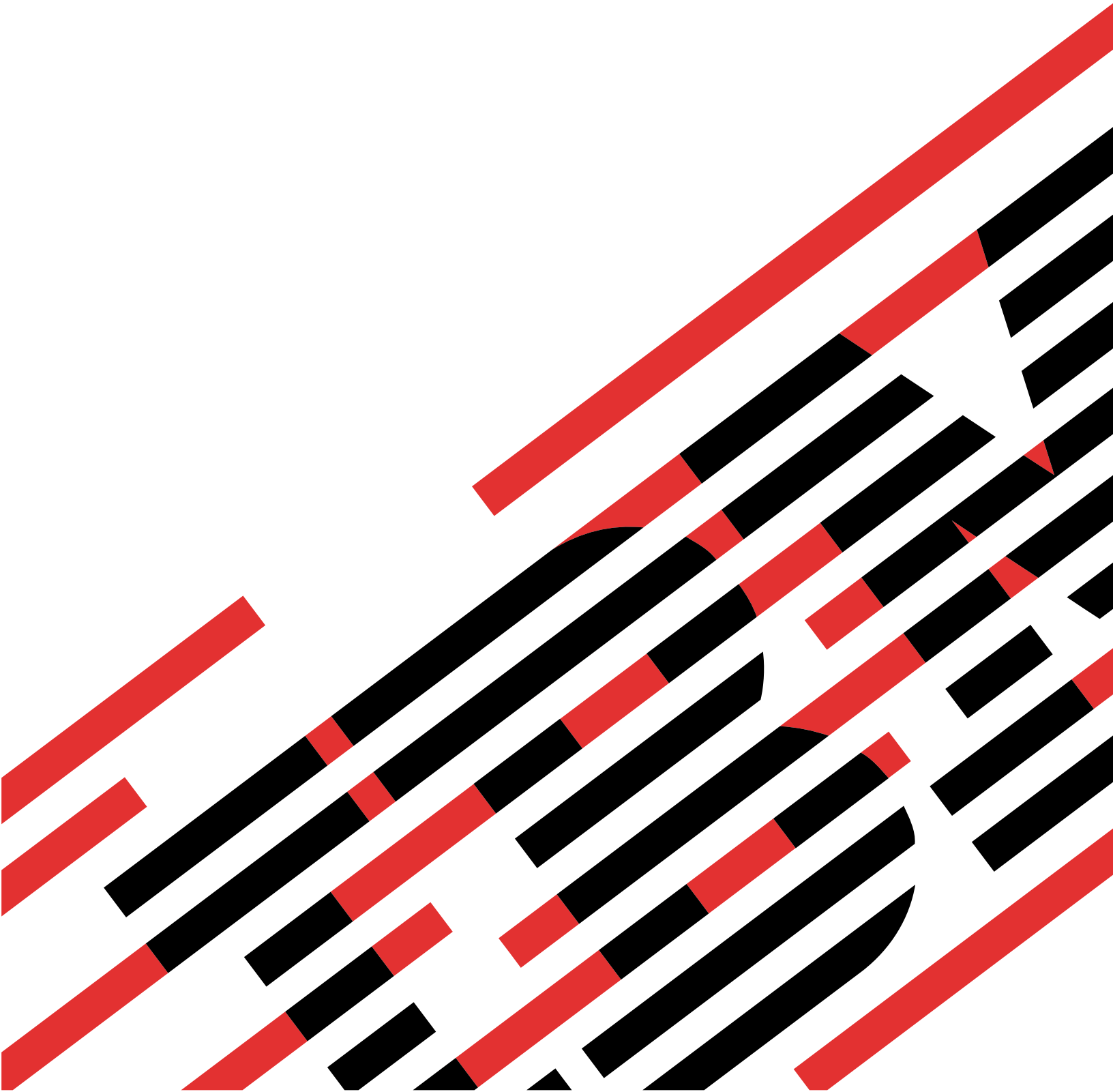
IBM

eserver

iSeries

Protokół SSL (Secure Sockets Layer)



IBM

@server

iSeries

Protokół SSL (Secure Sockets Layer)

Spis treści

Część 1. Protokół SSL (Secure Sockets Layer)

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 V5R2**
  Uwagi o nowych funkcjach i informacjach 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**
  Dodatkowe informacje o elementach składających się na protokół 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 o protokole SSL**
  Odsyłacze do dodatkowych zasobów informacji.

Rozdział 1. Co nowego w wersji V5R2

W wersji V5R2M0 dostępna jest opcja 2058 Cryptographic Accelerator for iSeries. Jest to opcja szyfrująca zrealizowana sprzętowo, zwiększająca wydajność SSL serwera iSeries. Więcej informacji na ten temat zawiera dokument o sprzęcie szyfrującym.

Nowy interfejs API: Global Secure Kit (GSKit)

Udostępniono także nowy interfejs API OS/400 Global Secure Toolkit (GSKit): gsk_secure_soc_startInit(). Więcej informacji zawiera artykuł Interfejsy API: Global Secure ToolKit (GSKit).

Więcej informacji o nowościach i zmianach, jakie znalazły się w tej wersji, zawiera dokument Informacje dla użytkowników

Graficzne wyróżnienie wprowadzonych zmian i nowości

Aby wyróżnić wprowadzone zmiany i nowości użyto:
- symbolu

  wskazującego miejsce, gdzie się one rozpoczynają,
- symbolu

  do oznaczenia miejsca, w którym się one kończą.

Rozdział 2. Drukowanie tego dokumentu

Wymienione informacje można przeglądać lub pobrać w wersji PDF. W tym celu należy wybrać Aplikacje chronione protokołem SSL (około 215 kB lub 34 strony).

Inne informacje

Można także przejrzeć lub wydrukować dowolne informacje pokrewne.

Zapisywanie plików 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. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij **Zapisz**.

Pobieranie programu Adobe Acrobat Reader

Jeśli do przeglądania lub drukowania tych informacji potrzebujesz programu Adobe Acrobat Reader, jego kopię możesz pobrać z serwisu WWW firmy Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Rozdział 3. Scenariusze SSL

Scenariusze, które pomagają maksymalizować korzyści płynące z uruchomienia protokołu SSL na serwerze iSeries:

- Scenariusz: ochrona Centrum Zarządzania za pomocą SSL
- Scenariusz: ochrona aplikacji FTP za pomocą SSL
- Scenariusz: ochrona aplikacji Telnet za pomocą SSL
- Scenariusz: poprawianie wydajności protokołu SSL serwera iSeries
- Scenariusz: wykorzystanie sprzętu szyfrującego do zabezpieczania prywatnych kluczy

Scenariusz SSL: ochrona Centrum Zarządzania za pomocą SSL

Opis sytuacji

W przedsiębiorstwie utworzono rozległą sieć zawierającą kilka oddalonych od siebie serwerów iSeries (systemy końcowe), zarządzanych centralnie z jednego serwera iSeries znajdującego się w centrali. Specjalista d/s ochrony w przedsiębiorstwie korzysta z Centrum Zarządzania klienta iSeries Navigator do łączenia się z serwerem iSeries w centrali (system centralny). Chce on chronić połączenia pomiędzy systemem centralnym i wszystkimi serwerami końcowymi za pomocą protokołu SSL.

Szczegóły

Centrum Zarządzania programu iSeries Navigator umożliwia mu zarządzanie wieloma systemami z jednego systemu centralnego. Dzięki wykorzystaniu protokołu SSL z programem Centrum Zarządzania, może on **pewnie** zarządzać tymi systemami. Aby skorzystać z protokołu SSL w programie Centrum Zarządzania, musi na komputerze PC, z którego uruchamia Centrum Zarządzania, chronić programy iSeries Access for Windows oraz iSeries Navigator.

W środowisku Centrum Zarządzania Tomasz ma do wyboru dwa poziomy 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. Rozwiązanie to jest uważane za skuteczniejsze, niż samo uwierzytelnianie 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.

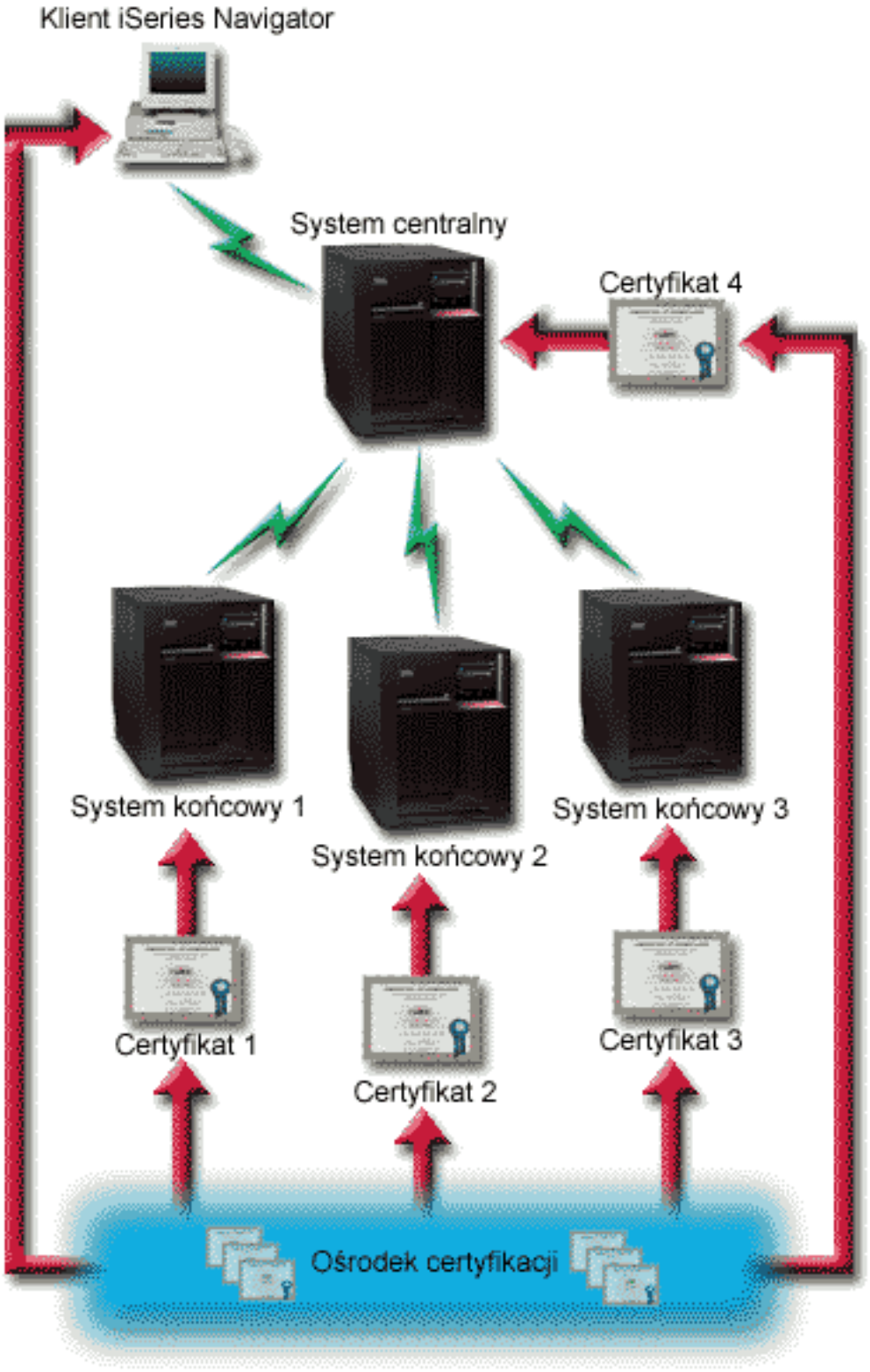
  W przeciwieństwie do innych aplikacji, Centrum Zarządzania umożliwia także uwierzytelnianie przez listę weryfikacji, nazywaną listą weryfikacji zaufanych grup. Zazwyczaj lista weryfikacji przechowuje

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 zazwyczaj nie umożliwia jednoczesnego uwierzytelniania serwera i klienta, ponieważ uwierzytelnianie serwera zawsze następuje podczas aktywacji 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 użytkownicy komputerów PC łączą się z systemem centralnym i protokół SSL jest włączony, system centralny działa jako serwer, jednak gdy jest połączony z systemem końcowym, działa jako klient. Rysunek ilustruje, jak system centralny funkcjonuje w sieci jako serwer i jako klient.

Uwaga: Poniższy rysunek ilustruje sytuację, w której certyfikat powiązany z ośrodkiem certyfikacji musi być przechowywany w bazie danych kluczy systemu centralnego lub na wszystkich systemach

końcowych.



Założenia i wymagania wstępne

Aby uruchomić Centrum Zarządzania z włączonym protokołem SSL, specjalista do spraw ochrony musi wykonać następujące zadania administracyjne i konfiguracyjne (patrz rysunek Centrum Zarządzania sieci WAN chronione protokołem SSL):

1. Przygotować serwer iSeries z Centrum Zarządzania spełniający wymagania wstępne dla protokołu SSL (patrz Wymagania wstępne dla protokołu SSL).
2. Zainstalować na serwerze iSeries w systemie centralnym i we wszystkich punktach końcowych wersję V5R2 systemu OS/400. Jeśli jest to wersja V5R1, konieczne jest zainstalowanie następujących poprawek PTF dla systemu OS/400 (5722-SS1):
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. Zainstalować na klientach PC program iSeries Navigator PC z wersją V5R2 programu iSeries Access for Windows. Jeśli klient jest w wersji V5R1, konieczne jest zainstalowanie pakietu serwisowego PTF SI01907 (lub nowszego) dla wersji V5R1 iSeries Access for Windows (5722-XE1). Więcej informacji zawiera strona ″Ochrona Centrum Zarządzania″ w Centrum informacyjnym V5R1.
4. Znaleźć ośrodek wydający certyfikaty (CA) dla serwerów iSeries.
5. Dla każdego serwera iSeries utworzyć certyfikat podpisany przez CA i zarządzany przez serwer Centrum Zarządzania z włączonym protokołem SSL.
6. Wysłać CA i certyfikat do każdego serwera iSeries, a następnie importować je do bazy danych kluczy.
7. Przypisać certyfikaty identyfikacjom aplikacji Centrum Zarządzania a identyfikacje aplikacji wszystkim serwerom końcowym, z których korzysta program 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 **Zarządzanie serwerem centralnym** i kliknij **Aktualizacja przypisania certyfikatów**. Serwerowi Centrum Zarządzania zostanie przypisany certyfikat wykorzystywany do ustalania tożsamości klientów programu iSeries Access for Windows.
   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. Zainstaluj wybrane komponenty SSL programu iSeries Navigator.
   b. Pobierz ośrodek CA z systemu, na którym został utworzony.

      Uwaga: Jeśli zostanie wybrany certyfikat ośrodka CA, którego certyfikatu nie ma w jego bazie danych kluczy klienta programu iSeries Access for Windows, to aby korzystać z protokołu SSL, trzeba będzie dodać ten certyfikat do bazy danych.

Konfiguracja

Przed włączeniem SSL w programie Centrum Zarządzania należy zainstalować wymagane wstępnie programy i skonfigurować na serwerze iSeries certyfikaty cyfrowe (patrz sekcja Założenia i wymagania wstępne dla tego scenariusza). Jeśli spełnia te wymagania, może postąpić zgodnie z następującą procedurą.

Uwaga: Jeśli protokół SSL dla programu iSeries Navigator jest włączony, to należy go wyłączyć przed włączeniem protokołu SSL dla programu Centrum Zarządzania. Jeśli protokół SSL jest włączony dla programu iSeries Navigator i nie jest włączony dla programu Centrum Zarządzania, próby połączenia programu iSeries Navigator z Centrum Zarządzania systemu centralnego nie powiodą się.

Zadania wymagane do uwierzytelniania serwera:

1. Skonfigurowanie systemu centralnego pod kątem uwierzytelniania serwera
2. Skonfigurowanie systemów końcowych pod kątem uwierzytelniania serwera

Zadania opcjonalne do uwierzytelniania klienta:

Uwaga: Konfiguracja uwierzytelniania klienta nie może zostać zakończona przed skonfigurowaniem uwierzytelniania serwera.

1. Konfigurowanie systemu centralnego pod kątem uwierzytelniania klienta
2. Konfigurowanie systemów końcowych pod kątem uwierzytelniania klienta

Konfigurowanie systemu centralnego 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. 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. Przed uwierzytelnieniem klienta należy skonfigurować uwierzytelnianie serwera.

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

   Uwaga: **NIE można** restartować serwera Centrum Zarządzania do czasu zakończenia konfiguracji systemów końcowych pod kątem uwierzytelniania serwera.
5. Konfigurowanie systemów końcowych pod kątem uwierzytelniania serwera.

Konfigurowanie systemów końcowych pod kątem uwierzytelniania serwera

Po włączeniu protokołu SSL w systemie centralnym celem uwierzytelniania serwera, należyw tym samym celu włączyć SSL we wszystkich systemach końcowych. Aby to wykonać:

1. Rozwiń widok **Centrum Zarządzania**.
2. **Porównaj i zaktualizuj wartości systemowe 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 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 zawartość pola **System modelowy** w systemie centralnym.
h. Wybierz kategorię **Centrum Zarządzania** i ustaw następujące wartości, zaznaczając odpowiednią pozycję:
   - Pole Użyj protokołu SSL ma mieć wartość **Tak**.
   - Pole Poziom uwierzytelniania ma mieć wartość **Serwer**.

   Wartości te zostają ustawione w systemie centralnym podczas procedury konfigurowania systemu centralnego pod kątem uwierzytelniania serwera.
i. Kliknij **OK**, aby ustawić te wartości w systemach końcowych w nowej grupie systemowej.
j. Przed restartem serwera Centrum Zarządzania zaczekaj na zakończenie procesu **Porównanie i aktualizacja**. Może to zająć kilka minut.

3. **Zrestartuj serwer Centrum Zarządzania w systemie centralnym:**
   a. W programie iSeries Navigator rozwiń **Moje połączenia**.
   b. Rozwiń widok systemu centralnego.
   c. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
   d. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**. Widok systemu centralnego zostanie zwinięty i pojawi się komunikat, że nie istnieje już połączenie z serwerem.
   e. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.
4. **Zrestartuj serwery Centrum Zarządzania we wszystkich systemach końcowych:**
   a. Rozwiń restartowany system końcowy.
   b. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
   c. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
   d. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.
   e. Powtórz procedurę dla każdego systemu końcowego.
5. **Uaktywnij protokół SSL dla klienta programu iSeries Navigator:**
   a. W programie iSeries Navigator rozwiń **Moje połączenia**.
   b. Kliknij prawym przyciskiem myszy system centralny i wybierz **Właściwości**.
   c. Kliknij zakładkę **SSL** i wybierz opcję **Używaj protokołu SSL do połączeń**.
   d. Wyjdź z programu iSeries Navigator i uruchom go ponownie.

Po zakończeniu konfigurowania uwierzytelniania serwera, można przystąpić do następujących opcjonalnych procedur uwierzytelniania klienta:

- Konfigurowanie systemu centralnego pod kątem uwierzytelniania klienta
- Konfigurowanie systemów końcowych pod kątem uwierzytelniania klienta

Uwierzytelnianie klienta zapewnia sprawdzanie ośrodka certyfikacji i zaufanych grup zarówno dla systemów końcowych, jak i dla systemu centralnego.

Konfigurowanie systemu centralnego pod kątem uwierzytelniania klienta

Gdy system centralny (klient SSL) próbuje użyć protokołu SSL do połączenia się z systemem końcowym (serwer SSL), system centralny i system końcowy uwierzytelniają swoje certyfikaty korzystając z uwierzytelniania klienta (nazywanego w Centrum Zarządzania uwierzytelnianiem CA i zaufanych grup).

1. W programie iSeries Navigator kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Właściwości**.

2. Kliknij zakładkę **Ochrona** i wybierz **Użyj protokołu SSL**.
3. Wybierz **Klient i serwer** w celu wybrania poziomu uwierzytelniania.
4. Kliknij **OK**, aby ustawić tę wartość w systemie centralnym.

   Uwaga: NIE można restartować serwera Centrum Zarządzania przed zakończeniem konfigurowania systemów końcowych pod kątem korzystania z SSL z uwierzytelnianiem klienta i serwera.
5. Skonfiguruj systemy końcowe pod kątem uwierzytelniania klienta.

Konfigurowanie systemów końcowych pod kątem uwierzytelniania klienta

1. **Porównaj i zaktualizuj wartości systemowe systemów końcowych:**

   Uwaga: Zadanie nie będzie działać na serwerach iSeries z wersją V4R5. Patrz dokumentacja techniczna wersji V4R4, ″Management Central: A Smart Way to Manage AS/400 Systems

   .″
   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 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 zawartość pola **System modelowy** w systemie centralnym.
   h. Wybierz kategorię **Centrum Zarządzania** i sprawdź, czy:
      - Pole Używaj SSL ma mieć wartość **Tak**.
      - Pole Poziom uwierzytelniania ma wartość **Klient i serwer**.

      Wartości te zostają ustawione w systemie centralnym podczas procedury konfigurowania 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.
2. **Kopiowanie listy weryfikacji do systemów końcowych:**
   a. W programie iSeries Navigator rozwiń **Centrum Zarządzania—>Definicje**.
   b. Kliknij prawym przyciskiem myszy **Pakiety** i wybierz **Nowa definicja**.
   c. 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/QUSRSYS.LIB/QYPSVLDL.VLDL.
   d. Kliknij zakładkę **Opcje** i wybierz **Zastępuj istniejące zbiory przysłanymi**.
   e. Kliknij **Zaawansowane**.
   f. W oknie **Opcje zaawansowane** wybierz **Tak**, aby zezwolić na różnice w obiektach podczas odtwarzania.
   g. Kliknij **OK**, aby odświeżyć spis definicji i wyświetlić nowy pakiet.
   h. Kliknij prawym przyciskiem myszy nowy pakiet i wybierz **Wyślij**.
   i. W oknie dialogowym **Wysyłanie**: dodaj zaufaną grupę, usuń pozostałe i kliknij **OK**. Zaufana grupa to grupa systemowa zdefiniowana w punkcie 1 tej procedury.

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.

3. **Zrestartuj serwer Centrum Zarządzania w systemie centralnym:**
   a. W programie iSeries Navigator rozwiń **Moje połączenia**.
   b. Rozwiń system centralny.
   c. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
   d. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**. Widok systemu centralnego zostanie zwinięty i pojawi się komunikat, że nie istnieje już połączenie z serwerem.
   e. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.
4. **Zrestartuj serwery Centrum Zarządzania we wszystkich systemach końcowych:**

   Uwaga: Powtórz procedurę dla każdego systemu końcowego.
   a. Rozwiń restartowany system końcowy.
   b. Rozwiń **Sieć—> Serwery** i wybierz **TCP/IP**.
   c. Kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz **Zatrzymaj**.
   d. Po zatrzymaniu serwera Centrum Zarządzania kliknij **Uruchom**, aby go zrestartować.

Rozdział 4. Pojęcia dotyczące protokołu SSL

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

W lepszym zrozumieniu zależności między protokołem SSL i serwerem iSeries pomagają następujące informacje:

- Historia SSL
- Jak działa SSL
- Obsługiwane protokoły SSL i TLS (Transport Layer Security)
- Uwierzytelnianie serwera
- Uwierzytelnianie klienta

Historia SSL

Protokół SSL (Secure Sockets Layer) został opracowany przez firmę Netscape w 1994 roku jako odpowiedź na rosnące zaniepokojenie związane z bezpieczeństwem w Internecie. Wprawdzie początkowo był opracowywany z myślą o ochronie przeglądarek WWW i komunikacji z serwerami, ale jego specyfikacja umożliwiła korzystanie z SSL także innym aplikacjom, takim jak TELNET czy FTP. Więcej informacji na temat SSL i innych podobnych protokołów zawiera sekcja Obsługiwane protokoły SSL i TLS (Transport Layer Security). 

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 do uwierzytelnienia jednego lub obu punktów końcowych sesji SSL korzysta z kryptografii asymetrycznej, certyfikatów cyfrowych i przepływu uzgodnień SSL. Zazwyczaj uwierzytelniany jest serwer, opcjonalnie klient. 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 wybranych informacji identyfikujących, 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 obydwa są w stanie dowieść, że mają dostęp do tych unikalnych informacji, ustanawiane są nowe klucze symetryczne i sesja SSL zostaje wznowiona. 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 wpływ wydajności uzgadniania SSL na główny procesor można zminimalizować dzięki sprzętowi szyfrującemu.

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 nie uda się wynegocjować użycia protokołu SSL w wersji 3.0, to uzgadnianie SSL nie powiedzie się.
  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 i to się nie uda, to uzgadnianie SSL nie powiedzie się.
- 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.
- Wersja 3.0 SSL korzysta z implementacji BSAFE 3.0 firmy 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. Algorytm SHA-1 umożliwia wersji 3.0 SSL obsługę dodatkowych zestawów algorytmów szyfrowania korzystających z SHA-1 zamiast z 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

Wersja 1.0 protokołu TLS, oparta na wersji 3.0 protokołu SSL, jest najnowszym standardem przemysłowym protokołu SSL. Jej specyfikacja została zdefiniowana przez grupę wykonawczą 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. Wersja 3.0 SSL także korzystała z uwierzytelniania komunikatu zabezpieczonego kluczem, jednak metoda HMAC jest uważana za bezpieczniejszą niż funkcja MAC (Message Authentication Code), używana przez wersję 3.0 SSL.
- **Rozszerzony pseudolosowy generator funkcji (PRF)**
  Generator PRF jest używany do generowania danych klucza. W protokole TLS PRF jest definiowany metodą HMAC. Generator PRF korzysta z dwóch algorytmów mieszających, które gwarantują jego ochronę. Jeśli jeden z algorytmów zostanie ujawniony, dane nadal pozostaną bezpieczne, dopóki nie zostanie ujawniony drugi algorytm.
- **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 rodzaj certyfikatu, który musi zostać wymieniony pomiędzy implementacjami 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. Po zakończeniu uzgadniania SSL, gdy jeden lub oba punkty końcowe zostaną uwierzytelnione, a unikalny klucz do szyfrowania i deszyfrowania wygenerowany, 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 (oryginalny),
- serwer HTTP IBM (oparty na Apache),
- serwer FTP,
- serwer Telnet,
- system końcowy Centrum Zarządzania,
- usługi katalogowe (LDAP).

Rozdział 5. 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)
- Aby korzystać z serwera HTTP do programu DCM, należy zainstalować program IBM Developer Kit for Java (5722–JV1), w przeciwnym razie serwer HTTP admin nie uruchomi się.
- 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. Dla serwera iSeries w wersji V5R2M0 dostępne są nasępujące opcje sprzętu szyfrującego:
  - 2058 Cryptographic Accelerator (opcja sprzętowa o kodzie 4805),
  - 4758 Cryptographic Coprocessor (opcja sprzętowa o kodzie 4801 lub 4802).

  Aby zainstalować sprzęt szyfrujący, należy zainstalować także opcję 35, Cryptographic Service Provider.

Aby korzystać z protokołu SSL z dowolnego elementu programu iSeries Access for Windows lub IBM Toolbox for Java, konieczne jest zainstalowanie produktu iSeries Client Encryption, 5722-CE3 (128-bitowy). Program iSeries Access for Windows potrzebuje go do nawiązania bezpiecznego połączenia.

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.

Rozdział 6. Aplikacje chronione przy użyciu protokołu SSL

Protokołem SSL można chronić następujące aplikacje serwera iSeries:
- IBM HTTP Server for iSeries (oryginalny),
- IBM HTTP Server for iSeries (oparty na Apache),
- serwer FTP,
- serwer Telnet,
- Distributed Relational Database Architecture (DRDA) i serwer Distributed Data Management (DDM),
- Centrum Zarządzania,
- serwer LDAP,
- Enterprise Identity Mapping (EIM),
- aplikacje iSeries Access for Windows włącznie z iSeries Navigator,
- aplikacje korzystające z zestawu interfejsów API programu iSeries Access for Windows,
- programy tworzone za pomocą produktu Developer Kit for Java i aplikacje klienckie korzystające z produktu IBM Toolbox for Java,
- 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.

Rozdział 7. 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 zostały spełnione powyższe warunki, a na serwerze iSeries nadal występują problemy związane z protokołem SSL, wypróbuj następujące opcje:

- Kod błędu SSL w protokole zadań serwera można odnieść do tabeli błędów, aby znaleźć więcej informacji o błędzie. Strona Komunikaty dla kodów błędu funkcji API SSL zawiera informacje o komunikatach dla kodów błędów SSL. Na przykład w tabeli tej błąd -93, który może wystąpić w protokole zadań serwera, jest odwzorowany na stałą 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 korzystają z tych funkcji API i wykorzystują ten opis do wpisania komunikatu do protokołu zadań.

  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.SSL

  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 związanych z serwerem iSeries zawiera strona Rozwiązywanie problemów i obsługa serwisowa.

Rozdział 8. 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 Java Secure Socket Layer (JSSL) zawiera krótki opis pakietu JSSL 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.