System i

Bezpieczeństwo
Protokół Secure Sockets Layer

Wersja 6 wydanie 1

System i

Bezpieczeństwo
Protokół Secure Sockets Layer

Wersja 6 wydanie 1

Uwaga

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 21.

To wydanie dotyczy wersji 6, wydania 1, modyfikacji 0 systemu operacyjnego i5/OS (5761–SS1) oraz wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie określono inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

Spis treści

Protokół Secure Sockets Layer

W tej publikacji opisano wykorzystanie na serwerach protokołu Secure Sockets Layer (SSL).

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

Co nowego w wersji V6R1

Poniżej opisano nowe i zmienione informacje w kolekcji tematów dotyczącej protokołu Secure Sockets Layer (SSL).

Nowe informacje o Systemie SSL

System SSL to zestaw ogólnych usług udostępnionych w Licencjonowanym Kodzie Wewnętrznym systemu i5/OS, które zabezpieczają połączenia TCP/IP przy użyciu protokołów SSL i TLS. System SSL jest ściśle powiązany z systemem operacyjnym oraz kodem gniazd, aby zwiększyć wydajność i poziom bezpieczeństwa.

Opis Systemu SSL został poszerzony o następujące tematy:

- "System SSL" na stronie 15
- "Właściwości Systemu SSL" na stronie 15

Nowe wartości systemowe w Systemie SSL

Zostały dodane następujące wartości systemowe:

- Wartość systemowa SSL: QSSLPCL
- Wartość systemowa SSL: QSSLCSLCTL
- Wartość systemowa SSL: QSSLCSL

Znajdowanie nowych lub zmienionych informacji

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

- symbol » służący do zaznaczania początku nowego lub zmienionego fragmentu;
- symbol « służący do zaznaczania końca nowego lub zmienionego fragmentu.

Nowe i zmienione informacje w plikach PDF mogą być oznaczone symbolem | na lewym marginesie.

Więcej informacji na temat zmian i nowości w bieżącej wersji zawiera Wiadomość dla użytkowników.

Plik PDF z informacjami na temat protokołu SSL

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

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

Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.

4. Kliknij opcję **Zapisz**.

Pobieranie programu Adobe Reader

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

Scenariusze: protokół SSL

Scenariusze dotyczące protokołu SSL mają za zadanie pomóc użytkownikom osiągnąć jak największe korzyści z włączenia protokołu SSL na platformie System i.

Scenariusze dotyczące protokołu SSL zawierają praktyczne przykłady zastosowania tego protokołu i pozwalają lepiej zrozumieć jego działanie w systemie i5/OS.

Informacje pokrewne

Scenariusz: zabezpieczanie aplikacji Telnet za pomocą protokołu SSL

Scenariusz: wykorzystanie sprzętu szyfrującego do zabezpieczania prywatnych kluczy

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

W scenariuszu opisano zabezpieczanie za pomocą protokołu SSL połączenia klienta zdalnego z serwerem System i działającym jako system centralny. Opisywane czynności wykonywane są przy użyciu serwera Centrum Zarządzania System i Navigator.

Sytuacja

Firma dysponuje siecią LAN, w której znajduje się kilka systemów i5/OS. Administrator systemu w tej firmie, Robert, wyznaczył jeden z systemów i5/OS na system centralny (System A) w sieci lokalnej. Robert używa serwera Centrum Zarządzania w Systemie A do zarządzania wszystkimi pozostałymi systemami końcowymi w tej sieci LAN.

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

Cele

Robert chce zabezpieczyć połączenie między swoim komputerem PC i serwerem Centrum Zarządzania. Robert nie wymaga dodatkowego zabezpieczenia połączenia między serwerem Centrum Zarządzania w Systemie A i systemami końcowymi w sieci LAN. Pozostali pracownicy biura nie potrzebują dodatkowego zabezpieczenia połączeń z serwerem Centrum Zarządzania. Robert planuje skonfigurować swój komputer PC i serwer Centrum Zarządzania w Systemie A tak, aby połączenie używało uwierzytelniania serwera. Połączenia z serwerem Centrum Zarządzania z komputerów PC lub systemów i5/OS w sieci lokalnej nie są zabezpieczone 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 zabezpieczonego za pomocą protokołu SSL

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

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

Wymagania wstępne i założenia

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

1. Sprawdzić, czy System A spełnia wymagania wstępne dla protokołu SSL.
2. Sprawdzić, czy na Systemie A działa system operacyjny i5/OS w wersji V5R3 lub nowszej.
3. Sprawdzić, czy na klienckim komputerze PC działa program System i Navigator, będący częścią oprogramowania System i Access for Windows w wersji V5R3 lub nowszej.
4. Uzyskać ośrodek certyfikacji dla systemów i5/OS.
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 do certyfikatu identyfikator serwera Centrum Zarządzania i identyfikatory aplikacji wszystkich systemów i5/OS. Systemami i5/OS są: serwer centralny TCP, serwer bazy danych, serwer kolejek danych, serwer plików, sieciowy serwer wydruków, serwer komend zdalnych i serwer wpisywania się do systemu.
   a. W Systemie A uruchom program IBM Digital Certificate Manager. Robert uzyskuje lub tworzy certyfikaty albo konfiguruje lub zmienia system certyfikacji.
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz hasło bazy certyfikatów *SYSTEM i kliknij przycisk **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.
   e. Kliknij **Aktualizacja przypisania certyfikatów**.
   f. Wybierz **Serwer** i kliknij **Kontynuuj**.
   g. Wybierz pozycję **Serwer Centrum Zarządzania** i kliknij przycisk **Aktualizacja przypisania certyfikatów**. Powoduje to przypisanie certyfikatu do serwera Centrum Zarządzania.
   h. Kliknij **Przypisanie nowego certyfikatu**. Program DCM zostanie przeładowany do strony Aktualizacja przypisania certyfikatów z komunikatem potwierdzającym.
   i. Kliknij **Gotowe**.
   j. Przypisz certyfikat do wszystkich serwerów dostępu klienta.
8. Pobrać ośrodek certyfikacji (CA) do klienta PC.

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

Etapy konfiguracji

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

1. “Czynność 1: dezaktywowanie protokołu SSL dla klienta System i Navigator”
2. “Czynność 2: ustawianie poziomu uwierzytelniania dla serwera Centrum Zarządzania”
3. “Czynność 3: restartowanie systemu Centrum Zarządzania w systemie centralnym” na stronie 5
4. “Czynność 4: aktywowanie protokołu SSL dla klienta System i Navigator” na stronie 5
5. “Punkt opcjonalny: dezaktywowanie protokołu SSL dla klienta System i Navigator” na stronie 5

Pojęcia pokrewne

“Wymagania wstępne dotyczące protokołu SSL” na stronie 18
Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

Informacje pokrewne

Konfigurowanie programu DCM

Uruchamianie programu Digital Certificate Manager

Szczegóły konfiguracji: zabezpieczanie połączenia klienta z systemem Centrum Zarządzania za pomocą protokołu SSL

W tym temacie szczegółowo przedstawiono etapy zabezpieczania połączeń klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

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

W tym scenariuszu serwer System i jest wyznaczony jako system centralny w sieci lokalnej firmy. Robert używa serwera Centrum Zarządzania w systemie centralnym (nazywanym tutaj Systemem A) do zarządzania systemami końcowymi w firmowej sieci. Poniższe informacje wyjaśniają sposób wykonywania czynności wymaganych do zabezpieczenia połączenia klienta zewnętrznego z serwerem Centrum Zarządzania. Należy śledzić sposób wykonywania przez Roberta czynności konfiguracyjnych w tym scenariuszu.

Pojęcia pokrewne

“Wymagania wstępne dotyczące protokołu SSL” na stronie 18
Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

“Scenariusz: zabezpieczanie wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL” na stronie 5
W scenariuszu opisano zabezpieczanie za pomocą protokołu SSL wszystkich połączeń z serwerem System i działającym jako system centralny. Opisywane czynności wykonywane są przy użyciu systemu Centrum Zarządzania System i Navigator.

Informacje pokrewne

Pierwsze konfigurowanie certyfikatów

Czynność 1: dezaktywowanie protokołu SSL dla klienta System i Navigator:
Ten etap jest konieczny tylko wtedy, gdy protokół SSL dla klienta System i Navigator został wcześniej aktywowany.

1. W programie System i Navigator rozwiń węzeł **Moje połączenia**.
2. Prawym przyciskiem myszy kliknij System A i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i usuń zaznaczenie z pola wyboru **Podczas połączenia używaj protokołu SSL**.
4. Wyjdź z programu System i Navigator i zrestartuj go.

Na elemencie Centrum Zarządzania w programie System i Navigator przestanie być wyświetlana kłódka, co oznacza połączenie niezabezpieczone. Informuje to Roberta o tym, że nie ma już zabezpieczonego przez SSL połączenia między klientem i systemem centralnym w swojej firmie.

Czynność 2: ustawianie poziomu uwierzytelniania dla serwera Centrum Zarządzania:

1. W programie System i Navigator kliknij prawym przyciskiem myszy **Centrum Zarządzania** i wybierz opcję **Właściwości**.
2. Kliknij zakładkę **Ochrona**, a następnie zaznacz opcję **Używaj protokołu SSL**.
3. Wybierz opcję **Dowolny** jako poziom uwierzytelniania (opcja dostępna w programie System i Access for Windows).
4. Kliknij **OK**, aby ustawić tę wartość w systemie centralnym.

Czynność 3: restartowanie systemu Centrum Zarządzania w systemie centralnym:

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

Czynność 4: aktywowanie protokołu SSL dla klienta System i Navigator:

1. W programie System i Navigator rozwiń węzeł **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. Wyjdź z programu System i Navigator i zrestartuj go.

W programie System i Navigator obok serwera Centrum Zarządzania zostanie wyświetlona kłódka, która oznacza połączenie zabezpieczone przez protokół SSL. Informuje ona Roberta o tym, że połączenie między jego klientem i systemem centralnym w jego firmie jest zabezpieczone przez protokół SSL.

Uwaga: Ta procedura zabezpiecza tylko połączenie między jednym komputerem PC i systemem Centrum Zarządzania. Pozostałe połączenia klientów z serwerem Centrum Zarządzania, jak również połączenia systemów końcowych z serwerem Centrum Zarządzania nie będą zabezpieczone. Aby chronić inne klienty, należy sprawdzić, czy spełniają one wymagania wstępne i powtórzyć “Czynność 4: aktywowanie protokołu SSL dla klienta System i Navigator”. Informacje o zabezpieczaniu innych połączeń z serwerem Centrum Zarządzania zawiera temat Scenariusz: zabezpieczanie wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL.

Punkt opcjonalny: dezaktywowanie protokołu SSL dla klienta System i Navigator:
Jeśli Robert chce pracować w biurze firmy i nie chce używać połączenia zabezpieczonego za pomocą protokołu SSL wpływającego na wydajność komputera PC, może je w prosty sposób dezaktywować, wykonując następujące czynności:

1. W programie System i Navigator rozwiń węzeł **Moje połączenia**.
2. Prawym przyciskiem myszy kliknij System A i wybierz **Właściwości**.
3. Kliknij zakładkę **Protokół SSL** i usuń zaznaczenie z pola wyboru **Podczas połączenia używaj protokołu SSL**.
4. Wyjdź z programu System i Navigator i zrestartuj go.

Scenariusz: zabezpieczanie wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL

W scenariuszu opisano zabezpieczanie za pomocą protokołu SSL wszystkich połączeń z serwerem System i działającym jako system centralny. Opisywane czynności wykonywane są przy użyciu systemu Centrum Zarządzania System i Navigator.

Sytuacja

W firmie skonfigurowano sieć WAN zawierającą kilka serwerów System i w miejscach zdalnych (systemy końcowe). Systemy końcowe są zarządzane przez jeden system centralny znajdujący się w głównym biurze. Tomek jest specjalistą do spraw bezpieczeństwa w firmie. Chce używać protokołu SSL (Secure Sockets Layer) do zabezpieczania wszystkich

połączeń między serwerem Centrum Zarządzania zainstalowanym w systemie centralnym firmy a wszystkimi systemami i klientami i5/OS.

Szczegóły

Tomek może **bezpiecznie**, za pomocą protokołu SSL, zarządzać wszystkimi połączeniami z serwerem Centrum Zarządzania. Aby używać protokołu SSL na serwerze Centrum Zarządzania, Tomek musi zabezpieczyć program System i Navigator na komputerze PC używanym do uzyskiwania dostępu do systemu centralnego.

Może wybrać jeden z dwóch poziomów uwierzytelniania serwera Centrum Zarządzania:

Uwierzytelnianie serwera
Uwierzytelnianie certyfikatu serwera. Klient musi sprawdzić poprawność serwera bez względu na to, czy tym klientem jest program System i Navigator na komputerze PC, czy serwer Centrum Zarządzania w systemie centralnym. Gdy program System i Navigator nawiązuje połączenie z systemem centralnym, komputer PC jest klientem SSL, a Centrum Zarządzania uruchomione na systemie centralnym jest serwerem SSL. System centralny podczas łączenia się z systemem końcowym działa jako klient SSL. System końcowy działa jako serwer SSL. Serwer musi udowodnić swoją tożsamość klientowi, dostarczając certyfikat wydany przez ośrodek certyfikacji, któremu ufa klient. Każdy serwer SSL musi mieć poprawny certyfikat wydany przez zaufany ośrodek certyfikacji (CA).

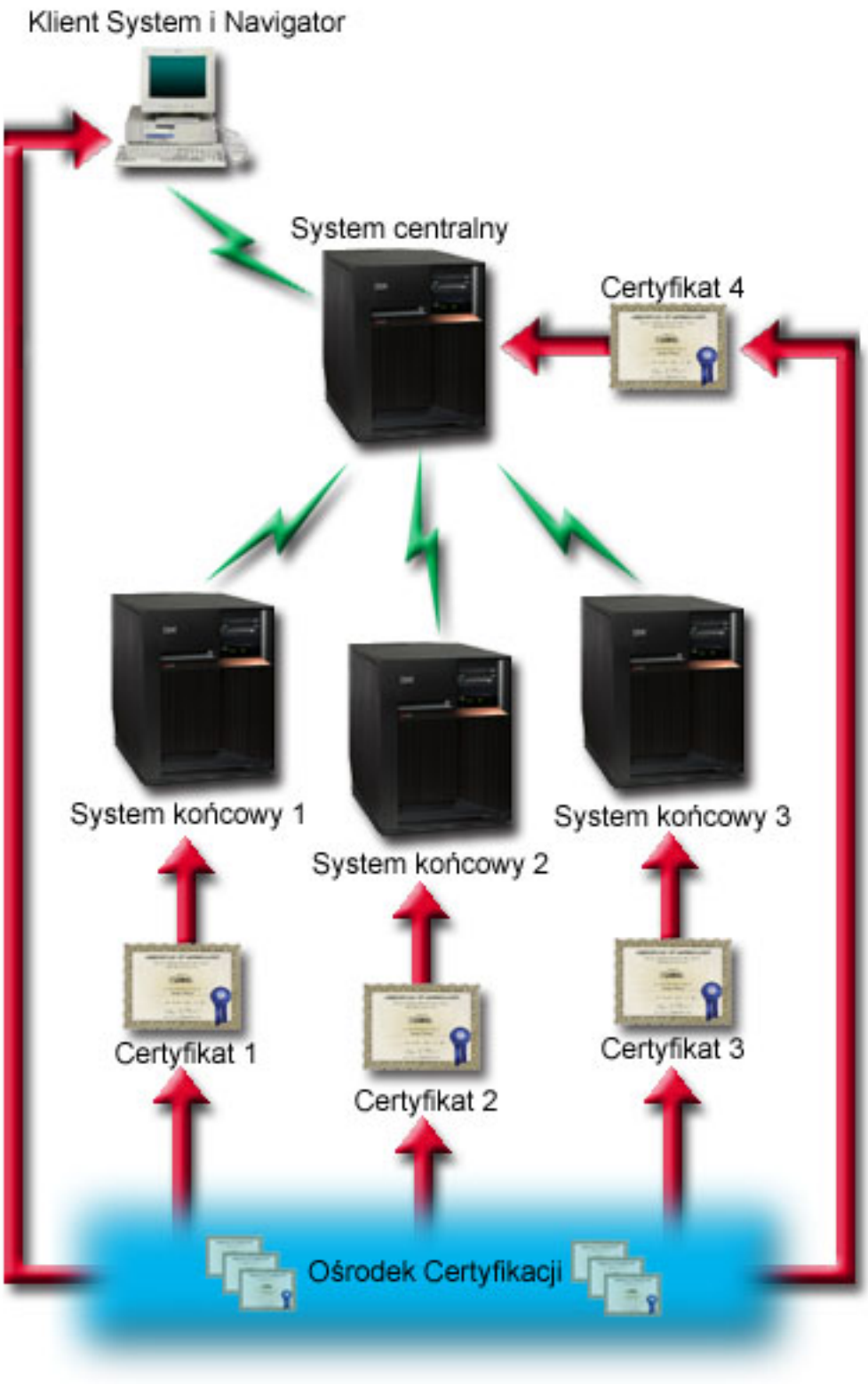
Uwierzytelnianie klienta i serwera
Uwierzytelnianie certyfikatów systemu centralnego i końcowego. Jest to wyższy poziom zabezpieczeń niż poziom uwierzytelniania serwera. W innych aplikacjach nazywane jest ono uwierzytelnianiem klienta, ponieważ klient musi dostarczyć poprawny zaufany certyfikat. Gdy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

Uwaga: Uwierzytelnianie klienta i serwera jest wykonywane tylko między dwoma serwerami System i. Serwer nie wykonuje uwierzytelniania klienta, gdy klientem jest komputer PC.

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

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

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



Wymagania wstępne i założenia

Tomek musi wykonać następujące zadania administrowania i konfiguracji, aby zabezpieczyć wszystkie połączenia z serwerem Centrum Zarządzania:

1. Sprawdzić, czy System A spełnia wymagania wstępne dla protokołu SSL.
2. Sprawdzić, czy na systemie centralnym i wszystkich systemach końcowych działa system operacyjny OS/400 w wersji V5R2 lub system operacyjny i5/OS w wersji V5R3 lub nowszej.

   Uwaga: System operacyjny i5/OS w wersji V5R4 oraz połączenia z systemem OS/400 V5R1 nie są dozwolone.
3. Sprawdzić, czy na klienckim komputerze PC działa program System i Navigator, będący częścią oprogramowania System i Access for Windows w wersji V5R3 lub nowszej.
4. Uzyskać ośrodek certyfikacji dla serwerów System i.
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 certyfikatom identyfikatory aplikacji Centrum Zarządzania i identyfikatory aplikacji wszystkich systemów i5/OS. Systemami i5/OS są: serwer centralny TCP, serwer bazy danych, serwer kolejek danych, serwer plików, sieciowy serwer wydruków, serwer komend zdalnych i serwer wpisywania się do systemu.
   a. Na serwerze Centrum Zarządzania uruchom program IBM Digital Certificate Manager. Jeśli chcesz uzyskać lub utworzyć certyfikaty, zmienić lub skonfigurować system certyfikatów, zrób to w tym momencie.
   b. Kliknij **Wybór ośrodka certyfikacji**.
   c. Wybierz ***SYSTEM** i kliknij **Kontynuuj**.
   d. Wpisz hasło bazy certyfikatów *SYSTEM i kliknij przycisk **Kontynuuj**. Po przeładowaniu menu rozwiń **Zarządzanie aplikacjami**.
   e. Kliknij **Aktualizacja przypisania certyfikatów**.
   f. Wybierz **Serwer** i kliknij **Kontynuuj**.
   g. Wybierz pozycję Serwer Centrum Zarządzania i kliknij przycisk **Aktualizacja przypisania certyfikatów**. Spowoduje to przypisanie certyfikatu do systemu Centrum Zarządzania.
   h. Wybierz certyfikat, który ma być przypisany do aplikacji i kliknij polecenie **Przypisz nowy certyfikat**. Program DCM zostanie przeładowany do strony **Aktualizacja przypisania certyfikatów** z komunikatem potwierdzającym.
   i. Kliknij przycisk **Anuluj**, aby powrócić do listy aplikacji.
   j. Powtórz tę procedurę dla wszystkich serwerów z systemem operacyjnym i5/OS.
8. Pobierz ośrodek CA na kliencki komputer PC z programem System i Navigator.

Etapy konfiguracji

Zanim Tomek będzie mógł włączyć protokół SSL na serwerze Centrum Zarządzania, musi zainstalować wymagane wstępnie programy oraz skonfigurować certyfikaty cyfrowe w systemie centralnym. Przed kontynuowaniem zapoznaj się z wymaganiami wstępnymi i założeniami dla tego scenariusza. Po spełnieniu wymagań wstępnych może wykonać poniższe procedury, aby zabezpieczyć wszystkie połączenia z serwerem Centrum Zarządzania:

Uwaga: Jeśli protokół SSL włączono w programie System i Navigator, Tomek musi go wyłączyć przed włączeniem protokołu SSL na serwerze Centrum Zarządzania. Jeśli protokół SSL włączono w programie System i Navigator, a nie włączono na serwerze Centrum Zarządzania, próby nawiązania połączenia programu System i Navigator z systemem centralnym zakończą się niepowodzeniem.

1. “Czynność 1: konfigurowanie systemu centralnego pod kątem uwierzytelniania serwera” na stronie 10
2. “Czynność 2: konfigurowanie systemów końcowych pod kątem uwierzytelniania serwera” na stronie 10
3. “Czynność 3: restartowanie systemu Centrum Zarządzania w systemie centralnym” na stronie 10
4. “Czynność 4: restartowanie systemu Centrum Zarządzania we wszystkich systemach końcowych” na stronie 11
5. “Czynność 5: aktywowanie protokołu SSL dla klienta System i Navigator” na stronie 11
6. “Czynność 6: konfigurowanie systemu centralnego pod kątem uwierzytelniania klientów” na stronie 11
7. “Czynność 7: konfigurowanie systemów końcowych pod kątem uwierzytelniania klientów” na stronie 11
8. “Czynność 8: kopiowanie listy sprawdzania do systemów końcowych” na stronie 12

9. “Czynność 9: restartowanie systemu Centrum Zarządzania w systemie centralnym” na stronie 12
10. “Czynność 10: restartowanie systemu Centrum Zarządzania we wszystkich systemach końcowych” na stronie 13

Pojęcia pokrewne

“Wymagania wstępne dotyczące protokołu SSL” na stronie 18
Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

“Zabezpieczanie aplikacji za pomocą protokołu SSL” na stronie 19
Ten temat zawiera listę aplikacji, które można zabezpieczyć za pomocą protokołu SSL na platformie System i.

Zadania pokrewne

“Szczegóły konfiguracji: zabezpieczanie połączenia klienta z systemem Centrum Zarządzania za pomocą protokołu SSL” na stronie 4
W tym temacie szczegółowo przedstawiono etapy zabezpieczania połączeń klienta z serwerem Centrum Zarządzania za pomocą protokołu SSL.

“Szczegóły konfiguracji: zabezpieczanie wszystkich połączeń z systemem Centrum Zarządzania za pomocą protokołu SSL”
W temacie przedstawiono szczegóły używania protokołu SSL do zabezpieczania wszystkich połączeń z serwerem Centrum Zarządzania.

Informacje pokrewne

Konfigurowanie programu DCM

Pierwsze konfigurowanie certyfikatów

Szczegóły konfiguracji: zabezpieczanie wszystkich połączeń z systemem Centrum Zarządzania za pomocą protokołu SSL

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

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

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

Zanim Tomek będzie mógł aktywować protokół SSL w systemie Centrum Zarządzania, musi zainstalować wymagane programy oraz skonfigurować certyfikaty cyfrowe na serwerze System i. Po spełnieniu wymagań wstępnych może wykonać poniższe procedury, aby zabezpieczyć wszystkie połączenia z serwerem Centrum Zarządzania.

Uwaga: Jeśli protokół SSL włączono w programie System i Navigator, Tomek musi go wyłączyć przed włączeniem protokołu SSL na serwerze Centrum Zarządzania. Jeśli protokół SSL włączono w programie System i Navigator, a nie włączono na serwerze Centrum Zarządzania, próby nawiązania połączenia między programem System i Navigator a systemem centralnym zakończą się niepowodzeniem.

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

Pojęcia pokrewne

“Wymagania wstępne dotyczące protokołu SSL” na stronie 18
Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

“Scenariusz: zabezpieczanie wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL” na stronie 5

W scenariuszu opisano zabezpieczanie za pomocą protokołu SSL wszystkich połączeń z serwerem System i działającym jako system centralny. Opisywane czynności wykonywane są przy użyciu systemu Centrum Zarządzania System i Navigator.

Informacje pokrewne

Pierwsze konfigurowanie certyfikatów

Czynność 1: konfigurowanie systemu centralnego pod kątem uwierzytelniania serwera:

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

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

Czynność 2: konfigurowanie systemów końcowych pod kątem uwierzytelniania serwera:
Po skonfigurowaniu systemu centralnego pod kątem uwierzytelniania serwera Tomek musi skonfigurować w tym celu również systemy końcowe. Należy wykonać następujące zadania:

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

      Uwaga: Jeśli te wartości nie są ustawione, wykonaj Czynność 1: konfigurowanie systemu centralnego pod kątem uwierzytelniania serwera .
   k. Kliknij przycisk **OK**. Zanim przejdziesz do kolejnego etapu, poczekaj na zakończenie przetwarzania polecenia **Porównaj i zaktualizuj**.

Czynność 3: restartowanie systemu Centrum Zarządzania w systemie centralnym:

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

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

Czynność 4: restartowanie systemu Centrum Zarządzania we wszystkich systemach końcowych:

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

Czynność 5: aktywowanie protokołu SSL dla klienta System i Navigator:

1. W programie System i Navigator rozwiń węzeł **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. Wyjdź z programu System i Navigator i zrestartuj go.

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

Czynność 6: konfigurowanie systemu centralnego pod kątem uwierzytelniania klientów:

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

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

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

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

Czynność 7: konfigurowanie systemów końcowych pod kątem uwierzytelniania klientów:
Porównaj i zaktualizuj wartości systemowe dla systemów końcowych:

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

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

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

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

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

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

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

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

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

Czynność 8: kopiowanie listy sprawdzania do systemów końcowych:

| Opisywana procedura zakłada, że na systemie centralnym działa system operacyjny i5/OS w wersji V5R3 lub nowszej.
| W systemie i5/OS w wersji V5R2 lub starszej obiekt QYPSVLDL.VLDL był umieszczony w bibliotece
| QUSRSYS.LIB, a nie QMGTC2.LIB. Dlatego w wersjach systemu starszych niż V5R3 konieczne będzie wysłanie listy
| sprawdzania do tych systemów i umieszczenie jej w bibliotece QUSRSYS.LIB, zamiast w bibliotece QMGTC2.LIB.
| Jeśli korzystasz z systemu w wersji V5R3 lub nowszej, przejdź do wykonywania następujących czynności:

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

   Uwaga: Zadanie **Wyślij** nigdy nie powiedzie się w systemie centralnym, gdyż jest on zawsze systemem źródłowym. Zadanie **Wyślij** powinno zakończyć się pomyślnie we wszystkich systemach końcowych.

| 10. Jeśli w **Zaufanej grupie** znajdują się jakiekolwiek serwery, na których działa system operacyjny i5/OS w wersji
| V5R3 lub starszej, należy na nich ręcznie przenieść obiekt QYPSVLDL.VLDL z biblioteki QMGTC2.LIB do
| biblioteki QUSRSYS.LIB. Jeśli w bibliotece QUSRSYS.LIB znajduje się już jedna wersja obiektu
| QYPSVLDL.VLDL, usuń ją i zastąp nowszą wersją z biblioteki QMGTC2.LIB

Czynność 9: restartowanie systemu Centrum Zarządzania w systemie centralnym:

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

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

Czynność 10: restartowanie systemu Centrum Zarządzania we wszystkich systemach końcowych:

Uwaga: Powtórz procedurę dla każdego systemu końcowego.

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

Pojęcia związane z protokołem SSL

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

Dzięki protokołowi SSL można nawiązywać bezpieczne 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.

Jak działa SSL

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

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

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

Uzgadnianie SSL, ze względu na operacje szyfrujące z użyciem kluczy publicznych i prywatnych, jest działaniem wymagającym dużej wydajności. Po nawiązaniu pomiędzy dwoma punktami końcowymi początkowej sesji SSL, informacje o sesji SSL przeznaczone dla nich i dla aplikacji mogą być przechowywane w pamięci chronionej, dzięki czemu kolejne aktywacje sesji SSL będą szybsze. Punkty końcowe korzystają ze skróconego przepływu uzgodnień do uwierzytelnienia, że każdy z nich ma dostęp do unikalnych danych bez korzystania z kluczy publicznych lub prywatnych, gdy sesja SSL jest wznawiana. Jeśli oba mogą udowodnić, że mają dostęp do tych unikalnych informacji, ustanawiane są nowe klucze symetryczne i wznawiana jest sesja SSL. W sesjach wersji 1.0 protokołu TLS i 3.0 protokołu SSL informacje nie są buforowane w pamięci chronionej dłużej niż 24 godziny. W wersji V5R2 systemu OS/400 i kolejnych wydaniach lub w systemie i5/OS można zminimalizować wpływ wydajności uzgadniania SSL na procesor główny poprzez używanie sprzętu szyfrującego.

Informacje pokrewne

Koncepcje dotyczące certyfikatów cyfrowych

Sprzęt szyfrujący

Obsługiwane wersje protokołów SSL i TLS

Ten temat zawiera informacje o wersjach protokołów Secure Sockets Layer (SSL) i Transport Layer Security (TLS) obsługiwanych przez ich implementację w systemie i5/OS.

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

- protokół TLS w wersji 1.0
- protokół TLS w wersji 1.0 w trybie zgodności z protokołem SSL w wersji 3.0

  Uwaga:

  1. Określenie protokół TLS w wersji 1.0 w trybie zgodności 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. Platforma System i obsługuje również protokół TLS w wersji 1.0 w trybie zgodności z protokołem SSL w wersji 2.0 i 3.0. 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 2.0 jest w konfiguracji fabrycznej wyłączony, ale można go włączyć ponownie, zmieniając wartość systemową QSSLPCL. Za pomocą wartości systemowej QSSLPCL można wyłączać i włączać wszystkie spośród opisanych protokołów.
- protokół SSL w wersji 3.0
- protokół SSL w wersji 2.0
- protokół SSL w wersji 3.0 w trybie zgodności z protokołem SSL w wersji 2.0

Protokół SSL wersja 3.0 a protokół SSL wersja 2.0

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

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

Protokół TLS wersja 1.0 a protokół SSL wersja 3.0

Najnowszym standardem przemysłowym protokołu SSL opartym na SSL w wersji 3.0 jest protokół TLS (Transport Layer Security) w wersji 1.0. Jego specyfikacje są zdefiniowane w dokumencie RFC 2246 grupy wykonawczej IETF - *The TLS Protocol*.

Głównym celem protokołu TLS jest uczynienie protokołu SSL bezpieczniejszym, 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″.

Wszystkie aplikacje na platformie System i, które mogą korzystać z protokołu SSL, będą automatycznie obsługiwać protokół TLS, chyba że dana aplikacja wymusi wprost używanie tylko protokołu SSL w wersji 2.0 lub 3.0.

TLS zapewnia następujące sposoby zwiększenia bezpieczeństwa:

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

Informacje pokrewne

Protokół TLS

System SSL

System SSL to zestaw ogólnych usług udostępnionych w Licencjonowanym Kodzie Wewnętrznym systemu i5/OS, które zabezpieczają połączenia TCP/IP przy użyciu protokołów SSL i TLS. System SSL jest ściśle powiązany z systemem operacyjnym oraz kodem gniazd, aby zwiększyć wydajność i poziom bezpieczeństwa.

System SSL jest dostępny dla programistów aplikacji poprzez następujące interfejsy programistyczne i implementacje JSSE:

- Interfejsy API Global Secure Toolkit (GSKit)
  - Te interfejsy API języka ILE C są dostępne przy użyciu innych języków środowiska ILE.
- Zintegrowane z systemem i5/OS interfejsy API SSL_
  - Te interfejsy API języka ILE C są dostępne przy użyciu innych języków środowiska ILE.
  - Używanie tego zestawu funkcji API nie jest zalecane. Zalecany interfejs w języku C to GSKit.
- Implementacja JSSE zintegrowana z systemem i5/OS
  - Domyślna implementacja JSSE dla oprogramowania JDK 1.4.
  - Dostępna jest implementacja JSSE systemu i5/OS dla oprogramowania JDK 1.5 i JDK 1.6, ale nie jest to implementacja domyślna.

Aplikacje korzystające z protokołu SSL utworzone przez firmę IBM, partnerów handlowych IBM, niezależnych producentów oprogramowania lub klientów, które korzystają z jednego z powyższych interfejsów Systemu SSL, będą wykorzystywać System SSL. Na przykład FTP i Telnet są aplikacjami firmy IBM, które wykorzystują System SSL. Nie wszystkie aplikacje na platformie System i, które mogą korzystać z protokołu SSL, wykorzystują System SSL.

Właściwości Systemu SSL

Właściwości Systemu SSL określają obsługiwane funkcje protokołu SSL oraz funkcje używane domyślnie, kiedy wymagane jest domyślne działanie.

Każda aplikacja określa, czy funkcjonalność domyślna powinna zostać użyta czy też przesłonięta przez ustawienia zakodowane w aplikacji. W wielu aplikacjach używane są wartości domyślne Systemu SSL, aby umożliwić korzystanie z jego nowych możliwości bez wprowadzania zmian w kodzie.

W systemie i5/OS w wersji V6R1 lub nowszej System SSL udostępnia administratorom systemu mechanizm pozwalający decydować o tym, które dokładnie protokoły SSL i zestawy algorytmów szyfrowania są obsługiwane w systemie. Z Systemem SSL związane są dwa podstawowe pojęcia, które należy zrozumieć przed rozpoczęciem pracy. Pierwszym pojęciem są wartości obsługiwane. Wartości obsługiwane to wszystkie wartości, które System SSL może obsłużyć. Fabrycznie w systemie jest włączony tylko podzbiór jego wszystkich możliwości. Drugim pojęciem są wartości domyślne. Wartości domyślne muszą być podzbiorem wartości obsługiwanych. Wartości domyślne są stosowane, gdy aplikacja żąda obsługi domyślnej. Aby chronić aplikacje IBM korzystające z wartości domyślnych Systemu SSL przed wymuszeniem przejścia na niższy poziom zabezpieczeń, kontrola administratora nad wartościami domyślnymi została ograniczona. Do obsługi domyślnej nie można dodawać żadnych funkcji wykraczających poza fabryczne wartości domyślne systemu. Administrator może w większym stopniu ograniczyć funkcje obsługiwane domyślnie, całkowicie wyłączając obsługę danej funkcji.

Protokoły SSL

System SSL obsługuje następujące protokoły:

- Protokół Secure Sockets Layer w wersji 2.0 (SSLv2)
- Protokół Secure Sockets Layer w wersji 3.0 (SSLv3)
- Protokół Transport Layer Security w wersji 1.0 (TLSv1)

Protokoły SSL obsługiwane w konfiguracji fabrycznej

W konfiguracji fabrycznej System SSL obsługuje następujące protokoły:

- Protokół Secure Sockets Layer w wersji 3.0 (SSLv3)
- Protokół Transport Layer Security w wersji 1.0 (TLSv1)

Uwaga: Protokół Secure Sockets Layer w wersji 2.0 (SSLv2) jest fabrycznie wyłączony w Systemie SSL. Można go włączyć, zmieniając wartość systemową QSSLPCL. Za pomocą wartości systemowej QSSLPCL można wyłączać i włączać wszystkie spośród opisanych protokołów.

Domyślne protokoły SSL w konfiguracji fabrycznej

Na żądanie aplikacji System SSL używa domyślnie następujących protokołów:

- Protokół Secure Sockets Layer w wersji 3.0 (SSLv3)
- Protokół Transport Layer Security w wersji 1.0 (TLSv1)

Uwaga: Jeśli administrator dodał protokół SSLv2 do listy obsługiwanych protokołów, nie jest on dodawany listy protokołów domyślnych. Usunięcie domyślnego protokołu z listy obsługiwanych protokołów spowoduje usunięcie go także z listy domyślnych protokołów.

Zestawy algorytmów szyfrowania SSL

System SSL obsługuje 13 zestawów algorytmów szyfrowania. Zestawy algorytmów szyfrowania są określane w różny sposób w poszczególnych interfejsach programistycznych. Konwencja nazewnictwa wartości systemowych jest przedstawiona poniżej.

System SSL obsługuje następujące zestawy algorytmów szyfrowania:

- *RSA_NULL_MD5
- *RSA_NULL_SHA
- *RSA_EXPORT_RC4_40_MD5

- *RSA_RC4_128_MD5
- *RSA_RC4_128_SHA
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_DES_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_AES_256_CBC_SHA
- *RSA_RC2_CBC_128_MD5
- *RSA_DES_CBC_MD5
- *RSA_3DES_EDE_CBC_MD5

Lista algorytmów szyfrowania SSL obsługiwanych w konfiguracji fabrycznej

Na poniższej liście wyszczególnione są zestawy algorytmów szyfrowania. System SSL obsługuje w konfiguracji fabrycznej 10 takich zestawów. Administratorzy mogą zmieniać algorytmy szyfrowania obsługiwane przez System SSL za pomocą wartości systemowych QSSLCSL i QSSLCSLCTL. Zestaw algorytmów szyfrowania nie może być obsługiwany, jeśli nie jest również obsługiwany protokół SSL, którego wymaga dany zestaw.

W konfiguracji fabrycznej System SSL obsługuje następujące zestawy algorytmów szyfrowania:
- *RSA_AES_256_CBC_SHA
- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5

Lista obsługiwanych algorytmów szyfrowania zależy od protokołów SSL obsługiwanych przez system oraz zmian dokonanych w wartości systemowej QSSLCSL. Listę algorytmów szyfrowania można obejrzeć, wyświetlając wartość QSSLCSL.

Lista domyślnych algorytmów szyfrowania SSL w konfiguracji fabrycznej

Kolejność listy domyślnych algorytmów szyfrowania w konfiguracji fabrycznej jest następująca:
- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA

Listę domyślnych algorytmów szyfrowania w konfiguracji fabrycznej można skrócić, a jej elementy zamienić miejscami, modyfikując wartość systemową QSSLCSL. Do listy nie można dodawać dodatkowych zestawów algorytmów szyfrowania.

Informacje pokrewne

Wartość systemowa SSL: QSSLPCL

Wartość systemowa SSL: QSSLCSLCTL

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 dostępne na platformie System i:

- IBM HTTP Server for i5/OS
- Serwer FTP
- Serwer Telnet
- System końcowy Centrum Zarządzania
- IBM Tivoli Directory Server for i5/OS

Informacje pokrewne

Protokoły SSL (Secure Sockets Layer) i TLS (Transport Layer Security) na serwerze Directory Server

Zabezpieczanie klientów FTP za pomocą protokołu TLS lub SSL

Zabezpieczanie programu Telnet za pomocą protokołu SSL

Konfigurowanie protokołu SSL dla serwera administracyjnego (ADMIN) serwera HTTP

Wymagania wstępne dotyczące protokołu SSL

Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

Przed rozpoczęciem używania protokołu SSL należy sprawdzić, czy w systemie zainstalowane są następujące opcje:

- IBM Digital Certificate Manager (DCM) (5761-SS1 Option 34)

  Uwaga: Program DCM nie jest wymagany przez oprogramowanie IBM Java Secure Socket Extension (JSSE) i OpenSSL.
- IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
- IBM HTTP Server for i5/OS (5761-DG1)
- Jeśli program DCM ma być używany na serwerze HTTP, należy zainstalować oprogramowanie IBM Developer Kit for Java (5761–JV1). W przeciwnym razie serwer administratora HTTP nie zostanie uruchomiony.
- Aby przyspieszyć przetwarzanie uzgadniania SSL, można zainstalować sprzęt szyfrujący do obsługi protokołu SSL. Jeśli ma zostać zainstalowany sprzęt szyfrujący, należy również zainstalować moduł Cryptographic Service Provider.

Uwaga: Kod opcji i produktów systemu i5/OS w wersjach starszych niż V6R1 to 5722.

Pojęcia pokrewne

“Rozwiązywanie problemów z protokołem SSL”
Ten temat zawiera podstawowe informacje, które mogą pomóc zmniejszyć liczbę potencjalnych problemów z protokołem SSL na platformie System i.

Informacje pokrewne

Sprzęt szyfrujący

Certyfikaty publiczne a certyfikaty prywatne

Konfigurowanie programu DCM

Zabezpieczanie aplikacji za pomocą protokołu SSL

Ten temat zawiera listę aplikacji, które można zabezpieczyć za pomocą protokołu SSL na platformie System i.

Za pomocą protokołu SSL można zabezpieczyć następujące aplikacje na platformie System i:

- Odwzorowywanie tożsamości dla przedsiębiorstwa (Enterprise Identity Mapping - EIM)
- Serwer FTP
- IBM HTTP Server for i5/OS
- System i Access for Windows
- IBM Tivoli Directory Server for i5/OS
- Distributed Relational Database Architecture (DRDA) i serwer Distributed Data Management (DDM)
- Centrum Zarządzania
- Serwer Telnet
- Websphere Application Server — Express
- Aplikacje napisane przy użyciu zestawu funkcji API programu System i Access for Windows
- Aplikacje napisane przy użyciu interfejsów API protokołu SSL obsługiwanych na platformie System i (obsługiwane interfejsy API to Global Secure Toolkit (GSKit) oraz SSL_System i)

Pojęcia pokrewne

“Scenariusz: zabezpieczanie wszystkich połączeń z serwerem Centrum Zarządzania za pomocą protokołu SSL” na stronie 5
W scenariuszu opisano zabezpieczanie za pomocą protokołu SSL wszystkich połączeń z serwerem System i działającym jako system centralny. Opisywane czynności wykonywane są przy użyciu systemu Centrum Zarządzania System i Navigator.

Informacje pokrewne

Odwzorowanie tożsamości dla przedsiębiorstwa (EIM)

Używanie protokołu SSL do zabezpieczania serwera FTP

Serwer HTTP

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

Scenariusz Telnet: zabezpieczanie aplikacji Telnet za pomocą SSL

Interfejs API protokołu SSL

Rozwiązywanie problemów z protokołem SSL

Ten temat zawiera podstawowe informacje, które mogą pomóc zmniejszyć liczbę potencjalnych problemów z protokołem SSL na platformie System i.

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

Sprawdź, czy zostały spełnione następujące warunki:

- spełnione są wymagania wstępne dotyczące protokołu SSL na platformie System i,

- ośrodek certyfikacji i certyfikaty są poprawne i nie wygasły.

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

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

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

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

Pojęcia pokrewne

“Wymagania wstępne dotyczące protokołu SSL” na stronie 18
Ten temat zawiera opis wymagań wstępnych dotyczących protokołu SSL na platformie System i, a także kilka przydatnych wskazówek.

Informacje pokrewne

Komunikaty kodów błędu funkcji API SSL

Informacje pokrewne dotyczące protokołu SSL

Poniżej znajdują się odsyłacze do innych zasobów i informacji dotyczących protokołu Secure Sockets Layer (SSL).

Serwisy WWW

- RFC 2246: ″The TLS Protocol Version 1.0 ″ (ftp://ftp.isi.edu/in-notes/rfc2246.txt)
  Zawiera szczegółowe informacje na temat protokołu TLS.
- RFC2818: ″HTTP Over TLS″ (ftp://ftp.isi.edu/in-notes/rfc2818.txt)
  Opisuje, jak korzystać z protokołu TLS do zabezpieczania połączeń HTTP w Internecie.

Inne informacje

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

Dodatek. Uwagi

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

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

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

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

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

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

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego: INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W 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 STRON 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 uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

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

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

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

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

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

Licencjonowany program opisany w niniejszym dokumencie 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, Umowie Licencyjnej IBM na Kod Maszynowy 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 możliwości 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.

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

LICENCJA W ZAKRESIE PRAW AUTORSKICH:

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

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

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

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

Znaki towarowe

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

| DRDA
| i5/OS
| IBM
| OS/400
| System i
| Tivoli

| Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi
| firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

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

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

Warunki

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

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

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

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

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

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

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

Drukowane w USA