

Bob 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 (patrz sekcja Wymagania wstępne dotyczące protokołu SSL).
2. W systemie A musi być zainstalowana wersja V5R3 (lub nowsza) systemu OS/400 Jeśli zainstalowano wersję V5R1 systemu OS/400, należy zainstalować następujące poprawki (PTF) dla systemu OS/400 (5722-SS1):
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. Klient PC iSeries Navigator ma zainstalowaną wersję V5R3 lub nowszą programu iSeries Access dla 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.
   a. W Systemie A: Uruchomić IBM Digital Certificate Manager. Bob uzyskuje lub tworzy certyfikaty albo konfiguruje lub zmienia system certyfikacji. Więcej informacji na temat konfigurowania systemu certyfikacji zawiera sekcja Korzystanie z Menedżera certyfikatów cyfrowych.
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz **hasło bazy certyfikatów** *SYSTEM i kliknij **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.

e. Kliknij **Aktualizacja przypisania certyfikatów**.
f. Wybierz **Serwer** i kliknij **Kontynuuj**.
g. Wybierz **Zarządzanie serwerem centralnym** i kliknij **Aktualizacja przypisania certyfikatów**. Powoduje to przypisanie certyfikatu do serwera Centrum Zarządzania, aby można było ustalać tożsamość klientów iSeries Access dla Windows.
h. Kliknij **Przypisanie nowego certyfikatu**. Program DCM zostanie przeładowany do strony **Aktualizacja przypisania certyfikatów** z komunikatem potwierdzającym.
i. Kliknij **Gotowe**.

8. Skonfigurować program iSeries Navigator:
   a. Selektywnie zainstalować komponent SSL programu iSeries Navigator w komputerze klienckim PC.
   b. Pobrać ośrodek certyfikacji (CA) do klienta PC.

Kroki konfiguracji:

Bob musi wykonać poniższe kroki, aby zabezpieczyć połączenie swojego komputera PC z serwerem Centrum Zarządzania w Systemie A za pomocą protokołu SSL:
1. Krok 1: Deaktywuj SSL dla klienta iSeries Navigator
2. Krok 2: Ustaw poziom uwierzytelniania dla serwera Centrum Zarządzania
3. Krok 3: Zrestartuj serwer Centrum Zarządzania w Systemie A
4. Krok 4: Uaktywnij protokół SSL dla klienta iSeries Navigator
5. Krok opcjonalny: Deaktywuj SSL dla klienta iSeries Navigator

Kroki rozszerzonej konfiguracji zawiera sekcja Ochrona połączenia klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

Szczegóły konfiguracji: Ochrona połączenia 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. Bob używa serwera Centrum Zarządzania w systemie centralnym (nazywanym tutaj Systemem A) do zarządzania systemami końcowymi w firmowej sieci. Poniższe informacje wyjaśniają sposób wykonywania kroków wymaganych do ochrony połączenia klienta zewnętrznego z serwerem Centrum Zarządzania. Należy śledzić sposób wykonywania przez Boba kroków konfiguracyjnych w tym scenariuszu.

Zanim Bob będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować programy wymagane wstępnie oraz skonfigurować certyfikaty cyfrowe na serwerze iSeries. Zanim przejdziesz dalej, zapoznaj się z sekcją Wymagania wstępne i założenia dla tego scenariusza. Po spełnieniu wymagań wstępnych Bob może wykonać poniższe procedury w celu włączenia protokołu SSL dla serwera Centrum Zarządzania.

Krok 1: Deaktywuj 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 **Chronione gniazda** 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 Boba o tym, że nie ma już chronionego przez SSL połączenia między klientem i systemem centralnym w swojej firmie.

Krok 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.

Krok 3: Restartuj 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 **Uruchom**, aby go zrestartować.

Krok 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 Boba 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 Krok 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.

Krok opcjonalny: Deaktywuj protokół SSL dla klienta iSeries Navigator

Jeśli Bob 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. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Właściwości**.
3. Kliknij zakładkę **Chronione gniazda** i usuń zaznaczenie z pola wyboru **Podczas połączenia używaj protokołu SSL**.
4. Zakończ program iSeries Navigator i uruchom go ponownie.

Znika kłódka znajdująca się obok serwera Centrum Zarządzania w programie iSeries Navigator, co oznacza, że połączenie jest niechronione. Dzięki temu Bob wie, że połączenie między jego klientem PC a serwerem Centrum Zarządzania w Systemie A nie jest już chronione za pomocą protokołu SSL.

W sekcji Scenariusze poszukaj odsyłaczy do innych scenariuszy dotyczących protokołu SSL.

Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania 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. Tom jest specjalistą do spraw ochrony w firmie. Chce używać protokołu SSL (Secure Sockets Layer) do ochrony wszystkich połączeń między serwerem Centrum Zarządzania zainstalowanym na systemie centralnym w firmie a wszystkimi serwerami końcowymi i klientami.

Szczegóły:

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

Może wybrać jeden z dwóch poziomów uwierzytelniania:

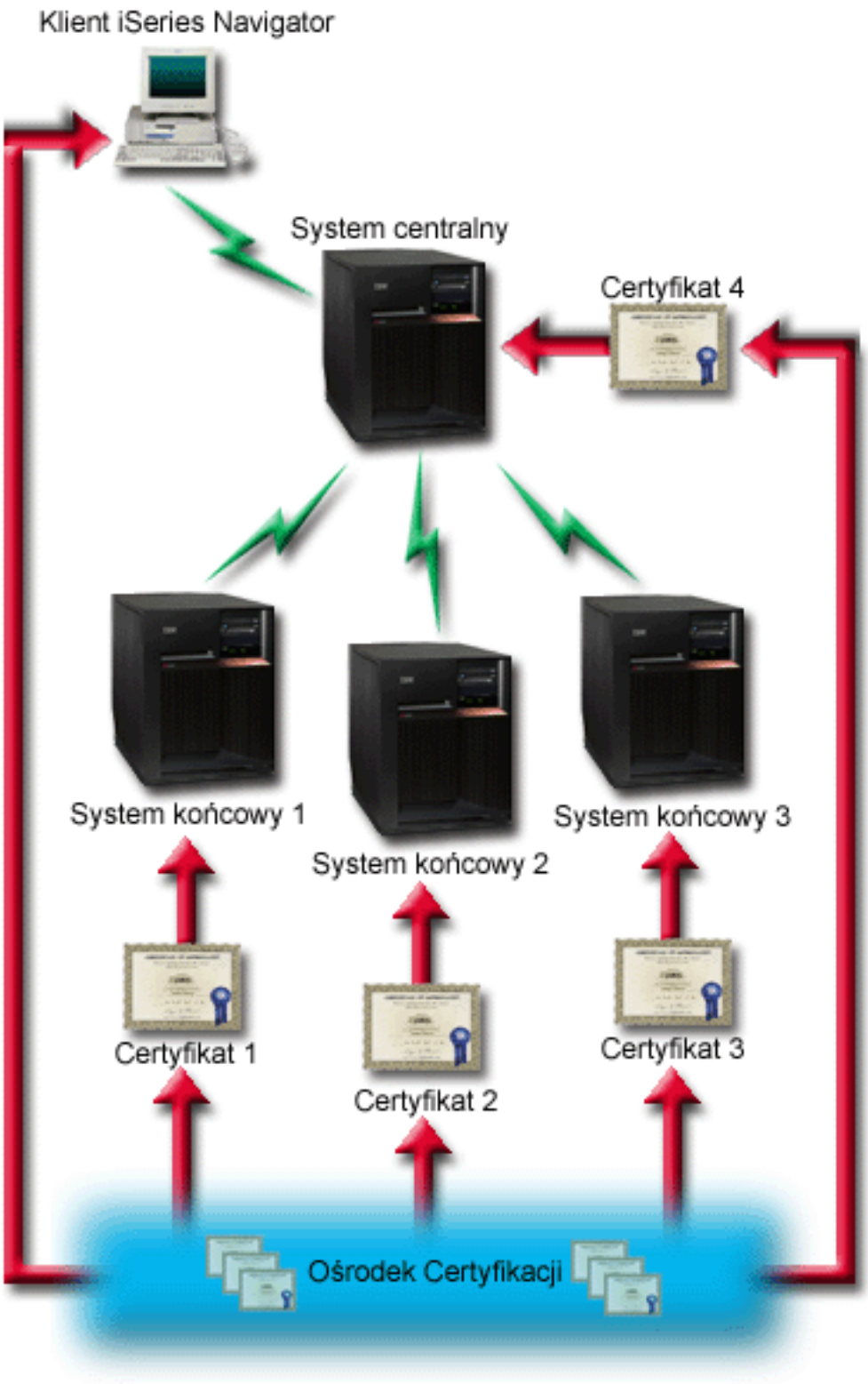
Uwierzytelnianie serwera
Uwierzytelnianie certyfikatu serwera systemu końcowego. System centralny podczas łączenia się z systemem końcowym działa jako klient SSL. System końcowy działa jako serwer SSL i musi udowadniać swoją tożsamość dostarczając certyfikat wydany przez ośrodek certyfikacji, któremu ufa system centralny. Każdy system końcowy 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.

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. Jeśli komputer PC używa połączenia z systemem centralnym i włączona jest warstwa SSL, 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.



Wymagania wstępne i założenia:

Tom musi wykonać zadania administrowania i konfiguracji (patrz ilustracja Sieć WAN Centrum Zarządzania chroniona za pomocą protokołu SSL), aby chronić wszystkie połączenia z serwerem Centrum Zarządzania:

1. System centralny spełnia wymagania wstępne dla protokołu SSL (patrz sekcja Wymagania wstępne dotyczące protokołu SSL).
2. System centralny i wszystkie serwery końcowe iSeries mają zainstalowaną wersję V5R2 lub nowszą systemu OS/400. Jeśli w systemie centralnym i w systemach końcowych jest zainstalowana wersja V5R1 systemu OS/400, należy zainstalować poniższe poprawki (PTF) dla systemu OS/400 (5722-SS1):
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. Klient PC iSeries Navigator ma zainstalowaną wersję V5R2 lub nowszą programu iSeries Access dla Windows. Jeśli klient ma zainstalowaną wersję V5R1, należy zainstalować pakiet serwisowy PTF SI01907 (lub nowszy) dla wersji V5R1 iSeries Access for Windows (5722-XE1).
4. Znaleźć ośrodek wydający certyfikaty (CA) dla serwerów iSeries.
5. Utworzyć certyfikat przypisany przez ośrodek certyfikacji każdemu serwerowi iSeries, który jest zarządzany przez serwer Centrum Zarządzania udostępniony poprzez SSL.
6. Wysłać CA i certyfikat do każdego serwera iSeries, a następnie importować je do bazy danych kluczy.
7. Przypisać certyfikaty z identyfikacją aplikacji Centrum Zarządzania i identyfikacjami aplikacji dla wszystkich serwerów końcowych używających iSeries Navigator:
   a. Na serwerze centralnym uruchom program IBM Digital Certificate Manager. Jeśli chcesz uzyskać lub utworzyć certyfikaty, zmienić lub skonfigurować system certyfikatów, zrób to w tym momencie (sekcja Korzystanie z programu Digital Certificate Manager zawiera informacje dotyczące konfigurowania systemu certyfikatów).
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz **hasło bazy certyfikatów** *SYSTEM i kliknij **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.
   e. Kliknij **Aktualizacja przypisania certyfikatów**.
   f. Wybierz **Serwer** i kliknij **Kontynuuj**.
   g. Wybierz **serwer Centrum Zarządzania** i kliknij **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. Powtórz procedurę dla wszystkich serwerów końcowych, z których korzysta program iSeries Navigator.
8. Skonfigurować program iSeries Navigator:
   a. Selektywnie zainstalować komponent SSL programu iSeries Navigator w komputerze klienckim PC.
   b. Pobrać ośrodek certyfikacji (CA) do klienta PC.

Kroki konfiguracji:

Zanim Tom będzie mógł włączyć SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy i skonfigurować certyfikaty cyfrowe w systemie centralnym. Zanim przejdziesz dalej, zapoznaj się z sekcją Wymagania wstępne i założenia dla tego scenariusza. 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, Tom 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.

- Krok 1: Skonfiguruj system centralny pod kątem uwierzytelniania serwera

- Krok 2: Skonfiguruj systemy końcowe pod kątem uwierzytelniania serwera
- Krok 3: Zrestartuj serwer Centrum Zarządzania w systemie centralnym
- Krok 4: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych
- Krok 5: Uaktywnij protokół SSL dla klienta iSeries Navigator
- Krok 6: Skonfiguruj system centralny pod kątem uwierzytelniania klientów
- Krok 7: Skonfiguruj systemy końcowe pod kątem uwierzytelniania klientów
- Krok 8: Skopiuj listę weryfikacji do systemów końcowych
- Krok 9: Zrestartuj serwer Centrum Zarządzania w systemie centralnym
- Krok 10: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych

Kroki rozszerzonej konfiguracji opisuje sekcja Szczegóły konfiguracji: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL.

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

W poniższych informacjach przyjęto, że użytkownik zapoznał się z następującymi informacjami: Scenariusz: Ochrona wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL. Użytkownik chce zrozumieć sposób wykonywania kroków wymaganych do ochrony wszystkich połączeń z serwerem Centrum Zarządzania. Należy śledzić sposób wykonywania operacji przez Toma w tym scenariuszu.

Zanim Tom będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy oraz skonfigurować certyfikaty cyfrowe na serwerze iSeries. Zanim przejdziesz dalej, zapoznaj się z sekcją Wymagania wstępne i założenia dla tego scenariusza. 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, Tom 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.

Krok 1: Skonfiguruj system centralny pod kątem uwierzytelniania serwera

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. Tom musi skonfigurować uwierzytelnianie serwera zanim skonfiguruje uwierzytelnianie klienta.

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 do momentu skonfigurowania systemów końcowych w celu przeprowadzenia uwierzytelniania serwera.
5. Konfigurowanie systemów końcowych pod kątem uwierzytelniania serwera.

Krok 2: Skonfiguruj systemy końcowe pod kątem uwierzytelniania serwera

Po skonfigurowaniu systemu centralnego pod kątem uwierzytelniania serwera Tom 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 **Zasoby—>Kolekcjonuj**.
b. Zaznacz opcję **Wartości systemowe** w oknie dialogowym kolekcjonowania, aby gromadzić ustawienia wartości systemowych w systemie centralnym. Usuń zaznaczenie wszystkich pozostałych opcji.
c. Kliknij prawym przyciskiem myszy **Grupy systemów—>Nowa grupa systemów**.
d. Zdefiniuj nową grupę systemową zawierającą wszystkie systemy końcowe, z którymi będziesz się łączyć korzystając z SSL.
e. Aby wyświetlić nową grupę, rozwiń grupy systemowe.
f. Po zakończeniu zbierania informacji kliknij prawym przyciskiem myszy nową grupę systemową i wybierz **Wartości systemowe—>Porównaj i zaktualizuj**.
g. Sprawdź, czy system centralny jest wyświetlany w polu **System modelowy**.
h. Wybierz kategorię **Centrum Zarządzania** i ustaw następujące wartości, zaznaczając odpowiednią pozycję:
   - Wybierz **Tak** dla **Używaj protokołu SSL**.
   - Jako poziom uwierzytelniania SSL wybierz **Serwer**.

   Wartości te są ustawiane w systemie centralnym podczas wykonywania procedury Konfigurowanie systemu centralnego dla uwierzytelniania serwera.
i. Kliknij **OK**, aby ustawić te wartości w systemach końcowych w nowej grupie systemowej.
j. Przed restartem serwera Centrum Zarządzania poczekaj na zakończenie procesu **porównania i aktualizacji**. Może to zająć kilka minut.

Krok 3: Restartuj serwer Centrum Zarządzania w systemie centralnym

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń widok systemu centralnego.
3. Rozwiń **Sieć—> Serwery** i wybierz **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 **Uruchom**, aby go zrestartować.

Krok 4: Restartuj serwer Centrum Zarządzania we wszystkich systemach końcowych

1. Rozwiń system końcowy, który chcesz zrestartować.
2. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
3. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
4. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.
5. Powtórz procedurę dla każdego systemu końcowego.

Krok 5: Uaktywnij 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.

Krok 6: Skonfiguruj system centralny pod kątem uwierzytelniania klienta (krok opcjonalny)

Po zakończeniu konfiguracji pod kątem uwierzytelniania serwera Tom 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 klienta. Taka operacja jest czasem nazywana uwierzytelnianiem ośrodka certyfikacji i zaufanej grupy.

Uwaga: Konfiguracji uwierzytelniania klienta nie można zakończyć do momentu skonfigurowania uwierzytelniania serwera.

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 do momentu skonfigurowania wszystkich systemów końcowych, aby używać SSL podczas uwierzytelniania klienta i serwera.
5. Skonfiguruj systemy końcowe pod kątem uwierzytelniania klienta.

Krok 7: Skonfiguruj systemy końcowe pod kątem uwierzytelniania klienta (krok opcjonalny)

1. Porównaj i zaktualizuj wartości systemowe dla systemów końcowych:

   Uwaga: Zadanie nie będzie działać na serwerach iSeries z zainstalowanym systemem w wersji V4R5.

   a. W oknie **Systemy końcowe** kliknij prawym przyciskiem myszy system centralny i wybierz **Zasoby—>Kolekcjonuj**.
   b. Zaznacz opcję **Wartości systemowe** w oknie dialogowym kolekcjonowania, aby gromadzić ustawienia wartości systemowych w systemie centralnym. Usuń zaznaczenie wszystkich pozostałych opcji.
   c. Kliknij prawym przyciskiem myszy **Grupy systemów—>Nowa grupa systemów**.
   d. Zdefiniuj nową grupę systemową zawierającą wszystkie systemy końcowe, z którymi będziesz się łączyć korzystając z SSL.
   e. Aby wyświetlić nową grupę, rozwiń grupy systemowe.
   f. Po zakończeniu zbierania informacji kliknij prawym przyciskiem myszy nową grupę systemową i wybierz **Wartości systemowe—>Porównaj i zaktualizuj**.
   g. Sprawdź, czy **System centralny** jest widoczny w polu **System modelowy**.
   h. Wybierz kategorię **Centrum Zarządzania** i sprawdź, czy:
      - Wybierz **Tak** dla **Używaj protokołu SSL**.
      - Jako poziom uwierzytelniania SSL wybierz **Klient i serwer**.

      Wartości te są ustawiane w systemie centralnym podczas wykonywania procedury Konfigurowanie systemu centralnego pod kątem uwierzytelniania klienta. Przy każdej wartości zaznacz pole **Aktualizuj**.
   i. Kliknij **OK**, aby ustawić te wartości w systemach końcowych w nowej grupie systemowej.

Krok 8: Skopiuj listę weryfikacji do systemów końcowych

1. Poniższa procedura zakłada, że systemem centralnym użytkownika jest system V5R3 lub nowszy: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:
   - **Nazwa:** wpisz nazwę definicji.
   - **System źródłowy:** wybierz nazwę systemu centralnego.
   - **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 **Tak**, aby zezwolić na różnice w obiektach podczas odtwarzania.
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 **Grupy systemowe->Zaufana grupa**, znajdującą się na liście **Dostępne systemy i grupy**. Osobno dodaj do listy **Wybrane systemy i grupa** wszystkie systemy wersji V5R3 lub nowsze.

Usuń wszystkie pozostałe systemy z listy **Wybrane systemy i grupa** i kliknij przycisk **OK**. Zaufana grupa jest grupą systemową zdefiniowaną w części 1.c. Kroku 7: Konfigurowanie systemów końcowych dla uwierzytelniania klienta.

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.

W wersjach systemu iSeries 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. Aby to zrobić:

a. Kliknij prawym przyciskiem myszy utworzoną definicję pakietu i wybierz **Nowa w oparciu o**.
b. Nadaj definicji nową nazwę, aby odróżnić ją od pierwszej definicji.
c. Na karcie **Ogólne** definicji, w kolumnie **Ścieżka docelowa**, kliknij ścieżkę /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL. Pozwala to na dokonanie edycji. Zmień QMGTC2 na QUSRSYS.

   Uwaga: Upewnij się, że zmieniana jest **Ścieżka docelowa**, a nie **Ścieżka źródłowa**.
d. Kliknij przycisk **OK**, aby zapisać nową definicję pakietu.
e. Kliknij prawym przyciskiem myszy nową definicję pakietu i wybierz **Wyślij**.
f. W oknie dialogowym **Wyślij**: Rozwiń **Grupy systemowe->Zaufana grupa**, znajdującą się na liście **Dostępne systemy i grupy**.Osobno dodaj do listy **Wybrane systemy i grupa** wszystkie systemy wersji starszych niż V5R3. Usuń wszystkie pozostałe systemy z listy **Wybrane systemy i grupa** i kliknij **OK**. **Zaufana grupa** jest grupą systemową zdefiniowaną w części 1.c Kroku 7: Konfigurowanie systemów końcowych.

Krok 9: Zrestartuj serwer Centrum Zarządzania w systemie centralnym

1. W programie iSeries Navigator rozwiń **Moje połączenia**.
2. Rozwiń system centralny.
3. Rozwiń **Sieć—> Serwery** i wybierz **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 **Uruchom**, aby go zrestartować.

Krok 10: Zrestartuj serwer Centrum Zarządzania we wszystkich systemach końcowych

Uwaga: Powtórz procedurę dla każdego systemu końcowego.

1. Rozwiń system końcowy, który chcesz zrestartować.
2. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
3. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
4. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.

W sekcji Scenariusze poszukaj odsyłaczy do innych scenariuszy dotyczących protokołu SSL.

Pojęcia

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.

Poniższe informacje pozwalają lepiej zrozumieć relacje między SSL i serwerem iSeries:

- Historia SSL
- Jak działa SSL

- Obsługiwane protokoły SSL i TLS (Transport Layer Security)
- Uwierzytelnianie serwera
- Uwierzytelnianie 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. Sekcja Obsługiwane protokoły SSL i TLS (Transport Layer Security) zawiera więcej informacji na temat SSL i protokołów pokrewnych.

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 V5R2M0 i kolejnych wydaniach można zminimalizować wpływ wydajności uzgadniania SSL na procesor główny poprzez używanie sprzętu szyfrującego.

Obsługiwane protokoły SSL i TLS (Transport Layer Security)

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 OS/400 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

Uwagi:

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. Obsługiwana jest również wersja 1.0 protokołu TLS zgodna 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 nastąpić. Wykorzystując słabość specyfikacji szyfru, osoba bez uprawnień mogła złamać klucz 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 przez Internet Engineering Task Force (IETF) w dokumencie RFC 2246, ″The TLS Protocol.″ 

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:

- **Metoda Key-Hashing for Message Authentication (HMAC)**
  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.
- **Ulepszona metoda weryfikacji komunikatu końcowego**
  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.

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,
- usługi katalogowe (LDAP).

Planowanie uruchomienia protokołu SSL

Planując uruchomienie protokołu SSL na serwerze iSeries, należy wziąć pod uwagę:

- wymagania wstępne protokołu SSL,
- rodzaj certyfikatów cyfrowych i miejsce ich uzyskania.

Wymagania wstępne protokołu SSL:

- Program IBM Digital Certificate Manager (DCM), opcja 34 (5722-SS1) systemu OS/400
- 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 IBM Developer Kit for Java (5722–JV1). W przeciwnym razie serwer administratora HTTP nie zostanie uruchomiony.
- Produkt IBM Cryptographic Access Provider, 5722-AC3 (128-bitowy). Ilość bitów podana dla tego produktu wskazuje maksymalną wielkość tajnego materiału wewnątrz klucza symetrycznego, którego można użyć w operacjach szyfrujących. Wielkość klucza symetrycznego określają w każdym kraju prawa związane z eksportem i importem. Użycie większej liczby bitów gwarantuje bezpieczniejsze połączenie.
- Aby przyspieszyć przetwarzanie uzgadniania SSL, można zainstalować sprzęt szyfrujący do obsługi protokołu SSL. Sekcja Sprzęt szyfrujący zawiera informacje na temat dostępnych opcji. Jeśli mają zostać zainstalowane adaptery 4758 IBM Cryptographic Coprocessor lub 4764 IBM Cryptographic Coprocessor, należy również zainstalować opcję 35, Cryptographic Service Provider.

Jeśli chcesz używać protokołu SSL z komponentami iSeries Access for Windows, musisz również zainstalować produkt iSeries Client Encryption, 5722-CE3 (128-bitowy). Program iSeries Access for Windows wymaga tego produktu, aby nawiązać chronione połączenie.

Uwaga: Aby korzystać z emulatora PC5250, dostarczanego z produktem Personal Communications, nie trzeba instalować produktu Client Encryption, gdyż Personal Communications ma wbudowany własny kod szyfrowania.

Certyfikaty cyfrowe

Aby lepiej zrozumieć różnice między publicznymi i prywatnymi certyfikatami cyfrowymi i opcje ich zamawiania, zapoznaj się z dokumentem Korzystanie z certyfikatów publicznych a wydawanie certyfikatów prywatnych.

Program IBM Digital Certificate Manager (DCM) jest rozwiązaniem służącym do zarządzania certyfikatami cyfrowymi, utworzonym z myślą o serwerze iSeries. Więcej informacji o programie DCM można znaleźć w artykule Korzystanie z programu Digital Certificate Manager w Centrum informacyjnym.

Aplikacje chronione protokołem SSL

Protokołem SSL można chronić następujące aplikacje serwera iSeries:
- Enterprise Identity Mapping (EIM),
- serwer FTP,
- serwer HTTP (oparty na Apache),
- program iSeries Access for Windows,
- Directory Services Server (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, przy czym takie funkcje mają: produkt Global Secure Toolkit (GSKit) oraz rodzime funkcje SSL_ serwera iSeries, zaś informacje o GSKit i SSL_API zawiera artykuł Secure Sockets APIs.

Rozwiązywanie problemów związanych 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 zauważyć, że nie jest to obszerne źródło informacji na ten temat, ale po prostu podręcznik.

Sprawdź, czy zostały spełnione następujące warunki:
- wymagania wstępne dla protokołu SSL na serwerze iSeries (patrz Wymagania wstępne dla protokołu SSL),
- jeśli korzystasz z Centrum Zarządzania programu iSeries Navigator z systemem w wersji V5R1, to czy masz w systemie zainstalowane następujące poprawki PTF:
  - SI01375
  - SI01376
  - SI01377
  - SI01378
  - SI01838
- 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. Strona Komunikaty dla kodów błędu funkcji API SSL zawiera informacje o komunikatach dla kodów błędów SSL. 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.

Więcej informacji na temat rozwiązywania problemów dotyczących serwera iSeries zawiera strona Rozwiązywanie problemów i obsługa.

Informacje pokrewne

Dodatkowe informacje dotyczące protokołu SSL można znaleźć w następujących dokumentach:

Źródła firmy **IBM**

- Strona SSL i Java Secure Socket Extension (JSSE) zawiera krótki opis pakietu JSSE i jego zastosowania.
- Strona IBM Toolbox for Java zawiera krótki opis dostępnych klas Java oraz ich zastosowania.

Dokumenty RFC

- RFC 2246: ″The TLS Protocol Version 1.0 ″ wyjaśnia szczegóły protokołu TLS.
- RFC2818: ″HTTP Over TLS″ opisuje, jak korzystać z protokołu TLS do ochrony połączeń HTTP w Internecie.

Inne źródła

- Dokument The SSL Protocol Version 3.0 przedstawia dużo szczegółów na temat protokołu SSL wersja 3.0.

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

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 CorporationLicensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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 używania 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 CorporationSoftware Interoperability Coordinator, Department 49XA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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.

Znaki towarowe

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

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

Lotus, Freelance oraz WordPro są znakami towarowymi International Business Machines Corporation i Lotus Development 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.

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

Warunki pobierania i drukowania publikacji

Zezwolenie na korzystanie z publikacji, które Użytkownik zamierza pobrać, jest przyznawane na poniższych warunkach. Warunki te wymagają akceptacji Użytkownika.

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 z nich 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 z tych publikacji ani z ich części 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 CZY PRZYDATNOŚCI DO OKREŚLONEGO CELU.

Pobieranie lub drukowanie publikacji z tego serwisu oznacza zgodę na warunki zawarte w niniejszym dokumencie.