7.5

Zabezpieczanie produktu IBM WebSphere MQ

Uwaga

Przed skorzystaniem z niniejszych informacji oraz produktu, którego one dotyczą, należy zapoznać się z informacjami zamieszczonymi w sekcji “Uwagi” na stronie 337.

Niniejsze wydanie dotyczy wersji 7 wydanie 5 produktu IBM® WebSphere MQ oraz wszystkich kolejnych wydań i modyfikacji, o ile nie zostanie to określone inaczej w nowych wydaniach.

Spis treści

Zabezpieczenia

Bezpieczeństwo jest ważnym zagadnieniem zarówno dla programistów aplikacji IBM WebSphere MQ , jak i dla administratorów systemu, którzy konfigurują uprawnienia IBM WebSphere MQ .

przegląd zabezpieczeń

Ta kolekcja tematów zawiera wprowadzenie do pojęć związanych z bezpieczeństwem produktu IBM WebSphere MQ .

Pojęcia i mechanizmy zabezpieczeń, stosowane w każdym systemie komputerowym, są prezentowane po raz pierwszy, a następnie omówienie tych mechanizmów zabezpieczeń, które są zaimplementowane w produkcie IBM WebSphere MQ.

Pojęcia i mechanizmy bezpieczeństwa

W tej kolekcji tematów opisano aspekty zabezpieczeń, które należy wziąć pod uwagę podczas instalowania produktu IBM WebSphere MQ .

Powszechnie akceptowane aspekty bezpieczeństwa są następujące:

- “Identyfikacja i uwierzytelnianie” na stronie 5
- “Autoryzacja” na stronie 6
- “Kontrola” na stronie 6
- “Poufność” na stronie 7
- “Integralność danych” na stronie 7

Mechanizmy zabezpieczeń to narzędzia techniczne i techniki używane do implementowania usług ochrony. Mechanizm może działać samodzielnie lub z innymi osobami w celu udostępnienia konkretnej usługi. Przykłady wspólnych mechanizmów bezpieczeństwa są następujące:

- “Kryptografia” na stronie 7
- “Streszczenia komunikatów i podpisy cyfrowe” na stronie 9
- “certyfikaty cyfrowe” na stronie 9
- “Infrastruktura klucza publicznego (PKI)” na stronie 14

Podczas planowania implementacji produktu IBM WebSphere MQ należy wziąć pod uwagę, które mechanizmy zabezpieczeń wymagają zaimplementowania tych aspektów bezpieczeństwa, które są istotne dla użytkownika. Informacje o tym, co należy wziąć pod uwagę po zapoznaniu się z tymi tematami, zawiera sekcja “Planowanie wymagań dotyczących bezpieczeństwa” na stronie 48.

Pojęcia pokrewne

“Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS” na stronie 214
Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

“Praca z protokołem SSL lub TLS” na stronie 114
W tych tematach znajdują się instrukcje dotyczące wykonywania pojedynczych zadań związanych z używaniem protokołu SSL lub TLS z produktem IBM WebSphere MQ.

Identyfikacja i uwierzytelnianie

Identyfikacja to możliwość jednoznacznego identyfikowania użytkownika systemu lub aplikacji, która działa w systemie. *Uwierzytelnianie* to możliwość udowodnienia, że użytkownik lub aplikacja jest rzeczywiście osobą, która ta osoba lub aplikacja twierdzi, że jest.

Na przykład należy wziąć pod uwagę użytkownika, który loguje się do systemu, wprowadzając identyfikator użytkownika i hasło. System używa ID użytkownika do identyfikacji użytkownika. System uwierzytelnia użytkownika w momencie logowania, sprawdzając, czy podane hasło jest poprawne.

Niezaprzeczalne

Usługę *non-repudiation* można wyświetlić jako rozszerzenie usługi identyfikacji i uwierzytelniania. Ogólnie rzecz biorąc, niezaprzecznienie ma zastosowanie w przypadku przekazywania danych drogą elektroniczną; na przykład zamówienie na zakup lub sprzedaż akcji przez maklera papierów wartościowych lub zlecenie banku w celu przekazania środków z jednego rachunku do innego.

Ogólnym celem nierenomowanej usługi jest możliwość udowodnienia, że konkretna wiadomość jest związana z konkretną osobą.

Usługa non-repudiation może zawierać więcej niż jeden komponent, w którym każdy komponent udostępnia inną funkcję. Jeśli nadawca komunikatu nigdy nie wysyła go, usługa nieodrzucana z *dowodem pochodzenia* może dostarczyć odbiornikowi niezaprzeczalne dowody na to, że wiadomość została wysłana przez tę konkretną osobę. Jeśli odbiorca komunikatu nigdy nie odbierze go, usługa nieodrzucana z *dowodem dostawy* może udostępnić nadawcę niezaprzeczalnym dowodzie, że wiadomość została odebrana przez daną osobę.

W praktyce, dowód z praktycznie 100% pewność, lub niezaprzeczalne dowody, jest trudnym celem. W prawdziwym świecie nic nie jest w pełni bezpieczne. Zarządzanie bezpieczeństwem jest bardziej związane z zarządzaniem ryzykiem do poziomu, który jest akceptowalny dla biznesu. W takim środowisku, bardziej realistycznym oczekiwaniem na nierenomowaną służbę jest możliwość przedstawienia dowodów, które są dopuszczalne, i popiera Państwa sprawę, w sądzie.

Nieodrzucana reputacja to odpowiednia usługa zabezpieczeń w środowisku IBM WebSphere MQ , ponieważ IBM WebSphere MQ jest sposobem przesyłania danych drogą elektroniczną. Na przykład może być wymagane podanie contemporannych dowodów, że konkretny komunikat został wysłany lub odebrany przez aplikację powiązaną z konkretną osobą.

Produkt IBM WebSphere MQ z produktem IBM WebSphere MQ Advanced Message Security nie udostępnia usługi nieodrzucanej jako części funkcji podstawowej. Ta dokumentacja produktu zawiera jednak sugestie dotyczące sposobu, w jaki można udostępnić własną, nieodrzucną usługę w środowisku WebSphere MQ , zapisując własne programy obsługi wyjścia.

Pojęcia pokrewne

“Identyfikacja i uwierzytelnianie w produkcie IBM WebSphere MQ” na stronie 21
W programie IBM WebSphere MQmożna zaimplementować identyfikację i uwierzytelnianie za pomocą informacji o kontekście komunikatów i wzajemnego uwierzytelniania.

Autoryzacja

Autoryzacja chroni newralgiczne zasoby w systemie, ograniczając dostęp tylko do autoryzowanych użytkowników i ich aplikacji. Uniemożliwia to nieautoryzowane użycie zasobu lub użycie zasobu w nieautoryzowany sposób.

Pojęcia pokrewne

“Autoryzacja w produkcie IBM WebSphere MQ” na stronie 21
Za pomocą autoryzacji można ograniczyć poszczególne osoby lub aplikacje, które mogą wykonywać w środowisku IBM WebSphere MQ .

Kontrola

Kontrolowanie jest procesem rejestrowania i sprawdzania zdarzeń w celu wykrycia, czy wystąpiło nieoczekiwane lub nieautoryzowane działanie, czy też podjęto próbę wykonania tego działania.

Więcej informacji na temat konfigurowania autoryzacji zawiera sekcja “Planowanie autoryzacji” na stronie 51 i powiązane podtematy.

Pojęcia pokrewne

“Kontrola w produkcie IBM WebSphere MQ” na stronie 22

Program IBM WebSphere MQ może wystawiać komunikaty zdarzeń w celu zarejestrowania, że zajęła się nietypowa aktywność.

Poufność

Usługa *poufności* zabezpiecza poufne informacje przed nieautoryzowanym ujawnieniem.

Gdy dane poufne są przechowywane lokalnie, mechanizmy kontroli dostępu mogą być wystarczające, aby chronić je przy założeniu, że nie można odczytać danych, jeśli nie można uzyskać do nich dostępu. Jeśli wymagany jest wyższy poziom bezpieczeństwa, dane mogą być szyfrowane.

Szyfrowanie danych poufnych, gdy jest przesyłane przez sieć komunikacyjną, w szczególności przez niezabezpieczoną sieć, taką jak Internet. W środowisku sieciowym mechanizmy kontroli dostępu nie są skuteczne w odniesieniu do prób przechwycenia danych, takich jak podsłup.

Integralność danych

Usługa *integralności danych* wykrywa, czy nieautoryzowana modyfikacja danych została nieautoryzowana.

Istnieją dwa sposoby zmiany danych: przypadkowo, za pomocą błędów sprzętu i transmisji, lub z powodu celowego ataku. Wiele produktów sprzętowych i protokołów transmisji posiada mechanizmy wykrywania i korygowania błędów sprzętowych i transmisjalnych. Celem usługi integralności danych jest wykrycie celowego ataku.

Usługa integralności danych ma na celu tylko wykrycie, czy dane zostały zmodyfikowane. Nie ma ona na celu odtworzenia danych do pierwotnego stanu, jeśli został on zmodyfikowany.

Mechanizmy kontroli dostępu mogą przyczyniać się do integralności danych w zakresie, w jakim nie można modyfikować danych, jeśli dostęp nie jest dostępny. Ale, podobnie jak w przypadku poufności, mechanizmy kontroli dostępu nie są skuteczne w środowisku sieciowym.

Pojęcia kryptograficzne

Ta kolekcja tematów zawiera opis pojęć związanych z kryptografią, które mają zastosowanie do produktu WebSphere MQ.

Termin *jednostka* służy do odwołania się do menedżera kolejek, klienta MQI produktu WebSphere MQ , pojedynczego użytkownika lub dowolnego innego systemu, który może wymieniać komunikaty.

Pojęcia pokrewne

“Kryptografia w produkcie IBM WebSphere MQ” na stronie 23
Produkt IBM WebSphere MQ udostępnia kryptografię za pomocą protokołów SSL (Secure Sockets Layer) i TLS (Transport Security Layer).

Kryptografia

Kryptografia to proces przekształcania tekstu w formie czytelnej, o nazwie *plaintext*i postaci nieczytelnej, o nazwie *ciphertext*.

Ma to miejsce w następujący sposób:

1. Nadawca przekształca wiadomość jawną w tekst zaszyfrować tekst zaszyfrować. Ta część procesu jest nazywana *szyfrowaniem* (czasem *encipherment*).
2. Tekst zaszyfrować jest przesyłany do odbiornika.
3. Odbiornik konwertuje komunikat zaszyfrować tekst z powrotem do postaci jawnego tekstu. Ta część procesu nosi nazwę *deszyfrowania* (czasem *decyferment*).

Definicja kryptografii zawiera Glosariusz .

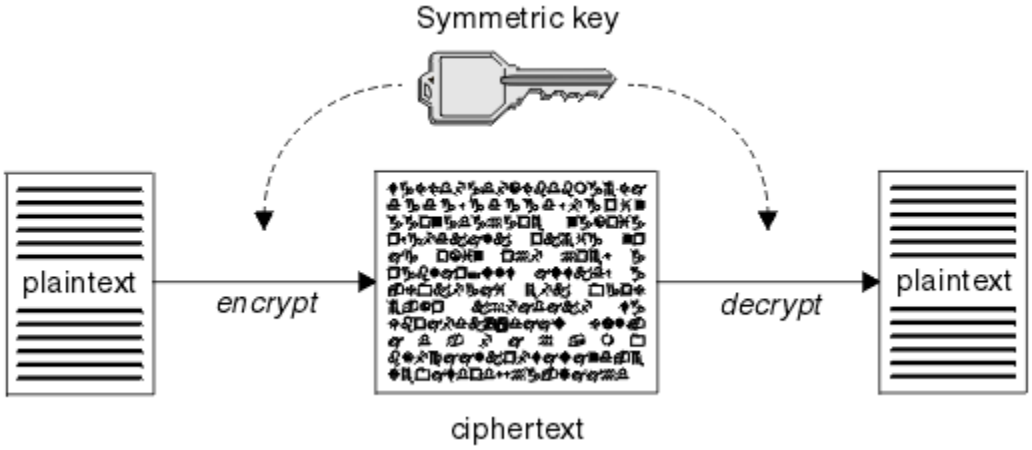
Konwersja obejmuje sekwencję operacji matematycznych, które zmieniają wygląd komunikatu podczas transmisji, ale nie mają wpływu na treść. Techniki kryptograficzne mogą zapewnić poufność i chronić wiadomości przed nieautoryzowanym wyświetlaniem (podsłuchiwaniem), ponieważ zaszyfrowana wiadomość jest niezrozumiała. Podpisy cyfrowe, które zapewniają zapewnienie integralności

komunikatów, używają technik szyfrowania. Więcej informacji na ten temat zawiera sekcja “Podpisy cyfrowe w protokole SSL i TLS” na stronie 19 .

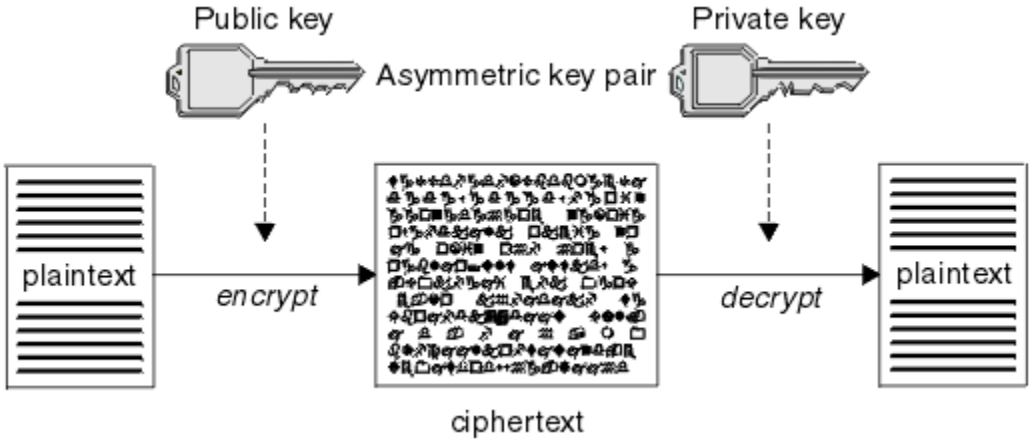
Techniki kryptograficzne wiążą się z ogólnym algorytmem, który jest specyficzny przy użyciu kluczy. Istnieją dwie klasy algorytmu:

- Te, które wymagają, aby obie strony używały tego samego klucza tajnego. Algorytmy, które korzystają z klucza współużytkowanego, są nazywane algorytmami *symetrycznymi* . Rysunek 1 na stronie 8 ilustruje kryptografię klucza symetrycznego.
- Te, które używają jednego klucza do szyfrowania i innego klucza do deszyfrowania. Jedno z nich musi być tajne, ale inne mogą być publiczne. Algorytmy, które używają par kluczy publicznych i prywatnych, są nazywane algorytmami *asymetryczne* . Rysunek 2 na stronie 8 ilustruje asymetryczną kryptografię klucza, która jest znana również pod nazwą *kryptografia klucza publicznego*.

Użyte algorytmy szyfrowania i deszyfrowania mogą być publiczne, ale współużytkowany klucz tajny i klucz prywatny muszą być przechowywane w tajemnicy.



Rysunek 1. szyfrowanie za pomocą klucza symetrycznego



Rysunek 2. szyfrowanie z użyciem klucza niesymetrycznego

Program Rysunek 2 na stronie 8 wyświetla tekst jawny zaszyfrowany przy użyciu klucza publicznego odbiorcy i zdeszyfrowany za pomocą klucza prywatnego odbiorcy. Tylko przeznaczony odbiornik przechowuje klucz prywatny do deszyfrowania tekstu zaszyfrowanych. Należy zwrócić uwagę, że nadawca może również szyfrować wiadomości za pomocą klucza prywatnego, co pozwala każdemu, kto posiada klucz publiczny nadawcy, na odszyfrowanie wiadomości, z zapewnieniem, że wiadomość musi pochodzić od nadawcy.

W przypadku algorytmów asymetrycznych komunikaty są szyfrowane zarówno z kluczem publicznym, jak i kluczem prywatnym, ale mogą być deszyfrowane tylko przy użyciu innego klucza. Tylko klucz

prywatny jest tajemnicą, klucz publiczny może być znany każdemu. Przy algorytmach symetrycznych klucz współużytkowany musi być znany tylko dwóm stronom. Jest to tzw. *problem z dystrybucją klucza* . Algorytmy asymetryczne są wolniejsze, ale mają tę zaletę, że nie ma problemu z dystrybucją kluczy.

Inna terminologia związana z kryptografią to:

Siła
Siła szyfrowania jest określana na podstawie wielkości klucza. Algorytmy asymetryczne wymagają dużych kluczy, na przykład:

1024 bity	Klucz asymetryczny o niskiej wytrzymałości
2048 bitów	Klucz asymetryczny o średniej wytrzymałości
4096 bitów	Klucz asymetryczny o dużej wytrzymałości

Klucze symetryczne są mniejsze: 256-bitowe klucze dają silne szyfrowanie.

Algorytm szyfrowania blokowego
Algorytmy te szyfrują dane za pomocą bloków. Na przykład algorytm RC2 z RSA Data Security Inc. używa bloków o długości 8 bajtów. Algorytmy blokowe są zazwyczaj wolniejsze niż algorytmy strumieniowe.

Algorytm szyfrowania strumienia
Algorytmy te działają na każdym bajcie danych. Algorytmy strumienia są zwykle szybsze niż algorytmy blokowe.

Streszczenia komunikatów i podpisy cyfrowe

Streszczenie komunikatu jest stałą wielkością liczbową reprezentacją treści komunikatu obliczoną przez funkcję mieszającą. Skrót wiadomości może być zaszyfrowany, tworząc podpis cyfrowy.

Komunikaty są ze względu na wielkość zmiennej wielkości. Streszczenie komunikatu jest stałą wielkością liczbową reprezentacją treści komunikatu. Streszczenie komunikatu jest obliczane przez funkcję mieszającą, która jest transformacją spełniającą dwa kryteria:

- Funkcja mieszająca musi być jedną ze sposobów. Nie może być możliwe odwrócenie funkcji w celu znalezienia komunikatu odpowiadającego konkretnym streszczonym komunikatom, innym niż testowanie wszystkich możliwych komunikatów.
- To musi być computacyjnie niewykonalne, aby znaleźć dwa komunikaty, które mieszają się do tego samego streszczenia.

Streszczenie komunikatu jest wysyłane razem z komunikatem. Odbiornik może generować streszczenie dla wiadomości i porównywać go ze streszczonym nadawcą. Integralność komunikatu jest weryfikowana w przypadku, gdy dwa streszczenia komunikatów są takie same. Każda ingerowanie w wiadomość podczas transmisji niemal na pewno skutkuje innym trawieniem wiadomości.

Streszczenie komunikatu utworzone przy użyciu klucza tajnego symetrycznego jest znane jako kod uwierzytelniania komunikatu (Message Authentication Code-MAC), ponieważ może on zapewnić, że komunikat nie został zmodyfikowany.

Nadawca może również wygenerować streszczenie wiadomości, a następnie zaszyfrować streszczenie za pomocą klucza prywatnego pary kluczy asymetrycznych, tworząc podpis cyfrowy. Podpis musi następnie zostać zdeszyfrowany przez odbiorcę przed porównaniem go z lokalnie wygenerowanym streszczaniem.

Pojęcia pokrewne
“Podpisy cyfrowe w protokole SSL i TLS” na stronie 19
Podpis cyfrowy jest tworzony przez zaszyfrowanie reprezentacji komunikatu. Szyfrowanie korzysta z klucza prywatnego sygnatariusza, a w przypadku efektywności zazwyczaj działa na streszczanie wiadomości, a nie na samym komunikacie.

certyfikaty cyfrowe

Certyfikaty cyfrowe chronią przed imitowaniem, poświadczając, że klucz publiczny należy do określonej jednostki. Są one wydawane przez ośrodek certyfikacji.

Certyfikaty cyfrowe zapewniają ochronę przed imitowaniem, ponieważ certyfikat cyfrowy wiąże klucz publiczny z jego właścicielem, niezależnie od tego, czy ten właściciel jest osobą indywidualną, menedżerem kolejek, czy inną jednostką. Certyfikaty cyfrowe są również nazywane certyfikatami klucza publicznego, ponieważ dają one pewność co do prawa własności klucza publicznego w przypadku korzystania z asymetrycznego schematu klucza. Certyfikat cyfrowy zawiera klucz publiczny dla jednostki i jest instrukcją, że klucz publiczny należy do tego obiektu:

- Jeśli certyfikat jest przeznaczony dla pojedynczego obiektu, certyfikat jest nazywany *certyfikatem osobistym* lub *certyfikatem użytkownika*.
- Jeśli certyfikat jest przeznaczony dla ośrodka certyfikacji, certyfikat jest nazywany *certyfikatem ośrodka CA* lub *certyfikatem osoby podpisującej*.

Jeśli klucze publiczne są wysyłane bezpośrednio przez ich właściciela do innego obiektu, istnieje ryzyko, że komunikat może zostać przechwycony, a klucz publiczny podstawiony przez inny. Jest on znany jako *man w ataku typu 'middle'*. Rozwiązaniem tego problemu jest wymiana kluczy publicznych za pośrednictwem zaufanej osoby trzeciej, co daje silne zapewnienie, że klucz publiczny naprawdę należy do jednostki, z którą się komunikują. Zamiast wysyłać bezpośrednio swój klucz publiczny, należy poprosić zaufaną osobę trzecią o włączenie jej do certyfikatu cyfrowego. Zaufana osoba trzecia, która wydaje certyfikaty cyfrowe, nosi nazwę ośrodka certyfikacji (CA), zgodnie z opisem w sekcji "Ośrodki certyfikacji" na stronie 11.

Co znajduje się w certyfikacie cyfrowym
Certyfikaty cyfrowe zawierają określone fragmenty informacji określone w standardzie X.509 .

Certyfikaty cyfrowe używane przez produkt WebSphere MQ są zgodne ze standardem X.509 , który określa wymagane informacje i format do wysyłania. X.509 to część standardu uwierzytelniania zgodna ze standardami X.500 .

Certyfikaty cyfrowe zawierają co najmniej następujące informacje na temat certyfikowanego podmiotu:

- Klucz publiczny właściciela
- Nazwa wyróżniająca właściciela
- Nazwa wyróżniająca ośrodka CA, który wystawił certyfikat
- Data, od której certyfikat jest ważny
- Data ważności świadectwa
- Numer wersji formatu danych certyfikatu zgodnie z definicją w X.509. Bieżąca wersja standardu X.509 to wersja 3, a większość certyfikatów jest zgodna z tą wersją.
- Numer seryjny. Jest to unikalny identyfikator przypisany przez ośrodek CA, który wystawił certyfikat. Numer seryjny jest unikalny w obrębie ośrodka CA, który wystawił certyfikat: nie ma dwóch certyfikatów podpisanych przez ten sam certyfikat CA, które mają ten sam numer seryjny.

Certyfikat X.509 w wersji 2 zawiera również identyfikator wystawcy i identyfikator podmiotu, a certyfikat X.509 w wersji 3 może zawierać pewną liczbę rozszerzeń. Niektóre rozszerzenia certyfikatów, takie jak rozszerzenie Podstawowe ograniczenie, są *standardowe*, ale inne są specyficzne dla implementacji. Rozszerzenie może mieć wartość *krytyczne*, w którym to przypadku system musi być w stanie rozpoznać pole. Jeśli pole nie rozpoznaje pola, musi odrzucić certyfikat. Jeśli rozszerzenie nie jest krytyczne, system może go zignorować, jeśli go nie rozpoznaje.

Podpis cyfrowy w certyfikacie osobistym jest generowany przy użyciu klucza prywatnego ośrodka CA, który podpisał ten certyfikat. Każdy, kto musi zweryfikować certyfikat osobisty, może skorzystać z klucza publicznego ośrodka CA, aby to zrobić. Certyfikat ośrodka CA zawiera klucz publiczny.

Certyfikaty cyfrowe nie zawierają klucza prywatnego. Musisz zachować tajemnicę klucza prywatnego.

Wymagania dotyczące świadectw osobistych
Produkt WebSphere MQ obsługuje certyfikaty cyfrowe zgodne ze standardem X.509 . Wymaga ona opcji uwierzytelniania klienta.

Ponieważ produkt IBM WebSphere MQ jest systemem równorzędnym, jest on wyświetlany jako uwierzytelnianie klienta w terminologii SSL. Z tego powodu każdy certyfikat osobisty używany do

uwierzytelniania SSL musi zezwalać na kluczowe użycie uwierzytelniania klienta. Nie wszystkie certyfikaty serwera mają włączoną tę opcję, dlatego może być konieczne włączenie uwierzytelniania klienta w głównym ośrodku certyfikacji (CA) dla certyfikatu zabezpieczonego.

Oprócz standardów, które określają format danych dla certyfikatu cyfrowego, istnieją również standardy określające, czy certyfikat jest ważny. Normy te zostały uaktualnione w czasie, aby zapobiec pewnym rodzajom naruszenia bezpieczeństwa. Na przykład starsze certyfikaty X.509 w wersji 1 i 2 nie wskazują, czy certyfikat może być legalnie używany do podpisywania innych certyfikatów. W związku z tym, złośliwy użytkownik mógł uzyskać certyfikat osobisty z legalnego źródła i utworzyć nowe certyfikaty, które mają wcielać się w rolę innych użytkowników.

Jeśli używane są certyfikaty X.509 w wersji 3, do określenia, które certyfikaty mogą być uprawnione do podpisywania innych certyfikatów, używane są rozszerzenia certyfikatów BasicConstraints i KeyUsage . Standard IETF RFC 5280 określa serię reguł sprawdzania poprawności certyfikatów, które muszą być implementowane przez oprogramowanie aplikacyjne, aby zapobiec atakom typu "personifikacja". Zestaw reguł certyfikatów jest znany jako strategia sprawdzania poprawności certyfikatów.

Więcej informacji na temat strategii sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ” na stronie 34.

Ośrodki certyfikacji
Ośrodek certyfikacji (CA) jest zaufaną osobą trzecią, która wydaje certyfikaty cyfrowe w celu zapewnienia, że klucz publiczny jednostki rzeczywiście należy do tego obiektu.

Role ośrodka CA są następujące:

- W sprawie otrzymania wniosku o wydanie certyfikatu cyfrowego, w celu weryfikacji tożsamości zamawiającego przed budynkiem, podpisaniem i zwrotem certyfikatu osobistego
- Aby udostępnić własny klucz publiczny ośrodka CA w certyfikacie ośrodka CA
- Publikowanie list certyfikatów, które nie są już zaufane na liście CRL (Certificate Revocation List). Aby uzyskać więcej informacji, zobacz: “Praca z odwołanymi certyfikatami” na stronie 155
- Aby zapewnić dostęp do statusu odwołania certyfikatu przez działanie serwera odpowiadającego OCSP,

Nazwy wyróżniające
Nazwa wyróżniająca (Distinguished Name-DN) jednoznacznie identyfikuje jednostkę w certyfikacie X.509 .

Następujące typy atrybutów są powszechnie dostępne w nazwie wyróżniającej:

SERIALNUMBER	Numer seryjny certyfikatu
MAIL	Adres e-mail
E	Adres e-mail (nieaktualny, zastąpiony podłańcuchem MAIL)
UID lub USERID	Identyfikator użytkownika
CN	Nazwa zwykła
T	Tytuł
OU	Nazwa jednostki organizacyjnej
DC	Komponent domeny
O	Nazwa organizacji
STREET	Ulica / Pierwszy wiersz adresu
L	Nazwa miejscowości
ST, SP lub S	Nazwa województwa lub rejonu
Komputer PC	Kod pocztowy
C	Kraj

UNSTRUCTUREDNAME	Nazwa hosta
UNSTRUCTUREDADDRESS	Adres IP
DNQ	Kwalifikator nazwy wyróżniającej

Standard X.509 definiuje inne atrybuty, które zwykle nie tworzą części nazwy wyróżniającej (DN), ale mogą udostępniać opcjonalne rozszerzenia certyfikatu cyfrowego.

Standard X.509 określa nazwę wyróżniającą (DN), która ma być określona w formacie łańcucha. Na przykład:

```
CN=John Smith, OU=Test, O=IBM, C=GB
```

Nazwa zwykła (CN) może zawierać opis pojedynczego użytkownika lub dowolnego innego obiektu, na przykład serwera WWW.

Nazwa wyróżniająca może zawierać wiele atrybutów OU i DC. Dozwolona jest tylko jedna instancja każdego z pozostałych atrybutów. Kolejność pozycji OU jest znacząca: w kolejności określa się hierarchię nazw jednostek organizacyjnych, najpierw z jednostką najwyższego poziomu. Kolejność pozycji w DC jest również istotna.

IBM WebSphere MQ toleruje niektóre zniekształcone nazwy wyróżniające. Więcej informacji na ten temat zawiera sekcja Reguły produktuWebSphere MQ dla wartości SSLPEER.

Pojęcia pokrewne

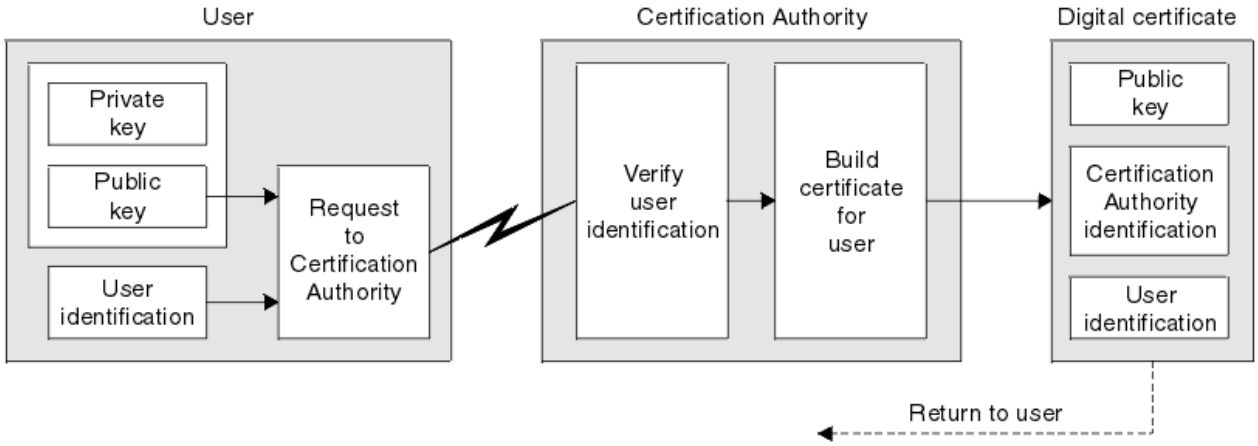
“Co znajduje się w certyfikacie cyfrowym” na stronie 10
Certyfikaty cyfrowe zawierają określone fragmenty informacji określone w standardzie X.509 .

Uzyskiwanie certyfikatów osobistych z ośrodka certyfikacji
Certyfikat można uzyskać z zaufanego zewnętrznego ośrodka certyfikacji (CA).

Certyfikat cyfrowy można uzyskać, wysyłając informacje do ośrodka CA, w postaci żądania certyfikatu. Standard X.509 definiuje format dla tych informacji, ale niektóre CAs mają własny format. Żądania certyfikatów są zwykle generowane przez narzędzie do zarządzania certyfikatami używane przez system, na przykład narzędzie iKeyman w systemach UNIX, Linux®i Windows , a także narzędzie RACF w systemie z/OS. Informacje te zawierają nazwę wyróżniającą i klucz publiczny. Gdy narzędzie do zarządzania certyfikatami wygeneruje żądanie certyfikatu, generuje on także klucz prywatny, który należy zabezpieczyć. Nigdy nie dystrybuuj klucza prywatnego.

Po odebraniu żądania przez ośrodek CA organ weryfikuje tożsamość użytkownika przed zbudowaniem certyfikatu i zwracając go do użytkownika jako certyfikat osobisty.

Rysunek 3 na stronie 12 ilustruje proces uzyskiwania certyfikatu cyfrowego z ośrodka CA.



Rysunek 3. Uzyskiwanie certyfikatu cyfrowego

Na diagramie:

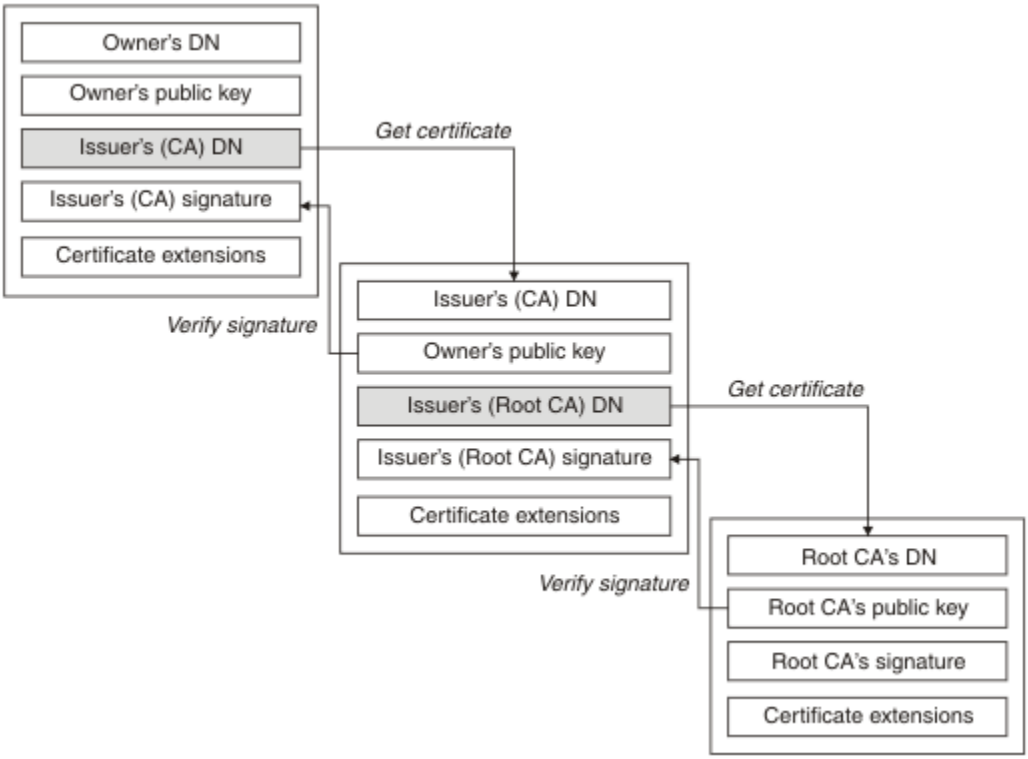
- "Identyfikacja użytkownika" zawiera nazwę wyróżniającą podmiotu.
- "Identyfikacja ośrodka certyfikacji" obejmuje nazwę wyróżniającą ośrodka certyfikacji, który wystawił certyfikat.
-

Certyfikaty cyfrowe zawierają dodatkowe pola inne niż te, które są wyświetlane na diagramie. Więcej informacji na temat pozostałych pól w certyfikacie cyfrowym zawiera sekcja “Co znajduje się w certyfikacie cyfrowym” na stronie 10.

Sposób działania łańcuchów certyfikatów
W przypadku otrzymania certyfikatu dla innej jednostki może być konieczne użycie *łańcucha certyfikatów* w celu uzyskania certyfikatu *głównego ośrodka CA* .

Łańcuch certyfikatów, znany również jako *ścieżka certyfikacji* , jest listą certyfikatów używanych do uwierzytelniania jednostki. Łańcuch lub ścieżka rozpoczyna się od certyfikatu tego obiektu, a każdy certyfikat w łańcuchu jest podpisywany przez jednostkę identyfikowaną przez następny certyfikat w łańcuchu. Łańcuch kończy się certyfikatem głównego ośrodka CA. Główny certyfikat ośrodka CA jest zawsze podpisywany przez ośrodek certyfikacji (CA). Podpisy wszystkich certyfikatów w łańcuchu muszą być weryfikowane, dopóki nie zostanie osiągnięty główny certyfikat ośrodka CA.

Rysunek 4 na stronie 13 ilustruje ścieżkę certyfikacji od właściciela certyfikatu do głównego ośrodka CA, w którym zaczyna się łańcuch zaufania.



Rysunek 4. Łańcuch zaufania

Każdy certyfikat może zawierać jedno lub więcej rozszerzeń. Certyfikat należący do ośrodka CA zwykle zawiera rozszerzenie BasicConstraints z opcją isCA ustawioną w celu wskazania, że może on podpisywać inne certyfikaty.

Gdy certyfikaty nie są już poprawne
Certyfikaty cyfrowe mogą utracać ważność lub zostać odwołane.

Certyfikaty cyfrowe wydawane są na czas określony i nie są ważne po upływie ich daty ważności.

Definicja okresu ważności certyfikatu znajduje się w sekcji Glosariusz .

Świadectwa mogą być odwołane z różnych powodów, w tym:

- Właściciel przeniósł się do innej organizacji.
- Klucz prywatny nie jest już tajny.

ProduktWebSphere MQ może sprawdzać, czy certyfikat został unieważniony, wysyłając żądanie do programu odpowiadającego protokołu OCSP (Online Certificate Status Protocol) (tylko w systemach UNIX, Linux i Windows). Alternatywnie mogą oni uzyskać dostęp do listy CRL na serwerze LDAP. Informacje o unieważnieniu OCSP i CRL są publikowane przez ośrodek certyfikacji. Więcej informacji na ten temat zawiera sekcja “Praca z odwołanymi certyfikatami” na stronie 155.

Infrastruktura klucza publicznego (PKI)

Infrastruktura klucza publicznego (Public Key Infrastructure-PKI) to system obiektów, strategii i usług, który obsługuje użycie kryptografii klucza publicznego do uwierzytelniania podmiotów biorących udział w transakcji.

Nie istnieje jeden standard, który definiuje komponenty infrastruktury klucza publicznego, ale PKI zazwyczaj składa się z ośrodków certyfikacji (CA) i organów rejestracji (RAs). CAs zapewniają następujące usługi:

- Wydawanie certyfikatów cyfrowych
- Sprawdzanie poprawności certyfikatów cyfrowych
- Unieważnianie certyfikatów cyfrowych
- Dystrybucja kluczy publicznych

Standardy X.509 stanowią podstawę dla branżowej standardowej infrastruktury klucza publicznego.

Więcej informacji na temat certyfikatów cyfrowych i ośrodków certyfikacji (CAs) zawiera sekcja “certyfikaty cyfrowe” na stronie 9 . RA weryfikuje, czy informacje podane podczas żądania certyfikatów cyfrowych są wymagane. Jeśli ośrodek certyfikacji (RA) weryfikuje te informacje, ośrodek CA może wydać żądający certyfikat cyfrowy.

W systemie PKI mogą być również dostępne narzędzia do zarządzania certyfikatami cyfrowymi i kluczami publicznymi. PKI jest czasem opisywany jako *hierarchia zaufania* do zarządzania certyfikatami cyfrowymi, ale większość definicji obejmuje dodatkowe usługi. Niektóre definicje obejmują szyfrowanie i usługi podpisu cyfrowego, ale usługi te nie są niezbędne do działania PKI.

Protokoły zabezpieczeń szyfrujących: SSL i TLS

Protokoły kryptograficzne zapewniają bezpieczne połączenia, umożliwiając dwóm stronom komunikowanie się z prywatnością i integralności danych. Protokół TLS (Transport Layer Security) wyewoluował z protokołu SSL (Secure Sockets Layer). Produkt IBM WebSphere MQ obsługuje zarówno protokół SSL, jak i TLS.

Podstawowym założeniami obu protokołów jest zapewnienie poufności (czasem nazywaja się *prywatność*), integralności danych, identyfikacji i uwierzytelniania przy użyciu certyfikatów cyfrowych.

Chociaż oba protokoły są podobne, różnice są wystarczająco istotne, aby protokół SSL 3.0 i różne wersje protokołu TLS nie współdziałały.

Pojęcia pokrewne

“Protokoły zabezpieczeń w produkcie IBM WebSphere MQ” na stronie 23
Produkt IBM WebSphere MQ obsługuje zarówno protokół TLS (Transport Layer Security), jak i protokoły SSL (Secure Sockets Layer) w celu zapewnienia bezpieczeństwa na poziomie łącza dla kanałów komunikatów i kanałów MQI.

Pojęcia związane z protokołem SSL (Secure Sockets Layer) i TLS (Transport Layer Security)

Protokoły SSL i TLS umożliwiają dwóm stronom identyfikowanie i uwierzytelnianie siebie nawzajem oraz komunikację z zachowaniem poufności i integralności danych. Protokół TLS ewoluował z protokołu Netscape SSL 3.0 , ale protokół TLS i SSL nie współdziałają.

Protokoły SSL i TLS zapewniają bezpieczeństwo komunikacji przez internet i umożliwiają aplikacjom klienckim/serwerowym komunikowanie się w sposób poufny i niezawodny. Protokoły mają dwie warstwy: protokół Record i protokół uzgadniania, a te są warstwowe powyżej protokołu transportowego, takiego jak TCP/IP. Oba wykorzystują techniki kryptograficzne asymetryczne i symetryczne.

Połączenie SSL lub TLS jest inicjowane przez aplikację, która staje się klientem SSL lub TLS. Aplikacja, która odbiera połączenie, staje się serwerem SSL lub TLS. Każda nowa sesja rozpoczyna się od uzgadniania, zgodnie z definicją protokołów SSL lub TLS.

Pełna lista opcji CipherSpecs obsługiwana przez produkt IBM WebSphere MQ jest dostępna pod adresem “Określanie CipherSpecs” na stronie 225.

Więcej informacji na temat protokołu SSL można znaleźć w informacjach podanych w sekcji https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt. Więcej informacji na temat protokołu TLS można znaleźć w informacjach dostarczonych przez grupę roboczą ds. TLS na stronie internetowej grupy roboczej ds. inżynierii internetowej w serwisie https://www.ietf.org .

Przegląd uzgadniania SSL lub TLS

Uzgadnianie SSL lub TLS umożliwia klientowi i serwerowi SSL lub TLS ustanowienie kluczy tajnych, z którymi się komunikują.

Ta sekcja zawiera podsumowanie kroków, które umożliwiają komunikację między klientem i serwerem protokołu SSL lub TLS oraz komunikację między serwerami.

- Uzgodnić wersję protokołu, który ma być używany.
- Wybierz algorytmy szyfrujące.
- Uwierzytelniaj się nawzajem, wymieniając i sprawdzając certyfikaty cyfrowe.
- Użyj technik szyfrowania asymetrycznego, aby wygenerować współużytkowany klucz tajny, który pozwala uniknąć problemu z dystrybucją klucza. Następnie protokół SSL lub TLS używa klucza współużytkowanego do symetrycznego szyfrowania komunikatów, co jest szybsze niż szyfrowanie asymetryczne.

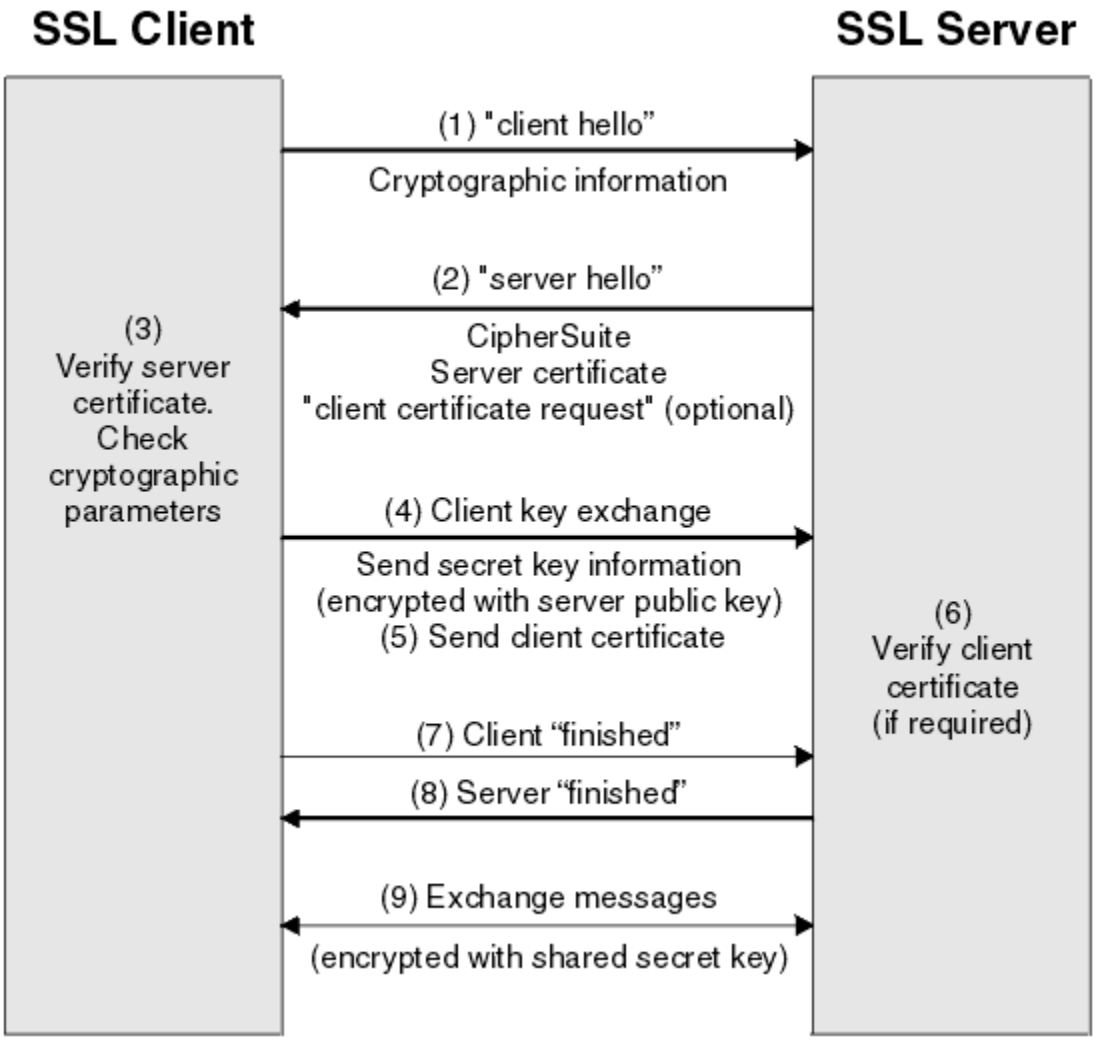
Więcej informacji na temat algorytmów szyfrowania i certyfikatów cyfrowych można znaleźć w informacjach pokrewnych.

W przeglądzie czynności związane z uzgadnianiem SSL są następujące:

1. Klient SSL lub TLS wysyła komunikat "klient hello" , który zawiera informacje kryptograficzne, takie jak wersja SSL lub TLS, a w preferowanej kolejności klienta- CipherSuites obsługiwane przez klienta. Komunikat zawiera również losowy łańcuch bajtowy, który jest używany w kolejnych obliczeniami. Protokół ten umożliwia "klientowi hello" dołączenie metod kompresji danych obsługiwanych przez klienta.
2. Serwer SSL lub TLS odpowiada na komunikat "server hello" , który zawiera pakiet CipherSuite wybrany przez serwer z listy udostępnianej przez klienta, identyfikator sesji i inny łańcuch o losowym bajcie. Serwer wysyła również certyfikat cyfrowy. Jeśli serwer wymaga certyfikatu cyfrowego na potrzeby uwierzytelniania klienta, serwer wysyła "żądanie certyfikatu klienta" , które zawiera listę typów obsługiwanych certyfikatów oraz nazwy wyróżniające akceptowanych ośrodków certyfikacji (CA).
3. Klient SSL lub TLS weryfikuje certyfikat cyfrowy serwera. Więcej informacji na ten temat zawiera sekcja “Jak SSL i TLS zapewniają identyfikację, uwierzytelnianie, poufność i integralność” na stronie 16.
4. Klient SSL lub TLS wysyła przypadkowy łańcuch bajtowy, który umożliwia zarówno klientowi, jak i serwerowi obliczenie klucza tajnego używanego do szyfrowania kolejnych danych komunikatu. Sam losowy łańcuch bajtów jest zaszyfrowany kluczem publicznym serwera.

5. Jeśli serwer SSL lub TLS wysłał "żądanie certyfikatu klienta", klient wysyła losowy łańcuch bajtowy zaszyfrowany za pomocą klucza prywatnego klienta, wraz z certyfikatem cyfrowym klienta lub "niealertem certyfikatu cyfrowego". Ten alert jest tylko ostrzeżeniem, ale w przypadku niektórych implementacji uzgadnianie nie powiedzie się, jeśli uwierzytelnianie klienta jest obowiązkowe.
6. Serwer SSL lub TLS weryfikuje certyfikat klienta. Więcej informacji na ten temat zawiera sekcja “Jak SSL i TLS zapewniają identyfikację, uwierzytelnianie, poufność i integralność” na stronie 16.
7. Klient SSL lub TLS wysyła serwer a "gotowy" komunikat, który jest zaszyfrowany kluczem tajnym, co oznacza, że część klienta została zakończona.
8. Serwer SSL lub TLS wysyła klientowi komunikat "gotowy" , który jest zaszyfrowany kluczem tajnym, co oznacza, że część serwera została zakończona.
9. Na czas trwania sesji SSL lub TLS serwer i klient mogą teraz wymieniać komunikaty, które są szyfrowane symetrycznie przy użyciu współużytkowanego klucza tajnego.

Rysunek 5 na stronie 16 przedstawia uzgadnianie SSL lub TLS.



Rysunek 5. Przegląd uzgadniania SSL lub TLS

Jak SSL i TLS zapewniają identyfikację, uwierzytelnianie, poufność i integralność

Podczas uwierzytelniania klienta i serwera istnieje krok, który wymaga, aby dane były szyfrowane za pomocą jednego z kluczy w pary kluczy asymetrycznych i zdeszyfrowane przy użyciu innego klucza pary. Streszczenie komunikatu jest używane w celu zapewnienia integralności.

Przegląd kroków związanych z uzgadnianiem TLS znajduje się w sekcji “Przegląd uzgadniania SSL lub TLS” na stronie 15.

Jak SSL i TLS zapewniają uwierzytelnianie

W przypadku uwierzytelniania serwera klient używa klucza publicznego serwera do szyfrowania danych, które są używane do obliczenia klucza tajnego. Serwer może wygenerować klucz tajny tylko wtedy, gdy będzie mógł odszyfrować te dane za pomocą poprawnego klucza prywatnego.

W przypadku uwierzytelniania klienta serwer używa klucza publicznego w certyfikacie klienta do deszyfrowania danych wysyłanych przez klienta podczas kroku “5” na stronie 16 uzgadniania. Wymiana gotowych komunikatów, które są szyfrowane kluczem tajnym (kroki “7” na stronie 16 i “8” na stronie 16 w przeglądzie) potwierdzi, że uwierzytelnianie zostało zakończone.

Jeśli wykonanie którejkolwiek z kroków uwierzytelniania nie powiedzie się, uzgadnianie nie powiedzie się i sesja zostanie zakończona.

Wymiana certyfikatów cyfrowych podczas uzgadniania SSLor TLS jest częścią procesu uwierzytelniania. Więcej informacji o tym, w jaki sposób certyfikaty zapewniają ochronę przed imitowaniem, można znaleźć w temacie pokrewnej informacji. Wymagane certyfikaty są następujące, gdzie ośrodek CA X wysyła certyfikat do klienta SSL lub TLS, a ośrodek CA Y wysyła certyfikat do serwera SSL lub TLS:

Tylko w przypadku uwierzytelniania serwera: serwer SSL lub TLS potrzebuje:

- Certyfikat osobisty wystawiony na serwer przez ośrodek CA Y
- Klucz prywatny serwera

i potrzeb klienta SSL lub TLS:

- Certyfikat CA dla ośrodka CA Y

Jeśli serwer SSL lub TLS wymaga uwierzytelniania klienta, serwer weryfikuje tożsamość klienta, weryfikując certyfikat cyfrowy klienta z kluczem publicznym ośrodka CA, który wystawił certyfikat osobisty dla klienta, w tym przypadku CA X . Zarówno w przypadku uwierzytelniania serwera, jak i klienta, serwer wymaga:

- Certyfikat osobisty wystawiony na serwer przez ośrodek CA Y
- Klucz prywatny serwera
- Certyfikat CA dla ośrodka CA X

a klient potrzebuje:

- Certyfikat osobisty wystawiony dla klienta przez ośrodek CA X
- Klucz prywatny klienta
- Certyfikat CA dla ośrodka CA Y

Zarówno serwer SSL, jak i serwer TLS i klient mogą potrzebować innych certyfikatów CA, aby utworzyć łańcuch certyfikatów do głównego certyfikatu ośrodka CA. Więcej informacji na temat łańcuchów certyfikatów można znaleźć w sekcji dotyczącej informacji pokrewnych.

Co dzieje się podczas weryfikacji certyfikatu

Jak zauważono w krokach “3” na stronie 15 i “6” na stronie 16 przeglądu, klient SSL lub TLS weryfikuje certyfikat serwera, a serwer SSL lub TLS weryfikuje certyfikat klienta. Weryfikacja ta ma cztery aspekty:

1. Podpis cyfrowy jest sprawdzany (patrz “Podpisy cyfrowe w protokole SSL i TLS” na stronie 19).
2. Łańcuch certyfikatów jest sprawdzany. Należy mieć certyfikaty pośrednie ośrodka CA (patrz sekcja “Sposób działania łańcuchów certyfikatów” na stronie 13).
3. Sprawdzane są daty ważności i aktywacji oraz okres ważności.
4. Status unieważnienia certyfikatu jest sprawdzany (patrz “Praca z odwołanymi certyfikatami” na stronie 155).

Resetowanie klucza tajnego

Podczas uzgadniania protokołu SSL lub TLS generowany jest *klucz tajny* służący do szyfrowania danych między klientem i serwerem SSL lub TLS. Klucz tajny jest używany w formule matematycznej, która jest stosowana do danych w celu transformowania jawnego tekstu jawnego w nieczytelny tekst zaszyfrowowy oraz do tekstu zaszyfrowalnego w postaci jawnego tekstu.

Klucz tajny jest generowany na podstawie losowego tekstu wysłanego w ramach uzgadniania i służy do szyfrowania tekstu jawnego w tekście zaszyfrowany. Klucz tajny jest również używany w algorytmie MAC (Message Authentication Code), który jest używany do określenia, czy komunikat został zmieniony. Więcej informacji na ten temat zawiera sekcja “Streszczenia komunikatów i podpisy cyfrowe” na stronie 9 .

Jeśli zostanie wykryty klucz tajny, można rozszyfrować jawny tekst komunikatu z tekstu zaszyfrować lub można obliczyć streszczenie komunikatu, umożliwiając zmianę komunikatów bez wykrywania. Nawet w przypadku skomplikowanego algorytmu, tekst jawny może zostać wykryty przez zastosowanie wszystkich możliwych transformacji matematycznych do tekstu zaszyfrowalnego. Aby zminimalizować ilość danych, które mogą być rozszyfrowane lub zmienione, jeśli klucz tajny jest uszkodzony, klucz tajny może być okresowo renegocjowany. Gdy klucz tajny został renegocjowany, poprzedni klucz tajny nie może być już używany do deszyfrowania danych zaszyfrowanych za pomocą nowego klucza tajnego.

Jak SSL i TLS zapewniają poufność

Protokół SSL i TLS korzystają z szyfrowania symetrycznego i asymetrycznego w celu zapewnienia prywatności komunikatów. Podczas uzgadniania protokołu SSL lub TLS klient i serwer SSL lub TLS uzgadnia algorytm szyfrowania i współużytkowany klucz tajny, który ma być używany tylko dla jednej sesji. Wszystkie komunikaty przesyłane między klientem i klientem protokołu SSL lub TLS są szyfrowane przy użyciu tego algorytmu i klucza, co zapewnia, że komunikat pozostaje prywatny, nawet jeśli jest przechwycony. Protokół SSL obsługuje szeroki zakres algorytmów szyfrujących. Ponieważ podczas transportowania współużytkowanego klucza tajnego SSL i TLS używają szyfrowania asymetrycznego, nie ma problemu z dystrybucją kluczy. Więcej informacji na temat technik szyfrowania można znaleźć w sekcji “Kryptografia” na stronie 7.

Jak protokół SSL i TLS zapewniają integralność

Protokół SSL i TLS zapewniają integralność danych, obliczając streszczenie komunikatu. Więcej informacji zawiera sekcja “Integralność danych komunikatów” na stronie 235.

Użycie protokołu SSL lub TLS zapewnia integralność danych, pod warunkiem, że parametr CipherSpec w definicji kanału używa algorytmu mieszającego zgodnie z opisem w tabeli w produkcie “Określanie CipherSpecs” na stronie 225.

W szczególności, jeśli integralność danych jest niepokojem, należy unikać wyboru CipherSpec , którego algorytm mieszający jest wymieniony jako "Brak". Użycie parametru MD5 jest również bardzo zalecane, ponieważ jest ono teraz bardzo stare i nie jest już bezpieczne dla większości praktycznych celów.

CipherSpecs i CipherSuites

Protokoły zabezpieczeń szyfrujących muszą być zgodne z algorytmami używannymi przez bezpieczne połączenie. Atrybuty CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

Parametr CipherSpec identyfikuje kombinację algorytmu szyfrowania i algorytmu uwierzytelniania komunikatów (Message Authentication Code-MAC). Oba końce protokołu TLS lub SSL muszą być zgodne z tym samym obiektem CipherSpec , aby móc komunikować się.

Ważne: W przypadku korzystania z kanałów produktu IBM WebSphere MQ używana jest specyfikacja CipherSpec. Podczas obsługi kanałów produktu Java, kanałów produktu JMS lub kanałów MQTT należy określić pakiet CipherSuite.

Więcej informacji na temat specyfikacji CipherSpecszawiera sekcja “Określanie CipherSpecs” na stronie 225.

CipherSuite to zestaw algorytmów szyfrujących używanych przez połączenie SSL lub TLS. Pakiet składa się z trzech różnych algorytmów:

- Algorytm wymiany kluczy i uwierzytelniania używany podczas uzgadniania
- Algorytm szyfrowania używany do szyfrowania danych
- Algorytm MAC (Message Authentication Code), używany do generowania streszczenia komunikatów

Dla każdego komponentu pakietu istnieje kilka opcji, ale tylko niektóre kombinacje są poprawne, jeśli są określone dla połączenia TLS lub SSL. Nazwa poprawnego zestawu algorytmów szyfrowania CipherSuite definiuje kombinację algorytmów używanych. Na przykład opcja CipherSuite SSL_RSA_WITH_RC4_128_MD5 określa:

- Algorytm wymiany kluczy RSA i algorytm uwierzytelniania
- Algorytm szyfrowania RC4 korzystający z klucza 128-bitowego
- Algorytm MD5 MAC

Kilka algorytmów jest dostępnych do wymiany kluczy i uwierzytelniania, ale algorytm RSA jest obecnie najczęściej używanym. W algorytmach szyfrowania i algorytmach MAC istnieje większa liczba różnych algorytmów szyfrowania.

Podpisy cyfrowe w protokole SSL i TLS

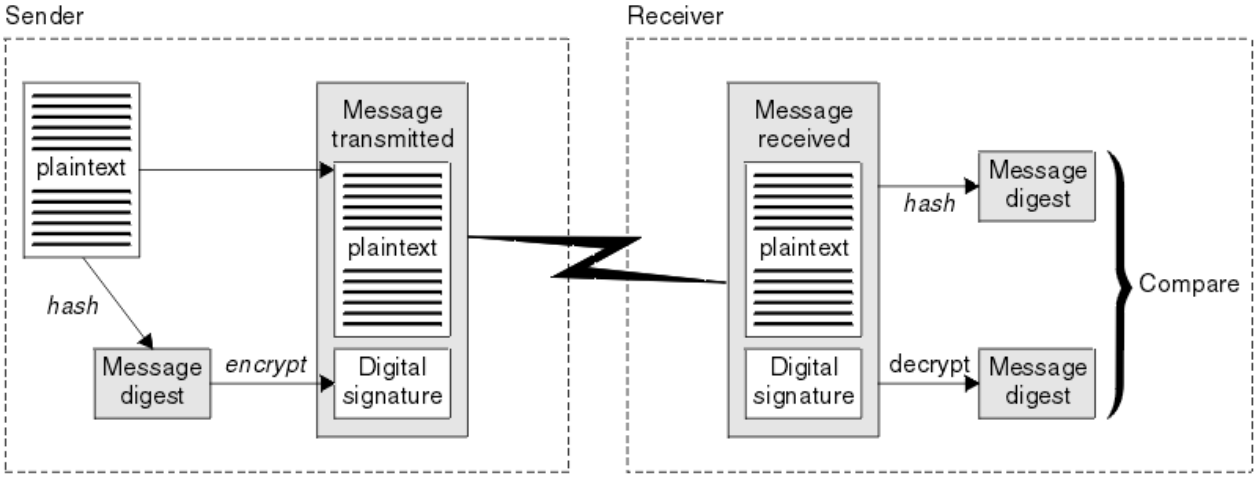
Podpis cyfrowy jest tworzony przez zaszyfrowanie reprezentacji komunikatu. Szyfrowanie korzysta z klucza prywatnego sygnatariusza, a w przypadku efektywności zazwyczaj działa na streszczanie wiadomości, a nie na samym komunikacie.

Podpisy cyfrowe różnią się w zależności od podpisanych danych, w przeciwieństwie do podpisów odręcznych, które nie zależą od treści podpisanego dokumentu. Jeśli dwa różne komunikaty są podpisywane cyfrowo przez ten sam obiekt, te dwa sygnatury różnią się, ale oba sygnatury mogą być weryfikowane z tym samym kluczem publicznym, czyli kluczem publicznym jednostki, która podpisała komunikaty.

Kroki procesu podpisywania cyfrowego są następujące:

1. Nadawca oblicza streszczenie wiadomości, a następnie szyfruje skrót za pomocą klucza prywatnego nadawcy, tworząc podpis cyfrowy.
2. Nadawca przesyła podpis cyfrowy z komunikatem.
3. Odbiornik deszyfruje podpis cyfrowy za pomocą klucza publicznego nadawcy, a następnie ponownie wygeneruje streszczenie komunikatu nadawcy.
4. Odbiorca oblicza streszczenie komunikatu na podstawie otrzymanych danych komunikatu i sprawdza, czy dwa streszczenia są takie same.

Rysunek 6 na stronie 19 ilustruje ten proces.



Rysunek 6. Proces podpisywania cyfrowego

Jeśli podpis cyfrowy jest weryfikowany, odbiorca wie, że:

- Komunikat nie został zmodyfikowany podczas transmisji.
- Komunikat został wysłany przez podmiot, który twierdzi, że go wysłał.

Podpisy cyfrowe są częścią integralności i usług uwierzytelniania. Podpisy cyfrowe stanowią również dowód pochodzenia. Tylko nadawca zna klucz prywatny, który dostarcza mocnych dowodów na to, że nadawca jest inicjatorem wiadomości.

Uwaga: Można również zaszyfrować sam komunikat, który zabezpiecza poufność informacji w komunikacie.

Standardy przetwarzania informacji federalnej

Rząd USA wytwarza doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Narodowy Instytut Norm i Technologii (NIST) to ważny organ, którego dotyczą systemy informatyczne i bezpieczeństwo. Program NIST generuje rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

Znaczącym jednym z tych standardów jest standard FIPS 140-2, który wymaga użycia mocnych algorytmów kryptograficznych. Standard FIPS 140-2 określa również wymagania dotyczące algorytmów mieszających, które mają być używane do zabezpieczania pakietów przed modyfikacją w tranzycie.

Produkt IBM WebSphere MQ udostępnia obsługę standardu FIPS 140-2, gdy została ona skonfigurowana do tego celu.

Z biegiem czasu analitycy opracowują ataki na istniejące algorytmy szyfrowania i kodowania mieszającego. Nowe algorytmy są przyjmowane, aby oprzeć się atakom. Standard FIPS 140-2 jest okresowo aktualizowany w celu uwzględnienia tych zmian.

National Security Agency (NSA) Suite B Cryptography

Rząd Stanów Zjednoczonych Ameryki produkuje doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Amerykańska Narodowa Agencja Bezpieczeństwa (NSA) zaleca zestaw interoperacyjnych algorytmów kryptograficznych w swoim standardzie Suite B.

Standard Suite B określa tryb działania, w którym używany jest tylko określony zestaw bezpiecznych algorytmów kryptograficznych. Standard Suite B określa:

- Algorytm szyfrowania (AES)
- Algorytm wymiany kluczy (Elliptic Curve Diffie-Hellman, znany również jako ECDH)
- Algorytm podpisu cyfrowego (Elliptic Curve Digital Signature Algorithm, znany również jako ECDSA)
- Algorytmy kodowania mieszającego (SHA-256 lub SHA-384)

Dodatkowo standard IETF RFC 6460 określa profile zgodne ze standardem Suite B, które definiują konfigurację i zachowanie szczegółowej aplikacji niezbędne do zachowania zgodności z normą Suite B. Definiuje on dwa profile:

1. Profil zgodny z pakietem B, który ma być używany z protokołem TLS w wersji 1.2. Po skonfigurowaniu dla operacji zgodnej ze standardem Suite B zostanie użyty tylko ograniczony zestaw algorytmów szyfrowania wymienionych powyżej.
2. Profil przejściowy do użycia z protokołem TLS w wersji 1.0 lub TLS w wersji 1.1. Ten profil umożliwia współdziałanie z serwerami zgodnymi z pakietem B innych niż Suite B. Po skonfigurowaniu dla operacji przejściowej Suite B można użyć dodatkowych algorytmów szyfrowania i kodowania mieszającego.

Standard Suite B jest koncepcyjnie podobny do standardu FIPS 140-2, ponieważ ogranicza on zestaw włączonych algorytmów szyfrujących w celu zapewnienia zapewnionego poziomu bezpieczeństwa.

W systemach Windows, UNIX i Linux , WebSphere MQ, można skonfigurować w taki sposób, aby odpowiadał profilowi TLS 1.2 zgodnego z pakietem B, ale nie obsługuje profilu przejściowego Suite B. Więcej informacji zawiera sekcja “Szyfrowanie NSA Suite B Cryptography w produkcie IBM WebSphere MQ” na stronie 31.

Informacje pokrewne

“Standardy przetwarzania informacji federalnej” na stronie 20

Rząd USA wytwarza doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Narodowy Instytut Norm i Technologii (NIST) to ważny organ, którego dotyczą systemy informatyczne i bezpieczeństwo. Program NIST generuje rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

IBM WebSphere MQ mechanizmy zabezpieczeń

W tej kolekcji tematów wyjaśniono, w jaki sposób można zaimplementować różne koncepcje zabezpieczeń w produkcie IBM WebSphere MQ.

Produkt IBM WebSphere MQ udostępnia mechanizmy implementowania wszystkich pojęć związanych z bezpieczeństwem wprowadzonych w produkcie “Pojęcia i mechanizmy bezpieczeństwa” na stronie 5. Są one omówione bardziej szczegółowo w poniższych sekcjach.

Identyfikacja i uwierzytelnianie w produkcie IBM WebSphere MQ

W programie IBM WebSphere MQmożna zaimplementować identyfikację i uwierzytelnianie za pomocą informacji o kontekście komunikatów i wzajemnego uwierzytelniania.

Poniżej przedstawiono kilka przykładów identyfikacji i uwierzytelniania w środowisku IBM WebSphere MQ :

- Każdy komunikat może zawierać informacje o *kontekście komunikatu* . Te informacje są przechowywane w deskryptorze komunikatu. Może ona być generowana przez menedżer kolejek, gdy komunikat jest umieszczany w kolejce przez aplikację. Alternatywnie aplikacja może podać informacje, jeśli ID użytkownika powiązany z aplikacją jest uprawniony do wykonania tego zadania.

  Informacje o kontekście w komunikacie pozwalają aplikacji odbierającej na znalezienie informacji o inicjatorze komunikatu. Zawiera ona na przykład nazwę aplikacji umieszczonej w komunikacie oraz identyfikator użytkownika powiązany z aplikacją.
- Po uruchomieniu kanału komunikatów agent kanału komunikatów (MCA) na każdym końcu kanału może uwierzytelnić swojego partnera. Ta technika jest nazywana *wzajemnym uwierzytelnianiem*. Dla wysyłającego agenta MCA zapewnia on pewność, że partner, który ma wysłać wiadomości, jest autentyczny. W przypadku odbierającego agenta MCA istnieje podobne zapewnienie, że ma on otrzymywać wiadomości od prawdziwego partnera.

Pojęcia pokrewne

“Identyfikacja i uwierzytelnianie” na stronie 5
Identyfikacja to możliwość jednoznacznego identyfikowania użytkownika systemu lub aplikacji, która działa w systemie. *Uwierzytelnianie* to możliwość udowodnienia, że użytkownik lub aplikacja jest rzeczywiście osobą, która ta osoba lub aplikacja twierdzi, że jest.

Autoryzacja w produkcie IBM WebSphere MQ

Za pomocą autoryzacji można ograniczyć poszczególne osoby lub aplikacje, które mogą wykonywać w środowisku IBM WebSphere MQ .

Poniżej przedstawiono kilka przykładów autoryzacji w środowisku IBM WebSphere MQ :

- Zezwalanie tylko autoryzowanym administratorom na wydawanie komend do zarządzania zasobami produktu IBM WebSphere MQ .
- Zezwalanie aplikacji na połączenie z menedżerem kolejek tylko wtedy, gdy autoryzowany jest do tego ID użytkownika powiązany z aplikacją.
- Zezwalanie aplikacji na otwieranie tylko tych kolejek, które są niezbędne do jego działania.
- Zezwalanie aplikacji na subskrybowanie tylko tych tematów, które są niezbędne do jego działania.
- Zezwalanie aplikacji na wykonywanie tylko tych operacji w kolejce, które są niezbędne do jej działania. Na przykład aplikacja może wymagać tylko przeglądania komunikatów w określonej kolejce, a nie do umieszczania lub pobierania komunikatów.

Więcej informacji na temat konfigurowania autoryzacji zawiera sekcja “Planowanie autoryzacji” na stronie 51 i powiązane podtematy.

Pojęcia pokrewne

“Autoryzacja” na stronie 6
Autoryzacja chroni newralgiczne zasoby w systemie, ograniczając dostęp tylko do autoryzowanych użytkowników i ich aplikacji. Uniemożliwia to nieautoryzowane użycie zasobu lub użycie zasobu w nieautoryzowany sposób.

Kontrola w produkcie IBM WebSphere MQ

Program IBM WebSphere MQ może wystawiać komunikaty zdarzeń w celu zarejestrowania, że zajęła się nietypowa aktywność.

Poniżej przedstawiono kilka przykładów kontroli w środowisku IBM WebSphere MQ :

- Aplikacja próbuje otworzyć kolejkę, do której nie ma uprawnień do otwarcia. Zostanie wyświetlony komunikat zdarzenia instrumentacji. Sprawdzając komunikat o zdarzeniu, można wykryć, że ta próba wystąpiła i może podjąć decyzję o tym, jakie działanie jest konieczne.
- Aplikacja próbuje otworzyć kanał, ale próba nie powiodła się, ponieważ protokół SSL nie zezwala na nawiązanie połączenia. Zostanie wyświetlony komunikat zdarzenia instrumentacji. Sprawdzając komunikat o zdarzeniu, można wykryć, że ta próba wystąpiła i może podjąć decyzję o tym, jakie działanie jest konieczne.

Pojęcia pokrewne

“Kontrola” na stronie 6
Kontrolowanie jest procesem rejestrowania i sprawdzania zdarzeń w celu wykrycia, czy wystąpiło nieoczekiwane lub nieautoryzowane działanie, czy też podjęto próbę wykonania tego działania.

Poufność w produkcie IBM WebSphere MQ

Poufność w produkcie IBM WebSphere MQ można zaimplementować, szyfrując komunikaty.

Poniżej przedstawiono kilka przykładów zapewnienia poufności w środowisku IBM WebSphere MQ :

- Gdy wysyłający agent MCA pobiera komunikat z kolejki transmisji, program IBM WebSphere MQ używa protokołu SSL lub TLS do zaszyfrowania komunikatu przed wysłaniem go przez sieć do odbierającego agenta MCA. Na drugim końcu kanału komunikat jest deszyfrowany, zanim odbierający agent MCA umieszcza go w kolejce docelowej.
- Podczas zapisywania komunikatów w kolejce lokalnej mechanizmy kontroli dostępu udostępniane przez produkt IBM WebSphere MQ mogą być uznane za wystarczające do ochrony ich zawartości przed nieuprawnionym ujawnieniem. Jednak w przypadku większego poziomu zabezpieczeń można użyć programu IBM WebSphere MQ Advanced Message Security do zaszyfrowania komunikatów zapisanych w kolejkach.

Pojęcia pokrewne

“Poufność” na stronie 7
Usługa *poufności* zabezpiecza poufne informacje przed nieautoryzowanym ujawnieniem.

Integralność danych w produkcie IBM WebSphere MQ

Istnieje możliwość użycia usługi integralności danych w celu wykrycia, czy komunikat został zmodyfikowany.

Poniżej przedstawiono kilka przykładów, w jaki sposób można zapewnić integralność danych w środowisku IBM WebSphere MQ :

- Za pomocą protokołu SSL lub TLS można wykryć, czy treść komunikatu została celowo zmodyfikowana w czasie, gdy była przesyłana przez sieć. W protokole SSL i TLS algorytm streszczenia komunikatów umożliwia wykrywanie zmodyfikowanych komunikatów w tranzycie. Wszystkie obiekty CipherSpecs produktu IBM WebSphere MQ udostępniają algorytm tworzenia skrótu komunikatu, z wyjątkiem TLS_RSA_WITH_NULL_NULL, który nie zapewnia integralności danych komunikatu.

- Podczas zapisywania komunikatów w kolejce lokalnej mechanizmy kontroli dostępu udostępniane przez produkt IBM WebSphere MQ mogą być uważane za wystarczające, aby zapobiec celowej modyfikacji treści komunikatów. Jednak w przypadku większego poziomu zabezpieczeń można użyć programu IBM WebSphere MQ Advanced Message Security w celu wykrycia, czy treść komunikatu została celowo zmodyfikowana w okresie między umieszczonym w kolejce komunikatem a tym razem, gdy został on pobrany z kolejki.

Pojęcia pokrewne

“Integralność danych” na stronie 7
Usługa *integralności danych* wykrywa, czy nieautoryzowana modyfikacja danych została nieautoryzowana.

Kryptografia w produkcie IBM WebSphere MQ

Produkt IBM WebSphere MQ udostępnia kryptografię za pomocą protokołów SSL (Secure Sockets Layer) i TLS (Transport Security Layer).

Więcej informacji na ten temat zawiera sekcja “Protokoły zabezpieczeń w produkcie IBM WebSphere MQ” na stronie 23.

Pojęcia pokrewne

“Pojęcia kryptograficzne” na stronie 7
Ta kolekcja tematów zawiera opis pojęć związanych z kryptografią, które mają zastosowanie do produktu WebSphere MQ.

Protokoły zabezpieczeń w produkcie IBM WebSphere MQ

Produkt IBM WebSphere MQ obsługuje zarówno protokół TLS (Transport Layer Security), jak i protokoły SSL (Secure Sockets Layer) w celu zapewnienia bezpieczeństwa na poziomie łącza dla kanałów komunikatów i kanałów MQI.

Kanały komunikatów i kanały MQI mogą korzystać z protokołu SSL lub TLS w celu zapewnienia bezpieczeństwa na poziomie łącza.Program wywołujący MCA jest klientem protokołu SSL lub TLS, a agent odbierający MCA jest serwerem SSL lub TLS. Produkt WebSphere MQ obsługuje wersję 3.0 protokołu SSL oraz wersję 1.0 i wersję 1.2 protokołu TLS (Transport Layer Security). Użytkownik określa algorytmy szyfrowania, które są używane przez protokół SSL lub protokół przez podanie wartości CipherSpec jako części definicji kanału.

Na każdym końcu kanału komunikatów i na końcu serwera kanału MQI, agent MCA działa w imieniu menedżera kolejek, z którym jest połączony. Podczas uzgadniania SSL lub TLS agent MCA wysyła certyfikat cyfrowy menedżera kolejek do jego partnerskiego agenta MCA na drugim końcu kanału. Kod produktu WebSphere MQ na końcu klienta kanału MQI działa w imieniu użytkownika aplikacji klienckiej WebSphere MQ . Podczas uzgadniania protokołu SSL lub TLS kod produktu WebSphere MQ wysyła certyfikat cyfrowy użytkownika do agenta MCA na końcu kanału MQI.

Menedżery kolejek i użytkownicy klienta WebSphere MQ nie muszą mieć przypisanych osobistych certyfikatów cyfrowych, gdy działają jako klienci SSL lub TLS, chyba że wartość SSLCAUTH (REQUIRED) jest określona po stronie serwera kanału.

Certyfikaty cyfrowe są przechowywane w *repozytorium kluczy* . The queue manager attribute *SSLKeyRepository* specifies the location of the key repository that holds the queue manager's digital certificate. On a WebSphere MQ client system, the MQSSLKEYR environment variable specifies the location of the key repository that holds the user's digital certificate. Alternatywnie aplikacja kliencka WebSphere MQ może określić jej położenie w polu *KeyRepository* struktury opcji konfiguracji protokołu SSL i TLS, MQSCO w wywołaniu MQCONNX. Więcej informacji na temat repozytoriów kluczy zawierają tematy pokrewne, a także sposób określania miejsc, w których znajdują się te repozytoria.

Pojęcia pokrewne

“Protokoły zabezpieczeń szyfrujących: SSL i TLS” na stronie 14
Protokoły kryptograficzne zapewniają bezpieczne połączenia, umożliwiając dwóm stronom komunikowanie się z prywatnością i integralności danych. Protokół TLS (Transport Layer Security) wyewoluował z protokołu SSL (Secure Sockets Layer). Produkt IBM WebSphere MQ obsługuje zarówno protokół SSL, jak i TLS.

Obsługa protokołu SSL i TLS w produkcie IBM WebSphere MQ

Produkt IBM WebSphere MQ obsługuje zarówno protokół Secure Sockets Layer (SSL), jak i protokół TLS (Transport Layer Security).

Więcej informacji na temat protokołów SSL i TLS można znaleźć w temacie pokrewnej informacji.

Produkt IBM WebSphere MQ udostępnia następujące wsparcie dla protokołu SSL w wersji 3.0 i TLS 1.0 oraz TLS 1.2:

Klienty Java i JMS
Klienty te korzystają z maszyny JVM w celu zapewnienia obsługi protokołu SSL i TLS.

Systemy UNIX, Linux, and Windowsi HP Integrity NonStop Server
W systemach UNIX, Linux, and Windowsi HP Integrity NonStop Server obsługa protokołu SSL i TLS jest instalowana wraz z produktem IBM WebSphere MQ.

For information about any prerequisites for IBM WebSphere MQ SSL and TLS support, see Wymagania systemowe produktu IBM WebSphere MQ.

Repozytorium kluczy SSL lub TLS
Wzajemnie uwierzytelnione połączenie SSL lub TLS wymaga repozytorium kluczy (które może być znane za pomocą różnych nazw na różnych platformach) na każdym końcu połączenia. Repozytorium kluczy zawiera certyfikaty cyfrowe i klucze prywatne.

W tych informacjach używany jest ogólny termin *repozytorium kluczy* w celu opisania sklepu dla certyfikatów cyfrowych i powiązanych z nimi kluczy prywatnych. Konkretne nazwy sklepów używane na platformach i środowiskach obsługujących protokół SSL i TLS są następujące:

Java i JMS	magazyn kluczy i magazyn zaufanych certyfikatów
Windows UNIX Linux Windows UNIX Linux Systemy Windows , UNIX and Linux	plik bazy danych kluczy

Więcej informacji na ten temat można znaleźć w sekcji “certyfikaty cyfrowe” na stronie 9 i “Pojęcia związane z protokołem SSL (Secure Sockets Layer) i TLS (Transport Layer Security)” na stronie 15.

Wzajemnie uwierzytelnione połączenie SSL lub TLS wymaga repozytorium kluczy na każdym końcu połączenia. Repozytorium kluczy może zawierać:

- Liczba certyfikatów ośrodków certyfikacji (CA) z różnych ośrodków certyfikacji, które umożliwiają menedżerowi kolejek lub klientowi weryfikowanie certyfikatów, które otrzymuje od partnera na zdalnym końcu połączenia. Poszczególne certyfikaty mogą znajdować się w łańcuchu certyfikatów.
- Jeden lub więcej certyfikatów osobistych otrzymanych od ośrodka certyfikacji. Istnieje możliwość powiązania osobnego certyfikatu osobistego z każdym menedżerem kolejek lub klientem MQI produktu WebSphere MQ . Certyfikaty osobiste są niezbędne w przypadku klienta SSL lub TLS, jeśli wymagane jest uwierzytelnianie wzajemne. Jeśli uwierzytelnianie wzajemne nie jest wymagane, certyfikaty osobiste nie są wymagane na kliencie. Repozytorium kluczy może również zawierać klucz prywatny odpowiadający każdemu certyfikatowi osobistą.
- Żądania certyfikatów, które oczekują na podpisanie przez zaufany certyfikat ośrodka CA.

Więcej informacji na temat ochrony repozytorium kluczy zawiera sekcja “Zabezpieczanie repozytoriów kluczy produktu IBM WebSphere MQ” na stronie 25.

Położenie repozytorium kluczy zależy od platformy używanej przez użytkownika:

Windows UNIX Linux **Systemy Windows, UNIX and Linux**
W systemach Windows, systemy UNIX and Linux to repozytorium kluczy, które jest plikiem bazy danych kluczy. Nazwa pliku bazy danych kluczy musi mieć rozszerzenie `.kdb`. Na przykład, w systemie UNIX and Linuxdomyślnym plikiem bazy danych kluczy dla menedżera kolejek `QM1` jest `/var/mqm/`

qmgrs/QM1/ssl/key.kdb . Jeśli produkt IBM WebSphere MQ jest zainstalowany w położeniu domyślnym, równoważną ścieżką w systemie Windows jest C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\key.kdb.

W systemach Windows , UNIX and Linux każdy plik bazy danych kluczy ma powiązany plik ukrytych haseł. Ten plik przechowuje zakodowane hasła, które umożliwiają programom dostęp do bazy danych kluczy. Plik ukrytych haseł musi znajdować się w tym samym katalogu i mieć ten sam plik macierzysty, co baza danych kluczy, i musi kończyć się przyrostkiem .sth , na przykład /var/mqm/qmgrs/QM1/ssl/key.sth

Uwaga: W systemach Windows, UNIX and Linux karty sprzętowe szyfrujące PKCS #11 mogą zawierać certyfikaty i klucze, które w przeciwnym razie znajdują się w pliku bazy danych kluczy. Jeśli certyfikaty i klucze są przechowywane na kartach #11 PKCS, produkt WebSphere MQ nadal wymaga dostępu do pliku bazy danych kluczy oraz pliku ukrytych haseł.

W systemach Windows i UNIX baza danych kluczy zawiera również klucz prywatny dla certyfikatu osobistego powiązanego z menedżerem kolejek lub klientem MQI produktu WebSphere MQ .

Zabezpieczanie repozytoriów kluczy produktu IBM WebSphere MQ
Repozytorium kluczy dla produktu IBM WebSphere MQ jest plikiem. Upewnij się, że tylko zamierzony użytkownik może uzyskać dostęp do pliku repozytorium kluczy. Zapobiega to włamaniowi lub innemu nieautoryzowanemu użytkownikowi, który kopiuje plik repozytorium kluczy do innego systemu, a następnie skonfigurowanie identycznego identyfikatora użytkownika w tym systemie w celu podszykowania się z zamierzonego użytkownika.

Uprawnienia do plików zależą od umask użytkownika i tego, które narzędzie jest używane. W systemie Windowskonta IBM WebSphere MQ wymagają uprawnień BypassTraverseChecking , co oznacza, że uprawnienia do folderów w ścieżce do pliku nie mają żadnego wpływu.

Sprawdź uprawnienia do plików repozytorium kluczy i upewnij się, że pliki i folder zawierający pliki nie są czytelne dla świata, a najlepiej nie można go odczytać z grupy.

Tworzenie magazynu kluczy w trybie tylko do odczytu jest dobrą praktyką, w zależności od tego, który system jest używany, przy czym tylko administrator może włączyć operacje zapisu w celu przeprowadzenia konserwacji.

W praktyce należy chronić wszystkie magazyny kluczy, niezależnie od tego, czy są one chronione hasłem, czy też nie, chronią repozytoria kluczy.

Odświeżanie repozytorium kluczy menedżera kolejek
Po zmianie treści repozytorium kluczy menedżer kolejek nie pobierze od razu nowej treści. Aby menedżer kolejek był używany z nową treścią repozytorium kluczy, należy wydać komendę REFRESH SECURITY TYPE (SSL).

Ten proces jest zamierzony i zapobiega sytuacji, w której wiele działających kanałów może używać różnych wersji repozytorium kluczy. Jako kontrola zabezpieczeń menedżer kolejek może w dowolnej chwili załadować tylko jedną wersję repozytorium kluczy.

Więcej informacji na temat komendy REFRESH SECURITY TYPE (SSL) zawiera sekcja REFRESH SECURITY(REFRESH SECURITY).

Repozytorium kluczy można również odświeżyć za pomocą komend PCF lub programu WebSphere MQ Explorer. Więcej informacji na ten temat zawiera publikacja MQCMD_REFRESH_SECURITY, komenda oraz temat *Odświeżanie zabezpieczeń SSL lub TLS* w sekcji WebSphere MQ Explorer w tej dokumentacji produktu.

Pojęcia pokrewne
“Odświeżanie widoku zawartości repozytorium kluczy SSL i ustawień protokołu SSL przez klienta” na stronie 26
Aby zaktualizować aplikację kliencką przy użyciu odświeżonej treści repozytorium kluczy, należy zatrzymać i zrestartować aplikację kliencką.

Odświeżanie widoku zawartości repozytorium kluczy SSL i ustawień protokołu SSL przez klienta
Aby zaktualizować aplikację kliencką przy użyciu odświeżonej treści repozytorium kluczy, należy zatrzymać i zrestartować aplikację kliencką.

Nie można odświeżyć zabezpieczeń na kliencie WebSphere MQ ; w przypadku klientów nie ma odpowiednika komendy REFRESH SECURITY TYPE (SSL) (więcej informacji na ten temat zawiera sekcja REFRESH SECURITY).

Aby zaktualizować aplikację kliencką przy użyciu odświeżonej treści repozytorium kluczy, należy zatrzymać i ponownie uruchomić aplikację po każdej zmianie certyfikatu bezpieczeństwa.

Jeśli restartowanie kanału zostanie odświeżone, a aplikacja ma logikę ponownego połączenia, możliwe jest odświeżenie zabezpieczeń na kliencie, wydając komendę STOP CHL STATUS (INACTIVE).

Pojęcia pokrewne

“Odświeżanie repozytorium kluczy menedżera kolejek” na stronie 25
Po zmianie treści repozytorium kluczy menedżer kolejek nie pobierze od razu nowej treści. Aby menedżer kolejek był używany z nową treścią repozytorium kluczy, należy wydać komendę REFRESH SECURITY TYPE (SSL).

Standardy FIPS (Federal Information Processing Standards)
Ten temat zawiera wprowadzenie do standardu FIPS (Federal Information Processing Standards) Cryptomodule Validation Program of the US National Institute of Standards and Technology oraz funkcji szyfrujących, które mogą być używane w kanałach SSL lub TLS, w systemach Windows, UNIX and Linuxi z/OS .

Zgodność z FIPS 140-2 połączenia IBM WebSphere MQ SSL lub TLS w systemach UNIX, Linuxi Windows znajduje się w tym miejscu “FIPS (Federal Information Processing Standards) dla systemów UNIX, Linuxi Windows” na stronie 27.

Jeśli sprzęt szyfrujący jest obecny, moduły kryptograficzne używane przez produkt IBM WebSphere MQ mogą być skonfigurowane tak, aby były dostarczane przez producenta sprzętu. W takim przypadku konfiguracja jest zgodna ze standardem FIPS, jeśli te moduły szyfrujące są certyfikowane przez FIPS.

Z biegiem czasu, federalne standardy przetwarzania informacji są aktualizowane, aby odzwierciedlić nowe ataki na algorytmy szyfrowania i protokoły. Na przykład niektóre obiekty CipherSpecs mogą przestać być certyfikowane przez FIPS. Gdy takie zmiany wystąpią, produkt IBM WebSphere MQ jest również aktualizowany w celu zaimplementowania najnowszego standardu. W rezultacie po zastosowaniu konserwacji mogą być widoczne zmiany w zachowaniu.

Pojęcia pokrewne

“Określanie, że w czasie wykonywania w kliencie MQI są używane tylko specyfikacje CipherSpecs z certyfikatem FIPS” na stronie 112
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi korzystać z certyfikatów CipherSpecsz certyfikatem FIPS.

“Korzystanie z komendy iKeyman, iKeycmd, runmqakm i runmqckm” na stronie 118
W systemach UNIX, Linux i Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą interfejsu GUI programu iKeyman lub z poziomu wiersza komend za pomocą komendy iKeycmd lub runmqakm.

Zadania pokrewne

Włączanie protokołu SSL w klasach produktu WebSphere MQ dla języka Java

Korzystanie z protokołu SSL (Secure Sockets Layer) z klasami produktu WebSphere MQ dla usługi JMS

Odsyłacze pokrewne

Właściwości SSL obiektów JMS

Informacje pokrewne

“Standardy przetwarzania informacji federalnej” na stronie 20
Rząd USA wytwarza doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Narodowy Instytut Norm i Technologii (NIST) to ważny organ, którego dotyczą systemy informatyczne i bezpieczeństwo. Program NIST generuje rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

FIPS (Federal Information Processing Standards) dla systemów UNIX, Linuxi Windows
Jeśli szyfrowanie jest wymagane w kanale SSL lub TLS w systemach Windowsi UNIX and Linux , produkt WebSphere MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach Windowsi UNIX and Linux oprogramowanie ICC przeszło program sprawdzania poprawności Cryptomodule FIPS (Federal Information Processing Standards) w Instytucie Standardów i Technologii Stanów Zjednoczonych (poziom 140-2).

Zgodność ze standardem FIPS 140-2 połączenia WebSphere MQ SSL lub TLS w systemach Windowsi UNIX and Linux jest następująca:

- Dla wszystkich kanałów komunikatów IBM WebSphere MQ (z wyjątkiem kanałów typu CLNTCONN) połączenie jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja pakietu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 w zainstalowanej wersji systemu operacyjnego i architekturze sprzętowej.
  - Atrybut SSLFIPS menedżera kolejek został ustawiony na wartość YES.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
- Dla wszystkich aplikacji klienckich MQI produktu IBM WebSphere MQ połączenie korzysta z pakietu GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja pakietu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 w zainstalowanej wersji systemu operacyjnego i architekturze sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w temacie pokrewnym dotyczącym klienta MQI.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
- W przypadku klas IBM WebSphere MQ dla aplikacji Java korzystających z trybu klienta połączenie używa implementacji SSL i TLS środowiska JRE i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Środowisko Java Runtime Environment używane do uruchamiania aplikacji jest zgodne ze standardem FIPS dla zainstalowanej wersji systemu operacyjnego i architektury sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w temacie pokrewnym dotyczącym klienta Java.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
- W przypadku klas IBM WebSphere MQ dla aplikacji JMS korzystających z trybu klienta połączenie używa implementacji SSL i TLS środowiska JRE i jest zgodne ze standardami FIPS, jeśli spełnione są następujące warunki:
  - Środowisko Java Runtime Environment używane do uruchamiania aplikacji jest zgodne ze standardem FIPS dla zainstalowanej wersji systemu operacyjnego i architektury sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w temacie pokrewnym dotyczącym klienta JMS.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
- W przypadku niezarządzanych aplikacji klienckich .NET połączenie używa pakietu GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja pakietu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 w zainstalowanej wersji systemu operacyjnego i architekturze sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w temacie pokrewnym dotyczącym klienta .NET.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .

- Dla niezarządzanych aplikacji klienckich .NET XMS połączenie używa pakietu GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja pakietu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 w zainstalowanej wersji systemu operacyjnego i architekturze sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w dokumentacji środowiska .NET XMS .
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .

Wszystkie obsługiwane platformy AIX, Linux, HP-UX, Solaris, Windowsi z/OS mają certyfikat FIPS 140-2, z wyjątkiem przypadków opisanych w pliku readme dołączonym do każdego pakietu poprawek lub pakietu aktualizacyjnego.

W przypadku połączeń SSL i TLS z użyciem pakietu GSKit komponent z certyfikatem FIPS 140-2 ma nazwę *ICC*. Jest to wersja tego komponentu, która określa zgodność pakietu GSKit ze standardem FIPS na dowolnej platformie. Aby określić aktualnie zainstalowaną wersję ICC, uruchom komendę **dspmqver -p 64 -v** .

Poniżej przedstawiono przykładowy fragment danych wyjściowych komendy **dspmqver -p 64 -v** dotyczących programu ICC:

```
  icc
 ============
@ (#)CompanyName: IBM Corporation
@(#)LegalTrademarks:  IBM
@ (#)FileDescription: IBM Crypto for C-language
@(#)FileVersion:      8.0.0.0
@ (#)LegalCopyright: Licensed Materials-Property of IBM
@ (#) ICC
@ (#) (C) Copyright IBM Corp. 2002, 2024.
@ (#) Wszelkie prawa zastrzeżone. Użytkownicy instytucji rządowych USA
@ (#) Zastrzeżone prawa-Używanie, powielanie lub ujawnianie
@ (#) zastrzeżone kontraktem GSA ADP Schedule Contract z IBM Corp.
@ (#)ProductName: icc_8.0 (GoldCoast Build) 100415
@(#)ProductVersion:   8.0.0.0
@(#)ProductInfo:      10/04/15.03:32:19.10/04/15.18:41:51
@ (#) CMVCInfo:
```

Instrukcję certyfikacji NIST dla pakietu GSKit ICC 8 (dołączonego do pakietu GSKit 8) można znaleźć pod następującym adresem: Cryptographic Module Validation Program(Program sprawdzania poprawności modułu szyfrującego).

Jeśli sprzęt szyfrujący jest obecny, moduły szyfrujące używane przez IBM WebSphere MQ można skonfigurować w taki sposób, aby były dostarczane przez producenta sprzętu. W takim przypadku konfiguracja jest zgodna ze standardem FIPS tylko wtedy, gdy te moduły szyfrujące mają certyfikat FIPS.

Uwaga: Działanie 32-bitowych klientów SSL i TLS systemu Solaris x86 skonfigurowanych na potrzeby operacji zgodnych ze standardem FIPS 140-2 zakończy się niepowodzeniem w przypadku uruchomienia w systemie z procesorem Intel. To niepowodzenie występuje, ponieważ 32-bitowy plik biblioteki GSKit-Crypto systemu Solaris x86 zgodny ze standardem FIPS 140-2 nie jest ładowany w układzie Intel. W systemach, których to dotyczy, w dzienniku błędów klienta zgłaszany jest błąd AMQ9655. Aby rozwiązać ten problem, należy wyłączyć zgodność ze standardem FIPS 140-2 lub ponownie skompilować aplikację kliencką w formacie 64-bitowym, ponieważ problem ten nie dotyczy kodu 64-bitowego.

Potrójne ograniczenia DES wymuszane podczas pracy zgodnie ze standardem FIPS 140-2

Jeśli produkt WebSphere MQ jest skonfigurowany do działania zgodnie ze standardem FIPS 140-2, dodatkowe ograniczenia są wymuszane w odniesieniu do CipherSpecsTriple DES (3DES). Te ograniczenia umożliwiają zachowanie zgodności z zaleceniem US NIST SP800-67 .

1. Wszystkie części klucza Triple DES muszą być unikalne.
2. Żadna część potrójnego klucza DES nie może być kluczem słabym, półsłabym lub ewentualnie słabym zgodnie z definicjami w NIST SP800-67.

3. Przed zresetowaniem klucza tajnego nie można przesłać więcej niż 32 GB danych za pośrednictwem połączenia. Domyślnie produkt WebSphere MQ nie resetuje tajnego klucza sesji, dlatego ten reset musi być skonfigurowany. Jeśli podczas używania Triple DES CipherSpec i zgodności ze standardem FIPS 140-2 nie zostanie włączony reset klucza tajnego, połączenie zostanie zamknięte z błędem AMQ9288 po przekroczeniu maksymalnej liczby bajtów. Więcej informacji na temat konfigurowania resetowania klucza tajnego zawiera sekcja “Resetowanie kluczy tajnych SSL i TLS” na stronie 232.

Produkt WebSphere MQ generuje klucze sesji Triple DES, które są już zgodne z regułami 1 i 2. Aby jednak spełnić trzecie ograniczenie, należy włączyć resetowanie klucza tajnego podczas używania algorytmu szyfrowania Triple DES CipherSpecs w konfiguracji FIPS 140-2. Można również uniknąć używania potrójnego algorytmu szyfrowania DES.

Pojęcia pokrewne

“Określanie, że w czasie wykonywania w kliencie MQI są używane tylko specyfikacje CipherSpecs z certyfikatem FIPS” na stronie 112
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi korzystać z certyfikatów CipherSpecsz certyfikatem FIPS.

“Korzystanie z komendy iKeyman, iKeycmd, runmqakm i runmqckm” na stronie 118
W systemach UNIX, Linux i Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą interfejsu GUI programu iKeyman lub z poziomu wiersza komend za pomocą komendy iKeycmd lub runmqakm.

Zadania pokrewne

Włączanie protokołu SSL w klasach WebSphere MQ dla języka Java

Używanie protokołu SSL (Secure Sockets Layer) z klasami WebSphere MQ dla usługi JMS

Odsyłacze pokrewne

Właściwości SSL obiektów JMS

Informacje pokrewne

“Standardy przetwarzania informacji federalnej” na stronie 20
Rząd USA wytwarza doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Narodowy Instytut Norm i Technologii (NIST) to ważny organ, którego dotyczą systemy informatyczne i bezpieczeństwo. Program NIST generuje rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

SSL i TLS na kliencie MQI produktu IBM WebSphere MQ

Produkt IBM WebSphere MQ obsługuje protokół SSL i TLS na klientach. Korzystanie z protokołu SSL lub TLS można dostosować na różne sposoby.

Produkt IBM WebSphere MQ udostępnia obsługę protokołu SSL i TLS dla klientów MQI produktu IBM WebSphere MQ w systemach Windows, UNIX and Linux . Jeśli używane są klasy produktu IBM WebSphere MQ dla języka Java, należy zapoznać się z sekcji Korzystanie z klas produktu WebSphere MQ dla języka Java , a jeśli używane są klasy produktu IBM WebSphere MQ dla usługi JMS, należy zapoznać się z sekcji Korzystanie z klas produktu WebSphere MQ dla usługi JMS. Pozostała część tej sekcji nie ma zastosowania do środowisk Java lub JMS.

Repozytorium kluczy dla klienta MQI produktu IBM WebSphere MQ można określić za pomocą wartości MQSSLKEYR w pliku konfiguracyjnym klienta produktu IBM WebSphere MQ lub w momencie wywołania przez aplikację wywołania MQCONNX. Dostępne są trzy opcje określające, że kanał używa protokołu SSL:

- Korzystanie z tabeli definicji kanału
- Korzystanie z struktury opcji konfiguracji protokołu SSL, MQSCO, w wywołaniu MQCONNX
- Korzystanie z Active Directory (w systemach Windows)

Nie można użyć zmiennej środowiskowej MQSERVER do określenia, że kanał używa protokołu SSL.

Można kontynuować uruchamianie istniejących aplikacji klienckich MQI produktu IBM WebSphere MQ bez użycia protokołu SSL, o ile protokół SSL nie zostanie określony na drugim końcu kanału.

Jeśli na komputerze klienta zostaną wprowadzone zmiany do zawartości repozytorium kluczy SSL, położenia repozytorium kluczy SSL, informacji uwierzytelniających lub parametrów sprzętu szyfrującego, należy zakończyć wszystkie połączenia SSL, aby odzwierciedlić te zmiany w kanałach połączenia

klienckiego, które aplikacja używa do łączenia się z menedżerem kolejek. Po zakończeniu wszystkich połączeń zrestartuj kanały SSL. Zostaną użyte wszystkie nowe ustawienia SSL. Te ustawienia są analogiczne do tych, które zostały odświeżone przy użyciu komendy REFRESH SECURITY TYPE (SSL) w systemach menedżera kolejek.

Gdy klient MQI produktu IBM WebSphere MQ działa w systemie Windows, system UNIX and Linux ze sprzętem szyfrującym, konfiguruje ten sprzęt za pomocą zmiennej środowiskowej MQSSLCRYP. Ta zmienna jest równoważna parametrowi SSLCRYP w komendzie ALTER QMGR MQSC. Opis parametru SSLCRYP komendy ALTER QMGR MQSC można znaleźć w opisie komendy ALTER QMGR . Jeśli używana jest wersja GSK_PCS11 parametru SSLCRYP, etykieta znacznika PKCS #11 musi być określona w całości w dolnej części sprawy.

Resetowanie klucza tajnego SSL i FIPS są obsługiwane w klientach MQI produktu IBM WebSphere MQ . Więcej informacji na ten temat zawierają sekcje “Resetowanie kluczy tajnych SSL i TLS” na stronie 232 i “FIPS (Federal Information Processing Standards) dla systemów UNIX, Linuxi Windows” na stronie 27.

Więcej informacji na temat obsługi protokołu SSL dla klientów MQI produktu IBM WebSphere MQ zawiera sekcja “Konfigurowanie zabezpieczeń klienta MQI produktu IBM WebSphere MQ” na stronie 111 .

Zadania pokrewne

Konfigurowanie klienta przy użyciu pliku konfiguracyjnego

Określanie, czy kanał MQI używa protokołu SSL

Aby kanał MQI mógł używać protokołu SSL, wartość atrybutu *SSLCipherSpec* kanału połączenia klienckiego musi być nazwą CipherSpec , która jest obsługiwana przez produkt IBM WebSphere MQ na platformie klienckiej.

Można zdefiniować kanał połączenia klienckiego z wartością dla tego atrybutu w jeden z następujących sposobów. Są one wymienione w kolejności malejącej kolejności.

1. Gdy wyjście PreConnect udostępnia strukturę definicji kanału, która ma być używana.

   Wyjście PreConnect może zawierać nazwę obiektu CipherSpec w polu *SSLCipherSpec* struktury definicji kanału, MQCD. Ta struktura jest zwracana w polu **ppMQCDArrayPtr** struktury parametru wyjścia MQNXP używanej przez program obsługi wyjścia PreConnect .

2. Gdy aplikacja kliencka MQI produktu WebSphere MQ wysyła wywołanie MQCONNX.

   Aplikacja może określić nazwę specyfikacji CipherSpec w polu *SSLCipherSpec* struktury definicji kanału, MQCD.Ta struktura jest przywoływana przez strukturę opcji łączenia, MQCNO, która jest parametrem w wywołaniu MQCONNX.

3. Korzystanie z tabeli definicji kanału klienta (CCDT).

   Co najmniej jedna pozycja w tabeli definicji kanału klienta może określać nazwę obiektu CipherSpec.Na przykład, jeśli zostanie utworzony wpis za pomocą komendy DEFINE CHANNEL MQSC, można użyć parametru SSLCIPH w komendzie w celu określenia nazwy CipherSpec.

4. Korzystanie z Active Directory w systemie Windows.

   W systemach Windows można użyć komendy sterującej **setmqscp** w celu opublikowania definicji kanału połączenia klienckiego w katalogu Active Directory. Co najmniej jedna z tych definicji może określać nazwę obiektu CipherSpec.

Na przykład, jeśli aplikacja kliencka udostępnia definicję kanału połączenia klienckiego w strukturze MQCD w wywołaniu MQCONNX, ta definicja jest używana w preferencjach do wszystkich wpisów w tabeli definicji kanału klienta, do których dostęp może uzyskać klient WebSphere MQ .

Nie można użyć zmiennej środowiskowej MQSERVER w celu udostępnienia definicji kanału na końcu klienta kanału MQI, który używa protokołu SSL.

Aby sprawdzić, czy certyfikat klienta ma przepływ, należy wyświetlić status kanału na końcu kanału w celu uzyskania wartości parametru nazwy węzła sieci.

Pojęcia pokrewne

“Określanie specyfikacji CipherSpec dla klienta MQI produktu IBM WebSphere MQ” na stronie 231

Dostępne są trzy opcje określania wartości CipherSpec dla klienta MQI produktu IBM WebSphere MQ .

CipherSpecs i CipherSuites w podręczniku IBM WebSphere MQ
Produkt IBM WebSphere MQ obsługuje zarówno algorytmy SSL, jak i TLS CipherSpecs, a także algorytmy RSA i Diffie-Hellman.

Produkt WebSphere MQ obsługuje protokoły SSL V3 i TLS V1.0 i V1.2 CipherSpecs.

Produkt WebSphere MQ obsługuje algorytmy wymiany kluczy RSA i Diffie-Hellmana oraz algorytmy uwierzytelniania. Wielkość klucza używanego podczas uzgadniania SSL może zależeć od używanego certyfikatu cyfrowego, ale niektóre atrybuty CipherSpecs zawierają specyfikację wielkości klucza uzgadniania. Klucze uzgadniania o większej długości zapewniają silniejsze uwierzytelnianie. Natomiast w przypadku kluczy o mniejszej długości uzgadnianie przebiega szybciej.

Pojęcia pokrewne
“CipherSpecs i CipherSuites” na stronie 18
Protokoły zabezpieczeń szyfrujących muszą być zgodne z algorytmami używannymi przez bezpieczne połączenie. Atrybuty CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

Szyfrowanie NSA Suite B Cryptography w produkcie IBM WebSphere MQ
Ta sekcja zawiera informacje na temat konfigurowania produktu IBM WebSphere MQ w systemach Windows, Linuxi UNIX w taki sposób, aby były zgodne z profilem TLS 1.2 zgodnym z pakietem Suite B.

Z biegiem czasu standard NSA Cryptography Suite B Standard jest aktualizowany w celu odzwierciedlenia nowych ataków na algorytmy szyfrowania i protokoły. Na przykład niektóre obiekty CipherSpecs mogą przestać być certyfikowane Suite B. Gdy takie zmiany wystąpią, produkt IBM WebSphere MQ jest również aktualizowany w celu zaimplementowania najnowszego standardu. W rezultacie po zastosowaniu konserwacji mogą być widoczne zmiany w zachowaniu. Plik readme produktu IBM WebSphere MQ Version 7.5 zawiera listę wersji pakietu B wymuszoną przez każdy poziom konserwacyjny produktu. Jeśli produkt IBM WebSphere MQ został skonfigurowany do wymuszania zgodności z pakietem B, należy zawsze zapoznać się z plikiem readme podczas planowania stosowania konserwacji (patrz IBM MQ, WebSphere MQi MQSeries-READMEs).

W systemach Windows, UNIXi Linux można skonfigurować produkt IBM WebSphere MQ w taki sposób, aby odpowiadał profilowi TLS 1.2 zgodnego z pakietem B, na poziomie bezpieczeństwa przedstawionym w tabeli 1.

Tabela 1. Poziomy zabezpieczeń Suite B z dozwolonymi algorytmami CipherSpecs i podpisami cyfrowymi

Poziom zabezpieczeń	**Dozwolone CipherSpecs**	**Dozwolone algorytmy podpisu cyfrowego**
128 bitów	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA z SHA-256 ECDSA z SHA-384
192 bity	ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA z SHA-384
Oba[1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA z SHA-256 ECDSA z SHA-384

1. Możliwe jest jednoczesne skonfigurowanie zarówno poziomu 128-bitowego, jak i 192-bitowego. Ponieważ konfiguracja Suite B określa minimalne akceptowalne algorytmy szyfrowania, konfigurowanie obu poziomów zabezpieczeń jest równoznaczne z konfigurowaniem tylko 128-bitowego poziomu zabezpieczeń. Algorytmy kryptograficzne 192-bitowego poziomu bezpieczeństwa są silniejsze od minimum wymaganego dla 128-bitowego poziomu bezpieczeństwa, dlatego są dozwolone dla 128-bitowego poziomu bezpieczeństwa nawet wtedy, gdy poziom bezpieczeństwa 192 bitów nie jest włączony.

Uwaga: Konwencje nazewnictwa używane dla opcji Poziom zabezpieczeń niekoniecznie reprezentują wielkość krzywej eliptycznej lub wielkość klucza algorytmu szyfrowania AES.

Konformacja CipherSpec do pakietu B

Mimo że domyślne działanie produktu IBM WebSphere MQ nie jest zgodne ze standardem Suite B, produkt IBM WebSphere MQ można skonfigurować w taki sposób, aby był zgodny albo z dwoma poziomami zabezpieczeń w systemach Windows, UNIX i Linux . Po pomyślnej konfiguracji produktu IBM WebSphere MQ w celu użycia pakietu Suite B każda próba uruchomienia kanału wychodzącego za pomocą specyfikacji CipherSpec , która nie jest zgodna z pakietem Suite B, powoduje błąd AMQ9282. To działanie powoduje również zwrócenie przez klienta MQI kodu przyczyny MQRC_CIPHER_SPEC_NOT_SUITE_B. Podobnie próba uruchomienia kanału danych przychodzących przy użyciu specyfikacji CipherSpec , która nie jest zgodna z konfiguracją pakietu B, powoduje wystąpienie błędu AMQ9616.

Więcej informacji na temat produktu WebSphere MQ CipherSpecszawiera sekcja “Określanie CipherSpecs” na stronie 225 .

Pakiet B i certyfikaty cyfrowe

Pakiet B ogranicza algorytmy podpisu cyfrowego, które mogą być używane do podpisywania certyfikatów cyfrowych. Pakiet B ogranicza również typ klucza publicznego, który może zawierać certyfikaty. Dlatego produkt WebSphere MQ musi być skonfigurowany tak, aby używać certyfikatów, których algorytm podpisu cyfrowego i typ klucza publicznego są dozwolone przez skonfigurowany poziom zabezpieczeń Suite B skonfigurowanego partnera zdalnego. Certyfikaty cyfrowe, które nie są zgodne z wymaganiami dotyczącymi poziomu zabezpieczeń, są odrzucane, a połączenie kończy się niepowodzeniem z błędem AMQ9633 lub AMQ9285.

W przypadku 128-bitowego poziomu zabezpieczeń Suite B klucz publiczny obiektu certyfikatu jest wymagany do użycia krzywej eliptycznej NIST P-256 lub krzywej eliptycznej NIST P-384 i do podpisania z krzywą eliptyczną NIST P-256 lub krzywą eliptyczną NIST P-384 . Na poziomie zabezpieczeń 192-bit Suite B klucz publiczny obiektu certyfikatu jest wymagany do użycia krzywej eliptycznej NIST P-384 i do podpisania z krzywą eliptyczną NIST P-384 .

Aby uzyskać certyfikat odpowiedni dla operacji zgodnej ze standardem Suite B, należy użyć komendy **runmqakm** i podać parametr **-sig_alg** , aby zażądać odpowiedniego algorytmu podpisu cyfrowego. The EC_ecdsa_with_SHA256 and EC_ecdsa_with_SHA384 **-sig_alg** parameter values correspond to elliptic curve keys signed by the allowed Suite B digital signature algorithms.

Więcej informacji na temat komendy **runmqakm** można znaleźć w sekcji runmqckm i runmqakm options.

Uwaga: Narzędzia **iKeycmd** i **iKeyman** nie obsługują tworzenia certyfikatów cyfrowych dla operacji zgodnych ze standardem Suite B.

Tworzenie i wysyłanie żądań certyfikatów cyfrowych

Informacje na temat tworzenia samopodpisanego certyfikatu cyfrowego na potrzeby testowania Suite B zawiera sekcja “Tworzenie samopodpisanego certyfikatu osobistego w systemach UNIX, Linux, and Windows” na stronie 126 .

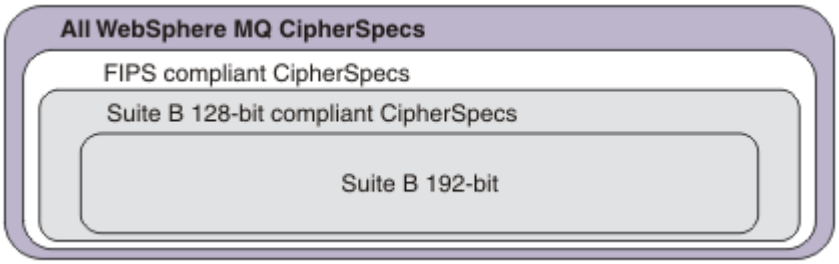
Więcej informacji na temat używania certyfikatu cyfrowego podpisanego przez ośrodek CA na potrzeby produkcji Suite B można znaleźć w sekcji “Żądanie certyfikatu osobistego w systemach UNIX, Linux, and Windows” na stronie 128.

Uwaga: Używany ośrodek certyfikacji musi generować certyfikaty cyfrowe, które spełniają wymagania opisane w dokumencie IETF RFC 6460.

FIPS 140-2 i Suite B

Standard Suite B jest koncepcyjnie podobny do standardu FIPS 140-2, ponieważ ogranicza on zestaw włączonych algorytmów szyfrujących w celu zapewnienia gwarantowanego poziomu bezpieczeństwa. Obecnie obsługiwany pakiet B CipherSpecs może być używany, gdy produkt IBM WebSphere MQ jest skonfigurowany do obsługi zgodnej ze standardem FIPS 140-2. Dlatego też możliwe jest skonfigurowanie produktu WebSphere MQ zarówno dla zgodności ze standardami FIPS, jak i pakietu B jednocześnie, w takim przypadku mają zastosowanie oba zestawy ograniczeń.

Na poniższym diagramie przedstawiono relacje między tymi



podzbiorami:

Konfigurowanie działania zgodnego z produktem WebSphere MQ for Suite B

Informacje na temat konfigurowania produktu IBM WebSphere MQ w systemie Windows, UNIX i Linux dla operacji zgodnych z pakietem Suite B zawiera sekcja “Konfigurowanie produktu IBM WebSphere MQ dla pakietu B” na stronie 33.

Produkt IBM WebSphere MQ nie obsługuje operacji zgodnych ze standardem Suite B na platformach IBM i i z/OS . Klienty Java i JMS produktu WebSphere MQ również nie obsługują operacji zgodnych ze standardem Suite B.

Pojęcia pokrewne

“Określanie, że w czasie wykonywania w kliencie MQI są używane tylko specyfikacje CipherSpecs z certyfikatem FIPS” na stronie 112
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi korzystać z certyfikatów CipherSpecsz certyfikatem FIPS.

Konfigurowanie produktu IBM WebSphere MQ dla pakietu B
Produkt IBM WebSphere MQ można skonfigurować w taki sposób, aby działał zgodnie ze standardem NSA Suite B w systemach UNIX, Linux, and Windows .

Pakiet B ogranicza zestaw włączonych algorytmów szyfrujących w celu zapewnienia zapewnionego poziomu zabezpieczeń. IBM WebSphere MQ można skonfigurować w taki sposób, aby działał zgodnie z pakietem B w celu zapewnienia zwiększonego poziomu bezpieczeństwa. Więcej informacji na temat pakietu Suite B można znaleźć w sekcji “National Security Agency (NSA) Suite B Cryptography” na stronie 20. Więcej informacji na temat konfiguracji Suite B oraz jego wpływu na kanały SSL i TLS można znaleźć w sekcji “Szyfrowanie NSA Suite B Cryptography w produkcie IBM WebSphere MQ” na stronie 31.

Menedżer kolejek

W przypadku menedżera kolejek należy użyć komendy **ALTER QMGR** z parametrem **SUITEB** , aby ustawić wartości odpowiednie dla wymaganego poziomu zabezpieczeń. Więcej informacji na ten temat zawiera sekcja ALTER QMGR.

Można również użyć komendy PCF **MQCMD_CHANGE_Q_MGR** z parametrem **MQIA_SUITE_B_STRENGTH** w celu skonfigurowania menedżera kolejek dla operacji zgodnej ze standardem Suite B.

MQI client

Klienty MQI domyślnie nie wymuszają zgodności z pakietem B. Istnieje możliwość włączenia klienta MQI dla zgodności z pakietem B, wykonując jedną z poniższych opcji:

1. Poprzez ustawienie pola **EncryptionPolicySuiteB** w strukturze MQSCO w wywołaniu MQCONNX do jednej lub większej liczby poniższych wartości:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   Użycie wartości MQ_SUITE_B_NONE z dowolną inną wartością jest niepoprawne.

2. Ustawiając zmienną środowiskową MQSUITEB na jedną lub więcej spośród poniższych wartości:
   - BRAK
   - 128_BIT
   - 192_BIT

   Można określić wiele wartości, korzystając z listy rozdzielanej przecinkami. Użycie wartości NONE z dowolną inną wartością jest niepoprawne.
3. Ustawiając atrybut **EncryptionPolicySuiteB** w sekcji SSL pliku konfiguracyjnego klienta MQI na jedną lub więcej poniższych wartości:
   - BRAK
   - 128_BIT
   - 192_BIT

   Można określić wiele wartości, korzystając z listy rozdzielanej przecinkami. Użycie NONE z żadną inną wartością jest niepoprawne.

Uwaga: Ustawienia klienta MQI są wymienione w kolejności priorytetów. Struktura MSCO w wywołaniu MQCONNX przesłania ustawienie w zmiennej środowiskowej MQSUITEB, która przesłania atrybut w sekcji SSL.

Szczegółowe informacje na temat struktury MQSCO można znaleźć w sekcji Opcje konfiguracji MQSCO-SSL.

Więcej informacji na temat korzystania z pakietu Suite B w pliku konfiguracyjnym klienta zawiera sekcja Sekcja SSL pliku konfiguracyjnego klienta .

Więcej informacji na temat korzystania ze zmiennej środowiskowej MQSUITEB zawiera sekcja Zmienne środowiskowe.

.NET

W przypadku klientów niezarządzanych .NET właściwość **MQC.ENCRYPTION_POLICY_SUITE_B** wskazuje typ wymaganego zabezpieczenia Suite B.

Informacje na temat korzystania z pakietu Suite B w klasach IBM WebSphere MQ dla platformy .NET zawiera sekcja Klasa .NET produktu MQEnvironment.

Strategie sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ
Strategia sprawdzania poprawności certyfikatów określa, w jaki sposób sprawdzanie poprawności łańcucha certyfikatów jest zgodne ze standardami bezpieczeństwa branżowego.

Strategia sprawdzania poprawności certyfikatu zależy od platformy i środowiska w następujący sposób:

- W przypadku aplikacji Java i JMS na wszystkich platformach strategia sprawdzania poprawności certyfikatu zależy od komponentu JSSE środowiska wykonawczego Java. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów znajduje się w dokumentacji środowiska JRE.
- W przypadku systemów UNIX, Linux, and Windows strategia sprawdzania poprawności certyfikatu jest dostarczana przez pakiet GSKit i może zostać skonfigurowana. Obsługiwane są dwie różne strategie sprawdzania poprawności certyfikatu:
  - Wcześniejsza strategia sprawdzania poprawności certyfikatu, używana w celu zapewnienia maksymalnej kompatybilności wstecznej i współdziałania ze starymi certyfikatami cyfrowymi, które nie są zgodne z aktualnymi standardami sprawdzania poprawności certyfikatu IETF. Ta strategia jest znana jako strategia podstawowa.
  - Ścisła, zgodna ze standardami strategia sprawdzania poprawności certyfikatu, która wymusza standard RFC 5280. Ta strategia jest znana jako strategia standardowa.

Więcej informacji na temat konfigurowania strategii sprawdzania poprawności certyfikatów w systemach UNIX, Linux, and Windows zawiera sekcja “Konfigurowanie strategii sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ” na stronie 35. Więcej informacji na temat różnic między

strategiami sprawdzania poprawności certyfikatów podstawowych i standardowych znajduje się w sekcji Sprawdzanie poprawności certyfikatu i projekt strategii zaufania w systemach UNIX, Linux i Windows .

Konfigurowanie strategii sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ
Istnieje możliwość określenia, która strategia sprawdzania poprawności certyfikatu SSL/TLS jest używana do sprawdzania poprawności certyfikatów cyfrowych odebranych ze zdalnych systemów partnerskich na cztery sposoby.

W menedżerze kolejek strategia sprawdzania poprawności certyfikatu może być ustawiona w następujący sposób:

- Korzystanie z atrybutu menedżera kolejek *CERTVPOL*. Więcej informacji na temat ustawiania tego atrybutu zawiera sekcja ALTER QMGR .

Na kliencie istnieje kilka metod, których można użyć do ustawienia strategii sprawdzania poprawności certyfikatu. Jeśli do ustawienia strategii używana jest więcej niż jedna metoda, klient korzysta z ustawień w następującym porządku priorytetowym:

1. Przy użyciu pola *CertificateValPolicy* w strukturze MQSCO klienta. Więcej informacji na temat używania tego pola zawiera sekcja Opcje konfiguracji MQSCO-SSL.
2. Za pomocą zmiennej środowiskowej klienta *MQCERTVPOL*. Więcej informacji na temat używania tej zmiennej zawiera sekcja MQCERTVPOL .
3. Przy użyciu ustawienia parametru strojenia sekcji SSL klienta *CertificateValPolicy*. Więcej informacji na temat używania tego ustawienia znajduje się w sekcji Sekcja SSL pliku konfiguracyjnego klienta .

Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ” na stronie 34.

Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ
Ten temat zawiera informacje na temat sposobu wyboru odpowiednich specyfikacji CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa, poprzez wykreślenie relacji między CipherSpecs a certyfikatami cyfrowymi w produkcie IBM WebSphere MQ.

We wcześniejszych wersjach produktu IBM WebSphere MQwszystkie obsługiwane protokoły SSL i TLS CipherSpecs użyły algorytmu RSA dla podpisów cyfrowych i umowy klucza. Wszystkie obsługiwane typy certyfikatów cyfrowych były zgodne ze wszystkimi obsługiwanymi CipherSpecs, więc można było zmienić CipherSpec dla dowolnego kanału bez konieczności zmiany certyfikatów cyfrowych.

W wersji IBM WebSphere MQ v7.5 tylko podzbiór obsługiwanych specyfikacji CipherSpecs może być używany ze wszystkimi obsługiwanymi typami certyfikatów cyfrowych. W związku z tym konieczne jest wybranie odpowiedniej specyfikacji CipherSpec dla certyfikatu cyfrowego. Podobnie, jeśli strategia bezpieczeństwa organizacji wymaga użycia określonej specyfikacji CipherSpec , należy uzyskać odpowiedni certyfikat cyfrowy dla tej specyfikacji CipherSpec.

Algorytm podpisu cyfrowego MD5 i TLS 1.2

Certyfikaty cyfrowe podpisane przy użyciu algorytmu MD5 są odrzucane, gdy używany jest protokół TLS 1.2 . Wynika to z faktu, że algorytm MD5 jest obecnie uznawany za słaby przez wielu analityków szyfrujących, a jego użycie jest zwykle niezalecane. Aby używać nowszych specyfikacji CipherSpecs opartych na protokole TLS 1.2 , należy upewnić się, że certyfikaty cyfrowe nie używają algorytmu MD5 w ich podpisach cyfrowych. Starsze atrybuty CipherSpecs , które używają protokołów SSL 3.0 i TLS 1.0 , nie podlegają temu ograniczeniu i mogą nadal używać certyfikatów z podpisami cyfrowymi MD5 .

Aby wyświetlić algorytm podpisu cyfrowego dla konkretnego certyfikatu, można użyć komendy **runmqakm** :

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

gdzie `cert_label` jest etykietą certyfikatu cyfrowego algorytmu podpisu, który ma być wyświetlany.

Uwaga: Chociaż narzędzie **iKeycmd (runmqckm)** i interfejs GUI programu **iKeyman (strmqikm)** mogą być używane do wyświetlania wyboru algorytmów podpisu cyfrowego, to narzędzie **runmqakm** udostępnia szerszy zakres.

Wykonanie komendy **runmqakm** spowoduje wyświetlenie danych wyjściowych wyświetlając użycie podanego algorytmu podpisywania:

```
Label : ibmwebspheremqexample
Key Size : 1024
Version : X509 V3
Serial : 4e4e93f1
Issuer : CN=Old Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : August 19, 2011 5:48:49 PM GMT+01:00
Not After : August 18, 2012 5:48:49 PM GMT+01:00
Public Key
    30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
    05 00 03 81 8D 00 30 81 89 02 81 81 00 98 5A 7A
    F0 18 21 EE E4 8A 6E DE C8 01 4B 3A 1E 41 90 3D
    CE 01 3F E6 32 30 6C 23 59 F0 FE 78 6D C2 80 EF
    BC 83 54 7A EB 60 80 62 6B F1 52 FE 51 9D C1 61
    80 A5 1C D4 F0 76 C7 15 6D 1F 0D 4D 31 3E DC C6
    A9 20 84 6E 14 A1 46 7D 4C F5 79 4D 37 54 0A 3B
    A9 74 ED E7 8B 0F 80 31 63 1A 0B 20 A5 99 EE 0A
    30 A6 B6 8F 03 97 F6 99 DB 6A 58 89 7F 27 34 DE
    55 08 29 D8 A9 6B 46 E6 02 17 C3 13 D3 02 03 01
    00 01
Public Key Type : RSA (1.2.840.113549.1.1.1)
Fingerprint : SHA1 :
    09 4E 4F F2 1B CB C1 F4 4F 15 C9 2A F7 32 0A 82
    DA 45 92 9F
Fingerprint : MD5 :
    44 54 81 7C 58 68 08 3A 5D 75 96 40 D5 8C 7A CB
Fingerprint : SHA256 :
    3B 47 C6 E7 7B B0 FF 85 34 E7 48 BE 11 F2 D4 35
    B7 9A 79 53 2B 07 F5 E7 65 E8 F7 84 E0 2E 82 55
Signature Algorithm : MD5WithRSASignature (1.2.840.113549.1.1.4)
Value
    3B B9 56 E6 F2 77 94 69 5B 3F 17 EA 7B 19 D0 A2
    D7 10 38 F1 88 A4 44 1B 92 35 6F 3B ED 99 9B 3A
    A5 A4 FC 72 25 5A A9 E3 B1 96 88 FC 1E 9F 9B F1
    C5 E8 8E CF C4 8F 48 7B 0E A6 BB 13 AE 2B BD D8
    63 2C 03 38 EF DC 01 E1 1F 7A 6F FB 2F 65 74 D0
    FD 99 94 BA B2 3A D5 B4 89 6C C1 2B 43 6D E2 39
    66 6A 65 CB C3 C4 E2 CC F5 49 39 A3 8B 93 5A DD
    B0 21 0B A8 B2 59 5B 24 59 50 44 89 DC 78 19 51
Trust Status : Enabled
```

Linia `Signature Algorithm` pokazuje, że używany jest algorytm `MD5WithRSASignature` . Ten algorytm jest oparty na MD5 i dlatego ten certyfikat cyfrowy nie może być używany z protokołem TLS 1.2 CipherSpecs.

Współdziałanie Elliptic Curve i RSA CipherSpecs

Nie wszystkie obiekty CipherSpecs mogą być używane ze wszystkimi certyfikatami cyfrowymi. Istnieją trzy typy CipherSpec, oznaczane przedrostkiem nazwy CipherSpec . Każdy typ obiektu CipherSpec nakłada różne ograniczenia na typ certyfikatu cyfrowego, który może być używany. Ograniczenia te dotyczą wszystkich połączeń SSL i TLS produktu WebSphere MQ , ale są szczególnie istotne dla użytkowników kryptografii krzywej eliptycznej.

Relacje między obiektami CipherSpecs i certyfikatami cyfrowymi są podsumowane w poniższej tabeli:

Tabela 2. Relacje między CipherSpecs a certyfikatami cyfrowymi

Typ	Przedrostek nazwy CipherSpec	Opis	Wymagany typ klucza publicznego	Algorytm szyfrowania podpisu cyfrowego	Metoda ustalania klucza tajnego
1	ECDHE_ECDSA_	CipherSpecs , które wykorzystują klucze publiczne Elliptic Curve, klucze tajne Elliptic Curve oraz algorytmy podpisu cyfrowego Elliptic Curve.	Krzywa eliptyczna	ECDSA	ECDHE
2	ECDHE_RSA_	CipherSpecs , które wykorzystują klucze publiczne RSA, klucze tajne Elliptic Curve oraz algorytmy podpisu cyfrowego Elliptic Curve.	RSA	RSA	ECDHE
3	(wszystkie inne)	CipherSpecs , które używają kluczy publicznych RSA i algorytmów podpisu cyfrowego RSA.	RSA	RSA	RSA

Uwaga: Typy 1 i 2 CipherSpecs są obsługiwane tylko przez menedżery kolejek produktu WebSphere MQ i klienty MQI na platformach UNIX, Linux, and Windows .

Kolumna wymaganego typu klucza publicznego zawiera typ klucza publicznego, który musi być używany przez certyfikat osobisty podczas korzystania z każdego typu obiektu CipherSpec. Certyfikat osobisty to certyfikat jednostki końcowej, który identyfikuje menedżera kolejek lub klienta dla jego zdalnego partnera.

Algorytm szyfrowania podpisu cyfrowego odwołuje się do algorytmu szyfrowania używanego do sprawdzania poprawności węzła sieci. Algorytm szyfrowania jest używany wraz z algorytmem mieszającym, takim jak MD5, SHA-1 lub SHA-256 , aby obliczyć podpis cyfrowy. Istnieją różne algorytmy podpisu cyfrowego, które mogą być używane, na przykład "RSA with MD5" lub "ECDSA with SHA-256". W tabeli ECDSA odnosi się do zestawu algorytmów podpisu cyfrowego, które wykorzystują ECDSA; RSA odnosi się do zestawu algorytmów podpisu cyfrowego, które wykorzystują RSA. Może być używany dowolny obsługiwany algorytm podpisu cyfrowego w zestawie, pod warunkiem, że jest on oparty na określonym algorytmie szyfrowania.

Typ 1 CipherSpecs wymaga, aby certyfikat osobisty miał klucz publiczny Elliptic Curve. Po użyciu tych specyfikacji CipherSpecs do ustalenia klucza tajnego dla połączenia używana jest umowa o kluczu Elliptic Curve Diffie Hellman Ephemeral key.

Typ 2 CipherSpecs (Specyfikacje szyfrowania) wymaga, aby certyfikat osobisty miał klucz publiczny RSA. Po użyciu tych specyfikacji CipherSpecs do ustalenia klucza tajnego dla połączenia używana jest umowa o kluczu Elliptic Curve Diffie Hellman Ephemeral key.

Typ 3 CipherSpecs wymaga, aby certyfikat osobisty miał klucz publiczny RSA. Po użyciu tych specyfikacji CipherSpecs do ustanowienia klucza tajnego połączenia używana jest wymiana kluczy RSA.

Ta lista ograniczeń nie jest wyczerpująca: w zależności od konfiguracji mogą istnieć dodatkowe ograniczenia, które mogą dodatkowo wpłynąć na zdolność do współdziałania. Jeśli na przykład produkt WebSphere MQ został skonfigurowany w taki sposób, aby spełniał standardy FIPS 140-2 lub NSA Suite B, będzie on również ograniczał zakres dopuszczalnych konfiguracji. Więcej informacji na ten temat można znaleźć w poniższej sekcji.

Menedżer kolejek produktu WebSphere MQ może używać tylko jednego certyfikatu osobistego do zidentyfikowania samego siebie. Oznacza to, że wszystkie kanały w menedżerze kolejek będą używać tego samego certyfikatu cyfrowego i dlatego każdy menedżer kolejek może używać tylko jednego typu obiektu CipherSpec naraz. Podobnie aplikacja kliencka WebSphere MQ może używać tylko jednego certyfikatu osobistego do identyfikacji samego siebie. Oznacza to, że wszystkie połączenia SSL i TLS w ramach pojedynczego procesu aplikacji będą używały tego samego certyfikatu cyfrowego i dlatego każdy proces aplikacji klienckiej może używać tylko jednego typu obiektu CipherSpec jednocześnie.

Trzy typy klasy CipherSpec nie współdziałają bezpośrednio: jest to ograniczenie obecnych standardów SSL i TLS. Załóżmy na przykład, że wybrano użycie klasy ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec dla kanału odbiorczego o nazwie TO.QM1 w menedżerze kolejek o nazwie QM1. ECDHE_ECDSA_AES_128_CBC_SHA256 jest typu 1 CipherSpec, więc QM1 musi mieć certyfikat osobisty z kluczem Elliptic Curve i podpisem cyfrowym opartym na ECDSA. Wszystkie klienty i inne menedżery kolejek komunikują się bezpośrednio z QM1 , dlatego muszą mieć certyfikaty cyfrowe, które spełniają wymagania typu 1 CipherSpec . Inne kanały łączące się z menedżerem kolejek QM1 mogą używać innych specyfikacji CipherSpecs (na przykład ECDHE_ECDSA_3DES_EDE_CBC_SHA256), ale mogą używać tylko typu 1 CipherSpecs do komunikowania się z QM1.

Podczas planowania sieci WebSphere MQ należy dokładnie rozważyć, które kanały wymagają protokołu SSL lub TLS, i upewnić się, że wszystkie klienty i menedżery kolejek, które muszą współdziałać, korzystają z tego samego typu specyfikacji CipherSpecs i odpowiednich certyfikatów cyfrowych. Standardy IETF RFC 4492, RFC 5246 i RFC 6460 opisują szczegółowo użycie krzywej eliptycznej CipherSpecs w protokole TLS 1.2.

Aby wyświetlić algorytm podpisu cyfrowego i typ klucza publicznego dla certyfikatu cyfrowego, można użyć komendy **runmqakm** :

```
runmqakm -cert -details -db key.kdb -pw password -label cert_label
```

gdzie `cert_label` jest etykietą certyfikatu, którego algorytm podpisu cyfrowego należy wyświetlić.

Wykonanie komendy **runmqakm** spowoduje wyświetlenie danych wyjściowych z wyświetlonymi typem klucza publicznego:

```
Label : ibmwebspheremqexample
Key Size : 384
Version : X509 V3
Serial : 9ad5eeef5d756f41
Issuer : CN=Example Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : 21 August 2011 13:10:24 GMT+01:00
Not After : 21 August 2012 13:10:24 GMT+01:00
Public Key
    30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B
    81 04 00 22 03 62 00 04 3E 6F A9 06 B6 C3 A0 11
    F8 D6 22 78 FE EF 0A FE 34 52 C0 8E AB 5E 81 73
    D0 97 3B AB D6 80 08 E7 31 E9 18 3F 6B DE 06 A7
    15 D6 9D 5B 6F 56 3B 7F 72 BB 6F 1E C9 45 1C 46
    60 BE F2 DC 1B AD AC EC 64 4C 0E 06 65 6E ED 93
    B8 F5 95 E0 F9 2A 05 D6 21 02 BD FB 06 63 A1 CC
    66 C6 8A 0A 5C 3F F7 D3
Public Key Type : EC_ecPublicKey (1.2.840.10045.2.1)
Fingerprint : SHA1 :
    3C 34 58 04 5B 63 5F 5C C9 7A E7 67 08 2B 84 43
    3D 43 7A 79
Fingerprint : MD5 :
```

```
    49 13 13 E1 B2 AC 18 9A 31 41 DC 8C B4 D6 06 68
Fingerprint : SHA256 :
    6F 76 78 68 F3 70 F1 53 CE 39 31 D9 05 C5 C5 9F
    F2 B8 EE 21 49 16 1D 90 64 6D AC EB 0C A7 74 17
Signature Algorithm : EC_ecdsa_with_SHA384 (1.2.840.10045.4.3.3)
Value
    30 65 02 30 0A B0 2F 72 39 9E 24 5A 22 FE AC 95
    0D 0C 6D 6C 2F B3 E7 81 F6 C1 36 1B 9A B0 6F 07
    59 2A A1 4C 02 13 7E DD 06 D6 FE 4B E4 03 BC B1
    AC 49 54 1E 02 31 00 90 0E 46 2B 04 37 EE 2C 5F
    1B 9C 69 E5 99 60 84 84 10 71 1A DA 63 88 33 E2
    22 CC E6 1A 4E F4 61 CC 51 F9 EE A0 8E F4 DC B5
    0B B9 72 58 C3 C7 A4
Trust Status : Enabled
```

Wiersz Typ klucza publicznego w tym przypadku wskazuje, że certyfikat ma klucz publiczny krzywa eliptycznego. Linia algorytmu podpisywania w tym przypadku pokazuje, że algorytm EC_ecdsa_with_SHA384 jest używany: jest to oparte na algorytmie ECDSA. Certyfikat ten jest zatem odpowiedni tylko do użytku z typem 1 CipherSpecs.

Można również użyć narzędzia **iKeycmd (runmqckm)** z tymi samymi parametrami. Za pomocą interfejsu GUI programu **iKeyman (strmqikm)** można wyświetlać algorytmy podpisu cyfrowego w przypadku otwarcia repozytorium kluczy, a następnie dwukrotnie kliknąć etykietę certyfikatu. Zaleca się jednak korzystanie z narzędzia **runmqakm** w celu wyświetlania certyfikatów cyfrowych, ponieważ obsługuje on szerszy zakres algorytmów.

Krzywa eliptyczna CipherSpecs i NSA Suite B

Gdy produkt WebSphere MQ jest skonfigurowany w taki sposób, że jest zgodny z profilem TLS 1.2 zgodnego z pakietem B, dozwolone algorytmy CipherSpecs i podpisu cyfrowego są ograniczone zgodnie z opisem w sekcji “Szyfrowanie NSA Suite B Cryptography w produkcie IBM WebSphere MQ” na stronie 31. Ponadto zakres dopuszczalnych kluczy Elliptic Curve jest zmniejszany zgodnie ze skonfigurowanymi poziomami zabezpieczeń.

Na poziomie bezpieczeństwa 128-bitowego Suite B klucz publiczny podmiotu certyfikatu jest wymagany do użycia krzywej eliptycznej NIST P-256 lub NIST P-384 i do podpisania z krzywą eliptyczną NIST P-256 lub krzywą eliptyczną NIST P-384 . Komenda **runmqakm** może być używana do żądania certyfikatów cyfrowych dla tego poziomu zabezpieczeń przy użyciu parametru -sig_alg EC_ecdsa_with_SHA256lub EC_ecdsa_with_SHA384.

Na poziomie zabezpieczeń 192-bitowego Suite B klucz publiczny podmiotu certyfikatu jest wymagany do użycia krzywej eliptycznej NIST P-384 i do podpisania z krzywą eliptyczną NIST P-384 . Komenda **runmqakm** może być używana do żądania certyfikatów cyfrowych dla tego poziomu zabezpieczeń przy użyciu parametru -sig_alg EC_ecdsa_with_SHA384.

Obsługiwane krzywe eliptyczne NIST są następujące:

Tabela 3. Obsługiwane krzywe eliptyczne NIST

NIST-nazwa krzywej FIPS 186-3	**Nazwa krzywej RFC 4492**	**Wielkość klucza krzywej eliptycznej (bity)**
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Uwaga: Krzywa eliptyczna NIST P-521 nie może być używana dla operacji zgodnej z pakietem B.

Pojęcia pokrewne

“Określanie CipherSpecs” na stronie 225
Określ parametr CipherSpec za pomocą parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** MQSC lub **ALTER CHANNEL** MQSC.

“Określanie, że w czasie wykonywania w kliencie MQI są używane tylko specyfikacje CipherSpecs z certyfikatem FIPS” na stronie 112
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi korzystać z certyfikatów CipherSpecsz certyfikatem FIPS.

“Szyfrowanie NSA Suite B Cryptography w produkcie IBM WebSphere MQ” na stronie 31
Ta sekcja zawiera informacje na temat konfigurowania produktu IBM WebSphere MQ w systemach Windows, Linuxi UNIX w taki sposób, aby były zgodne z profilem TLS 1.2 zgodnym z pakietem Suite B.

“National Security Agency (NSA) Suite B Cryptography” na stronie 20
Rząd Stanów Zjednoczonych Ameryki produkuje doradztwo techniczne w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowanie danych. Amerykańska Narodowa Agencja Bezpieczeństwa (NSA) zaleca zestaw interoperacyjnych algorytmów kryptograficznych w swoim standardzie Suite B.

Wartości CipherSpec obsługiwane w produkcie IBM WebSphere MQ
Zestaw domyślnych obiektów CipherSpecs dopuszcza tylko następujące wartości:

TLS 1.0

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

TLS 1.2

- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Włączanie nieaktualnych specyfikacji CipherSpecs

Domyślnie nie jest dozwolone określanie nieaktualnego atrybutu CipherSpec w definicji kanału. Jeśli zostanie podjęta próba określenia nieaktualnego atrybutu CipherSpec, w dzienniku błędów menedżera kolejek zostanie wyświetlony komunikat AMQ9788 .

Możliwe jest ponowne włączenie nieaktualnej specyfikacji CipherSpecs przez edycję pliku `qm.ini` . W sekcji SSL w pliku `qm.ini` dodaj następujący wiersz:

```
SSL:
AllowWeakCipherSpec=Yes
```

Można również ponownie włączyć co najmniej jeden nieaktualny atrybut CipherSpecs w czasie wykonywania na serwerze, ustawiając zmienną środowiskową *AMQ_SSL_WEAK_CIPHER_ENABLE* na dowolną wartość. Ta zmienna środowiskowa umożliwia włączenie specyfikacji CipherSpecs niezależnie od wartości określonej w pliku `qm.ini` .

Rekordy uwierzytelniania kanału

Aby umożliwić bardziej precyzyjną kontrolę na poziomie kanału nad dostępem przydzielonym do systemów, które nawiązują połączenie, można użyć rekordów uwierzytelniania kanału.

Może się okazać, że klienty próbują nawiązać połączenie z menedżerem kolejek przy użyciu pustego ID użytkownika lub ID użytkownika najwyższego poziomu i w ten sposób umożliwić sobie wykonywanie niepożądanych działań. Dostęp do tych klientów można zablokować za pomocą rekordów uwierzytelniania kanału. Alternatywnie klient może zapewnić ID użytkownika, który jest poprawny na platformie klienta, ale na platformie serwera jest nieznany lub ma niepoprawny format. Przy użyciu rekordu uwierzytelniania kanału można odwzorować zapewniany ID użytkownika na poprawny ID użytkownika.

Aplikacja kliencka nawiązująca połączenie z menedżerem kolejek może przejawiać niepożądane zachowanie. Aby chronić serwer przed problemami, które taka aplikacja powoduje, należy zablokować jej adres IP do czasu, gdy zostaną zaktualizowane reguły firewalla lub dana aplikacja kliencka zostanie naprawiona. Za pomocą rekordu uwierzytelniania kanału można zablokować adres IP, z którego aplikacja kliencka nawiązuje połączenie.

Jeśli skonfigurowano narzędzie administracyjne, takie jak IBM WebSphere MQ Explorer, oraz specjalny kanał, konieczne może być skonfigurowanie tego narzędzia w taki sposób, aby korzystać z niego mogły tylko konkretne komputery klienckie. W celu zagwarantowania, że kanał będzie używany tylko z określonych adresów IP, można użyć rekordu uwierzytelniania kanału.

Jeśli pierwsze kroki zostały uruchomione z przykładowymi aplikacjami działaniowymi jako klienty, zapoznaj się z sekcją Przygotowywanie i uruchamianie programów przykładowych , aby uzyskać przykład bezpiecznego konfigurowania menedżera kolejek przy użyciu rekordów uwierzytelniania kanału.

Aby rekordy uwierzytelniania kanału kontrolowały kanały przychodzące, należy użyć komendy MQSC **ALTER QMGR CHLAUTH(ENABLED)**.

W odniesieniu do MCA kanału utworzonego w reakcji na nowe połączenie przychodzące stosowane są reguły **CHLAUTH**. W przypadku MCA kanału utworzonego w wyniku lokalnego uruchomienia kanału nie są stosowane reguły **CHLAUTH**.

Tabela 4. Zastosowanie reguł CHLAUTH do różnych par kanałów

Typ kanału	**MCA z zastosowaniem reguł CHLAUTH**
SDR-RCVR	RCVR
RQSTR-SVR (uruchamiany na SVR)	RQSTR
RQSTR-SVR (uruchamiany na RQSTR)	SVR
RQSTR-SDR (uruchamiany na SDR)	RQSTR
RQSTR-SDR (uruchamiany na RQSTR)	SDR dla początkowego połączenia. RQSTR dla połączenia zwrotnego.

Rekordy uwierzytelniania kanału można tworzyć w celu realizowania następujących funkcji:

- Blokowanie połączeń z konkretnych adresów IP
- Blokowanie połączeń z konkretnych ID użytkownika
- Ustawianie wartości atrybutu MCAUSER przeznaczonej do użycia przez dowolne kanały nawiązujące połączenie z konkretnego adresu IP
- Ustawianie wartości atrybutu MCAUSER przeznaczonej do użycia przez dowolne kanały zapewniające konkretny ID użytkownika
- Ustawianie wartości atrybutu MCAUSER przeznaczonej do użycia przez dowolne kanały, które mają konkretną nazwę wyróżniającą (DN) SSL lub TLS
- Ustawianie wartości MCAUSER przeznaczonej do użycia przez dowolne kanały nawiązujące połączenie z konkretnego menedżera kolejek

- Blokowanie połączeń zgłaszających pochodzenie z pewnego menedżera kolejek, jeśli nie są nawiązywane z konkretnego adresu IP
- Blokowanie połączeń przedstawiających pewne certyfikaty SSL lub TLS, jeśli nie są to połączenia z konkretnego adresu IP

Zastosowania te opisano w następujących sekcjach.

Za pomocą komendy MQSC **SET CHLAUTH** lub komendy PCF **Set Channel Authentication Record**tworzy się, modyfikuje lub usuwa rekordy uwierzytelniania kanału.

Uwaga: Duża liczba rekordów uwierzytelniania kanału może mieć negatywny wpływ na wydajność menedżera kolejek.

Blokowanie adresów IP

Blokowanie dostępu z pewnych adresów IP jest zasadniczo rolą firewalla. Czasem jednak mogą być podejmowane próby nawiązania połączenia z adresu IP, który nie powinien mieć dostępu do systemu produktu WebSphere MQ. Należy wówczas zablokować dany adres do czasu zaktualizowania firewalla. Te próby nawiązania połączenia mogą nie być nawet przychodzące z kanałów produktu WebSphere MQ , ale z innych aplikacji używających gniazd, które zostały niepoprawnie skonfigurowane w celu ukierunkowania procesu nasłuchiwania produktu WebSphere MQ . Aby zablokować adresy IP, należy ustawić rekord uwierzytelniania kanału typu BLOCKADDR. Można podać jeden lub wiele pojedynczych adresów, zakresy adresów lub wzorce zawierające znaki wieloznaczne.

Za każdym razem, gdy zostanie odrzucone połączenie przychodzące z powodu zablokowania adresu IP w ten sposób, generowany jest komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_ADDRESS, pod warunkiem, że są włączone zdarzenia kanału i jest uruchomiony menedżer kolejek. Dodatkowo, połączenie pozostaje otwarte przez 30 sekund przed zwróceniem błędu, aby proces nasłuchujący nie został nadmiernie obciążony wielokrotnymi próbami nawiązania połączenia, które zostały zablokowane.

Aby zablokować adresy IP tylko na konkretnych kanałach lub aby uniknąć opóźnienia przed zgłoszeniem błędu, należy ustawić rekord uwierzytelniania kanału typu ADDRESSMAP z parametrem USERSRC(NOACCESS).

Za każdym razem, gdy połączenie przychodzące zostanie odrzucone z tego powodu, zostanie wygenerowany komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_NOACCESS, pod warunkiem, że są włączone zdarzenia kanału i jest uruchomiony menedżer kolejek.

Przykład można znaleźć w sekcji “Blokowanie konkretnych adresów IP” na stronie 188.

Blokowanie ID użytkowników

Aby uniemożliwić określonym ID użytkowników nawiązywanie połączeń przez kanał klienta, należy ustawić rekord uwierzytelniania kanału typu BLOCKUSER. Ten typ rekordu uwierzytelniania kanału ma zastosowanie tylko do kanałów klienta, a nie do kanałów komunikatu. Określić można jeden lub wiele pojedynczych ID użytkowników do zablokowania, jednak nie można używać znaków wieloznacznych.

Za każdym razem, gdy zostanie odrzucone połączenie przychodzące z tej przyczyny, generowany jest komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_USERID, pod warunkiem, że są włączone zdarzenia kanału.

Przykład można znaleźć w sekcji “Blokowanie konkretnych ID użytkowników” na stronie 190.

Ponadto można całkowicie zablokować dostęp dla określonych ID użytkowników w pewnych kanałach, ustawiając rekord uwierzytelniania kanału typu USERMAP z parametrem USERSRC(NOACCESS).

Za każdym razem, gdy połączenie przychodzące zostanie odrzucone z tego powodu, zostanie wygenerowany komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_NOACCESS, pod warunkiem, że są włączone zdarzenia kanału i jest uruchomiony menedżer kolejek.

Przykład można znaleźć w sekcji “Blokowanie dostępu dla ID użytkownika potwierdzonego przez klienta” na stronie 193.

Blokowanie nazw menedżerów kolejek

Aby określić, że żaden kanał nawiązujący połączenie z określonego menedżera kolejek nie będzie mieć dostępu, należy ustawić rekord uwierzytelniania kanału typu QMGRMAP z parametrem USERSRC(NOACCESS). Określić można pojedynczy menedżer kolejek lub wzorzec zawierający znaki wieloznaczne. Rozwiązanie równoznaczne z funkcją BLOCKUSER służące do blokowania dostępu z menedżerów kolejek nie istnieje.

Za każdym razem, gdy połączenie przychodzące zostanie odrzucone z tego powodu, zostanie wygenerowany komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_NOACCESS, pod warunkiem, że są włączone zdarzenia kanału i jest uruchomiony menedżer kolejek.

Przykład można znaleźć w sekcji “Blokowanie dostępu ze zdalnego menedżera kolejek” na stronie 192.

Blokowanie nazw wyróżniających SSL i TLS

Aby określić, że żaden użytkownik, który przedstawia certyfikat osobisty SSL lub TLS zawierający określoną nazwę wyróżniającą, nie będzie mieć dostępu, należy ustawić rekord uwierzytelniania kanału typu SSLPEERMAP z parametrem USERSRC(NOACCESS). Określić można pojedynczą nazwę wyróżniającą lub wzorzec zawierający znaki wieloznaczne. Rozwiązanie równoznaczne z funkcją BLOCKUSER służące do blokowania dostępu dla nazw wyróżniających nie istnieje.

Za każdym razem, gdy połączenie przychodzące zostanie odrzucone z tego powodu, zostanie wygenerowany komunikat o zdarzeniu MQRC_CHANNEL_BLOCKED z kwalifikatorem przyczyny MQRQ_CHANNEL_BLOCKED_NOACCESS, pod warunkiem, że są włączone zdarzenia kanału i jest uruchomiony menedżer kolejek.

Przykład można znaleźć w sekcji “Blokowanie dostępu dla nazwy wyróżniającej SSL” na stronie 193.

Odwzorowanie adresów IP na ID użytkowników, które mają być używane

Aby określić, że każdy kanał nawiązujący połączenie z określonego adresu IP ma używać konkretnego atrybutu MCAUSER, należy ustawić rekord uwierzytelniania kanału typu ADDRESSMAP. Określić można pojedynczy adres, zakres adresów lub wzorzec zawierający znaki wieloznaczne.

Jeśli używany jest serwer przekazujący porty, podział sesji strefy DMZ lub jakakolwiek inna konfiguracja zmieniająca adres IP przedstawiany menedżerowi kolejek, odwzorowanie adresów IP może okazać się nieodpowiednie do danego zastosowania.

Przykład można znaleźć w sekcji “Odwzorowywanie adresu IP na identyfikator użytkownika MCAUSER” na stronie 194.

Odwzorowanie nazw menedżerów kolejek na ID użytkowników, które mają być używane

Aby określić, że każdy kanał nawiązujący połączenie z określonego menedżera kolejek ma używać konkretnego atrybutu MCAUSER, należy ustawić rekord uwierzytelniania kanału typu QMGRMAP. Określić można pojedynczy menedżer kolejek lub wzorzec zawierający znaki wieloznaczne.

Przykład można znaleźć w sekcji “Odwzorowywanie zdalnego menedżera kolejek na identyfikator użytkownika MCAUSER” na stronie 191.

Odwzorowanie ID użytkowników zapewnianych przez klient na ID użytkowników, które mają być używane

Aby określić, że jeśli pewien ID użytkownika jest używany przez połączenie z klienta produktu WebSphere MQ MQI, to ma być używany inny określony atrybut MCAUSER, należy ustawić rekord uwierzytelniania kanału typu USERMAP. W odwzorowaniu ID użytkownika nie są używane znaki wieloznaczne.

Przykład można znaleźć w sekcji “Odwzorowywanie identyfikatora użytkownika potwierdzonego przez klienta na identyfikator użytkownika MCAUSER” na stronie 191.

Odwzorowanie nazw wyróżniających SSL lub TLS na ID użytkowników, które mają być używane

Aby określić, że każdy użytkownik, który przedstawia certyfikat osobisty SSL/TLS zawierający określoną nazwę wyróżniającą, ma używać konkretnego atrybutu MCAUSER, należy ustawić rekord uwierzytelniania kanału typu SSLPEERMAP. Określić można pojedynczą nazwę wyróżniającą lub wzorzec zawierający znaki wieloznaczne.

Przykład można znaleźć w sekcji “Odwzorowywanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER” na stronie 192.

Przypisywanie menedżerów kolejek, klientów albo nazw wyróżniających SSL lub TLS zgodnie z adresem IP

W pewnych okolicznościach inna firma może fałszywie przedstawiać nazwę menedżera kolejek. Może również dojść do kradzieży i ponownego użycia certyfikatu SSL lub TLS bądź bazy danych kluczy. W celu ochrony przed tymi zagrożeniami można określić, że połączenie z pewnego menedżera kolejek lub klienta bądź przy użyciu pewnej nazwy wyróżniającej musi być nawiązywane z określonego adresu IP. Należy ustawić rekord uwierzytelniania kanału typu USERMAP, QMGRMAP lub SSLPEERMAP i podać dozwolony adres IP lub wzorzec adresów IP przy użyciu parametru ADDRESS.

Przykład można znaleźć w sekcji “Odwzorowywanie zdalnego menedżera kolejek na identyfikator użytkownika MCAUSER” na stronie 191.

Interakcja między rekordami uwierzytelniania kanału

Istnieje możliwość, że kanał próbujący nawiązać połączenie będzie zgodny z więcej niż jednym rekordem uwierzytelniania kanału, przy czym rekordy te mają przeciwstawne działanie. Na przykład kanał może zapewniać ID użytkownika, który jest blokowany przez rekord uwierzytelniania kanału BLOCKUSER, ale z certyfikatem SSL lub TLS, który jest zgodny z rekordem SSLPEERMAP ustawiającym inny ID użytkownika. Dodatkowo, jeśli rekordy uwierzytelniania kanału używają znaków wieloznacznych, pojedynczy adres IP, nazwa menedżera kolejek lub nazwa wyróżniająca SSL bądź TLS mogą być zgodne z kilkoma wzorcami. Na przykład adres IP 192.0.2.6 jest zgodny z wzorcem 192.0.2.0-24, 192.0.2.* oraz 192.0.*.6. Podejmowane działanie jest określane w sposób opisany poniżej.

- Rekord uwierzytelniania kanału, który ma zostać użyty, jest wybierany w następujący sposób:
  - Rekord uwierzytelniania kanału jawnie zgodny z nazwą kanału ma priorytet przed rekordem uwierzytelniania kanału zgodnym z nazwą kanału dzięki użyciu znaku wieloznacznego.
  - Rekord uwierzytelniania kanału używający nazwy wyróżniającej SSL lub TLS ma priorytet przed rekordem używającym ID użytkownika, nazwy menedżera kolejek lub adresu IP.
  - Rekord uwierzytelniania kanału używający ID użytkownika lub nazwy menedżera kolejek ma priorytet przed rekordem używającym adresu IP.
- Jeśli zostanie znaleziony zgodny rekord uwierzytelniania kanału określający atrybut MCAUSER, atrybut ten zostanie przypisany do kanału.
- Jeśli zostanie znaleziony zgodny rekord uwierzytelniania kanału określający, że kanał nie ma dostępu, do kanału zostanie przypisana wartość *NOACCESS atrybutu MCAUSER. Wartość tę można później zmienić za pomocą programu obsługi wyjścia zabezpieczeń.
- W sytuacji, gdy nie zostanie znaleziony zgodny rekord uwierzytelniania kanału, a także wtedy, gdy zostanie znaleziony zgodny rekord uwierzytelniania kanału określający, że ma zostać użyty ID użytkownika kanału, zostanie sprawdzone pole MCAUSER.
  - Jeśli pole MCAUSER jest puste, do kanału zostanie przypisany ID użytkownika klienta.
  - Jeśli pole MCAUSER nie jest puste, do kanału zostanie przypisana jego wartość.
- Jest uruchamiany dowolny program obsługi wyjścia zabezpieczeń. Ten program obsługi wyjścia może ustawić ID użytkownika kanału lub określić, że dostęp ma być blokowany.

- Jeśli połączenie jest blokowane lub pole MCAUSER jest ustawione na wartość *NOACCESS, kanał zostanie zakończony.
- Jeśli połączenie nie jest blokowane, dla każdego kanału z wyjątkiem kanału klienta zostanie sprawdzone, czy na liście zablokowanych użytkowników znajduje się ID użytkownika kanału określony w poprzednich krokach.
  - Jeśli ID użytkownika znajduje się na liście zablokowanych użytkowników, kanał zostanie zakończony.
  - Jeśli ID użytkownika nie znajduje się na liście zablokowanych użytkowników, kanał zostanie uruchomiony.

W sytuacji, gdy wiele rekordów uwierzytelniania kanału jest zgodnych z nazwą kanału, adresami IP, nazwą menedżera kolejek bądź nazwą wyróżniającą SSL lub TLS, zostanie użyta najbardziej konkretna zgodność. Zgodność uważaną za najbardziej konkretną jest określana w sposób opisany poniżej.

- Dla nazwy kanału:
  - Najbardziej konkretna zgodność to nazwa bez znaków wieloznacznych, np. A.B.C.
  - Zgodnością najbardziej ogólną jest pojedyncza gwiazdka (*), która jest zgodna ze wszystkimi nazwami kanałów.
  - Wzorzec, którego pierwszym znakiem z lewej strony jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Wzorzec *.B.C jest więc bardziej ogólny niż wzorzec A.*.
  - Wzorzec, którego drugim znakiem jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Ta zasada odnosi się do każdej kolejnej pozycji. Wobec tego wzorzec A.*.C jest bardziej ogólny niż wzorzec A.B.*
  - W przypadku, gdy co najmniej dwa wzorce mają gwiazdkę w tej samej pozycji, bardziej ogólny jest ten wzorzec, który ma mniej węzłów po gwiazdce. W ten sposób A. * jest bardziej ogólne niż A.*.C
- W przypadku adresu IP:
  - Najbardziej konkretna zgodność to nazwa bez znaków wieloznacznych, np. 192.0.2.6.
  - Zgodnością najbardziej ogólną jest pojedyncza gwiazdka (*), która jest zgodna ze wszystkimi nazwami kanałów.
  - Wzorzec, którego pierwszym znakiem z lewej strony jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Wzorzec *.0.2.6 jest więc bardziej ogólny niż wzorzec 192.*.
  - Wzorzec, którego drugim znakiem jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Ta zasada odnosi się do każdej kolejnej pozycji. Wzorzec 192.*.2.6 jest więc bardziej ogólny niż wzorzec 192.0.*.
  - W przypadku, gdy co najmniej dwa wzorce mają gwiazdkę w tej samej pozycji, bardziej ogólny jest ten wzorzec, który ma mniej węzłów po gwiazdce. Tym samym 192 .* jest bardziej ogólne niż 192.*.2.*.
  - Zakres wskazywany przez łącznik (-) jest bardziej konkretny niż w przypadku gwiazdki. Zatem wzorzec 192.0.2.0-24 jest bardziej konkretny niż wzorzec 192.0.2.*.
  - Zakres, który jest podzbiorem innego zakresu, jest bardziej konkretny niż większy zakres. Zatem wzorzec 192.0.2.5-15 jest bardziej konkretny niż wzorzec 192.0.2.0-24.
  - Nakładanie się zakresów jest niedozwolone. Na przykład nie można użyć rekordów uwierzytelniania kanału jednocześnie dla zakresów 192.0.2.0-15 i 192.0.2.10-20.
  - Wzorzec nie może mieć mniejszej niż wymagana liczby części, chyba że kończy się pojedynczą gwiazdką. Na przykład wartość 192.0.2 jest niepoprawna, ale 192.0.2.* jest poprawna.
  - Końcowa gwiazdka musi być oddzielona od pozostałych znaków adresu odpowiednim separatorem - kropką (.) w przypadku adresów IPv4 lub dwukropkiem (:) w przypadku adresów IPv6. Na przykład adres 192.0* jest niepoprawny, ponieważ gwiazdka nie znajduje się w swojej własnej części.
  - Wzorzec może zawierać dodatkowe gwiazdki, pod warunkiem że żadna gwiazdka nie przylega do gwiazdki końcowej. Na przykład 192.*.2.* jest poprawne, ale 192.0.*.* jest nieprawidłowa.

  - Wzorzec adresu w formacie IPv6 nie może zawierać podwójnego dwukropka ani końcowej gwiazdki, ponieważ adres wynikowy byłby niejednoznaczny. Na przykład wzorzec 2001::* może zostać rozwinięty do postaci 2001:0000:*, 2001:0000:0000:* itd.
- W przypadku nazwy menedżera kolejek:
  - Najbardziej konkretna zgodność to nazwa bez znaków wieloznacznych, np. 192.0.2.6.
  - Zgodnością najbardziej ogólną jest pojedyncza gwiazdka (*), która jest zgodna ze wszystkimi nazwami kanałów.
  - Wzorzec, którego pierwszym znakiem z lewej strony jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Wzorzec *QUEUEMANAGER jest więc bardziej ogólny niż wzorzec QUEUEMANAGER*.
  - Wzorzec, którego drugim znakiem jest gwiazdka, jest bardziej ogólny niż wzorzec, który w tej pozycji ma zdefiniowaną wartość. Ta zasada odnosi się do każdej kolejnej pozycji. Wzorzec Q*MANAGER jest więc bardziej ogólny niż wzorzec QUEUE*.
  - W przypadku, gdy co najmniej dwa wzorce mają gwiazdkę w tej samej pozycji, bardziej ogólny jest ten wzorzec, który ma mniej znaków po gwiazdce. Wzorzec Q* jest więc bardziej ogólny niż wzorzec Q*MGR.
- W przypadku nazwy wyróżniającej SSL lub TLS (DN) kolejność podłańcuchów jest następująca:

Tabela 5. Pierwszeństwo podłańcuchów

Kolejność	**Podłańcuch nazwy wyróżniającej**	**Nazwa**
1	SERIALNUMBER=	Numer seryjny certyfikatu
2	MAIL=	Adres e-mail
3	E=	Adres e-mail (nieaktualny, zastąpiony podłańcuchem MAIL)
4	UID=, USERID=	Identyfikator użytkownika
5	CN=	Nazwa zwykła
6	T=	Tytuł
7	OU=	Jednostka organizacyjna
8	DC=	Komponent domeny
9	O=	Organizacja
10	STREET=	Ulica / Pierwszy wiersz adresu
11	L=	Miejscowość
12	ST=, SP=, S=	Nazwa województwa lub rejonu
13	PC=	Kod pocztowy
14	C=	Kraj
15	UNSTRUCTUREDNAME=	Nazwa hosta
16	UNSTRUCTUREDADDRESS=	Adres IP
17	DNQ=	Kwalifikator nazwy wyróżniającej

Wobec powyższego, jeśli zostanie przedstawiony certyfikat SSL lub TLS z nazwą wyróżniającą zawierającą jednocześnie oba podłańcuchy O=IBM i C=UK, produkt WebSphere MQ użyje rekordu uwierzytelniania kanału dla podłańcucha O=IBM, a nie dla C=UK.

Nazwa wyróżniająca może zawierać wiele podłańcuchów OU, które muszą być podane w porządku hierarchicznym, tzn. na początku muszą się znajdować duże jednostki organizacyjne. Jeśli dwie nazwy wyróżniające są równorzędne pod każdym względem z wyjątkiem wartości OU, bardziej konkretna nazwa wyróżniająca jest określana w następujący sposób:

1. Jeśli ich liczba atrybutów OU jest różna, bardziej konkretna jest nazwa wyróżniająca, która ma więcej wartości OU. Jest tak, ponieważ nazwa wyróżniająca z większą liczbą jednostek organizacyjnych jest nazwą bardziej pełną, która zawiera więcej szczegółów i kryteriów zgodności. Nazwa wyróżniająca z większą liczbą atrybutów OU jest uznawana zawsze za bardziej konkretną, nawet jeśli wartością atrybutu OU najwyższego poziomu jest znak wieloznaczny (OU=*).
2. Jeśli liczba atrybutów OU jest taka sama, porównywane są odpowiednie pary wartości atrybutów OU w sekwencji od lewej do prawej, gdzie pierwszy atrybut OU po lewej stronie jest atrybutem najwyższego poziomu (najmniej konkretnym), zgodnie z następującymi regułami.
   a. Atrybut OU bez wartości wyrażonych znakami wieloznacznymi jest najbardziej konkretny, ponieważ jest zgodny dokładnie z jednym łańcuchem.
   b. Atrybut OU z jednym znakiem wieloznacznym na początku lub na końcu (np. OU=ABC* lub OU=*ABC) jest drugim w kolejności atrybutem najbardziej konkretnym.
   c. Następnym w kolejności konkretnym atrybutem jest atrybut OU z dwoma znakami wieloznacznymi (np. OU=*ABC*).
   d. Atrybut OU zawierający tylko gwiazdkę (OU=*) jest najmniej konkretny.
3. Jeśli porównywane są łańcuchy między dwiema wartościami atrybutów na tym samym poziomie konkretności, to bardziej konkretny jest ten łańcuch atrybutu, który jest dłuższy.
4. Jeśli porównywane są łańcuchy między dwiema wartościami atrybutów na tym samym poziomie konkretności i o tej samej długości, wówczas rezultat jest określany przez porównanie łańcuchów bez rozróżniania wielkości liter w części nazwy wyróżniającej z wykluczeniem wszelkich znaków wieloznacznych.

Jeśli dwie nazwy wyróżniające są równe pod każdym względem, z wyjątkiem ich wartości DC, mają zastosowanie te same reguły zgodności co w przypadku obiektów OU - z tą różnicą, że w wartościach DC lewa strona stanowi najniższy poziom (najbardziej specyficzny), a kolejność porównywania różni się w odpowiedni sposób.

Wyświetlanie rekordów uwierzytelniania kanału

Aby wyświetlić rekordy uwierzytelniania kanału, należy użyć komendy MQSC **DISPLAY CHLAUTH** lub komendy PCF **Inquire Channel Authentication Records**. Wybrać można zwrócenie wszystkich rekordów zgodnych z podaną nazwą kanału lub jawne dopasowanie. Jawne dopasowanie stanowi informację o tym, który rekord uwierzytelniania kanału zostałby użyty, gdyby kanał podjął próbę nawiązania połączenia z konkretnego adresu IP, z konkretnego menedżera kolejek lub przy użyciu konkretnego ID użytkownika oraz opcjonalnie przedstawiającego certyfikat osobisty SSL/TLS zawierający określoną nazwę wyróżniającą.

Pojęcia pokrewne

“Zabezpieczenia dla zdalnego przesyłania komunikatów” na stronie 58

W tej sekcji opisano aspekty bezpieczeństwa dotyczące zdalnego przesyłania komunikatów.

Bezpieczeństwo komunikatów w produkcie IBM WebSphere MQ

Zabezpieczenia komunikatów w infrastrukturze IBM WebSphere MQ są udostępniane przez oddzielnie licencjonowany komponent IBM WebSphere MQ Advanced Message Security.

IBM WebSphere MQ Advanced Message Security (AMS) rozszerza usługi zabezpieczeń produktu IBM WebSphere MQ , aby zapewnić podpisywanie danych i szyfrowanie na poziomie komunikatu. Rozszerzone usługi gwarantują, że dane komunikatu nie zostały zmodyfikowane, gdy jest pierwotnie umieszczone w kolejce i po jego pobraniu. Ponadto program AMS sprawdza, czy nadawca danych komunikatu ma uprawnienia do umieszczania podpisanych komunikatów w kolejce docelowej.

Pojęcia pokrewne

“IBM WebSphere MQ Advanced Message Security” na stronie 279

Produkt IBM WebSphere MQ Advanced Message Security (AMS) jest oddzielnie licencjonowanym komponentem produktu IBM WebSphere MQ Advanced Message Security , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM WebSphere MQ Advanced Message Security , a jednocześnie nie ma wpływu na aplikacje końcowe.

Planowanie wymagań dotyczących bezpieczeństwa

Ta kolekcja tematów wyjaśnia, co należy wziąć pod uwagę podczas planowania zabezpieczeń w środowisku IBM WebSphere MQ .

Produktu IBM WebSphere MQ można używać w przypadku wielu różnych aplikacji na różnych platformach. Wymagania dotyczące zabezpieczeń mogą być różne dla każdej aplikacji. Dla niektórych bezpieczeństwo będzie kwestią krytyczną.

Produkt WebSphere MQ udostępnia szereg usług zabezpieczeń na poziomie łącza, w tym obsługę protokołu SSL (Secure Sockets Layer) i TLS (Transport Layer Security).

Podczas implementowania produktu WebSpherenależy wziąć pod uwagę pewne aspekty zabezpieczeń. W systemach UNIX, Linux i Windows , jeśli użytkownik zignoruje te aspekty i nic nie zrobi, nie będzie można używać produktu WebSphere MQ.

Uwagi dotyczące zabezpieczeń opisano poniżej.

Uprawnienie do administrowania produktem WebSphere MQ

Administratorzy produktu WebSphere MQ muszą mieć uprawnienia do:

- Wydawanie komend do administrowania produktem WebSphere MQ
- Korzystanie z Eksploratora IBM WebSphere MQ

Aby uzyskać więcej informacji, patrz:

- “Uprawnienie do administrowania produktem IBM WebSphere MQ w systemach UNIX, Linux, and Windows” na stronie 204

Uprawnienia do pracy z obiektami WebSphere MQ

Aplikacje mogą uzyskiwać dostęp do następujących obiektów produktu WebSphere MQ przez wywołanie wywołań MQI:

- Menedżery kolejek
- Kolejki
- Procesy
- Listy nazw
- Tematy

Aplikacje mogą również używać komend PCF (Programmable Command Format) w celu uzyskania dostępu do tych obiektów WebSphere MQ oraz do uzyskiwania dostępu do kanałów i obiektów informacji uwierzytelniających. Obiekty te mogą być chronione przez produkt WebSphere MQ , dzięki czemu identyfikatory użytkowników powiązane z aplikacjami muszą mieć uprawnienia do uzyskiwania dostępu do tych obiektów.

Więcej informacji na ten temat zawiera sekcja “Autoryzacja aplikacji do używania produktu IBM WebSphere MQ” na stronie 52.

Bezpieczeństwo kanału

Identyfikatory użytkowników powiązane z agentami kanału komunikatów (MCAs) wymagają uprawnień dostępu do różnych zasobów produktu WebSphere MQ . Na przykład agent MCA musi być w stanie połączyć się z menedżerem kolejek. Jeśli jest to wysyłający agent MCA, musi być w stanie otworzyć kolejkę transmisji dla kanału. Jeśli jest to odbierający agent MCA, musi być w stanie otworzyć kolejki

docelowe. Identyfikatory użytkowników powiązane z aplikacjami, które muszą administrować kanałami, inicjatorami kanału i nasłuchiwaczami, potrzebują uprawnień do korzystania z odpowiednich komend PCF. Jednak większość aplikacji nie potrzebuje takiego dostępu.

Więcej informacji na ten temat zawiera sekcja “Autoryzacja kanału” na stronie 72.

Dodatkowe uwarunkowania

Należy wziąć pod uwagę następujące aspekty bezpieczeństwa tylko wtedy, gdy używane są określone funkcje produktu WebSphere MQ lub podstawowe rozszerzenia produktu:

- “Zabezpieczenia klastrów menedżerów kolejek” na stronie 81
- “Zabezpieczenia dla publikowania/subskrypcji produktu IBM WebSphere MQ” na stronie 82
- “Zabezpieczenia dla programu IBM WebSphere MQ tranzytu internetowego” na stronie 84

Planowanie identyfikacji i uwierzytelniania

Zdecyduj, jakie identyfikatory użytkowników mają być używane, oraz w jaki sposób i na jakich poziomach mają być stosowane elementy sterujące uwierzytelniania.

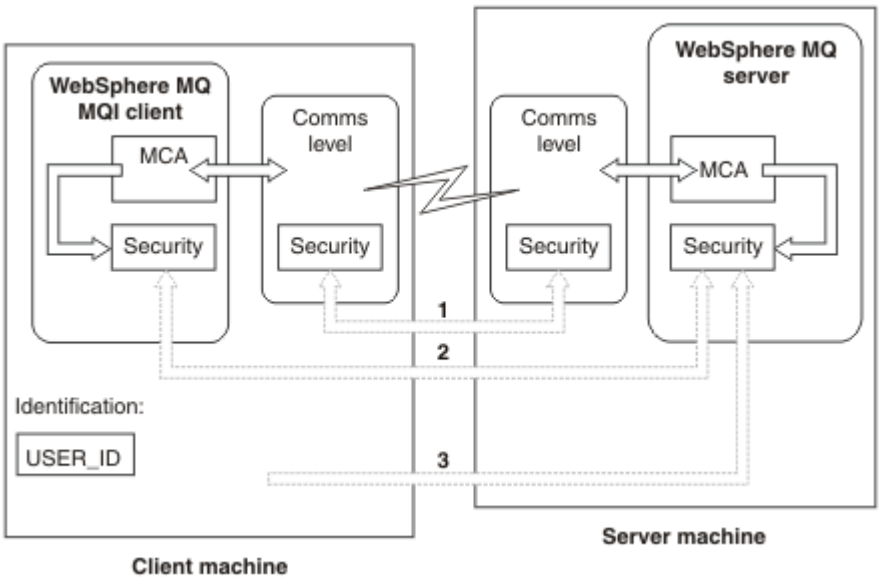
Użytkownik musi zdecydować, w jaki sposób będzie identyfikować użytkowników aplikacji IBM WebSphere MQ , pamiętając o tym, że różne systemy operacyjne obsługują identyfikatory użytkowników o różnych długościach. Za pomocą rekordów uwierzytelniania kanału można odwzorować jeden identyfikator użytkownika na inny lub określić ID użytkownika na podstawie pewnego atrybutu połączenia. Kanały IBM WebSphere MQ korzystające z protokołu SSL lub TLS używają certyfikatów cyfrowych jako mechanizmu identyfikacji i uwierzytelniania. Każdy certyfikat cyfrowy ma nazwę wyróżniającą podmiotu, która może być odwzorowana na konkretne tożsamości za pomocą rekordów uwierzytelniania kanału. Dodatkowo certyfikaty ośrodka CA w repozytorium kluczy określają, które certyfikaty cyfrowe mogą być używane do uwierzytelniania w produkcie IBM WebSphere MQ. Więcej informacji na ten temat zawierają następujące sekcje:

- “Odwzorowywanie zdalnego menedżera kolejek na identyfikator użytkownika MCAUSER” na stronie 191
- “Odwzorowywanie identyfikatora użytkownika potwierdzonego przez klienta na identyfikator użytkownika MCAUSER” na stronie 191
- “Odwzorowywanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER” na stronie 192
- “Odwzorowywanie adresu IP na identyfikator użytkownika MCAUSER” na stronie 194

Planowanie uwierzytelniania dla aplikacji klienckiej

Elementy sterujące uwierzytelniania można zastosować na czterech poziomach: na poziomie komunikacji, w wyjściach zabezpieczeń, w rekordach uwierzytelniania kanału oraz w zakresie identyfikacji, które są przekazywane do wyjścia zabezpieczeń.

Istnieją cztery poziomy bezpieczeństwa do rozważenia. Diagram przedstawia klienta MQI produktu IBM WebSphere MQ , który jest połączony z serwerem. Zabezpieczenia są stosowane na czterech poziomach, zgodnie z opisem w poniższym tekście. Agent MCA jest agentem kanału komunikatów.



Rysunek 7. Zabezpieczenia w połączeniu klient/serwer

1. Poziom komunikacji

   Patrz strzałka 1. Aby zaimplementować zabezpieczenia na poziomie komunikacji, należy użyć protokołu SSL lub TLS. Aby uzyskać więcej informacji, zobacz: “Protokoły zabezpieczeń szyfrujących: SSL i TLS” na stronie 14

2. Rekordy uwierzytelniania kanału

   Patrz strzałki 2 i 3. Uwierzytelnianie może być sterowane za pomocą adresu IP lub nazw wyróżniających SSL/TLS na poziomie zabezpieczeń. ID użytkownika może być również zablokowany lub asertywny ID użytkownika może zostać odwzorowany na poprawny ID użytkownika. Pełny opis jest dostępny w produkcie “Rekordy uwierzytelniania kanału” na stronie 41.

3. Wyjścia zabezpieczeń kanału

   Patrz strzałka 2. Wyjścia zabezpieczeń kanału dla komunikacji klienta z serwerem mogą działać w ten sam sposób, jak w przypadku komunikacji z serwerem. Niezależna para wyjść protokołu może być napisana w celu zapewnienia wzajemnego uwierzytelniania zarówno klienta, jak i serwera. Pełny opis znajduje się w sekcji Programy obsługi wyjścia bezpieczeństwa kanału.

4. Identyfikacja przekazywana do wyjścia zabezpieczeń kanału

   Patrz strzałka 3. W komunikacji klienta z serwerem wyjścia zabezpieczeń kanału nie muszą działać jako para. Wyjście po stronie klienta IBM WebSphere MQ może zostać pominięte. W tym przypadku identyfikator użytkownika jest umieszczany w deskryptorze kanału (MQCD), a wyjście zabezpieczeń po stronie serwera może je zmienić, jeśli jest to wymagane.

   Klienty Windows wysyłają również dodatkowe informacje w celu ułatwienia identyfikacji.

   - Identyfikator użytkownika, który jest przekazywany do serwera, jest aktualnie zalogowanym identyfikatorem użytkownika na kliencie.
   - Identyfikator zabezpieczeń aktualnie zalogowanego użytkownika.

   Aby ułatwić identyfikację klienta IBM WebSphere MQ dla produktu HP Integrity NonStop Server, klient przekazuje alias zabezpieczeń OSS, pod którym aplikacja kliencka jest uruchomiona. Ten identyfikator jest zwykle używany w postaci <PRIMARYGROUP>.<ALIAS>. Jeśli jest to wymagane, można odwzorować ten identyfikator użytkownika na alternatywny identyfikator użytkownika w menedżerze kolejek przy użyciu rekordów uwierzytelniania kanału lub wyjścia zabezpieczeń. Więcej informacji na temat wyjść komunikatów zawiera sekcja “Odwzorowywanie tożsamości w wyjściach komunikatów” na stronie 154. Więcej informacji na temat definiowania rekordów uwierzytelniania kanału zawiera

sekcja “Odwzorowywanie identyfikatora użytkownika potwierdzonego przez klienta na identyfikator użytkownika MCAUSER” na stronie 191.

Wartości identyfikatora użytkownika i, jeśli są dostępne, identyfikatora zabezpieczeń, mogą być używane przez wyjście zabezpieczeń serwera w celu ustalenia tożsamości klienta MQI produktu IBM WebSphere MQ .

Identyfikatory użytkownika

Jeśli klient MQI produktu IBM WebSphere MQ znajduje się w systemie Windows , a serwer IBM WebSphere MQ jest również w systemie Windows i ma dostęp do domeny, w której zdefiniowany jest identyfikator użytkownika klienta, program IBM WebSphere MQ obsługuje identyfikatory użytkowników o długości do 20 znaków. Na platformach UNIX and Linux i konfiguracjach maksymalna długość wynosi 12 znaków.

Serwer WebSphere MQ for Windows nie obsługuje połączenia klienta Windows , jeśli klient jest uruchomiony z identyfikatorem użytkownika, który zawiera znak @, na przykład `abc@d`. Kod powrotu do wywołania `MQCONN` na kliencie to MQRC_NOT_AUTHORIZED.

Można jednak określić ID użytkownika, używając dwóch znaków @, na przykład `abc@@d`. Preferowaną procedurą jest użycie formatu `id@domain` , aby upewnić się, że identyfikator użytkownika jest rozstrzygany w poprawnej domenie spójnie; w ten sposób `abc@@d@domain`.

Należy zauważyć, że `UNKNOWN` jest zarezerwowanym identyfikatorem użytkownika, a identyfikator użytkownika produktu `NOBODY` również ma specjalne znaczenie dla produktu WebSphere MQ. Tworzenie identyfikatorów użytkowników w systemie operacyjnym o nazwie `UNKNOWN` lub `NOBODY` może mieć niezamierzone wyniki.

Chociaż identyfikatory użytkowników są używane do uwierzytelniania, grupy są używane do autoryzacji, z wyjątkiem systemu Windows.

Jeśli konta usługi są tworzone bez zwracania uwagi na grupy, a wszystkie identyfikatory użytkowników będą autoryzowane w inny sposób, każdy użytkownik może uzyskać dostęp do informacji o każdym innym użytkowniku.

Planowanie autoryzacji

Zaplanuj użytkowników, którzy będą mieli uprawnienia administracyjne i planują autoryzowanie użytkowników aplikacji do odpowiedniego używania obiektów IBM WebSphere MQ , w tym tych, które łączą się z klientem MQI produktu IBM WebSphere MQ .

Osoby lub aplikacje muszą mieć nadane prawa dostępu, aby można było używać produktu IBM WebSphere MQ. Wymagany dostęp do nich zależy od ról, które podejmują, oraz od zadań, które muszą wykonać. Autoryzacja w programie IBM WebSphere MQ może być podzielona na dwie główne kategorie:

- Autoryzacja do wykonywania operacji administracyjnych
- Autoryzacja aplikacji do korzystania z produktu IBM WebSphere MQ

Obie klasy operacji są kontrolowane przez ten sam komponent, a dana osoba może mieć uprawnienia do wykonywania obu kategorii operacji.

W poniższych tematach znajdują się dodatkowe informacje o konkretnych obszarach autoryzacji, które należy wziąć pod uwagę:

Uprawnienie do administrowania produktem IBM WebSphere MQ

Administratorzy produktu IBM WebSphere MQ muszą mieć uprawnienia do wykonywania różnych funkcji. Uprawnienia te są uzyskiwane w różny sposób na różnych platformach.

Administratorzy produktu IBM WebSphere MQ muszą mieć uprawnienia do:

- Wydawanie komend do administrowania produktem IBM WebSphere MQ
- UżyjIBM WebSphere MQ Explorer

Więcej informacji na ten temat można znaleźć w temacie odpowiednim dla używanego systemu operacyjnego.

Uprawnienie do administrowania produktem IBM WebSphere MQ w systemach UNIX i Windows

Administrator produktu IBM WebSphere MQ należy do grupy mqm. Ta grupa ma dostęp do wszystkich zasobów IBM WebSphere MQ i może wydawać komendy sterujące IBM WebSphere MQ . Administrator może nadać określone uprawnienia innym użytkownikom.

Aby być administratorem produktu IBM WebSphere MQ w systemach UNIX i Windows , użytkownik musi być członkiem grupy *mqm*. Ta grupa jest tworzona automatycznie podczas instalowania produktu WebSphere MQ. Aby zezwolić użytkownikom na wydawanie komend sterujących, należy dodać je do grupy mqm. Obejmuje to użytkownika root w systemach UNIX .

Użytkownikom, którzy nie są członkami grupy mqm, mogą być nadane uprawnienia administracyjne, ale nie są w stanie wydawać komend sterujących IBM WebSphere MQ i są uprawnieni do wykonywania tylko tych komend, dla których przyznano im dostęp.

Ponadto w systemach Windows konta SYSTEM i Administrator mają pełny dostęp do zasobów systemu IBM WebSphere MQ .

Wszyscy członkowie grupy mqm mają dostęp do wszystkich zasobów produktu WebSphere MQ w systemie, w tym możliwość administrowania dowolnym menedżerem kolejek uruchomionym w systemie. Ten dostęp może zostać odwołany tylko przez usunięcie użytkownika z grupy mqm. W systemach Windows członkowie grupy Administratorzy mają również dostęp do wszystkich zasobów produktu WebSphere MQ .

Administratorzy mogą używać komendy sterującej **runmqsc** do wydawania komend WebSphere MQ Script (MQSC). Jeśli komenda **runmqsc** jest używana w trybie pośrednim do wysyłania komend MQSC do zdalnego menedżera kolejek, każda komenda MQSC jest hermetyzowana w komendzie Escape PCF. Administratorzy muszą mieć wymagane uprawnienia dla komend MQSC, które mają być przetwarzane przez zdalny menedżer kolejek.

Program WebSphere MQ Explorer wydaje komendy PCF w celu wykonywania zadań administracyjnych. Administratorzy nie wymagają dodatkowych uprawnień do korzystania z programu WebSphere MQ Explorer w celu administrowania menedżerem kolejek w systemie lokalnym. Gdy program WebSphere MQ Explorer jest używany do administrowania menedżerem kolejek w innym systemie, administratorzy muszą mieć wymagane uprawnienia do komend PCF, które mają być przetwarzane przez zdalny menedżer kolejek.

Więcej informacji na temat sprawdzania uprawnień wykonywanych po przetworzeniu komend PCF i MQSC zawierają następujące tematy:

- Informacje na temat komend, które działają w menedżerach kolejek, kolejkach, kanałach, procesach, listach nazw i obiektach informacji uwierzytelniających, zawiera sekcja “Autoryzacja aplikacji do używania produktu IBM WebSphere MQ” na stronie 52.
- Informacje na temat komend, które działają na kanałach, inicjatorach kanałów, nasłuchiwaniach i klastrach, zawiera sekcja Zabezpieczenia kanału.

Więcej informacji na temat uprawnień wymaganych do administrowania produktem WebSphere MQ w systemach UNIX i Windows można znaleźć w pokrewnych informacjach.

Autoryzacja aplikacji do używania produktu IBM WebSphere MQ

Gdy aplikacje uzyskują dostęp do obiektów, identyfikatory użytkowników powiązane z aplikacjami muszą mieć odpowiednie uprawnienia.

Aplikacje mogą uzyskiwać dostęp do następujących obiektów produktu IBM WebSphere MQ , wywołując wywołania MQI:

- Menedżery kolejek
- Kolejki

- Procesy
- Listy nazw
- Tematy

Aplikacje mogą również używać komend PCF do administrowania obiektami produktu IBM WebSphere MQ . Gdy komenda PCF jest przetwarzana, używa kontekstu uprawnień identyfikatora użytkownika, który umieł komunikat PCF.

Aplikacje, w tym kontekście, obejmują te, które są zapisywane przez użytkowników i dostawców.

Aplikacje, które korzystają z klas IBM WebSphere MQ dla języka Java, klas IBM WebSphere MQ dla usługi JMS, klas IBM WebSphere MQ dla środowiska .NET lub Message Service Clients for C/C++ and .NET używają pośrednio interfejsu MQI.

W celu uzyskania dostępu do obiektów WebSphere MQ wymagane są również wywołania MQI i identyfikatory użytkowników powiązane z MCA. Więcej informacji na temat tych identyfikatorów użytkowników i wymaganych przez nie uprawnień zawiera sekcja "Autoryzacja kanału" na stronie 72.

Gdy przeprowadzane są kontrole uprawnień

Sprawdzanie uprawnień jest wykonywane, gdy aplikacja próbuje uzyskać dostęp do menedżera kolejek, kolejki, procesu lub listy nazw.

Kontrole są przeprowadzane w następujących okolicznościach:

Gdy aplikacja łączy się z menedżerem kolejek przy użyciu wywołania MQCONN lub MQCONNX
Menedżer kolejek zwraca się do systemu operacyjnego o podanie identyfikatora użytkownika powiązanego z aplikacją. Następnie menedżer kolejek sprawdza, czy ID użytkownika jest uprawniony do łączenia się z nim i zachowuje ID użytkownika w celu przeprowadzenia przyszłych operacji sprawdzania.

Użytkownicy nie muszą logować się do produktu IBM WebSphere MQ. Program IBM WebSphere MQ zakłada, że użytkownicy są wpisani do bazowego systemu operacyjnego i są przez niego uwierzytelniani.

Gdy aplikacja otwiera obiekt IBM WebSphere MQ przy użyciu wywołania MQOPEN lub MQPUT1
Wszystkie sprawdzenia uprawnień są wykonywane po otwarciu obiektu, a nie w przypadku, gdy jest on dostępny później. Na przykład sprawdzanie uprawnień jest wykonywane po otwarciu kolejki przez aplikację. Nie są one wykonywane, gdy aplikacja umieszcza komunikaty w kolejce lub pobiera komunikaty z kolejki.

Gdy aplikacja otwiera obiekt, określa on typy operacji, które musi wykonać na obiekcie. Na przykład aplikacja może otworzyć kolejkę w celu przeglądania komunikatów na niej, pobrać z niej komunikaty, ale nie umieszczać na nim komunikatów. Dla każdego typu operacji menedżer kolejek sprawdza, czy identyfikator użytkownika powiązany z aplikacją ma uprawnienia do wykonania tej operacji.

Gdy aplikacja otwiera kolejkę, wykonywane są sprawdzenia uprawnień względem obiektu określonego w polu ObjectName deskryptora obiektu. Pole ObjectName jest używane w wywołaniach produktu MQOPEN lub MQPUT1 . Jeśli obiekt jest kolejką aliasową lub definicją kolejki zdalnej, sprawdzane są, czy są one wykonywane względem samego obiektu. Nie są one wykonywane w kolejce, do której tłumaczona jest kolejka aliasowa lub definicja kolejki zdalnej. Oznacza to, że użytkownik nie potrzebuje uprawnień dostępu do niego. Ogranicz uprawnienia do tworzenia kolejek do użytkowników uprzywilejowanych. Jeśli nie, użytkownicy mogą ominąć zwykłą kontrolę dostępu po prostu przez utworzenie aliasu.

Aplikacja może jawnie odwoływać się do kolejki zdalnej. Ustawia pola ObjectName i ObjectQMgrName w deskryptorze obiektu na nazwy kolejki zdalnej i zdalnego menedżera kolejek. Sprawdzanie uprawnień jest wykonywane względem kolejki transmisji o takiej samej nazwie, jak nazwa zdalnego menedżera kolejek. W systemie UNIX, Linux, and Windowsjest wykonywane sprawdzenie profilu RQMNAME, który jest zgodny z nazwą zdalnego menedżera kolejek, jeśli używane jest łączenie w klastry. Aplikacja może odwoływać się jawnie do kolejki klastra, ustawiając pole ObjectName w deskryptorze obiektu na nazwę kolejki klastra. Sprawdzanie uprawnień jest wykonywane względem kolejki transmisji klastra SYSTEM.CLUSTER.TRANSMIT.QUEUE.

Uprawnienie do kolejki dynamicznej jest oparte na kolejce modelowej, z której pochodzi, ale niekoniecznie jest takie same; patrz uwaga 1.

Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest uzyskiwany z systemu operacyjnego. Identyfikator użytkownika jest uzyskiwany, gdy aplikacja łączy się z menedżerem kolejek. Odpowiednio autoryzowana aplikacja może wywołać wywołanie MQOPEN , określając alternatywny ID użytkownika. Następnie zostaną przeprowadzone sprawdzenia kontroli dostępu na alternatywnym identyfikatorze użytkownika. Użycie alternatywnego identyfikatora użytkownika nie powoduje zmiany identyfikatora użytkownika powiązanego z aplikacją, a tylko tego, który jest używany do sprawdzania kontroli dostępu.

Gdy aplikacja subskrybuje temat przy użyciu wywołania MQSUB
Gdy aplikacja subskrybuje temat, określa on typ operacji, którą musi wykonać. Jest to utworzenie subskrypcji, zmiana istniejącej subskrypcji lub ponowne utworzenie istniejącej subskrypcji bez jej zmiany. Dla każdego typu operacji menedżer kolejek sprawdza, czy identyfikator użytkownika powiązany z aplikacją ma uprawnienia do wykonania operacji.

Gdy aplikacja subskrybuje temat, wykonywane są sprawdzenia uprawnień względem obiektów tematów, które znajdują się w drzewie tematów. Obiekty tematów znajdują się w punkcie drzewa tematów, w którym aplikacja została zasubskrybowana, lub powyżej. Sprawdzanie uprawnień może obejmować sprawdzenie więcej niż jednego obiektu tematu. Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest uzyskiwany z systemu operacyjnego. Identyfikator użytkownika jest uzyskiwany, gdy aplikacja łączy się z menedżerem kolejek.

Menedżer kolejek wykonuje sprawdzanie uprawnień w kolejkach subskrybenta, ale nie w kolejkach zarządzanych.

Gdy aplikacja usuwa stałą kolejkę dynamiczną za pomocą wywołania MQCLOSE
Uchwyt obiektu określony w wywołaniu MQCLOSE nie musi być taki sam, jak zwrócony przez wywołanie MQOPEN , które utworzyło stałą kolejkę dynamiczną. Jeśli jest inaczej, menedżer kolejek sprawdza identyfikator użytkownika powiązany z aplikacją, która wywołała wywołanie MQCLOSE . Sprawdza, czy ID użytkownika jest uprawniony do usunięcia kolejki.

Jeśli aplikacja, która zamknie subskrypcję w celu usunięcia jej, nie utworzyła jej, wymagane są odpowiednie uprawnienia do jej usunięcia.

Gdy komenda PCF działająca na obiekcie WebSphere MQ jest przetwarzana przez serwer komend.
Ta reguła obejmuje przypadek, w którym komenda PCF działa na obiekcie informacji uwierzytelniającej.

Identyfikator użytkownika, który jest używany do sprawdzania uprawnień, jest identyfikatorem znalezionym w polu UserIdentifier w deskryptorze komunikatu komendy PCF. Ten identyfikator użytkownika musi mieć wymagane uprawnienia w menedżerze kolejek, w którym komenda jest przetwarzana. Równoważna komenda MQSC enkapsulowana w komendzie Escape PCF jest traktowana w ten sam sposób. Więcej informacji na temat pola UserIdentifier oraz sposobu jego ustawiania zawiera sekcja “Kontekst komunikatu” na stronie 55.

Alternatywne uprawnienia użytkownika

Gdy aplikacja otworzy obiekt lub subskrybuje temat, aplikacja może podać identyfikator użytkownika w wywołaniu MQOPEN, MQPUT1lub MQSUB. Może on zwrócić się do menedżera kolejek o użycie tego identyfikatora użytkownika do sprawdzania uprawnień zamiast do powiązanego z aplikacją.

Aplikacja powiedzie się, otwierając obiekt tylko wtedy, gdy spełnione są oba poniższe warunki:

- ID użytkownika powiązany z aplikacją ma uprawnienia do podania innego identyfikatora użytkownika w celu sprawdzenia uprawnień. Aplikacja jest mówiła, że ma *alternatywne uprawnienia użytkownika*.
- Identyfikator użytkownika podany przez aplikację ma uprawnienia do otwierania obiektu dla typów żądanych operacji lub do subskrybowania tematu.

Kontekst komunikatu

Informacja *Kontekst komunikatu* umożliwia aplikacji, która pobiera komunikat, w celu uzyskania informacji o inicjatorze komunikatu. Informacje są przechowywane w polach w deskryptorze komunikatu, a pola są podzielone na trzy części logiczne.

Są to następujące części:

kontekst tożsamości
Te pola zawierają informacje o użytkowniku aplikacji, która umieła umieścić komunikat w kolejce.

kontekst źródłowy
Pola te zawierają informacje o samej aplikacji oraz o tym, kiedy komunikat został umieszczony w kolejce.

kontekst użytkownika
Te pola zawierają właściwości komunikatów, których aplikacje mogą używać do wybierania komunikatów, które menedżer kolejek powinien dostarczyć.

Gdy aplikacja umieszcza komunikat w kolejce, aplikacja może zwrócić się do menedżera kolejek o wygenerowanie informacji kontekstowych w komunikacie. Jest to działanie domyślne. Alternatywnie można określić, że pola kontekstu nie zawierają żadnych informacji. Identyfikator użytkownika powiązany z aplikacją nie wymaga uprawnień specjalnych do wykonania żadnej z tych czynności.

Aplikacja może ustawić pola kontekstu tożsamości w komunikacie, zezwalając menedżerowi kolejek na wygenerowanie kontekstu źródłowego lub ustawić wszystkie pola kontekstu. Aplikacja może również przekazać pola kontekstu tożsamości z komunikatu, który został pobrany na komunikat, który umieszcza w kolejce lub może przekazać wszystkie pola kontekstu. Jednak identyfikator użytkownika powiązany z aplikacją wymaga uprawnień do ustawiania lub przekazywania informacji kontekstowych. Aplikacja określa, że ma zamiar ustawić lub przekazać informacje kontekstowe, gdy otwiera kolejkę, na której ma zostać umieszczone komunikaty, a jego uprawnienia są teraz sprawdzane.

Poniżej znajduje się krótki opis każdego z pól kontekstu:

kontekst tożsamości

UserIdentifier
Identyfikator użytkownika powiązany z aplikacją, która umieła komunikat. Jeśli menedżer kolejek ustawia to pole, jest on ustawiany na identyfikator użytkownika uzyskany z systemu operacyjnego, gdy aplikacja łączy się z menedżerem kolejek.

AccountingToken
Informacje, które mogą być używane do naliczania opłat za pracę wykonanego w wyniku komunikatu.

Dane_tożsamości_aplikacji
Jeśli identyfikator użytkownika powiązany z aplikacją ma uprawnienie do ustawiania pól kontekstu tożsamości lub do ustawienia wszystkich pól kontekstu, wówczas aplikacja może ustawić to pole na dowolną wartość powiązaną z tożsamością. Jeśli to pole jest ustawione przez menedżera kolejek, to pole jest puste.

Kontekst źródłowy

Typ_aplikacji_wstawiającej
Typ aplikacji, która umieszczała komunikat; na przykład transakcja CICS .

Nazwa_aplikacji_wstawiającej
Nazwa aplikacji umieszczonej w komunikacie.

PutDate
Data umieszczenia komunikatu.

PutTime
Czas, w którym komunikat został umieszczony.

Dane_pochodzenia_aplikacji
Jeśli identyfikator użytkownika powiązany z aplikacją ma uprawnienie do ustawiania wszystkich pól kontekstu, wówczas aplikacja może ustawić to pole na dowolną wartość powiązaną z pochodzeniem. Jeśli to pole jest ustawione przez menedżera kolejek, to pole jest puste.

Kontekst użytkownika

Dla produktu **MQINQMP** lub **MQSETMP**obsługiwane są następujące wartości:

MQPD_USER _CONTEXT

Właściwość jest powiązana z kontekstem użytkownika.

Do ustawienia właściwości powiązanej z kontekstem użytkownika przy użyciu wywołania MQSETMP nie jest wymagana żadna specjalna autoryzacja.

W przypadku menedżera kolejek w wersji V7.0 lub nowszej, właściwość powiązana z kontekstem użytkownika jest zapisywana w sposób opisany w tabeli MQOO_SAVE_ALL_CONTEXT. Wartość MQPUT z podaną wartością MQOO_PASS_ALL_CONTEXT powoduje, że właściwość zostanie skopiowana z zapisanego kontekstu do nowego komunikatu.

MQPD_NO_CONTEXT

Ta właściwość nie jest powiązana z kontekstem komunikatu.

Nierozpoznana wartość jest odrzucana za pomocą wywołania MQRC_PD_ERROR. Wartością początkową tego pola jest **MQPD_NO_CONTEXT**.

Szczegółowy opis każdego z pól kontekstu znajduje się w sekcji MQMD-deskryptor komunikatu. Więcej informacji na temat sposobu korzystania z kontekstu komunikatu zawiera sekcja Kontekst komunikatu.

Uprawnienia do pracy z obiektami IBM WebSphere MQ w systemach UNIX, Linux i Windows

Komponent usługi autoryzacji dostarczany z produktem IBM WebSphere MQ jest nazywany *menedżerem uprawnień do obiektów (OAM)*. Zapewnia kontrolę dostępu za pomocą sprawdzania uwierzytelniania i autoryzacji.

1. AUTHENTICATION.

   Sprawdzanie uwierzytelniania wykonywane przez usługę OAM udostępniane z produktem IBM WebSphere MQ jest podstawowe i jest wykonywane tylko w określonych okolicznościach. Nie jest on przeznaczony do spełnienia surowych wymagań oczekiwanych w wysoce bezpiecznym środowisku.

   OAM wykonuje sprawdzenie uwierzytelniania, gdy aplikacja łączy się z menedżerem kolejek, a następujące warunki są spełnione.

   Jeśli struktura MQCSP została dostarczona przez aplikację nawiązaną do połączenia, a atrybut *AuthenticationType* w strukturze MQCSP ma wartość MQCSP_AUTH_USER_ID_AND_PWD, to sprawdzanie jest wykonywane przez OAM w swojej funkcji MQZID_AUTHENTICATE_USER. Jest to sprawdzenie, czy identyfikator użytkownika w strukturze MQCSP jest porównywany z identyfikatorem użytkownika w *IdentityContext* (MQZIC), aby określić, czy są one zgodne. Jeśli nie są one zgodne, sprawdzenie nie powiedzie się.

   Ta podstawowa kontrola nie jest przeznaczona do pełnego uwierzytelnienia użytkownika. Na przykład nie ma sprawdzania autentyczności użytkownika, sprawdzając hasło podane w strukturze MQCSP. Ponadto, jeśli aplikacja pomija strukturę MQCSP, to nie jest wykonywane żadne sprawdzenie.

   Jeśli w menedżerze kolejek wymagane są pełniejsze usługi uwierzytelniania za pośrednictwem komponentu usługi autoryzacji, program OAM z produktem IBM WebSphere MQ nie oferuje tego usługi. Należy napisać nowy komponent usługi autoryzacji lub pobrać go od dostawcy.

2. Autoryzacja.

   Kontrole autoryzacji są wyczerpujące i są przeznaczone do spełnienia najbardziej normalnych wymagań.

   Sprawdzenia autoryzacji są wykonywane, gdy aplikacja wysyła wywołanie MQI w celu uzyskania dostępu do menedżera kolejek, kolejki, procesu, tematu lub listy nazw. Są one również wykonywane w innych sytuacjach, na przykład gdy komenda jest wykonywana przez serwer komend.

W systemach UNIX, Linux i Windows , *usługa autoryzacji* zapewnia kontrolę dostępu, gdy aplikacja wysyła wywołanie MQI w celu uzyskania dostępu do obiektu IBM WebSphere MQ , który jest menedżerem

kolejek, kolejką, procesem, tematem lub listą nazw. Obejmuje to sprawdzanie uprawnień alternatywnych użytkowników oraz uprawnienia do ustawiania lub przekazywania informacji kontekstowych.

W systemie WindowsOAM daje członkom grupy Administratorzy uprawnienia do uzyskiwania dostępu do wszystkich obiektów IBM WebSphere MQ , nawet jeśli włączona jest opcja UAC.

Dodatkowo w systemach Windows konto SYSTEM ma pełny dostęp do zasobów IBM WebSphere MQ .

Usługa autoryzacji zapewnia również sprawdzanie uprawnień, gdy komenda PCF działa na jednym z tych obiektów produktu IBM WebSphere MQ lub na obiekcie informacji uwierzytelniającej. Równoważna komenda MQSC enkapsulowana w komendzie Escape PCF jest traktowana w ten sam sposób.

Usługa autoryzacji jest *usługą instalowalną*, co oznacza, że jest ona implementowana przez co najmniej jeden *instalowalny komponent usługi*. Każdy komponent jest wywoływany przy użyciu udokumentowanego interfejsu. Dzięki temu użytkownicy i dostawcy mogą udostępniać komponenty do rozszerzania lub zastępowania produktów dostarczanych przez produkty IBM WebSphere MQ .

Komponent usługi autoryzacji dostarczany z produktem IBM WebSphere MQ jest nazywany *menedżerem uprawnień do obiektów (OAM)*. OAM jest automatycznie włączany dla każdego menedżera kolejek, który został utworzony.

OAM zarządza listą kontroli dostępu (ACL) dla każdego obiektu IBM WebSphere MQ , do którego steruje dostępem. W systemach UNIX and Linux tylko identyfikatory grup mogą być wyświetlane na liście ACL. Oznacza to, że wszyscy członkowie grupy mają te same uprawnienia. W systemach Windows na liście ACL mogą być wyświetlane zarówno identyfikatory użytkowników, jak i identyfikatory grup. Oznacza to, że uprawnienia mogą być przyznawane poszczególnym użytkownikom i grupom.

Ograniczenie dotyczące 12 znaków dotyczy zarówno grupy, jak i identyfikatora użytkownika. Platformy UNIX zwykle ograniczają długość identyfikatora użytkownika do 12 znaków. AIX i produkt Linux podniósł ten limit, ale produkt IBM WebSphere MQ nadal obserwuje 12 znaków ograniczenia na wszystkich platformach UNIX . Jeśli używany jest identyfikator użytkownika o długości większej niż 12 znaków, IBM WebSphere MQ zastąpi go wartością "UNKNOWN". Nie należy definiować ID użytkownika o wartości "UNKNOWN".

OAM może uwierzytelnić użytkownika i zmienić odpowiednie pola kontekstu tożsamości. Tę opcję należy włączyć, określając strukturę parametrów zabezpieczeń połączenia (MQCSP) w wywołaniu MQCONNX. Struktura jest przekazywana do funkcji OAM Authenticate User (MQZ_AUTHENTICATE_USER), która ustawia odpowiednie pola kontekstu tożsamości. W przypadku połączenia MQCONNX z klienta IBM WebSphere MQ informacje w module MQCSP są wyświetlane w menedżerze kolejek, z którym łączy się klient przez kanał połączenia klienckiego i kanału połączenia z serwerem. Jeśli wyjścia zabezpieczeń są zdefiniowane w tym kanale, protokół MQCSP jest przekazywany do każdego wyjścia zabezpieczeń i może zostać zmieniony przez wyjście. Wyjścia zabezpieczeń mogą również tworzyć protokół MQCSP. Więcej informacji na temat korzystania z wyjść zabezpieczeń w tym kontekście można znaleźć w sekcji Programy obsługi wyjścia zabezpieczeń kanału.

W systemach UNIX, Linux i Windows komenda sterująca **setmqaut** nadaje uprawnienia i odbiera uprawnienia i jest używana do obsługi list ACL. Na przykład komenda:

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER +browse +get
```

umożliwia członkom grupy VOYAGER przeglądanie komunikatów w kolejce MOON.EUROPA , której właścicielem jest menedżer kolejek JUPITER. Pozwala ona członkom na pobieranie komunikatów z kolejki. Aby odebrać te uprawnienia później, wprowadź następującą komendę:

```
setmqaut -m JUPITER -t queue -n MOON.EUROPA -g VOYAGER -browse -get
```

Komenda:

```
setmqaut -m JUPITER -t queue -n MOON.* -g VOYAGER +put
```

umożliwia członkom grupy VOYAGER umieszczanie komunikatów w dowolnej kolejce o nazwie, która rozpoczyna się od znaków `MOON.` . MOON.* to nazwa profilu ogólnego.*Profil ogólny* umożliwia nadanie uprawnień do zbioru obiektów za pomocą jednej komendy **setmqaut** .

Komenda sterująca **dspmqaut** jest dostępna do wyświetlania bieżących uprawnień użytkownika lub grupy dla określonego obiektu.Komenda sterowania **dmpmqaut** jest również dostępna w celu wyświetlenia bieżących uprawnień powiązanych z profilami ogólnymi.

Jeśli użytkownik nie chce, aby jakiekolwiek kontrole uprawnień, na przykład w środowisku testowym, można wyłączyć OAM.

Korzystanie z PCF w celu uzyskania dostępu do komend OAM
W systemach UNIX, Linux i Windows można użyć komend PCF w celu uzyskania dostępu do komend administracyjnych OAM.

Komendy PCF i ich równoważne komendy OAM są następujące:

Tabela 6. Komendy PCF i odpowiadające im komendy OAM

PCF, komenda	**OAM, komenda**
Sprawdź rekordy uprawnień	dmpmqaut
Sprawdź uprawnienia jednostki	dspmqaut
Ustaw rekord uprawnień	setmqaut
Usuń rekord uprawnień	setmqaut z opcją -remove

Komendy **setmqaut** i **dmpmqaut** są ograniczone do członków grupy mqm. Równoważne komendy PCF mogą być wykonywane przez użytkowników w dowolnej grupie, dla której przyznano uprawnienia dsp i chg w menedżerze kolejek.

Więcej informacji na temat używania tych komend zawiera sekcja Wprowadzenie do formatów komend programowalnych .

Zabezpieczenia dla zdalnego przesyłania komunikatów

W tej sekcji opisano aspekty bezpieczeństwa dotyczące zdalnego przesyłania komunikatów.

Użytkownik musi udostępnić użytkownikom uprawnienia do korzystania z urządzeń IBM WebSphere MQ . Jest to zorganizowane zgodnie z działaniami, które należy podjąć w odniesieniu do obiektów i definicji. Na przykład:

- Menedżerowie kolejek mogą być uruchamiani i zatrzymani przez autoryzowanych użytkowników.
- Aplikacje muszą łączyć się z menedżerem kolejek i mieć uprawnienia do korzystania z kolejek.
- Kanały komunikatów muszą być tworzone i kontrolowane przez autoryzowanych użytkowników.
- Obiekty są przechowywane w bibliotekach, a dostęp do tych bibliotek może być ograniczony

Agent kanału komunikatów w ośrodku zdalnym musi sprawdzić, czy dostarczony komunikat pochodzi od użytkownika z uprawnieniami do wykonania w tym zdalnym ośrodku. Ponadto, jako że MCAs może być uruchomiony zdalnie, może być konieczne sprawdzenie, czy zdalne procesy, które próbują uruchomić MCA, są do tego upoważnione. Istnieją cztery możliwe sposoby radzenia sobie z tym:

1. Użyj atrybutu PutAuthority dla definicji kanału RCVR, RQSTR lub CLUSRCVR, aby określić, który użytkownik jest używany do sprawdzania autoryzacji w czasie umieszczania komunikatów przychodzących w kolejkach. Zapoznaj się z opisem komendy DEFINE CHANNEL w podręczniku MQSC Command Reference.
2. Zaimplementuj rekordy uwierzytelniania kanału, aby odrzucić niepożądane próby połączenia, lub aby ustawić wartość MCAUSER na podstawie: zdalnego adresu IP, identyfikatora użytkownika zdalnego, podanej nazwy wyróżniającej (DN) protokołu SSL lub TLS lub nazwy zdalnego menedżera kolejek.
3. Zaimplementuj sprawdzanie zabezpieczeń *wyjść użytkownika* , aby upewnić się, że odpowiedni kanał komunikatów jest autoryzowany. Bezpieczeństwo instalacji udostępniające odpowiedni kanał zapewnia, że wszyscy użytkownicy są odpowiednio autoryzowani, dzięki czemu nie ma potrzeby sprawdzania poszczególnych wiadomości.

4. Zaimplementuj przetwarzanie komunikatów *wyjścia użytkownika* , aby upewnić się, że pojedyncze komunikaty są sprawdzane w celu autoryzacji.

Zabezpieczenia obiektów w systemach UNIX and Linux

Użytkownicy administracyjni muszą być częścią grupy mqm w systemie użytkownika (w tym użytkownika root), jeśli ten identyfikator będzie używać komend administracyjnych produktu IBM WebSphere MQ .

Zawsze należy uruchamiać amqcrsta jako identyfikator użytkownika "mqm".

Identyfikatory użytkowników w systemach UNIX and Linux

Menedżer kolejek przekształca wszystkie wielkie lub mieszane identyfikatory użytkownika w małe litery. Następnie menedżer kolejek wstawia identyfikatory użytkowników do części kontekstu komunikatu lub sprawdza ich autoryzację. W związku z tym autoryzacje są oparte tylko na małych identyfikatorach.

Zabezpieczenia obiektów w systemach Windows

Jeśli ten identyfikator będzie używać komend administracyjnych produktu IBM WebSphere MQ , użytkownicy administracyjni muszą należeć do grupy mqm i do grupy administratorów w systemach Windows .

Identyfikatory użytkowników w systemach Windows

W systemach Windows , *jeśli nie zainstalowano wyjścia komunikatów*, menedżer kolejek przekształca wszystkie wielkie lub mieszane identyfikatory użytkownika w małe litery. Następnie menedżer kolejek wstawia identyfikatory użytkowników do części kontekstu komunikatu lub sprawdza ich autoryzację. W związku z tym autoryzacje są oparte tylko na małych identyfikatorach.

Identyfikatory użytkowników w systemach

Platformy inne niż Windows , w systemach UNIX and Linux używają wielkich liter dla identyfikatorów użytkowników w komunikatach.

Aby system Windows, UNIX and Linux mógł używać małych identyfikatorów użytkowników w komunikatach, następujące konwersje są wykonywane przez agenta kanału komunikatów (MCA) na tych platformach:

Na końcu wysyłającej
Znaki alfabetu we wszystkich identyfikatorach użytkowników są przekształcane na wielkie litery, jeśli nie jest zainstalowany żaden program obsługi wyjścia komunikatów.

Na końcu odbioru
Znaki alfabetu we wszystkich identyfikatorach użytkowników są przekształcane na małe litery, jeśli nie jest zainstalowany żaden program obsługi wyjścia komunikatów.

Konwersje automatyczne nie są wykonywane, jeśli użytkownik udostępni wyjście komunikatów w systemach UNIX, Linux i Windows z innych przyczyn.

Korzystanie z niestandardowej usługi autoryzacji

Produkt IBM WebSphere MQ udostępnia instalowalną usługę autoryzacji. Istnieje możliwość zainstalowania usługi alternatywnej.

Komponent usługi autoryzacji dostarczany z produktem IBM WebSphere MQ jest nazywany menedżerem uprawnień do obiektów (Object Authority Manager-OAM). Jeśli OAM nie dostarcza potrzebnych narzędzi autoryzacji, możesz napisać własny komponent usługi autoryzacji. Możliwe do zainstalowania funkcje usługi, które muszą być zaimplementowane przez komponent usługi autoryzacji, są opisane w sekcji Informacje uzupełniające dotyczące interfejsu usług instalowalnych.

Kontrola dostępu dla klientów

Kontrola dostępu oparta jest na identyfikatorach użytkowników. Może istnieć wiele identyfikatorów użytkowników do administrowania, a identyfikatory użytkowników mogą być w różnych formatach.

Dla właściwości kanału połączenia serwera MCAUSER można ustawić specjalną wartość identyfikatora użytkownika, która będzie używana przez klienty.

Kontrola dostępu w produkcie IBM WebSphere MQ jest oparta na identyfikatorach użytkowników. Zwykle używany jest identyfikator użytkownika procesu tworzenia wywołań MQI. W przypadku klientów MQI produktu MQ agent MCA połączenia z serwerem wykonuje wywołania MQI w imieniu klientów MQI produktu MQ . Istnieje możliwość wybrania alternatywnego ID użytkownika dla agenta MCA połączenia z serwerem, który ma być używany do wykonywania wywołań MQI. Alternatywny identyfikator użytkownika może być powiązany z kliencką stacją roboczą albo z dowolnym elementem, który ma zostać zorganizowany i sterowany dostępem klientów. ID użytkownika musi mieć przypisane do niego odpowiednie uprawnienia na serwerze, aby wywołać wywołania MQI. Wybór alternatywnego identyfikatora użytkownika jest preferowany, aby umożliwić klientom nawiąże połączenia MQI z uprawnieniami MCA połączenia z serwerem.

Tabela 7. Identyfikator użytkownika używany przez kanał połączenia z serwerem.

ID użytkownika	W przypadku użycia
Identyfikator użytkownika, który jest ustawiany przez wyjście zabezpieczeń	Używane, o ile nie jest zablokowane przez regułę **CHLAUTH TYPE(BLOCKUSER)** . Więcej informacji można znaleźć w poniższej sekcji “Ustawianie identyfikatora użytkownika w wyjściu zabezpieczeń” na stronie 61 .
Identyfikator użytkownika ustawiony za pomocą reguły CHLAUTH	Używane, o ile nie zostało ono zastąpione przez wyjście zabezpieczeń. Więcej informacji na ten temat zawiera sekcja Rekordy uwierzytelniania kanału .
Identyfikator użytkownika, który jest zdefiniowany w atrybucie **MCAUSER** w definicji kanału SVRCONN	Używany, o ile nie jest on używany przez wyjście zabezpieczeń lub regułę CHLAUTH.
Identyfikator użytkownika, który jest dostępny z komputera klienta	Używany, gdy żaden identyfikator nie jest ustawiony w żaden inny sposób.
ID użytkownika, który uruchomił kanał połączenia z serwerem	Używana, gdy żaden inny identyfikator użytkownika nie jest ustawiony na żaden inny sposób, a żaden identyfikator użytkownika klienta nie jest dostępny. Więcej informacji można znaleźć w poniższej sekcji “Identyfikator użytkownika, który uruchamia program kanału” na stronie 61 .

Ponieważ agent MCA połączenia z serwerem wykonuje wywołania MQI w imieniu zdalnych użytkowników, ważne jest, aby uwzględnić konsekwencje związane z zabezpieczeniami agenta MCA połączenia z serwerem wysyłającego wywołania MQI w imieniu klientów zdalnych oraz sposób administrowania dostępem potencjalnie dużej liczby użytkowników.

- Jedno z nich dotyczy połączenia serwera MCA z serwerem MCA w celu wywołania interfejsu MQI w ramach własnego uprawnienia. Jednak ze względu na to, że agent MCA połączy się z jego potężnymi możliwościami dostępu, zwykle jest to niepożądane, aby wywołać wywołania MQI w imieniu użytkowników klienta.
- Innym podejściem jest użycie ID użytkownika, który przepływa od klienta. Agent MCA połączenia z serwerem może wydawać wywołania MQI za pomocą możliwości dostępu dla identyfikatora użytkownika klienta. Podejście to przedstawia kilka pytań, które należy wziąć pod uwagę:

  1. Istnieją różne formaty dla ID użytkownika na różnych platformach. Czasami powoduje to problemy, jeśli format identyfikatora użytkownika na kliencie różni się od dopuszczalnych formatów na serwerze.
  2. Istnieje potencjalnie wiele klientów, z różnymi i zmieniających się identyfikatorów użytkowników. Identyfikatory muszą być zdefiniowane i zarządzane na serwerze.

3. Czy identyfikator użytkownika ma być zaufany? Każdy ID użytkownika może być używany przez klienta, a nie musi być identyfikatorem zalogowanego użytkownika. Na przykład, klient może przepływać ID z pełnym uprawnieniami `mqm` , które zostało celowo zdefiniowane tylko na serwerze ze względów bezpieczeństwa.

- Preferowanym podejściem jest zdefiniowanie tokenów identyfikacji klienta na serwerze, a więc ograniczenie możliwości aplikacji połączonych z klientem. Zazwyczaj jest to realizowane przez ustawienie właściwości MCAUSER kanału połączenia z serwerem na specjalną wartość identyfikatora użytkownika, która ma być używana przez klienty, a także definiowanie kilku identyfikatorów używanych przez klienty z różnym poziomem autoryzacji na serwerze.

Ustawianie identyfikatora użytkownika w wyjściu zabezpieczeń

W przypadku klientów MQI produktu IBM WebSphere MQ proces, który wydaje wywołania MQI, jest agentem MCA połączenia z serwerem. Identyfikator użytkownika używany przez agenta MCA połączenia z serwerem jest zawarty w polach `MCAUserIdentifier` lub `LongMCAUserIdentifier` na zmaterializowanych tabelach MQCD. Zawartość tych pól jest ustawiana przez:

- Wszystkie wartości ustawione przez wyjścia zabezpieczeń
- Identyfikator użytkownika z klienta
- MCAUSER (w definicji kanału połączenia z serwerem)

Wyjście zabezpieczeń może przesłonić wartości, które są widoczne dla niego, po wywołaniu.

- Jeśli atrybut MCAUSER kanału połączenia z serwerem jest ustawiony na wartość niepustą, używana jest wartość MCAUSER.
- Jeśli atrybut MCAUSER kanału połączenia z serwerem jest pusty, używany jest identyfikator użytkownika otrzymany od klienta.
- Jeśli atrybut MCAUSER kanału połączenia z serwerem jest pusty, a klient nie otrzymuje żadnego identyfikatora użytkownika, używany jest identyfikator użytkownika, który uruchomił kanał połączenia z serwerem.

Upewnij się, że pole MCAUSER jest ograniczone do 12 znaków na platformach Windows, ponieważ wszystkie dodatkowe znaki zostaną obcięte, co może prowadzić do awarii autoryzacji.

Klient IBM WebSphere MQ nie przepływa asertywnego identyfikatora użytkownika na serwerze, gdy używane jest wyjście zabezpieczeń po stronie klienta.

Identyfikator użytkownika, który uruchamia program kanału

Gdy pola ID użytkownika są pobierane z ID użytkownika, który uruchomił kanał połączenia z serwerem, używana jest następująca wartość:

- W przypadku bazy danych z/OSidentyfikator użytkownika przypisany do uruchomionego zadania inicjatora kanału przez tabelę procedur uruchomionych w produkcie z/OS .
- Dla TCP/IP (non-z/OS) identyfikator użytkownika z pozycji `inetd.conf` lub identyfikator użytkownika, który uruchomił program nasłuchujący.
- Dla SNA (non-z/OS): ID użytkownika z pozycji serwera SNA lub (jeśli nie istnieje) przychodzące żądanie przyłączenia lub ID użytkownika, który uruchomił program nasłuchujący.
- W protokole NetBIOS lub SPX identyfikator użytkownika, który uruchomił proces nasłuchiwania.

Jeśli istnieją definicje kanału połączenia z serwerem, które mają atrybut MCAUSER ustawiony na wartość pustą, klienty mogą używać tej definicji kanału do łączenia się z menedżerem kolejek przy użyciu uprawnień dostępu określonych przez identyfikator użytkownika dostarczony przez klienta. Może to być ekspozycja zabezpieczeń, jeśli system, na którym działa menedżer kolejek, zezwala na nieautoryzowane połączenia sieciowe. Domyślny kanał połączenia serwera IBM WebSphere MQ (SYSTEM.DEF.SVRCONN), atrybut MCAUSER ma wartość pustą. Aby zapobiec dostępowi bez uprawnień, należy zaktualizować atrybut MCAUSER definicji domyślnej z identyfikatorem użytkownika, który nie ma dostępu do obiektów produktu IBM WebSphere MQ MQ .

Wielkość liter w identyfikatorach użytkowników

Podczas definiowania kanału za pomocą programu `runmqsc`atrybut MCAUSER jest zmieniany na wielkie litery, chyba że identyfikator użytkownika jest zawarty w pojedynczych znakach cudzysłowu.

W przypadku serwerów w systemach UNIX, Linux i Windows zawartość pola `MCAUserIdentifier` , które jest odbierane od klienta, jest zmieniana na małe litery.

W przypadku serwerów w systemie IBM itreść pola `LongMCAUserIdentifier` otrzymanego od klienta jest zmieniana na wielkie litery.

W przypadku serwerów w systemach UNIX and Linux treść pola `LongMCAUserIdentifier` otrzymanego od klienta jest zmieniana na małe litery.

Domyślnie identyfikator użytkownika, który jest przekazywany, gdy używana jest aplikacja powiązania MQ JMS , jest identyfikatorem użytkownika wirtualnej maszyny języka Java, na której działa aplikacja.

Istnieje również możliwość przekazania identyfikatora użytkownika za pomocą metody `createQueueConnection` .

Planowanie poufności

Zaplanuj, w jaki sposób zachować poufność danych.

Poufność można zaimplementować na poziomie aplikacji lub na poziomie łącza. Użytkownik może zdecydować się na użycie protokołu SSL lub TLS, w którym to przypadku należy zaplanować użycie certyfikatów cyfrowych. Programów obsługi wyjścia kanału można również używać, jeśli standardowe urządzenia nie spełniają wymagań.

Pojęcia pokrewne

“Porównywanie zabezpieczeń na poziomie łącza i zabezpieczeń na poziomie aplikacji” na stronie 62
Ten temat zawiera informacje na temat różnych aspektów zabezpieczeń na poziomie łącza oraz zabezpieczeń na poziomie aplikacji, a także porównuje dwa poziomy zabezpieczeń.

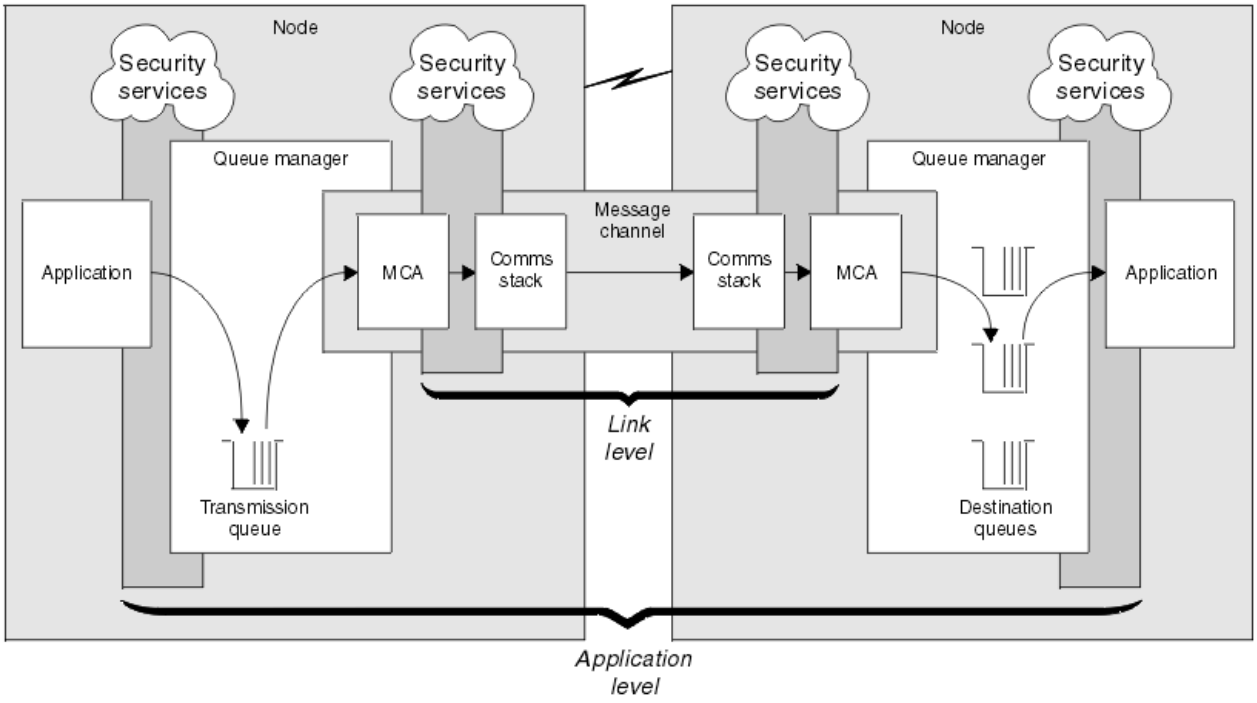
“Programy obsługi wyjścia kanału” na stronie 68
Programy obsługi wyjścia kanału to programy, które są wywoływane w zdefiniowanych miejscach w sekwencji przetwarzania MCA. Użytkownicy i dostawcy mogą zapisywać własne programy obsługi wyjścia kanału. Niektóre z nich są dostarczane przez IBM.

“Ochrona kanałów za pomocą protokołu SSL” na stronie 74
Obsługa protokołu SSL w produkcie IBM WebSphere MQ korzysta z obiektu informacji uwierzytelniających menedżera kolejek i różnych komend MQSC. Należy również rozważyć użycie certyfikatów cyfrowych.

Porównywanie zabezpieczeń na poziomie łącza i zabezpieczeń na poziomie aplikacji

Ten temat zawiera informacje na temat różnych aspektów zabezpieczeń na poziomie łącza oraz zabezpieczeń na poziomie aplikacji, a także porównuje dwa poziomy zabezpieczeń.

Zabezpieczenia na poziomie łącza i poziomu aplikacji są ilustrowane w produkcie Rysunek 8 na stronie 63.



Rysunek 8. Zabezpieczenia na poziomie łącza i zabezpieczenia na poziomie aplikacji

Zabezpieczanie komunikatów w kolejkach

Zabezpieczenia na poziomie łącza mogą zabezpieczać komunikaty podczas przesyłania ich z jednego menedżera kolejek do innego. Jest to szczególnie ważne, gdy komunikaty są przesyłane przez niezabezpieczoną sieć. Jednak nie może on zabezpieczać komunikatów, gdy są one przechowywane w kolejkach w źródłowym menedżerze kolejek, docelowym menedżerze kolejek lub pośrednim menedżerze kolejek.

Zabezpieczenia na poziomie aplikacji mogą zabezpieczać komunikaty, gdy są przechowywane w kolejkach i mają zastosowanie nawet wtedy, gdy nie jest używane kolejkowanie rozproszone. Jest to główna różnica między bezpieczeństwem na poziomie łącza a bezpieczeństwem na poziomie aplikacji. Jest to ilustrowane w sekcji Rysunek 8 na stronie 63.

Menedżery kolejek nie działają w środowiskach kontrolowanych i zaufanych

Jeśli menedżer kolejek jest uruchomiony w kontrolowanym i zaufanym środowisku, mechanizmy kontroli dostępu udostępniane przez produkt WebSphere MQ mogą zostać uznane za wystarczające do ochrony komunikatów przechowywanych w jego kolejkach. Jest to szczególnie istotne, jeśli w kolejce są używane tylko lokalne kolejkowanie, a komunikaty nigdy nie opuszczają menedżera kolejek. Zabezpieczenia na poziomie aplikacji w tym przypadku mogą być uważane za zbędne.

Zabezpieczenia na poziomie aplikacji mogą być również uważane za zbędne, jeśli komunikaty są przesyłane do innego menedżera kolejek, który jest również uruchomiony w środowisku kontrolowanym i zaufanym, lub są odbierane z takiego menedżera kolejek. Zapotrzebowanie na zabezpieczenia na poziomie aplikacji staje się większe, gdy komunikaty są przesyłane do menedżera kolejek lub odbierane z menedżera kolejek, który nie jest uruchomiony w kontrolowanym i zaufanym środowisku.

Różnice w kosztach

Bezpieczeństwo na poziomie aplikacji może kosztować więcej niż bezpieczeństwo na poziomie łącza w zakresie administrowania i wydajności.

Koszt administrowania może być większy, ponieważ istnieje potencjalnie więcej ograniczeń do skonfigurowania i utrzymania. Na przykład może być konieczne upewnie się, że dany użytkownik wysyła

tylko określone typy komunikatów i wysyła komunikaty tylko do określonych miejsc docelowych. Z kolei może być konieczne upewnianie się, że dany użytkownik otrzymuje tylko określone typy komunikatów i odbiera komunikaty tylko z określonych źródeł. Zamiast zarządzać usługami zabezpieczeń na poziomie łącza w pojedynczym kanale komunikatów, może być konieczne skonfigurowanie i utrzymywanie reguł dla każdej pary użytkowników, którzy wymieniają komunikaty w tym kanale.

Jeśli usługi zabezpieczeń są wywoływane za każdym razem, gdy aplikacja umieszcza lub pobiera komunikat, może wystąpić wpływ na wydajność.

Organizacje zwykle rozważają bezpieczeństwo na poziomie łącza, ponieważ może być łatwiej zaimplementować. Uważają, że zabezpieczenia na poziomie aplikacji wykrywają, że zabezpieczenia na poziomie łącza nie spełniają wszystkich ich wymagań.

Dostępność komponentów

Ogólnie w środowisku rozproszonym usługa bezpieczeństwa wymaga komponentu w co najmniej dwóch systemach. Na przykład komunikat może być zaszyfrowany w jednym systemie i deszyfrowany na innym. Ma to zastosowanie zarówno do zabezpieczeń na poziomie łącza, jak i zabezpieczeń na poziomie aplikacji.

W środowisku heterogenicznym, w którym używane są różne platformy, każdy z różnymi poziomami funkcji zabezpieczeń, wymagane komponenty usługi zabezpieczeń mogą nie być dostępne dla każdej platformy, na której są one potrzebne, oraz w postaci łatwej do użycia. Jest to prawdopodobnie bardziej zagadnienie dla bezpieczeństwa na poziomie aplikacji niż w przypadku zabezpieczeń na poziomie łącza, szczególnie w przypadku, gdy użytkownik zamierza zapewnić własne bezpieczeństwo na poziomie aplikacji, kupując w komponentach z różnych źródeł.

Komunikaty w kolejce niedostarczanych komunikatów

Jeśli komunikat jest chroniony przez zabezpieczenia na poziomie aplikacji, może wystąpić problem, jeśli z jakiegokolwiek powodu komunikat nie dotrze do miejsca docelowego i zostanie umieszczony w kolejce niedostarczanych komunikatów. Jeśli nie można określić sposobu przetwarzania komunikatu na podstawie informacji zawartych w deskryptorze komunikatu i w nagłówku martwego listu, może być konieczne sprawdzenie treści danych aplikacji. Nie można tego zrobić, jeśli dane aplikacji są zaszyfrowane, a tylko zamierzony odbiorca może je zdeszyfrować.

Jakich zabezpieczeń na poziomie aplikacji nie można wykonać

Zabezpieczenia na poziomie aplikacji nie są kompletnym rozwiązaniem. Nawet jeśli zaimplementowane są zabezpieczenia na poziomie aplikacji, nadal mogą być wymagane pewne usługi zabezpieczeń na poziomie łącza. Na przykład:

- Po uruchomieniu kanału wzajemne uwierzytelnianie obu MCAs może być nadal wymaganiem. Może to być wykonywane tylko przez usługę zabezpieczeń na poziomie łącza.
- Zabezpieczenia na poziomie aplikacji nie mogą chronić nagłówka kolejki transmisji (MQXQH), który zawiera osadzony deskryptor komunikatu. Nie można również chronić danych w przepływach protokołu kanału WebSphere MQ innych niż dane komunikatu. Ta ochrona może być zapewniona tylko przez zabezpieczenia na poziomie łącza.
- Jeśli usługi zabezpieczeń na poziomie aplikacji są wywoływane na końcu serwera kanału MQI, usługi nie mogą zabezpieczać parametrów wywołań MQI wysyłanych przez kanał. W szczególności dane aplikacji w wywołaniu MQPUT, MQPUT1lub MQGET są niechronione. Ochrona w tym przypadku może być zapewniona tylko przez zabezpieczenia na poziomie łącza.

zabezpieczenia na poziomie łącza

Zabezpieczenia na poziomie łącza odnoszą się do tych usług bezpieczeństwa, które są wywoływane, bezpośrednio lub pośrednio, przez agenta MCA, podsystem komunikacyjny lub połączenie tych dwóch współpracujących.

Zabezpieczenia na poziomie łącza są ilustrowane w sekcji Rysunek 8 na stronie 63.

Poniżej przedstawiono kilka przykładów usług ochrony na poziomie łącza:

- Agent MCA na każdym końcu kanału komunikatów może uwierzytelnić swojego partnera. Jest to wykonywane podczas uruchamiania kanału i nawiązano połączenie komunikacyjne, ale przed rozpoczęciem przepływu komunikatów. Jeśli uwierzytelnianie zakończy się niepowodzeniem, kanał jest zamknięty i nie są przesyłane żadne komunikaty. Jest to przykład usługi identyfikacji i uwierzytelniania.
- Komunikat może być zaszyfrowany w wysyłającym końcu kanału i zdeszyfrowanym na końcu odbierającym. Jest to przykład usługi poufności.
- Komunikat można sprawdzić na końcu odbierającego kanału, aby określić, czy jego zawartość została celowo zmodyfikowana podczas przesyłania przez sieć. Jest to przykład usługi integralności danych.

Zabezpieczenia na poziomie łącza udostępniane przez produkt IBM WebSphere MQ

Podstawowym sposobem zapewnienia poufności i integralności danych w produkcie IBM WebSphere MQ jest użycie protokołu SSL lub TLS. Więcej informacji na temat korzystania z protokołów SSL i TLS w produkcie IBM WebSphere MQzawiera sekcja “Obsługa protokołu SSL i TLS w produkcie IBM WebSphere MQ” na stronie 24. W przypadku uwierzytelniania produkt IBM WebSphere MQ udostępnia narzędzie do korzystania z rekordów uwierzytelniania kanału. Rekordy uwierzytelniania kanału oferują precyzyjną kontrolę dostępu przyznanego do systemów łączących, na poziomie poszczególnych kanałów lub grup kanałów. Więcej informacji na ten temat zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 41.

Zapewnianie bezpieczeństwa na poziomie łącza
W tej kolekcji tematów opisano, w jaki sposób można udostępnić własne usługi zabezpieczeń na poziomie łącza. Pisanie własnych programów obsługi wyjścia kanału jest głównym sposobem udostępniania własnych usług ochrony na poziomie łącza.

Programy obsługi wyjścia kanału są wprowadzane w produkcie “Programy obsługi wyjścia kanału” na stronie 68. W tym samym temacie opisano także program obsługi wyjścia kanału dostarczany z produktem IBM WebSphere MQ dla programu Windows (program obsługi wyjścia kanału SSPI). Ten program obsługi wyjścia kanału jest dostarczany w formacie źródłowym, aby można było zmodyfikować kod źródłowy tak, aby odpowiadał wymaganiom. Jeśli ten program obsługi wyjścia kanału lub programy obsługi wyjścia kanału dostępne są od innych dostawców, nie spełniają wymagań użytkownika, można zaprojektować i napisać własny. W tym temacie opisano sposoby, w jaki programy obsługi wyjścia kanału mogą udostępniać usługi zabezpieczeń. Informacje na temat pisania programu obsługi wyjścia kanału znajdują się w sekcji Pisanie programów obsługi wyjścia kanału.

Zabezpieczenia na poziomie łącza przy użyciu wyjścia zabezpieczeń
Wyjścia bezpieczeństwa zwykle pracują w parach; po jednym na każdym końcu kanału. Są one wywoływane natychmiast po zakończeniu początkowego negocjowania danych przy uruchamianiu kanału.

Wyjścia zabezpieczeń mogą być używane do określania tożsamości i uwierzytelniania, kontroli dostępu i poufności.

Zabezpieczenia na poziomie łącza przy użyciu wyjścia komunikatu
Wyjście komunikatu może być używane tylko w kanale komunikatów, a nie w kanale MQI. Ma on dostęp zarówno do nagłówka kolejki transmisji (MQXQH), który zawiera osadzony deskryptor komunikatu, jak i do danych aplikacji w komunikacie. Może ona modyfikować treść wiadomości i zmieniać jej długość.

Wyjście komunikatu może być używane w dowolnym celu, który wymaga dostępu do całego komunikatu, a nie jego części.

Wyjścia komunikatów mogą być używane do identyfikacji i uwierzytelniania, kontroli dostępu, poufności, integralności danych i nie do odrzucenia oraz z powodów innych niż zabezpieczenia.

Zabezpieczenia na poziomie łącza za pomocą wyjść wysyłania i odbierania
Wyjścia wysyłania i odbierania mogą być używane zarówno w kanałach komunikatów, jak i w kanałach MQI. Są one wywoływane dla wszystkich typów danych, które przepływają przez kanał, i dla przepływów w obu kierunkach.

Wyjścia nadawcze i odbiorcze mają dostęp do każdego segmentu transmisji. Mogą modyfikować jego zawartość i zmieniać jej długość.

W przypadku kanału komunikatów, jeśli agent MCA musi rozdzielić komunikat i wysłać go w więcej niż jednym segmencie transmisji, wywoływane jest wyjście wysyłania dla każdego segmentu transmisji zawierającego fragment komunikatu, a przy odbierającym końcu dla każdego segmentu transmisji jest wywoływany wyjście odbierania. Taka sama sytuacja występuje w przypadku kanału MQI, jeśli parametry wejściowe lub wyjściowe wywołania MQI są zbyt duże, aby mogły zostać wysłane w pojedynczym segmencie transmisji.

W kanale MQI bajt 10 segmentu transmisji identyfikuje wywołanie MQI i wskazuje, czy segment transmisji zawiera parametry wejściowe, czy wyjściowe wywołania. Wyjścia wysyłania i odbierania mogą sprawdzać ten bajt w celu określenia, czy wywołanie MQI zawiera dane aplikacji, które mogą wymagać zabezpieczenia.

Gdy wyjście wysyłania jest wywoływane po raz pierwszy, do pozyskania i inicjowania wszystkich zasobów, których potrzebuje, może zwrócić się do agenta MCA o zarezerwowanie określonej ilości miejsca w buforze, w którym znajduje się segment transmisji. Jeśli później zostanie wywołana w celu przetworzenia segmentu transmisji, może on użyć tej przestrzeni do dodania zaszyfrowanego klucza lub podpisu cyfrowego, na przykład. Odpowiednie wyjście odbierania na drugim końcu kanału może usunąć dane dodane przez wyjście wysyłania, a następnie użyć go do przetworzenia segmentu transmisji.

Wyjścia nadawcze i odbiorcze najlepiej nadają się do celów, w których nie muszą rozumieć struktury danych, które są obarczane i w związku z tym mogą traktować każdy segment transmisowy jako obiekt binarny.

Wyjścia wysyłania i odbierania mogą być używane w celu zapewnienia poufności i integralności danych oraz do zastosowań innych niż zabezpieczenia.

Zadania pokrewne

Identyfikowanie wywołania funkcji API w programie obsługi wyjścia wysyłania lub odbierania

zabezpieczenia na poziomie aplikacji

Zabezpieczenia na poziomie aplikacji odnoszą się do tych usług zabezpieczeń, które są wywoływane przez interfejs między aplikacją a menedżerem kolejek, z którym jest on połączony.

Te usługi są wywoływane, gdy aplikacja wysyła wywołania MQI do menedżera kolejek. Usługi mogą być wywoływane, bezpośrednio lub pośrednio, przez aplikację, menedżer kolejek, inny produkt obsługujący produkt WebSphere MQlub kombinację dowolnego z tych współpracujących ze sobą. Zabezpieczenia na poziomie aplikacji są ilustrowane w produkcie Rysunek 8 na stronie 63.

Zabezpieczenia na poziomie aplikacji są zwane również *zabezpieczeniem na całej trasie* lub *bezpieczeństwem na poziomie komunikatu*.

Poniżej przedstawiono kilka przykładów usług ochrony na poziomie aplikacji:

- Gdy aplikacja umieszcza komunikat w kolejce, deskryptor komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Jednak nie ma żadnych danych, takich jak zaszyfrowane hasło, które mogą być używane do uwierzytelniania ID użytkownika. Usługa zabezpieczeń może dodać te dane. Gdy komunikat zostanie ostatecznie pobrany przez aplikację odbierającą, inny komponent usługi może uwierzytelnić identyfikator użytkownika przy użyciu danych, które zostały przejechane przez ten komunikat.Jest to przykład usługi identyfikacji i uwierzytelniania.
- Komunikat może być zaszyfrowany, gdy jest umieszczany w kolejce przez aplikację i zdeszyfrowany, gdy jest pobierany przez aplikację odbierającą.Jest to przykład usługi poufności.
- Komunikat może zostać sprawdzony, gdy jest on pobierany przez aplikację odbierającą. To sprawdzenie określa, czy jego zawartość została celowo zmodyfikowana, ponieważ została ona po raz pierwszy umieszczana w kolejce przez aplikację wysyłający.Jest to przykład usługi integralności danych.

Planowanie dla produktu Advanced Message Security

Produkt IBM WebSphere MQ Advanced Message Security (AMS) jest oddzielnie licencjonowanym komponentem produktu IBM WebSphere MQ , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM WebSphere MQ , a jednocześnie nie ma wpływu na aplikacje końcowe.

W przypadku przenoszenia bardzo wrażliwych lub cennych informacji, w szczególności informacji poufnych lub związanych z płatnościami, takich jak dane dotyczące pacjenta lub karty kredytowej, należy zwrócić szczególną uwagę na bezpieczeństwo informacji. Zapewnienie, że informacje poruszające się wokół przedsiębiorstwa zachowuje swoją integralność i są chronione przed nieautoryzowanym dostępem, jest trwającym wyzwaniem i odpowiedzialnością. Prawdopodobnie jesteś zobowiązany do przestrzegania przepisów bezpieczeństwa, na ryzyko kar za brak zgodności.

Istnieje możliwość tworzenia własnych rozszerzeń zabezpieczeń dla produktu IBM WebSphere MQ. Takie rozwiązania wymagają jednak specjalistycznych umiejętności i mogą być skomplikowane i kosztowne w utrzymaniu. IBM WebSphere MQ Advanced Message Security pomaga w sprostaniu tym wyzwaniom podczas przenoszenia informacji wokół przedsiębiorstwa pomiędzy praktycznie każdym rodzajem komercyjnego systemu informatycznego.

Produkt IBM WebSphere MQ Advanced Message Security rozszerza funkcje zabezpieczeń produktu IBM WebSphere MQ w następujący sposób:

- Udostępnia on na poziomie aplikacji, kompleksową ochronę danych dla infrastruktury przesyłania komunikatów w punktach, przy użyciu szyfrowania lub cyfrowego podpisywania komunikatów.
- Zapewnia kompleksową ochronę bez zapisywania skomplikowanego kodu zabezpieczeń lub modyfikując lub rekompilując istniejące aplikacje.
- Wykorzystuje ona technologię PKI (Public Key Infrastructure) w celu zapewnienia usług uwierzytelniania, autoryzacji, poufności i integralności danych dla komunikatów.
- Udostępnia on administrowanie strategiami bezpieczeństwa dla komputerów mainframe i serwerów rozproszonych.
- Obsługuje on zarówno serwery IBM WebSphere MQ , jak i klienty.
- Integruje się z produktem IBM WebSphere MQ Managed File Transfer w celu udostępnienia kompleksowego bezpiecznego rozwiązania do przesyłania komunikatów.

Aby uzyskać więcej informacji, patrz “IBM WebSphere MQ Advanced Message Security” na stronie 279.

Zapewnianie bezpieczeństwa na poziomie aplikacji
W tej kolekcji tematów opisano, w jaki sposób można zapewnić własne usługi bezpieczeństwa na poziomie aplikacji.

W celu ułatwienia zaimplementowania zabezpieczeń na poziomie aplikacji produkt IBM WebSphere MQ udostępnia dwa wyjścia, wyjście funkcji API oraz wyjście funkcji API.

Wyjścia te mogą zapewnić identyfikację i uwierzytelnianie, kontrolę dostępu, poufność, integralność danych i usługi niezaprzeczalne, a także inne funkcje niezwiązane z bezpieczeństwem.

Jeśli wyjście funkcji API lub wyjście funkcji API nie jest obsługiwane w danym środowisku systemowym, warto rozważyć inne sposoby zapewnienia własnego bezpieczeństwa na poziomie aplikacji. Jednym ze sposobów jest opracowanie interfejsu API wyższego poziomu, który hermetyzuje MQI. Programiści korzystają z tego interfejsu API zamiast interfejsu MQI w celu pisania aplikacji produktu IBM WebSphere MQ .

Najczęstsze przyczyny korzystania z interfejsu API wyższego poziomu są następujące:

- Aby ukryć bardziej zaawansowane funkcje interfejsu MQI z programistami.
- Aby wymusić stosowanie standardów w użyciu interfejsu MQI.
- Aby dodać funkcję do interfejsu MQI. Ta dodatkowa funkcja może być usługami bezpieczeństwa.

Niektóre produkty dostawcy korzystają z tej techniki w celu zapewnienia bezpieczeństwa na poziomie aplikacji dla produktu IBM WebSphere MQ.

Jeśli planowane jest świadczenie usług ochrony w ten sposób, należy zwrócić uwagę na następujące informacje dotyczące konwersji danych:

- Jeśli znacznik bezpieczeństwa, taki jak podpis cyfrowy, został dodany do danych aplikacji w komunikacie, każdy kod, który wykonuje konwersję danych, musi być świadomy obecności tego znacznika.

- Znacznik bezpieczeństwa mógł zostać uzyskany z obrazu binarnego danych aplikacji. Dlatego przed przekształceniem danych konieczne jest sprawdzenie tokenu.
- Jeśli dane aplikacji w komunikacie zostały zaszyfrowane, musi zostać zdeszyfrowane przed konwersją danych.

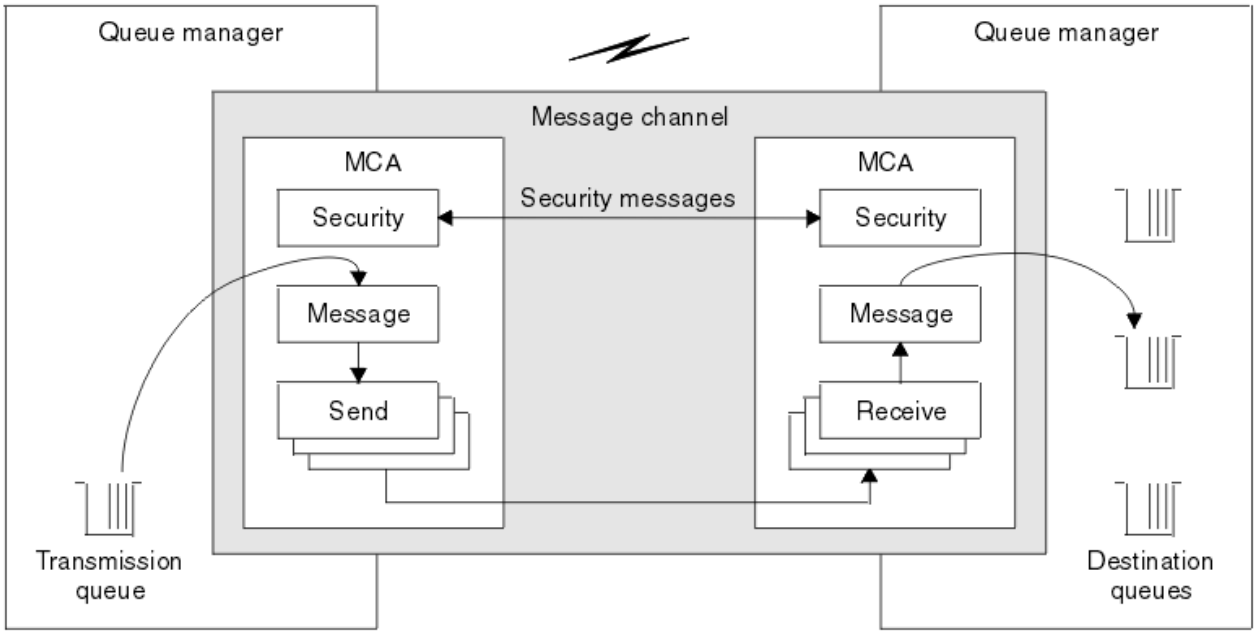
Programy obsługi wyjścia kanału

Programy obsługi wyjścia kanału to programy, które są wywoływane w zdefiniowanych miejscach w sekwencji przetwarzania MCA. Użytkownicy i dostawcy mogą zapisywać własne programy obsługi wyjścia kanału. Niektóre z nich są dostarczane przez IBM.

Istnieje kilka typów programów obsługi wyjścia kanału, ale tylko cztery z nich mają rolę w zapewnieniu bezpieczeństwa na poziomie łącza:

- Wyjście zabezpieczeń
- Wyjście komunikatu
- Wyjście wysyłania
- Wyjście odbierania

Te cztery typy programów obsługi wyjścia kanału są ilustrowane w programie Rysunek 9 na stronie 68 i są opisane w poniższych tematach.



Rysunek 9. Wyjścia zabezpieczeń, komunikatów, wysyłania i odbierania w kanale komunikatów

Pojęcia pokrewne

Programy obsługi wyjścia kanału dla kanałów przesyłania komunikatów

Wyjście zabezpieczeń-przegląd

Wyjścia bezpieczeństwa zwykle pracują w parach. Są one wywoływane przed przepływem komunikatów, a ich celem jest umożliwienie agentowi MCA uwierzytelnienie jego partnera.

Wyjścia zabezpieczeń zwykle pracują w parach; po jednej na każdym końcu kanału. Są one wywoływane bezpośrednio po zakończeniu początkowego negocjowania danych w momencie uruchamiania kanału, ale przed rozpoczęciem przepływu komunikatów. Podstawowym celem wyjścia zabezpieczeń jest włączenie agenta MCA na każdym końcu kanału w celu uwierzytelnienia jego partnera. Jednak nic nie stoi na przeszło, aby wyjść bezpieczeństwa z wykonywania innych funkcji, nawet funkcji, która nie ma nic wspólnego z bezpieczeństwem.

Wyjścia zabezpieczeń mogą komunikować się ze sobą, wysyłając *komunikaty bezpieczeństwa*. Format komunikatu zabezpieczeń nie jest zdefiniowany i jest określany przez użytkownika. Jednym z możliwych rezultatów wymiany komunikatów dotyczących zabezpieczeń jest to, że jedno z wyjść zabezpieczeń może podjąć decyzję o niekontynuowaniu dalszych działań. W takim przypadku kanał jest zamknięty, a komunikaty nie są wysyłane. Jeśli istnieje wyjście zabezpieczeń tylko na jednym końcu kanału, wyjście jest nadal wywoływane i może wybrać, czy kanał ma być kontynuowany, czy też ma być zamknięty.

Wyjścia zabezpieczeń mogą być wywoływane zarówno w kanałach komunikatów, jak i w kanałach MQI. Nazwa wyjścia zabezpieczeń jest określona jako parametr w definicji kanału na każdym końcu kanału.

Aby uzyskać więcej informacji na temat wyjść zabezpieczeń, zobacz: "Zabezpieczenia na poziomie łącza przy użyciu wyjścia zabezpieczeń" na stronie 65.

Wyjście komunikatu

Wyjścia komunikatów działają tylko na kanałach komunikatów i normalnie pracują w parach. Wyjście komunikatu może działać na całym komunikacie i wprowadzać w nim różne zmiany.

Wyjścia komunikatów przy wysyłaniu i odbierającym końcach kanału zwykle pracują w parach. Wyjście komunikatu w wysyłającym końcu kanału jest wywoływane po tym, jak agent MCA ma komunikat z kolejki transmisji. Na końcu kanału odbierającego kanał wywoływany jest wyjście komunikatu, zanim agent MCA umieszcza komunikat w kolejce docelowej.

Wyjście komunikatu ma dostęp zarówno do nagłówka kolejki transmisji (MQXQH), który zawiera osadzony deskryptor komunikatu, jak i do danych aplikacji w komunikacie. Wyjście komunikatu może zmodyfikować treść komunikatu i zmienić jego długość. Zmiana długości może być wynikiem kompresowania, dekompresowania, szyfrowania lub deszyfrowania komunikatu. Może to być także wynik dodawania danych do komunikatu lub usuwania z niego danych.

Wyjścia komunikatów mogą być używane w dowolnym celu, który wymaga dostępu do całego komunikatu, a nie do jego części, a niekoniecznie do bezpieczeństwa.

Wyjście komunikatu może określić, że komunikat, który jest obecnie przetwarzany, nie powinien być kontynuowany w kierunku jego miejsca docelowego. Następnie agent MCA umieszcza komunikat w kolejce niedostarczanych komunikatów. Wyjście komunikatu może również zamknąć kanał.

Wyjścia komunikatów mogą być wywoływane tylko w kanałach komunikatów, a nie w kanałach MQI. Jest to spowodowane tym, że celem kanału MQI jest włączenie parametrów wejściowych i wyjściowych wywołań MQI w celu przepływu między aplikacją kliencką MQI produktu IBM WebSphere MQ a menedżerem kolejek.

Nazwa wyjścia komunikatu jest określona jako parametr w definicji kanału na każdym końcu kanału. Można również określić listę wyjść komunikatów, które mają być uruchamiane w ramach dziedziczenia.

Więcej informacji na temat wyjść komunikatów zawiera sekcja "Zabezpieczenia na poziomie łącza przy użyciu wyjścia komunikatu" na stronie 65.

Wyjścia wysyłania i odbierania

Wyjścia wysyłania i odbierania zwykle pracują w parach. Działają one na segmentach przesyłowych i są najlepiej wykorzystywane tam, gdzie struktura przetwarzanej przez nie danych nie jest istotna.

Wyjście wysyłania na jednym końcu kanału i *wyjście odbierania* na drugim końcu normalnie pracuje w parach. Wyjście wysyłania jest wywoływane tuż przed wystaniem przez agenta MCA komunikacji wysyłanej w celu wysłania danych za pośrednictwem połączenia komunikacyjnego. Wyjście odbierania jest wywoływane tuż po odzyskaniu przez agenta MCA kontroli po odebraniu połączenia i odebraniu danych z połączenia komunikacyjnego. Jeśli współużytkowanie konwersacji jest używane, za pośrednictwem kanału MQI używana jest inna instancja wyjścia wysyłania i odbierania dla każdej konwersacji.

Przepływy protokołów kanału IBM WebSphere MQ między dwiema MCami w kanale komunikatów zawierają informacje sterujące, a także dane komunikatu. Podobnie w kanale MQI przepływy zawierają informacje sterujące, jak również parametry wywołań MQI. Wyjścia wysyłania i odbierania są wywoływane dla wszystkich typów danych.

Dane komunikatów przepływają tylko w jednym kierunku w kanale komunikatów, ale w kanale MQI parametry wejściowe przepływu wywołania MQI w jednym kierunku i w przepływie parametrów wyjściowych są w drugim kierunku. W obu kanałach komunikatów i kanałów MQI przepływ informacji sterujących jest generowany w obu kierunkach. W rezultacie wyjścia wysyłania i odbierania mogą być wywoływane na obu końcach kanału.

Jednostka danych, która jest przesyłana w pojedynczym przepływie między dwiema MCAs, jest nazywana *segmentem transmisji*. Wyjścia nadawcze i odbiorcze mają dostęp do każdego segmentu transmisji. Mogą modyfikować jego zawartość i zmieniać jej długość. Wyjście wysyłania nie może jednak zmieniać pierwszych 8 bajtów segmentu transmisji. Te 8 bajtów stanowi część nagłówka protokołu kanału produktu IBM WebSphere MQ . Istnieją również ograniczenia dotyczące tego, jak bardzo możliwe jest zwiększenie długości segmentu transmisji. W szczególności wyjście wysyłania nie może zwiększyć swojej długości poza maksimum wynegocjowane między dwiema MCAs podczas uruchamiania kanału.

W przypadku kanału komunikatów, jeśli komunikat jest zbyt duży, aby można go było wysłać w pojedynczym segmencie transmisji, wysyłający agent MCA splituje ten komunikat i wysyła go w więcej niż jeden segment transmisji. W związku z tym dla każdego segmentu transmisji zawierającego część komunikatu wywoływana jest procedura zewnętrzna wysyłania, a w momencie odbioru zostanie wywołana procedura obsługi wyjścia odbierania dla każdego segmentu transmisjalnego. Odbierający agent MCA ponownie rozpoznaje komunikat z segmentów transmisji po ich przetworzeniu przez wyjście odbierania.

Podobnie, w przypadku kanału MQI parametry wejściowe lub wyjściowe wywołania MQI są wysyłane w więcej niż jednym segmencie transmisji, jeśli są zbyt duże. Może to mieć miejsce na przykład w przypadku wywołania MQPUT, MQPUT1lub MQGET, jeśli dane aplikacji są wystarczająco duże.

Biorąc pod uwagę powyższe rozważania, bardziej odpowiednie jest wykorzystywanie wyjść nadawanych i odbierających do celów, w których nie są one potrzebne do zrozumienia struktury danych, którymi się one dotyczą, i w związku z tym może traktować każdy segment transmisji jako obiekt binarny.

Wysłanie lub wyjście odbierania może zamknąć kanał.

Nazwy wyjścia wysyłania i wyjścia odbierania są określone jako parametry w definicji kanału na każdym końcu kanału. Można również określić listę wyjść wysyłania, które mają zostać uruchomione w ramach dziedziczenia. W podobny sposób można określić listę wyjść odbierania.

Aby uzyskać więcej informacji o wyjściach wysyłania i odbierania, zobacz: “Zabezpieczenia na poziomie łącza za pomocą wyjść wysyłania i odbierania” na stronie 65.

Planowanie integralności danych

Zaplanuj sposób zachowania integralności danych.

Integralność danych można zaimplementować na poziomie aplikacji lub na poziomie łącza.

Na poziomie aplikacji można wybrać użycie produktu IBM WebSphere MQ Advanced Message Security do cyfrowego podpisywania komunikatów w celu ochrony przed nieautoryzowaną modyfikacją. Można również użyć programów obsługi wyjścia funkcji API, jeśli standardowe urządzenia nie spełniają wymagań.

Na poziomie łącza można wybrać użycie protokołu SSL lub TLS, w którym to przypadku należy zaplanować użycie certyfikatów cyfrowych. Programów obsługi wyjścia kanału można również używać, jeśli standardowe urządzenia nie spełniają wymagań.

Pojęcia pokrewne

“Ochrona kanałów za pomocą protokołu SSL” na stronie 74
Obsługa protokołu SSL w produkcie IBM WebSphere MQ korzysta z obiektu informacji uwierzytelniających menedżera kolejek i różnych komend MQSC. Należy również rozważyć użycie certyfikatów cyfrowych.

“Integralność danych w produkcie IBM WebSphere MQ” na stronie 22
Istnieje możliwość użycia usługi integralności danych w celu wykrycia, czy komunikat został zmodyfikowany.

“Planowanie dla produktu Advanced Message Security” na stronie 66

Produkt IBM WebSphere MQ Advanced Message Security (AMS) jest oddzielnie licencjonowanym komponentem produktu IBM WebSphere MQ , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM WebSphere MQ , a jednocześnie nie ma wpływu na aplikacje końcowe.

Odsyłacze pokrewne

Odwołanie do wyjścia funkcji API

Wywołania wyjścia kanału i struktury danych

Planowanie kontroli

Zdecyduj, jakie dane mają być kontrolowane oraz w jaki sposób przechwytywać i przetwarzać informacje kontroli. Zastanów się, w jaki sposób sprawdzić, czy system jest poprawnie skonfigurowany.

Monitorowanie działań jest kilka aspektów. Aspekty, które należy wziąć pod uwagę, są często definiowane przez wymagania audytorów, a wymagania te są często napędzane przez standardy regulacyjne, takie jak HIPAA (Health Insurance Portability and Accountability Act) lub SOX (Sarbanes-Oxley). Produkt IBM WebSphere MQ udostępnia funkcje, które mają pomóc w spełnieniu takich standardów.

Zastanów się, czy interesujesz się tylko wyjątkami, czy też interesuje Cię zachowanie całego systemu.

Niektóre aspekty kontroli można również uznać za monitorowanie operacyjne; jedno rozróżnienie na audyt polega na tym, że często obserwujesz historyczne dane, nie tylko patrząc na alerty w czasie rzeczywistym. Monitorowanie jest ujęte w sekcji Monitorowanie i wydajność .

Jakie dane mają być kontrolowane

Zastanów się, jakie typy danych lub działań należy kontrolować, zgodnie z opisem w poniższych sekcjach:

Zmiany wprowadzone w produkcie IBM WebSphere MQ przy użyciu interfejsów produktu IBM WebSphere MQ

Skonfiguruj produkt IBM WebSphere MQ w taki sposób, aby wystawiał zdarzenia instrumentacji, a w szczególności zdarzenia komend i zdarzenia konfiguracji.

Zmiany wprowadzone w produkcie IBM WebSphere MQ poza jego kontrolą

Niektóre zmiany mogą mieć wpływ na zachowanie produktu IBM WebSphere MQ , ale nie mogą być bezpośrednio monitorowane przez produkt IBM WebSphere MQ. Przykładami takich zmian są zmiany w plikach konfiguracyjnych `mqs.ini`, `qm.ini`i `mqclient.ini`, tworzenie i usuwanie menedżerów kolejek, instalowanie plików binarnych, takich jak programy obsługi wyjścia użytkownika, a także zmiany uprawnień do plików. Aby monitorować te działania, należy użyć narzędzi działających na poziomie systemu operacyjnego. Dostępne i odpowiednie dla różnych systemów operacyjnych są różne narzędzia. Użytkownik może również posiadać dzienniki utworzone za pomocą powiązanych narzędzi, takich jak *sudo*.

Kontrola operacyjna produktu IBM WebSphere MQ

Do kontrolowania działań, takich jak uruchamianie i zatrzymywanie menedżerów kolejek, może być konieczne użycie narzędzi systemu operacyjnego. W niektórych przypadkach IBM WebSphere MQ można skonfigurować w taki sposób, aby wystawiał zdarzenia instrumentacji.

Działanie aplikacji w produkcie IBM WebSphere MQ

W celu kontrolowania działań aplikacji, na przykład otwierania kolejek, umieszczania i pobierania komunikatów, należy skonfigurować produkt IBM WebSphere MQ w taki sposób, aby wydało odpowiednie zdarzenia.

Alerty włamań

Aby kontrolować próby naruszenia bezpieczeństwa, należy skonfigurować system w taki sposób, aby wystawiał zdarzenia autoryzacji. Zdarzenia kanału mogą być również przydatne do wyświetlania działań, szczególnie jeśli kanał zostanie nieoczekiwanie zakończony.

Planowanie przechwytywania, wyświetlania i archiwizowania danych kontroli

Wiele elementów, które są potrzebne, są zgłaszane jako komunikaty zdarzeń produktu IBM WebSphere MQ . Należy wybrać narzędzia, które mogą odczytywać i formatować te komunikaty. Jeśli jesteś

zainteresowany długoterminową pamięcią masową i analizą, musisz przenieść je do pomocniczego mechanizmu pamięci masowej, takiego jak baza danych. Jeśli te komunikaty nie zostaną przetworzone, pozostaną one w kolejce zdarzeń, prawdopodobnie zapełniając kolejkę. Użytkownik może podjąć decyzję o zaimplementowaniu narzędzia, które automatycznie podejmuje działania na podstawie niektórych zdarzeń, na przykład w celu wydania alertu, gdy wystąpi awaria zabezpieczeń.

Sprawdzanie, czy system został poprawnie skonfigurowany

Zestaw testów jest dostarczany razem z IBM WebSphere MQ Explorer. Użyj tych opcji, aby sprawdzić definicje obiektów pod kątem problemów.

Należy także okresowo sprawdzać, czy konfiguracja systemu jest taka, jak się spodziewa. Chociaż zdarzenia komend i konfiguracji mogą być raportowane po zmianie, warto również wykonać zrzut konfiguracji i porównać ją ze znaną dobrą kopią.

Planowanie zabezpieczeń według topologii

Ta sekcja obejmuje zabezpieczenia w konkretnych sytuacjach, a mianowicie w przypadku kanałów, klastrów menedżerów kolejek, aplikacji publikowania/subskrypcji i rozsyłania grupowego, a także w przypadku korzystania z firewalla.

Więcej informacji można znaleźć w następujących podtematach:

Autoryzacja kanału

Po wysłaniu lub odebraniu komunikatu za pośrednictwem kanału potrzebny jest identyfikator użytkownika, który ma dostęp do różnych zasobów produktu IBM WebSphere MQ .

Aby odbierać komunikaty w czasie PUT dla konsoli MCAs, można użyć identyfikatora użytkownika powiązanego z agentem MCA lub identyfikatora użytkownika powiązanego z tym komunikatem.

W czasie CONNECT można odwzorować asertywny identyfikator użytkownika na alternatywnego użytkownika, korzystając z rekordów uwierzytelniania kanału produktu **CHLAUTH** .

W produkcie WebSphere MQkanały mogą być chronione przez obsługę protokołu SSL lub TLS.

Identyfikatory użytkowników powiązane z kanałami wysyłającym i odbierającym, z wyjątkiem kanału nadawczego, w którym atrybut MCAUSER nie jest używany, wymagają dostępu do następujących zasobów:

- ID użytkownika powiązany z kanałem wysyłającym wymaga dostępu do menedżera kolejek, kolejki transmisji, kolejki niedostarczonych komunikatów oraz dostępu do innych zasobów wymaganych przez wyjścia kanału.
- ID użytkownika MCAUSER dla kanału odbiorczego wymaga uprawnienia *+ setall* .

  Wynika to z tego, że kanał odbiorczy musi utworzyć pełną strukturę MQMD, w tym wszystkie pola kontekstu, używając danych odebranych ze zdalnego kanału nadawczego.

  Dlatego też menedżer kolejek wymaga, aby użytkownik wykonujący to działanie miał uprawnienie *+ setall* . Ten użytkownik *+ setall* musi być nadany użytkownikowi w celu:

  – Wszystkie kolejki, do których kanał odbiorczy poprawnie umieszcza komunikaty.
  – Obiekt menedżera kolejek. Więcej informacji na ten temat zawiera sekcja Autoryzacje dla kontekstu .
- Identyfikator użytkownika MCAUSER kanału odbiorczego, w którym inicjator zażądał komunikatu raportu COA, wymaga uprawnienia *+ passid* w kolejce transmisji, która zwraca komunikat raportu. Bez tego uprawnienia rejestrowane są komunikaty o błędach AMQ8077 .
- Za pomocą identyfikatora użytkownika powiązanego z kanałem odbierającym można otworzyć kolejki docelowe w celu umieszczenia komunikatów w kolejkach.

  Dotyczy to interfejsu MQI (Message queuing Interface), więc może być konieczne dodatkowe sprawdzenie kontroli dostępu, jeśli nie jest używany menedżer uprawnień do obiektów WebSphere MQ (OAM). Użytkownik może określić, czy sprawdzenia autoryzacji są przeprowadzane względem

identyfikatora użytkownika powiązanego z agentem MCA (zgodnie z opisem w tym temacie), czy też z identyfikatorem użytkownika powiązanym z komunikatem (z pola UserIdentifier MQMD).

W przypadku typów kanałów, do których ma zastosowanie, parametr **PUTAUT** definicji kanału określa, który ID użytkownika jest używany dla tych sprawdzeń.

– Wartością domyślną kanału jest korzystanie z konta usługi menedżera kolejek, które będzie miało pełne prawa administracyjne i nie wymaga żadnych specjalnych autoryzacji.

  W przypadku kanałów połączenia z serwerem połączenia administracyjne są blokowane domyślnie przez reguły CHLAUTH i wymagają jawnego udostępniania.

  Kanały odbiornika typu, requestera i odbiornika klastrów umożliwiają lokalne administrowanie przez dowolny przylegający menedżer kolejek, chyba że administrator podejmie kroki w celu ograniczenia tego dostępu.

– Jeśli używany jest ID użytkownika, który nie ma uprawnień administracyjnych WebSphere , należy nadać uprawnienia dsp i ctrlx dla kanału do tego identyfikatora użytkownika, aby kanał działał. Atrybut MCAUSER nie jest używany dla typu kanału SDR.

– Jeśli używany jest identyfikator użytkownika powiązany z komunikatem, jest prawdopodobne, że ID użytkownika pochodzi z systemu zdalnego.

  Ten ID użytkownika systemu zdalnego musi być rozpoznawany przez system docelowy. Na przykład wprowadź następujące komendy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect +inq +setall
```

```
setmqaut -m QMgrName -t chl -n Profile -g GroupName +dsp +ctrlx
```

gdzie *Profil* jest kanałem.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

gdzie *Profil* jest kolejką niedostarczonych komunikatów, jeśli jest ustawiona.

```
setmqaut -m QMgrName -t q -n Profile -g GroupName +put +setall
```

gdzie *Profil* jest listą autoryzowanych kolejek.

Ostrzeżenie: Należy zachować ostrożność podczas autoryzowania identyfikatora użytkownika w celu umieszczania komunikatów w kolejce komend lub w innych wrażliwych kolejkach systemowych.

Identyfikator użytkownika powiązany z agentem MCA zależy od typu agenta MCA. Istnieją dwa typy MCA:

MCA programu wywołującego
MCAs inicjujący kanał. MCAs programu wywołującego może być uruchamiany jako pojedyncze procesy, jako wątki inicjatora kanału lub jako wątki w puli procesów. Używany ID użytkownika jest identyfikatorem użytkownika powiązanym z procesem nadrzędnym (inicjatorem kanału) lub identyfikatorem użytkownika powiązanym z procesem, który uruchamia agenta MCA.

MCA respondenta
MCAs respondentów to MCAs, które są uruchamiane w wyniku żądania przez MCA programu wywołującego. Konsole MCAs mogą być uruchamiane jako pojedyncze procesy, jako wątki procesu nasłuchiwania, lub jako wątki puli procesów. Identyfikator użytkownika może być dowolny z następujących typów (w tej kolejności preferencji):

1. W przypadku APPC program wywołujący MCA może wskazać identyfikator użytkownika, który ma być używany przez agenta MCA odpowiadającego. Ten identyfikator jest nazywany identyfikatorem użytkownika sieci i dotyczy tylko kanałów uruchomionych jako poszczególne procesy. Ustaw identyfikator użytkownika sieci, korzystając z parametru USERID definicji kanału.
2. Jeśli parametr **USERID** nie jest używany, definicja kanału odbieranego MCA może określać identyfikator użytkownika, który musi być używany przez agenta MCA. Ustaw identyfikator użytkownika za pomocą parametru **MCAUSER** definicji kanału.

3. Jeśli ID użytkownika nie został ustawiony za pomocą żadnej z poprzednich (dwóch) metod, używany jest identyfikator użytkownika procesu, który uruchamia agent MCA lub identyfikator użytkownika procesu nadrzędnego (obiekt nasłuchiwania).

Pojęcia pokrewne

“Rekordy uwierzytelniania kanału” na stronie 41
Aby umożliwić bardziej precyzyjną kontrolę na poziomie kanału nad dostępem przydzielonym do systemów, które nawiązują połączenie, można użyć rekordów uwierzytelniania kanału.

Właściwości rekordu uwierzytelniania kanału

Ochrona definicji inicjatora kanału

Tylko członkowie grupy mqm mogą manipulować inicjatorami kanału.

Inicjatory kanału IBM WebSphere MQ nie są obiektami IBM WebSphere MQ , dostęp do nich nie jest kontrolowany przez OAM. Produkt IBM WebSphere MQ nie zezwala użytkownikom ani aplikacjom na manipulowanie tymi obiektami, chyba że ich identyfikator użytkownika jest członkiem grupy mqm. Jeśli istnieje aplikacja, która wydaje komendę PCF `StartChannelInitiator`, identyfikator użytkownika określony w deskryptorze komunikatu komunikatu PCF musi być elementem grupy mqm w docelowym menedżerze kolejek.

ID użytkownika musi być również członkiem grupy mqm na komputerze docelowym, aby wydać równoważne komendy MQSC za pomocą komendy Escape PCF lub za pomocą `runmqsc` w trybie pośrednim.

Kolejki transmisji

Menedżery kolejek automatycznie umieszczają zdalne komunikaty w kolejce transmisji; nie jest wymagane żadne uprawnienie specjalne.

Jeśli jednak konieczne jest umieszczenie komunikatu bezpośrednio w kolejce transmisji, wymaga to specjalnej autoryzacji. Patrz sekcja Tabela 10 na stronie 93.

Wyjścia kanału

Jeśli rekordy uwierzytelniania kanału nie są odpowiednie, można użyć wyjść kanału w celu dodania zabezpieczeń. Wyjście zabezpieczeń tworzy bezpieczne połączenie między dwoma programami obsługi wyjścia zabezpieczeń. Jeden program jest przeznaczony dla wysyłającego agenta kanału komunikatów (MCA), a jeden jest przeznaczony dla odbierającego agenta MCA.

Więcej informacji na temat wyjść kanału znajduje się w sekcji “Programy obsługi wyjścia kanału” na stronie 68 .

Ochrona kanałów za pomocą protokołu SSL

Obsługa protokołu SSL w produkcie IBM WebSphere MQ korzysta z obiektu informacji uwierzytelniających menedżera kolejek i różnych komend MQSC. Należy również rozważyć użycie certyfikatów cyfrowych.

Komendy i atrybuty dla obsługi protokołu SSL

Protokół SSL (Secure Sockets Layer) zapewnia ochronę kanału, ochronę przed podsłuchiwaniem, manipulowaniem i personifikacją. Obsługa protokołu SSL w produkcie IBM WebSphere MQ umożliwia określenie, w definicji kanału, że dany kanał używa zabezpieczeń SSL. Można również określić szczegóły dotyczące typu zabezpieczeń, na przykład algorytm szyfrowania, który ma być używany.

Następujące komendy MQSC obsługują protokół SSL:

ALTER AUTHINFO
Modyfikuje atrybuty obiektu informacji uwierzytelniającej.

DEFINE AUTHINFO
Tworzy obiekt informacji uwierzytelniającej.

USUŃ INFORMACJE O AUTORYZACJI
Usuwa obiekt informacji uwierzytelniającej.

WYŚWIETLENIE INFORMACJI UWIERZYTELNIAJĄCYCH
Wyświetla atrybuty dla konkretnego obiektu informacji uwierzytelniającej.

Następujące parametry menedżera kolejek obsługują protokół SSL:

SSLCRLNL
Atrybut SSLCRLNL określa listę nazw obiektów informacji uwierzytelniających, które są używane do udostępniania położeń odwołań certyfikatów w celu umożliwienia rozszerzonej kontroli certyfikatu TLS/SSL.

SSLCRYP
W systemach Windows, UNIX and Linux , ustawia atrybut SSLCryptoHardware menedżera kolejek. Ten atrybut jest nazwą łańcucha parametru, którego można użyć do skonfigurowania sprzętu szyfrującego, który ma być w systemie.

SSLEV
Określa, czy komunikat zdarzenia SSL jest zgłaszany, jeśli kanał korzystający z protokołu SSL nie nawiąże połączenia SSL.

SSLFIPS
Określa, czy tylko algorytmy certyfikowane przez FIPS mają być używane, jeśli kryptografia jest przeprowadzana w produkcie IBM WebSphere MQ, a nie w sprzęcie szyfrującym. Jeśli sprzęt szyfrujący jest skonfigurowany, używane są moduły szyfrujące udostępniane przez produkt sprzętowy, które mogą być zgodne ze standardem FIPS dla określonego poziomu. Zależy to od produktu sprzętowego.

SSLKEYR
W systemach Windows,UNIX and Linux , wiąże repozytorium kluczy z menedżerem kolejek. Baza danych kluczy jest wstrzymana w bazie danych kluczy *GSKit* . (Pakiet IBM Global Security Kit (GSKit) umożliwia korzystanie z zabezpieczeń SSL w systemach WindowsiUNIX and Linux).

SSLRKEYC
Liczba bajtów, które mają zostać wysłane i odebrane w ramach konwersacji SSL przed renegocjacją klucza tajnego. Liczba bajtów obejmuje informacje sterujące wysłane przez agenta MCA.

Następujące parametry kanału obsługują protokół SSL:

SSLCAUTH
Określa, czy produkt IBM WebSphere MQ wymaga i sprawdza poprawność certyfikatu z klienta SSL.

SSLCIPH
Określa siłę i funkcję szyfrowania (CipherSpec), na przykład NULL_MD5 lub RC4_MD5_US. Specyfikacja CipherSpec musi być zgodna z obu końcami kanału.

SSLPEER
Określa nazwę wyróżniającą (unikalny identyfikator) dozwolonych partnerów.

W tej sekcji przedstawiono opis komend `setmqaut`, `dspmqaut`, `dmpmqaut`, `rcrmqobj`, `rcdmqimg`i `dspmqfls` w celu obsługi obiektu informacji uwierzytelniających. Opisano także komendę iKeycmd w celu zarządzania certyfikatami w systemach UNIX and Linux oraz narzędzie runmqakm do zarządzania certyfikatami w systemach UNIX, Linux i Windows . Patrz następujące sekcje:

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Zarządzanie kluczami i certyfikatami

Przegląd zabezpieczeń kanału za pomocą protokołu SSL-patrz

- “Obsługa protokołu SSL i TLS w produkcie IBM WebSphere MQ” na stronie 24

Szczegółowe informacje na temat komend MQSC powiązanych z protokołem SSL można znaleźć w sekcji

- ALTER AUTHINFO
- DEFINE AUTHINFO
- USUŃ INFORMACJE O AUTORYZACJI
- WYŚWIETL INFORMACJE O AUTORYZACJI

Szczegółowe informacje na temat komend PCF powiązanych z protokołem SSL można znaleźć w sekcji

- Zmiana, kopiowanie i tworzenie obiektu informacji uwierzytelniającej
- Usuń obiekt informacji uwierzytelniającej
- Zapytanie o obiekt informacji uwierzytelniającej

Certyfikaty samopodpisane i podpisane przez ośrodek CA

Ważne jest, aby zaplanować korzystanie z certyfikatów cyfrowych, zarówno podczas programowania, jak i testowania aplikacji, a także w celu wykorzystania ich w produkcji. W zależności od sposobu użycia menedżerów kolejek i aplikacji klienckich można używać certyfikatów podpisanych przez ośrodek CA lub samopodpisanych certyfikatów.

Certyfikaty podpisane przez ośrodek CA
W przypadku systemów produkcyjnych uzyskaj certyfikaty z zaufanego ośrodka certyfikacji (CA). Po uzyskaniu certyfikatu z zewnętrznego ośrodka CA płacisz za usługę.

Certyfikaty samopodpisane
Podczas tworzenia aplikacji można korzystać z samopodpisanych certyfikatów lub certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA), w zależności od platformy:

W systemach Windows, UNIXi Linux można używać certyfikatów samopodpisanych. Instrukcje na ten temat zawiera sekcja “Tworzenie samopodpisanego certyfikatu osobistego w systemach UNIX, Linux, and Windows” na stronie 126 .

Samopodpisane certyfikaty nie nadają się do użytku produkcyjnego, z następujących powodów:

- Certyfikat samopodpisany nie może zostać odwołany, co może pozwolić atakującemu na łyżkę tożsamości po skompromitywaniu klucza prywatnego. CAs może odwołać skompromiowany certyfikat, co uniemożliwia jego dalsze korzystanie. Certyfikaty podpisane przez ośrodek CA są więc bezpieczniejsze w środowisku produkcyjnym, chociaż samopodpisane certyfikaty są wygodniejsze dla systemu testowego.
- Samopodpisane certyfikaty nigdy nie tracą ważności. Jest to zarówno wygodne, jak i bezpieczne w środowisku testowym, ale w środowisku produkcyjnym pozostawia je otwarte na ewentualne naruszenia bezpieczeństwa. Ryzyko jest skomplikowane przez fakt, że samopodpisane certyfikaty nie mogą zostać odwołane.
- Certyfikat samopodpisany jest używany zarówno jako certyfikat osobisty, jak i jako główny (lub baza zaufania) certyfikat ośrodka CA. Użytkownik z samopodpisanym certyfikatem osobistym może używać go do podpisywania innych certyfikatów osobistych. Ogólnie rzecz ujmowana jest to, że nie jest to prawda o certyfikatach osobistych wystawianych przez ośrodek CA i stanowi znaczną ekspozycję.

CipherSpecs i certyfikaty cyfrowe

Tylko podzbiór obsługiwanych specyfikacji CipherSpecs może być używany ze wszystkimi obsługiwanymi typami certyfikatów cyfrowych. W związku z tym konieczne jest wybranie odpowiedniej specyfikacji CipherSpec dla certyfikatu cyfrowego. Analogicznie, jeśli strategia bezpieczeństwa organizacji wymaga użycia określonej specyfikacji CipherSpec , należy uzyskać odpowiedni certyfikat cyfrowy.

Więcej informacji na temat relacji między obiektami CipherSpecs i certyfikatami cyfrowymi można znaleźć w sekcji “Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35 .

Strategie sprawdzania poprawności certyfikatów

Standard IETF RFC 5280 określa serię reguł sprawdzania poprawności certyfikatów, które muszą być implementowane przez oprogramowanie aplikacyjne, aby zapobiec atakom typu "personifikacja". Zestaw reguł sprawdzania poprawności certyfikatów jest znany jako strategia sprawdzania poprawności certyfikatów. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów w produkcie WebSphere MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ” na stronie 34.

Usługi bezpieczeństwa SNA LU 6.2

Jednostka logiczna SNA 6.2 oferuje szyfrowanie na poziomie sesji, uwierzytelnianie na poziomie sesji i uwierzytelnianie na poziomie konwersacji.

Uwaga: W tej kolekcji tematów założono, że użytkownik ma podstawową wiedzę na temat architektury systemów sieciowych (Systems Network Architecture-SNA). Inna dokumentacja, o której mowa w niniejszej sekcji, zawiera krótkie wprowadzenie do odpowiednich pojęć i terminologii. Jeśli wymagane jest wprowadzenie bardziej kompleksowego technicznego wprowadzenia do sieci SNA, patrz *Przegląd techniczny architektury systemów sieciowych*, GC30-3073.

Jednostka logiczna SNA 6.2 udostępnia trzy usługi zabezpieczeń:

- Kryptografia na poziomie sesji
- Uwierzytelnianie na poziomie sesji
- Uwierzytelnianie na poziomie konwersacji

W przypadku szyfrowania na poziomie sesji i uwierzytelniania na poziomie sesji, architektura SNA korzysta z algorytmu *Data Encryption Standard (DES)* . Algorytm DES jest algorytmem szyfru blokowego, który używa klucza symetrycznego do szyfrowania i deszyfrowania danych. Zarówno blok, jak i klucz mają długość 8 bajtów.

Kryptografia na poziomie sesji
Kryptografia na poziomie sesji szyfruje i deszyfruje dane sesji za pomocą algorytmu DES. Można go zatem użyć do udostępnienia usługi poufności na poziomie łącza w kanałach SNA LU 6.2 .

Jednostki logiczne (LU) mogą udostępniać obowiązkowe (lub wymagane) szyfrowanie danych, selektywne kryptografie danych lub bez szyfrowania danych.

W *obowiązkowej sesji kryptograficznej*jednostka logiczna szyfruje wszystkie jednostki żądania danych wychodzących i deszyfruje wszystkie jednostki żądania danych przychodzących.

W *selektywnej sesji kryptograficznej*jednostka logiczna szyfruje tylko jednostki żądania danych określone przez program transakcyjny wysyłający (TP). Wysyłający sygnał LU sygnalizuje, że dane są szyfrowane, ustawiając indykator w nagłówku żądania. Zaznaczając ten wskaźnik, jednostka logiczna odbierającego może określić, które jednostki żądają odszyfrować przed przekazaniem ich do odbierającego TP.

W sieci SNA program WebSphere MQ MCAs to programy transakcyjne. MCAs nie żąda szyfrowania dla wszystkich danych, które wysyłają. Selektywna kryptografia danych nie jest opcją, dlatego w sesji jest możliwe tylko obowiązkowe szyfrowanie danych lub szyfrowanie danych.

Informacje na temat implementowania obowiązkowych kryptografii danych zawiera dokumentacja podsystemu SNA. Zapoznaj się z tą samą dokumentacją, aby uzyskać informacje na temat mocniejszych form szyfrowania, które mogą być używane na używanej platformie, na przykład szyfrowanie Triple DES 24-bajtowe w systemie z/OS.

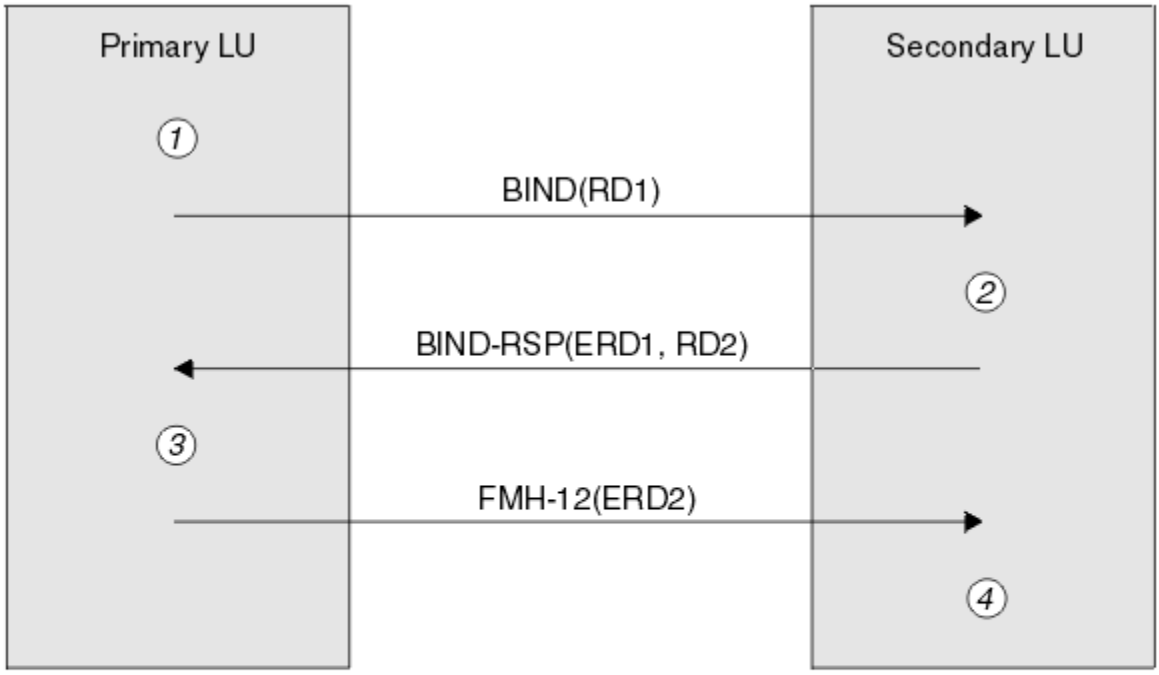
Więcej ogólnych informacji o kryptografii na poziomie sesji zawiera sekcja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*(Skorowidz protokołów równorzędnych), SC31-6808(jednostka logiczna architektury sieci).

Uwierzytelnianie na poziomie sesji
Uwierzytelnianie na poziomie sesji to protokół zabezpieczeń na poziomie sesji, który umożliwia dwóm jednostkom LU uwierzytelnianie się nawzajem podczas aktywowania sesji. Jest on również znany jako *weryfikacja LU-LU*.

Ponieważ jednostka logiczna jest w rzeczywistości "bramą" w systemie z sieci, można uznać, że ten poziom uwierzytelniania jest wystarczający w pewnych okolicznościach. Jeśli na przykład menedżer kolejek musi wymieniać komunikaty ze zdalnym menedżerem kolejek, który działa w kontrolowanym i zaufanym środowisku, można być przygotowanym do zaufaniu tożsamości pozostałych komponentów systemu zdalnego po uwierzytelnieniu jednostki logicznej.

Uwierzytelnianie na poziomie sesji jest realizowane przez każdą jednostkę logiczną weryfikując hasło partnera. Hasło jest nazywane *hasłem LU LU-LU* , ponieważ między każdą parą jednostek logicznych jest ustanawiane jedno hasło. Sposób tworzenia hasła LU-LU jest zależny od implementacji i poza zasięgiem SNA.

Rysunek 10 na stronie 78 przedstawia przepływy na potrzeby uwierzytelniania na poziomie sesji.



Legend:

BIND	=	BIND request unit
BIND-RSP	=	BIND response unit
ERD	=	Encrypted random data
FMH-12	=	Function Management Header 12
RD	=	Random data

Rysunek 10. Przepływy dla uwierzytelniania na poziomie sesji

Protokół dla uwierzytelniania na poziomie sesji jest następujący. Liczby w procedurze odpowiadają numerom w sekcji Rysunek 10 na stronie 78.

1. Podstawowa jednostka logiczna generuje losową wartość danych (RD1) i wysyła ją do drugorzędnej jednostki logicznej w żądaniu BIND.
2. Gdy drugorzędna jednostka logiczna otrzymuje żądanie BIND z danymi losowymi, szyfruje dane za pomocą algorytmu DES, używając jego kopii hasła LU-LU jako klucza. Następnie drugorzędna jednostka logiczna generuje drugą losową wartość danych (RD2) i wysyła ją wraz z zaszyfrowanymi danymi (ERD1) do podstawowej jednostki logicznej w odpowiedzi BIND.
3. Gdy podstawowa jednostka logiczna otrzymuje odpowiedź BIND, wylicza ona własną wersję zaszyfrowanych danych z danych losowych, które wygenerowała oryginalnie. W tym celu należy użyć algorytmu DES z jego kopią hasła LU-LU jako klucza. Następnie porównuje jego wersję z zaszyfrowanymi danymi, które zostały odebrane w odpowiedzi BIND. Jeśli te dwie wartości są

takie same, podstawowa jednostka logiczna wie, że drugorzędna jednostka logiczna ma takie samo hasło, jak i dodatkowa jednostka logiczna jest uwierzytelniana. Jeśli te dwie wartości nie są zgodne, podstawowa jednostka logiczna kończy sesję.

Następnie podstawowa jednostka logiczna szyfruje losowe dane odebrane w odpowiedzi BIND i wysyła zaszyfrowane dane (ERD2) do drugorzędnej jednostki logicznej w nagłówku 12 (FMH-12) zarządzania funkcjami.

4. Gdy drugorzędna jednostka logiczna otrzymuje wartość FMH-12, wylicza ona własną wersję zaszyfrowanych danych z losowych danych, które wygenerowała. Następnie porównuje jego wersję z zaszyfrowanymi danymi, które zostały odebrane w FMH-12. Jeśli te dwie wartości są takie same, podstawowa jednostka logiczna jest uwierzytelniana. Jeśli te dwie wartości nie są zgodne, drugorzędna jednostka logiczna kończy sesję.

W rozszerzonej wersji protokołu, która zapewnia lepszą ochronę przed atakami typu man, drugorzędna jednostka logiczna oblicza kod uwierzytelniania DES (Message Authentication Code-MAC) z RD1, RD2i pełną nazwę drugorzędnej jednostki logicznej, używając jej jako klucza kopii hasła LU-LU. Drugorzędna jednostka logiczna wysyła kod MAC do podstawowej jednostki logicznej w odpowiedzi BIND, a nie do ERD1.

Podstawowa jednostka logiczna uwierzytelnia drugorzędną jednostkę logiczną przez obliczanie własnej wersji MAC, którą porównuje z kodem MAC otrzymanego w odpowiedzi BIND. Następnie podstawowa jednostka logiczna oblicza drugi kod MAC z RD1 i RD2, a następnie wysyła kod MAC do dodatkowej jednostki logicznej w FMH-12 zamiast ERD2.

Drugorzędna jednostka logiczna uwierzytelnia podstawową jednostkę logiczną przez obliczanie własnej wersji drugiego MAC, który porównuje się z kodem MAC otrzymanego w FMH-12.

Informacje na temat konfigurowania uwierzytelniania na poziomie sesji znajdują się w dokumentacji podsystemu SNA. Więcej ogólnych informacji na temat uwierzytelniania na poziomie sesji zawiera sekcja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*(Skorowidz protokołów równorzędnych), SC31-6808.

Uwierzytelnianie na poziomie konwersacji
Gdy lokalna jednostka logiczna TP próbuje przydzielić konwersację z partnerem TP, lokalna jednostka logiczna wysyła żądanie przyłączenia do partnerskiej jednostki logicznej, prosząc ją o dołączenie partnerskiego przetwarzania transakcyjnego. W pewnych okolicznościach żądanie przyłączenia może zawierać informacje o zabezpieczeniach, których partnerska jednostka logiczna może użyć do uwierzytelniania lokalnego TP. Jest to określane jako *uwierzytelnianie na poziomie konwersacji*lub *weryfikacja użytkownika końcowego*.

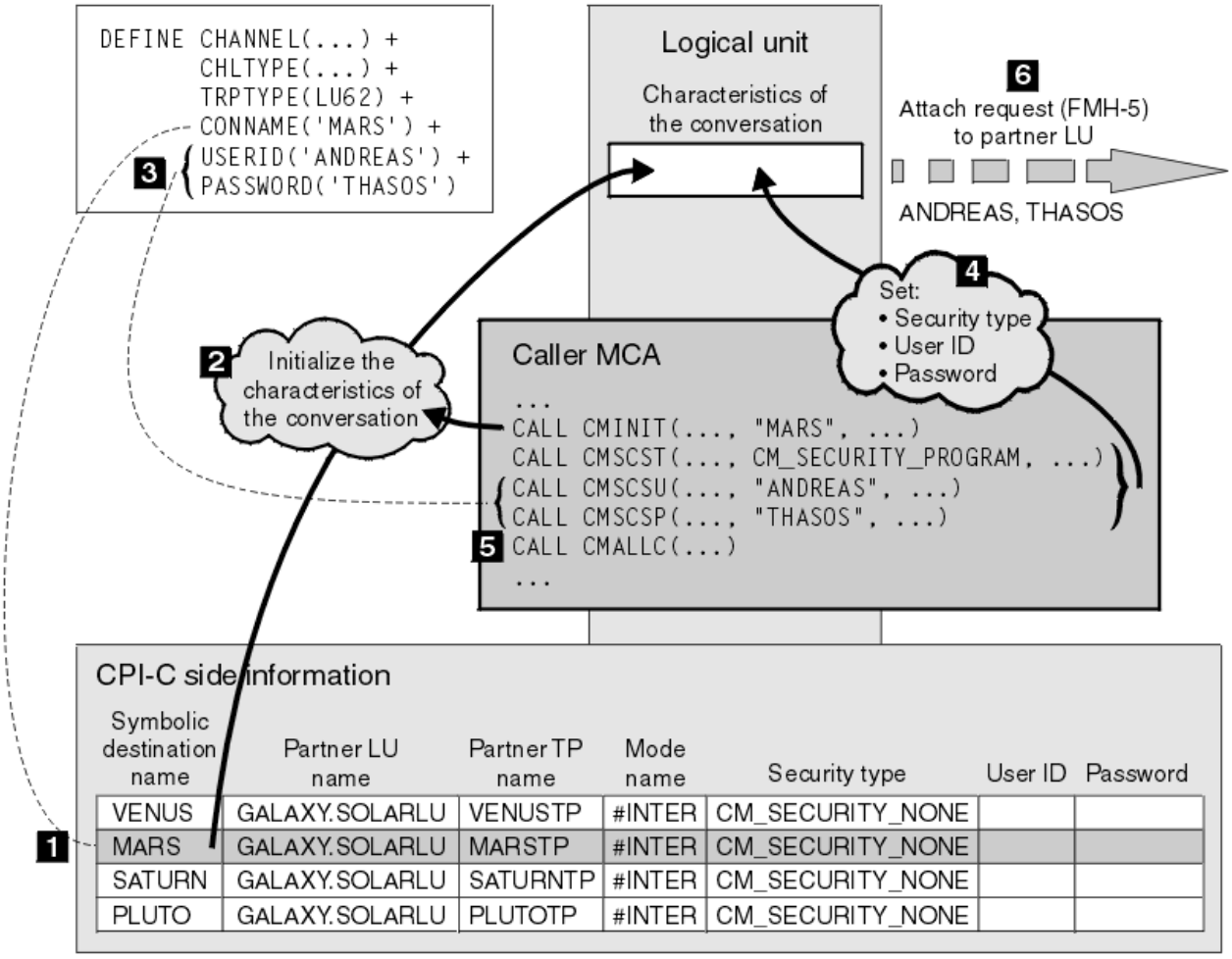
W poniższych tematach opisano, w jaki sposób produkt IBM WebSphere MQ udostępnia obsługę uwierzytelniania na poziomie konwersacji.

Więcej informacji na temat uwierzytelniania na poziomie konwersacji znajduje się w podręczniku *Systems Network Architecture LU 6.2 Reference: Peer Protocols*(Skorowidz protokołów równorzędnych), SC31-6808. For information specific to z/OS, see *z/OS MVS Planning: APPC/MVS Management*, SA22-7599.

Więcej informacji na temat interfejsu CPI-C znajduje się w sekcji *Common Programming Interface Communications CPI-C Specification*(Specyfikacja komunikacji CPI-C interfejsu programowania wspólnego), SC31-6180. Więcej informacji na temat aplikacji APPC/MVS TP Conversation Callable Services zawiera sekcja *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Obsługa uwierzytelniania na poziomie konwersacji w produkcie IBM WebSphere MQ w systemach w systemach UNIX i Windows
W tym temacie opisano sposób uzyskiwania informacji o sposobie działania uwierzytelniania na poziomie konwersacji w systemie UNIX, Linux, and Windows.

Obsługa uwierzytelniania na poziomie konwersacji w produkcie IBM WebSphere MQ dla produktów WebSphere MQ w systemach UNIX i WebSphere MQ for Windows jest ilustrowana w podręczniku Rysunek 11 na stronie 80. Liczby na diagramie odpowiadają numerom w opisie, który znajduje się poniżej.



Symbolic destination name	Partner LU name	Partner TP name	Mode name	Security type	User ID	Password
VENUS	GALAXY.SOLARLU	VENUSTP	#INTER	CM_SECURITY_NONE		
MARS	GALAXY.SOLARLU	MARSTP	#INTER	CM_SECURITY_NONE		
SATURN	GALAXY.SOLARLU	SATURNTP	#INTER	CM_SECURITY_NONE		
PLUTO	GALAXY.SOLARLU	PLUTOTP	#INTER	CM_SECURITY_NONE		

Rysunek 11. Obsługa uwierzytelniania na poziomie konwersacji w produkcie WebSphere MQ

W systemach IBM i, UNIX i Windows agent MCA używa połączeń CPI-C do komunikowania się z partnerskim agentem MCA w sieci SNA. W definicji kanału na końcu programu wywołującego kanału wartość parametru CONNAME jest symboliczną nazwą docelową, która identyfikuje pozycję informacji po stronie CPI-C (1). Ten wpis określa:

- Nazwa partnerskiej jednostki logicznej
- Nazwa partnera TP, który jest agentem odbierający
- Nazwa trybu, który ma być używany do konwersacji.

Wpis informacji po stronie może również określać następujące informacje dotyczące zabezpieczeń:

- Typ zabezpieczeń.

  Powszechnie zaimplementowane typy zabezpieczeń to: CM_SECURITY_NONE, CM_SECURITY_PROGRAM i CM_SECURITY_SAME, ale inne są zdefiniowane w specyfikacji CPI-C.
- tylko identyfikator użytkownika.
- Hasło.

Program wywołujący MCA przygotowuje się do przydzielenia konwersacji z agentem odbierającego MCA poprzez wywołanie CPI-C wywołania CMINIT, przy użyciu wartości CONNAME jako jednego z parametrów w wywołaniu. Wywołanie CMINIT identyfikuje, z korzyścią dla lokalnej jednostki logicznej, wpis informacji bocznej, który agent MCA zamierza wykorzystać do konwersacji. Lokalna jednostka logiczna używa wartości znajdujących się w tej pozycji w celu zainicjowania parametrów konwersacji (2).

Agent MCA programu wywołującego sprawdza następnie wartości parametrów USERID i PASSWORD w definicji kanału (3). Jeśli parametr USERID jest ustawiony, agent MCA programu wywołującego wysyła następujące wywołania CPI-C (4):

- CMSCST, aby ustawić typ zabezpieczeń dla konwersacji na CM_SECURITY_PROGRAM.
- CMSCSU, aby ustawić ID użytkownika dla konwersacji na wartość USERID.
- CMSCSP, aby ustawić hasło do konwersacji na wartość PASSWORD. Opcja CMSCSP nie jest wywoływana, jeśli nie ustawiono parametru PASSWORD.

Typ zabezpieczeń, ID użytkownika i hasło ustawione przez te wywołania przesłaniają wszystkie wartości uzyskane wcześniej z pozycji informacji bocznej.

Program wywołujący MCA następnie wysyła wywołanie CPI-C CMALLC w celu przydzielenia konwersacji (5). W odpowiedzi na to wywołanie, lokalna jednostka logiczna wysyła żądanie przyłączenia (Function Management Header 5 lub FMH-5) do partnerskiej jednostki logicznej (6).

Jeśli partnerska jednostka logiczna zaakcepta identyfikator użytkownika i hasło, w żądaniu przyłączenia dołączane są wartości USERID i PASSWORD. Jeśli partnerska jednostka logiczna nie zaakceptują identyfikatora użytkownika i hasła, wartości te nie są uwzględniane w żądaniu przyłączenia. Lokalna jednostka logiczna wykrywa, czy partnerska jednostka logiczna zaakceptują ID użytkownika i hasło w ramach wymiany informacji, gdy jednostki logiczne wiążą się z formularzem sesji.

W późniejszej wersji żądania przyłączenia substytut hasła może przepływać między jednostkami logicznymi zamiast jawnego hasła.Zastępcą hasła jest kod uwierzytelniania DES (DES Message Authentication Code-MAC) lub skrót komunikatu SHA-1 utworzony na podstawie hasła. Substytuty haseł mogą być używane tylko wtedy, gdy oba jednostki logiczne obsługują je.

Gdy partnerska jednostka logiczna otrzymuje przychodzące żądanie przyłączenia zawierające identyfikator użytkownika i hasło, może on używać identyfikatora użytkownika i hasła do celów identyfikacji i uwierzytelniania. Odwołując się do list kontroli dostępu, partnerska jednostka logiczna może również określić, czy identyfikator użytkownika ma uprawnienia do przydzielania konwersacji, a także do dołączania programu odpowiadającego MCA.

Ponadto agent odbierający odpowiedź może działać pod identyfikatorem użytkownika dołączonym do żądania przyłączenia.W takim przypadku identyfikator użytkownika staje się domyślnym identyfikatorem użytkownika dla programu odpowiadającego MCA i jest używany do sprawdzania uprawnień, gdy agent MCA próbuje nawiązać połączenie z menedżerem kolejek. Może być również używany do sprawdzania uprawnień w późniejszym czasie, gdy agent MCA próbuje uzyskać dostęp do zasobów menedżera kolejek.

Sposób, w jaki identyfikator użytkownika i hasło w żądaniu przyłączenia mogą być używane do identyfikacji, uwierzytelniania i kontroli dostępu, są zależne od implementacji. Informacje specyficzne dla podsystemu SNA można znaleźć w odpowiedniej dokumentacji.

Jeśli parametr USERID nie jest ustawiony, agent MCA programu wywołującego nie wywoła CMSCST, CMSCSU i CMSCSP. W tym przypadku informacje o zabezpieczeniach, które przepływają w żądaniu przyłączenia, są określane wyłącznie przez elementy określone w pozycji informacji po stronie i akceptują partnerską jednostkę logiczną.

Zabezpieczenia klastrów menedżerów kolejek

Chociaż klastry menedżerów kolejek mogą być wygodne w użyciu, należy zwrócić szczególną uwagę na ich zabezpieczenia.

Klaster menedżera kolejek to sieć menedżerów kolejek, które są logicznie powiązane w pewien sposób. Menedżer kolejek, który należy do klastra, jest nazywany *menedżerem kolejek klastra*.

Kolejka, która należy do menedżera kolejek klastra, może być znana innym menedżerom kolejek w klastrze. Taka kolejka jest nazywana *kolejką klastra*. Każdy menedżer kolejek w klastrze może wysyłać komunikaty do kolejek klastra bez konieczności użycia następujących elementów:

- Jawna definicja kolejki zdalnej dla każdej kolejki klastra
- Jawnie zdefiniowane kanały do i z każdego zdalnego menedżera kolejek

- Oddzielna kolejka transmisji dla każdego kanału danych wychodzących.

Istnieje możliwość utworzenia klastra, w którym dwa lub więcej menedżerów kolejek jest klonami. Oznacza to, że mają one instancje tych samych kolejek lokalnych, w tym wszystkie kolejki lokalne zadeklarowane jako kolejki klastra, a także mogą obsługiwać instancje tych samych aplikacji serwera.

Gdy aplikacja połączona z menedżerem kolejek klastra wysyła komunikat do kolejki klastra, która ma instancję na każdym z klonowanych menedżerów kolejek, program IBM WebSphere MQ decyduje o tym, który menedżer kolejek ma wysłać ten komunikat. Gdy wiele aplikacji wysyła komunikaty do kolejki klastra, produkt WebSphere MQ równoważy obciążenie dla każdego z menedżerów kolejek, które mają instancję kolejki. Jeśli jeden z systemów udostępniających sklonowany menedżer kolejek nie powiedzie się, program WebSphere MQ będzie nadal równoważyć obciążenie pozostałych menedżerów kolejek aż do momentu zrestartowania systemu.

Jeśli używane są klastry menedżerów kolejek, należy wziąć pod uwagę następujące zagadnienia dotyczące zabezpieczeń:

- Zezwalanie tylko wybranym menedżerom kolejek na wysyłanie komunikatów do menedżera kolejek
- Zezwalanie tylko wybranym użytkownikom zdalnego menedżera kolejek na wysyłanie komunikatów do kolejki w menedżerze kolejek
- Zezwalanie aplikacjom połączonym z menedżerem kolejek na wysyłanie komunikatów tylko do wybranych kolejek zdalnych

Te rozważania są istotne nawet wtedy, gdy nie są używane klastry, ale stają się one ważniejsze, jeśli używane są klastry.

Jeśli aplikacja może wysyłać komunikaty do jednej kolejki klastra, może wysyłać komunikaty do dowolnej innej kolejki klastra bez konieczności użycia dodatkowych definicji kolejek zdalnych, kolejek transmisji lub kanałów. W związku z tym ważniejsze staje się rozważenie, czy należy ograniczyć dostęp do kolejek klastra w menedżerze kolejek, a także ograniczyć kolejki klastrów, do których aplikacje mogą wysyłać komunikaty.

Istnieją dodatkowe uwagi dotyczące zabezpieczeń, które są istotne tylko wtedy, gdy używane są klastry menedżera kolejek:

- Zezwalanie tylko wybranym menedżerom kolejek na dołączenie do klastra
- Zmuszanie menedżerów kolejek do opuszczenia klastra

Więcej informacji na temat tych zagadnień znajduje się w temacie Keeping clusters secure(bezpieczne klastry bezpieczne).

Zadania pokrewne

“Zapobieganie odbierającym komunikaty menedżerom kolejek” na stronie 257
Można zapobiec otrzymywanie komunikatów przez menedżera kolejek klastra przez użycie programów obsługi wyjścia, które nie są uprawnione do odbierania.

Zabezpieczenia dla publikowania/subskrypcji produktu IBM WebSphere MQ

Jeśli używany jest produkt IBM WebSphere MQ Publish/Subscribe, należy wziąć pod uwagę dodatkowe uwagi dotyczące zabezpieczeń.

W systemie publikowania/subskrypcji istnieją dwa typy aplikacji: publikator i subskrybent. *Publikatory* dostarczają informacji w postaci komunikatów produktu IBM WebSphere MQ . Gdy publikator publikuje komunikat, określa on *temat*, który identyfikuje temat informacji wewnątrz komunikatu.

Subskrybenty są konsumentami publikowanych informacji. Subskrybent określa tematy, którymi się interesuje, subskrybując je.

Menedżer kolejek to aplikacja dostarczona z publikowania/subskrybowania produktu IBM WebSphere MQ . Odbiera on publikowane komunikaty od publikatorów i żądań subskrypcji od subskrybentów, a następnie kieruje publikowane komunikaty do subskrybentów. Subskrybent wysyła komunikaty tylko do tych tematów, do których został subskrybowany.

Więcej informacji na ten temat zawiera sekcja Zabezpieczenia publikowania/subskrypcji.

Zabezpieczenia rozsyłania grupowego

Informacje zawarte w tej sekcji umożliwiają zrozumienie, dlaczego procesy zabezpieczeń mogą być wymagane przy użyciu programu IBM WebSphere MQ Multicast.

IBM WebSphere MQ Multicast nie ma wbudowanych zabezpieczeń. Sprawdzanie zabezpieczeń jest obsługiwane w menedżerze kolejek w czasie operacji MQOPEN, a ustawienie pola MQMD jest obsługiwane przez klienta. Niektóre aplikacje w sieci mogą nie być aplikacjami IBM WebSphere MQ (na przykład aplikacje LLM, więcej informacji na ten temat zawiera sekcja Współdziałanie rozsyłania grupowego z niskim opóźnieniem przesyłania komunikatów WebSphere MQ), dlatego może być konieczne zaimplementowanie własnych procedur bezpieczeństwa, ponieważ odbieranie aplikacji nie może być określone w kontekście poprawności pól kontekstu.

Istnieją trzy procesy zabezpieczeń, które należy rozważyć:

Kontrola dostępu

Kontrola dostępu w produkcie IBM WebSphere MQ jest oparta na identyfikatorach użytkowników. Aby uzyskać więcej informacji na ten temat, zobacz: “Kontrola dostępu dla klientów” na stronie 59.

Bezpieczeństwo sieci

Odizolowana sieć może być opłacalną opcją bezpieczeństwa, aby zapobiec fałszowaniu wiadomości. Aplikacja na adres grupy rozsyłania grupowego może publikować złośliwe komunikaty przy użyciu rodzimych funkcji komunikacyjnych, które nie mogą być odróżniane od komunikatów MQ , ponieważ pochodzą one z aplikacji na tym samym adresie grupowym rozsyłania grupowego.

Możliwe jest również, aby klient na adres grupy rozsyłania grupowego odbierał komunikaty, które były przeznaczone dla innych klientów na tym samym adresie grupowym rozsyłania grupowego.

Izolowanie sieci rozsyłania grupowego zapewnia, że dostęp mają tylko poprawne klienty i aplikacje. Ten środek ostrożności może zapobiec przychodzącaniu złośliwych wiadomości i informacji poufnych przed ich wychodzić.

Informacje na temat adresów sieciowych grup rozsyłania grupowego zawiera sekcja Ustawianie odpowiedniej sieci dla ruchu rozsyłania grupowego .

Podpisy cyfrowe

Podpis cyfrowy jest tworzony przez zaszyfrowanie reprezentacji komunikatu. Szyfrowanie korzysta z klucza prywatnego sygnatariusza, a w przypadku efektywności zazwyczaj działa na streszczanie wiadomości, a nie na samym komunikacie. Cyfrowe podpisywanie komunikatu przed wykonaniem operacji MQPUT jest dobrym środkiem ostrożności, ale ten proces może mieć szkodliwy wpływ na wydajność, jeśli istnieje duża liczba komunikatów.

Podpisy cyfrowe różnią się w zależności od podpisanych danych. Jeśli dwa różne komunikaty są podpisywane cyfrowo przez ten sam obiekt, te dwa sygnatury różnią się, ale oba sygnatury mogą być weryfikowane z tym samym kluczem publicznym, czyli kluczem publicznym jednostki, która podpisała komunikaty.

Jak wspomniano wcześniej w tej sekcji, możliwe jest, że aplikacja na adres grupy rozsyłania grupowego może publikować złośliwe komunikaty przy użyciu rodzimych funkcji komunikacyjnych, które nie mogą być odróżniane od komunikatów MQ . Podpisy cyfrowe stanowią dowód pochodzenia, a jedynie nadawca zna klucz prywatny, który dostarcza mocnych dowodów na to, że nadawca jest inicjatorem wiadomości.

Więcej informacji na ten temat zawiera sekcja “Pojęcia kryptograficzne” na stronie 7.

Firewalle i internet pass-thru

Zwykle używany jest firewall, aby zapobiec dostępowi do hostów z wrogimi adresami IP, na przykład w ataku typu Denial of Service (Odmowa usługi). Jednak może być konieczne tymczasowe zablokowanie adresów IP w produkcie IBM WebSphere MQ, na przykład podczas oczekiwania na aktualizację reguł firewalla przez administratora zabezpieczeń.

Aby zablokować jeden lub większą liczbę adresów IP, należy utworzyć rekord uwierzytelniania kanału typu BLOCKADDR lub ADDRESSMAP. Więcej informacji zawiera sekcja “Blokowanie konkretnych adresów IP” na stronie 188.

Zabezpieczenia dla programu IBM WebSphere MQ tranzytu internetowego

Internet pass-thru może uprościć komunikację poprzez firewall, ale ma to wpływ na bezpieczeństwo.

IBM WebSphere MQ internet pass-thru to podstawowe rozszerzenie produktu IBM WebSphere MQ , które jest dostarczane w katalogu SupportPac MS81.

WebSphere MQ internet pass-thru enables two queue managers to exchange messages, or a WebSphere MQ client application to connect to a queue manager, over the Internet without requiring a direct TCP/IP connection. Jest to przydatne w przypadku, gdy firewall zabrania bezpośredniego połączenia TCP/IP między dwoma systemami. Powoduje to, że przejście protokołu kanału WebSphere MQ do firewalla jest prostsze i łatwiejsze do opanowania przez tunelowanie przepływów wewnątrz protokołu HTTP lub przez działanie jako serwer proxy. Za pomocą protokołu SSL (Secure Sockets Layer) można go również używać do szyfrowania i deszyfrowania wiadomości wysyłanych przez Internet.

Jeśli system WebSphere MQ komunikuje się z IPT, o ile nie jest używany tryb SSLProxyMode w protokole IPT, należy upewnić się, że specyfikacja CipherSpec używana przez produkt WebSphere MQ jest zgodna z zestawem CipherSuite używanym przez IPT:

- Jeśli protokół IPT działa jako serwer SSL lub TLS, a produkt WebSphere MQ łączy się jako klient SSL lub TLS, wartość CipherSpec używana przez produkt WebSphere MQ musi odpowiadać CipherSuite , który jest włączony w odpowiednim pierścieniu kluczy IPT.
- Gdy IPT działa jako klient SSL lub TLS i łączy się z serwerem WebSphere MQ SSL lub TLS, IPT CipherSuite musi być zgodny z atrybutem CipherSpec zdefiniowanym w odbierającym kanale WebSphere MQ .

W przypadku migracji z IPT do zintegrowanej obsługi protokołu SSL i TLS produktu WebSphere MQ , należy przesłać certyfikaty cyfrowe z IPT za pomocą programu iKeyman.

Więcej informacji na ten temat zawiera sekcja WebSphere MQ Internet Pass-Thru (SupportPac MS81).

Konfigurowanie zabezpieczeń

Ta kolekcja tematów zawiera informacje specyficzne dla różnych systemów operacyjnych, a także dla klientów.

Konfigurowanie zabezpieczeń w systemach UNIX, Linux, and Windows

Zagadnienia dotyczące bezpieczeństwa specyficzne dla systemów UNIX, Linux, and Windows .

Menedżery kolejek produktu IBM WebSphere MQ przesyłają informacje, które są potencjalnie cenne, dlatego należy użyć systemu uprawnień, aby upewnić się, że nieautoryzowani użytkownicy nie będą mieli dostępu do menedżerów kolejek. Należy wziąć pod uwagę następujące typy kontroli zabezpieczeń:

Kto może administrować programem IBM WebSphere MQ
Istnieje możliwość zdefiniowania zestawu użytkowników, którzy mogą wydawać komendy do administrowania produktem IBM WebSphere MQ.

Kto może używać obiektów IBM WebSphere MQ
Można zdefiniować, którzy użytkownicy (zwykle aplikacje) będą mogli używać wywołań MQI i PCF, aby wykonać następujące czynności:

- Kto może połączyć się z menedżerem kolejek.
- Kto może uzyskiwać dostęp do obiektów (kolejek, definicji procesów, list nazw, kanałów, kanałów połączenia klienckiego, obiektów nasłuchiwania, usług i obiektów informacji uwierzytelniających) oraz tego, jaki typ dostępu do tych obiektów ma dostęp.
- Kto może uzyskać dostęp do komunikatów programu IBM WebSphere MQ .
- Kto może uzyskać dostęp do informacji kontekstowych powiązanych z komunikatem.

Bezpieczeństwo kanału
Należy upewnić się, że kanały używane do wysyłania komunikatów do systemów zdalnych mogą uzyskiwać dostęp do wymaganych zasobów.

Do nadawania dostępu do bibliotek programów, bibliotek dowiązań MQI i komend można używać standardowych narzędzi operacyjnych. Jednak katalog zawierający kolejki i inne dane menedżera kolejek jest prywatny dla IBM WebSphere MQ; nie należy używać standardowych komend systemu operacyjnego do nadawania lub odbierania uprawnień do zasobów MQI.

Nawiąże połączenie z produktem IBM WebSphere MQ przy użyciu usług

Jeśli korzystasz z usług terminalowych, może to spowodować problemy z użytkownikiem **Create global objects** .

Jeśli połączenie z systemem Okna jest nawiązane z użyciem usług terminalowych i występują problemy podczas tworzenia lub uruchamiania menedżera kolejek, może to być spowodowane prawem użytkownika, **Create global objects**, w ostatnich wersjach produktu Okna.

Prawo użytkownika **Create global objects** ogranicza uprawnienia użytkowników do tworzenia obiektów w globalnej przestrzeni nazw. Aby aplikacja została utworzona w celu utworzenia obiektu globalnego, musi ona działać w globalnej przestrzeni nazw lub użytkownik, pod którym aplikacja jest uruchomiona, musi mieć do niego zastosowanie odpowiednie uprawnienia użytkownika **Create global objects** .

Administratorzy mają domyślnie stosowane uprawnienia użytkownika **Create global objects** , dzięki czemu administrator może tworzyć i uruchamiać menedżery kolejek po połączeniu za pomocą usług terminalowych bez zmiany praw użytkownika.

Jeśli różne metody administrowania produktem WebSphere MQ nie działają w przypadku korzystania z usług terminalowych, należy spróbować ustawić prawo użytkownika **Create global objects** :

1. Otwórz panel Narzędzia administracyjne:

   Windows 2003 i Windows XP
   Dostęp do tego panelu można uzyskać za pomocą opcji **Panel sterowania** > **Narzędzia administracyjne**.

   Windows Vista i Windows Server 2008
   Dostęp do tego panelu można uzyskać za pomocą opcji **Panel sterowania** > **System i konserwacja** > **Narzędzia administracyjne**.
2. Kliknij dwukrotnie opcję **Zasady zabezpieczeń lokalnych**.
3. Rozwiń `Local Policies`.
4. Kliknij opcję `User Rights Assignment`.
5. Dodaj nowego użytkownika lub grupę do strategii **Create global objects** .

Tworzenie grup i zarządzanie nimi w systemie Windows

Te instrukcje prowadzą użytkownika przez proces administrowania grupami na stacji roboczej lub na serwerze składowym.

W przypadku kontrolerów domeny, użytkownicy i grupy są administrowane za pomocą Active Directory. Więcej informacji na temat korzystania z opcji Active Directory można znaleźć w odpowiednich instrukcjach systemu operacyjnego.

Wszelkie zmiany wprowadzone w przypisaniu do grupy użytkownika nie zostaną rozpoznane do momentu zrestartowania menedżera kolejek lub jeśli zostanie wydana komenda MQSC REFRESH SECURITY (lub odpowiednik PCF).

Panel Zarządzanie komputerem służy do pracy z użytkownikami i grupami. Wszelkie zmiany wprowadzone w bieżącym zalogowanym użytkowniku mogą nie być skuteczne, dopóki użytkownik nie zaloguje się ponownie.

Windows 2003 i Windows XP
Dostęp do tego panelu można uzyskać za pomocą opcji **Panel sterowania** > **Narzędzia administracyjne** > **Zarządzanie komputerem**.

Windows Vista i Windows Server 2008
Dostęp do tego panelu można uzyskać za pomocą opcji **Panel sterowania** > **System i konserwacja** > **Narzędzia administracyjne** > **Zarządzanie komputerem**.

Windows 7
Dostęp do tego panelu można uzyskać przy użyciu opcji **Narzędzia administracyjne** > **Zarządzanie komputerem** .

Tworzenie grupy w systemie Windows
Utwórz grupę za pomocą panelu sterowania.

Procedura

1. Otwórz panel sterujący
2. Kliknij dwukrotnie opcję **Narzędzia administracyjne**.
   Zostanie otwarty panel Narzędzia administracyjne.
3. Kliknij dwukrotnie opcję **Zarządzanie komputerem**.
   Zostanie otwarty panel Zarządzanie komputerem.
4. Rozwiń pozycję **Użytkownicy i grupy lokalne**.
5. Kliknij prawym przyciskiem myszy opcję **Grupy**, a następnie wybierz opcję **Nowa grupa ...**.
   Zostanie wyświetlony panel Nowa grupa.
6. Wpisz odpowiednią nazwę w polu Nazwa grupy, a następnie kliknij przycisk **Utwórz**.
7. Naciśnij przycisk **Zamknij**.

Dodawanie użytkownika do grupy w systemie Windows
Dodaj użytkownika do grupy za pomocą panelu sterującego.

Procedura

1. Otwórz panel sterujący
2. Kliknij dwukrotnie opcję **Narzędzia administracyjne**.
   Zostanie otwarty panel Narzędzia administracyjne.
3. Kliknij dwukrotnie opcję **Zarządzanie komputerem**.
   Zostanie otwarty panel Zarządzanie komputerem.
4. W panelu Zarządzanie komputerem rozwiń pozycję **Użytkownicy i grupy lokalne**.
5. Wybierz opcję **Użytkownicy** .
6. Kliknij dwukrotnie użytkownika, który ma zostać dodany do grupy.
   Zostanie wyświetlony panel właściwości użytkownika.
7. Wybierz kartę **Element** .
8. Wybierz grupę, do której chcesz dodać użytkownika. Jeśli grupa, której chcesz użyć, nie jest widoczna:
   a) Kliknij przycisk **Dodaj**.
      Zostanie wyświetlony panel Wybierz grupy.
   b) Kliknij opcję **Położenia ...**.
      Zostanie wyświetlony panel Lokalizacje.
   c) Wybierz położenie grupy, do której ma zostać dodany użytkownik z listy, a następnie kliknij przycisk **OK**.
   d) Wpisz nazwę grupy w udostępnionym polu.

Alternatywnie można kliknąć opcję **Zaawansowane ...** a następnie **Znajdź teraz** , aby wyświetlić listę grup dostępnych w aktualnie wybranej lokalizacji. W tym miejscu wybierz grupę, do której ma zostać dodany użytkownik, a następnie kliknij przycisk **OK**.

e) Kliknij przycisk **OK**.

Zostanie wyświetlony panel właściwości użytkownika, w którym wyświetlana jest grupa, którą dodano.

f) Wybierz grupę.

9. Kliknij przycisk **OK**.

Zostanie wyświetlony panel Zarządzanie komputerem.

Wyświetlanie informacji o tym, kto jest w grupie w systemie Windows

Wyświetlaj elementy grupy za pomocą panelu sterującego.

Procedura

1. Otwórz panel sterujący
2. Kliknij dwukrotnie opcję **Narzędzia administracyjne**.

   Zostanie otwarty panel Narzędzia administracyjne.
3. Kliknij dwukrotnie opcję **Zarządzanie komputerem**.

   Zostanie otwarty panel Zarządzanie komputerem.
4. W panelu Zarządzanie komputerem rozwiń pozycję **Użytkownicy i grupy lokalne**.
5. Wybierz opcję **Grupy**.
6. Kliknij dwukrotnie grupę. Zostanie wyświetlony panel właściwości grupy.

   Zostanie wyświetlony panel właściwości grupy.

Wyniki

Zostaną wyświetlone elementy grupy.

Usuwanie użytkownika z grupy w systemie Windows

Usuń użytkownika z grupy za pomocą panelu sterującego.

Procedura

1. Otwórz panel sterujący
2. Kliknij dwukrotnie opcję **Narzędzia administracyjne**.

   Zostanie otwarty panel Narzędzia administracyjne.
3. Kliknij dwukrotnie opcję **Zarządzanie komputerem**.

   Zostanie otwarty panel Zarządzanie komputerem.
4. W panelu Zarządzanie komputerem rozwiń pozycję **Użytkownicy i grupy lokalne**.
5. Wybierz opcję **Użytkownicy**.
6. Kliknij dwukrotnie użytkownika, który ma zostać dodany do grupy.

   Zostanie wyświetlony panel właściwości użytkownika.
7. Wybierz kartę **Element** .
8. Wybierz grupę, z której chcesz usunąć użytkownika, a następnie kliknij przycisk **Usuń**.
9. Kliknij przycisk **OK**.

   Zostanie wyświetlony panel Zarządzanie komputerem.

Wyniki

Użytkownik został usunięty z grupy.

Tworzenie grup w systemie HP-UX i zarządzanie nimi

W systemie HP-UX, pod warunkiem, że nie jest używany system NIS lub NIS +, należy użyć menedżera administrowania systemem (SAM) w celu pracy z grupami.

Tworzenie grupy w systemie HP-UX

Dodawanie użytkownika do grupy przy użyciu menedżera administrowania systemem

Procedura

1. Z poziomu menedżera administrowania systemem (SAM) kliknij dwukrotnie konta kont użytkowników i grup.
2. Kliknij dwukrotnie grupy.
3. Wybierz opcję Dodaj z menu Działania, aby wyświetlić panel Dodaj nową grupę.
4. Wprowadź nazwę grupy i wybierz użytkowników, którzy mają zostać dodani do grupy.
5. Kliknij przycisk Zastosuj, aby utworzyć grupę.

Wyniki

Grupa została utworzona.

Dodawanie użytkownika do grupy w systemie HP-UX

Dodaj użytkownika do grupy za pomocą programu System Administration Manager.

Procedura

1. Z poziomu menedżera administrowania systemem (SAM) kliknij dwukrotnie konta kont użytkowników i grup.
2. Kliknij dwukrotnie grupy.
3. Podświetl nazwę grupy i wybierz opcję Modyfikuj z menu Działania, aby wyświetlić panel Modyfikuj istniejący panel grupowy.
4. Wybierz użytkownika, który ma zostać dodany do grupy, i kliknij przycisk Dodaj.
5. Jeśli chcesz dodać innych użytkowników do grupy, powtórz krok 4 dla każdego użytkownika.
6. Po zakończeniu dodawania nazw do listy kliknij przycisk OK.

Wyniki

Użytkownik dodał użytkownika do grupy.

Wyświetlanie informacji o tym, kto znajduje się w grupie w systemie HP-UX

Wyświetlaj, kto znajduje się w grupie za pomocą Menedżera Administracji Systemu

Procedura

1. Z poziomu menedżera administrowania systemem (SAM) kliknij dwukrotnie konta kont użytkowników i grup.
2. Kliknij dwukrotnie grupy.
3. Podświetl nazwę grupy i wybierz opcję Modyfikuj z menu Działania, aby wyświetlić panel Modyfikuj istniejący grupę, wyświetlając listę użytkowników w grupie.

Wyniki

Zostaną wyświetlone elementy grupy.

Usuwanie użytkownika z grupy w systemie HP-UX

Usuwanie użytkownika z grupy przy użyciu menedżera administrowania systemem.

Procedura

1. Z poziomu menedżera administrowania systemem (SAM) kliknij dwukrotnie konta kont użytkowników i grup.
2. Kliknij dwukrotnie grupy.
3. Podświetl nazwę grupy i wybierz opcję Modyfikuj z menu Działania, aby wyświetlić panel Modyfikuj istniejący panel grupowy.
4. Wybierz użytkownika, który ma zostać usunięty z grupy, i kliknij przycisk Usuń.
5. Jeśli chcesz usunąć innych użytkowników z grupy, powtórz krok 4 dla każdego użytkownika.
6. Po zakończeniu usuwania nazw z listy kliknij przycisk OK.

Wyniki

Użytkownik usunł użytkownika z grupy

Tworzenie grup i zarządzanie nimi w systemie AIX

W systemie AIX, pod warunkiem, że nie jest używany system NIS lub NIS +, należy użyć SMITTY do pracy z grupami.

Tworzenie grupy

Utwórz grupę przy użyciu SMITTY.

Procedura

1. Z poziomu SMITTY wybierz opcję Zabezpieczenia i Użytkownicy, a następnie naciśnij klawisz Enter.
2. Wybierz grupy i naciśnij klawisz Enter.
3. Wybierz opcję Dodaj grupę i naciśnij klawisz Enter.
4. Wprowadź nazwę grupy i nazwy wszystkich użytkowników, którzy mają zostać dodani do grupy, rozdzielając je przecinkami.
5. Naciśnij klawisz Enter, aby utworzyć grupę.

Wyniki

Grupa została utworzona.

Dodawanie użytkownika do grupy

Dodaj użytkownika do grupy za pomocą interfejsu SMITTY.

Procedura

1. Z poziomu SMITTY wybierz opcję Zabezpieczenia i Użytkownicy, a następnie naciśnij klawisz Enter.
2. Wybierz grupy i naciśnij klawisz Enter.
3. Wybierz opcję Zmień/Pokaż charakterystykę grup i naciśnij klawisz Enter.
4. Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.
5. Dodaj nazwy użytkowników, którzy mają być dodawani do grupy, oddzielając je przecinkami.
6. Naciśnij klawisz Enter, aby dodać nazwy do grupy.

Wyświetlanie, kto znajduje się w grupie

Wyświetlaj, kto jest w grupie za pomocą SMITTY.

Procedura

1. Z poziomu SMITTY wybierz opcję Zabezpieczenia i Użytkownicy, a następnie naciśnij klawisz Enter.
2. Wybierz grupy i naciśnij klawisz Enter.

3. Wybierz opcję Zmień/Pokaż charakterystykę grup i naciśnij klawisz Enter.
4. Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.

Wyniki
Zostaną wyświetlone elementy grupy.

Usuwanie użytkownika z grupy
Usuń użytkownika z grupy za pomocą SMITTY.

Procedura

1. Z poziomu SMITTY wybierz opcję Zabezpieczenia i Użytkownicy, a następnie naciśnij klawisz Enter.
2. Wybierz grupy i naciśnij klawisz Enter.
3. Wybierz opcję Zmień/Pokaż charakterystykę grup i naciśnij klawisz Enter.
4. Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.
5. Usuń z grupy nazwy użytkowników, którzy mają zostać usunięci.
6. Naciśnij klawisz Enter, aby usunąć nazwy z grupy.

Wyniki
Użytkownik usunł użytkownika z grupy.

Tworzenie grup i zarządzanie nimi w systemie Solaris

W systemie Solaris, pod warunkiem, że nie jest używany system NIS lub NIS +, należy użyć pliku `/etc/group` do pracy z grupami.

Tworzenie grupy w systemie Solaris
Tworzenie grupy za pomocą komendy **groupadd** .

Procedura

Wywołaj następującą komendę: `groupadd` *`group-name`*

gdzie *nazwa_grupy* jest nazwą grupy.

Wyniki
Plik `/etc/group` pliku zawiera informacje o grupie.

Dodawanie użytkownika do grupy w systemie Solaris
Dodaj użytkownika do grupy za pomocą komendy **usermod** .

Procedura

Aby dodać członka do grupy uzupełniającej, wykonaj komendę `usermod` i wyświetl listę grup dodatkowych, których członkiem jest aktualnie użytkownik, oraz grup dodatkowych, do których użytkownik ma zostać członkiem.
Na przykład, jeśli użytkownik jest członkiem grupy `groupa`i ma zostać członkiem produktu `groupb` , należy użyć następującej komendy: `usermod -G groupa,groupb` *`user-name`* , gdzie *nazwa-użytkownika* jest nazwą użytkownika.

Wyświetlanie informacji o tym, kto jest w grupie w systemie Solaris
Aby wykryć osobę, która jest członkiem grupy, należy sprawdzić pozycję dla tej grupy w pliku `/etc/group` .

Usuwanie użytkownika z grupy w systemie Solaris
Usuń użytkownika z grupy za pomocą komendy **usermod** .

Procedura

Aby usunąć członka z grupy uzupełniającej, należy wykonać komendę **usermod** z listą grup dodatkowych, do których użytkownik ma pozostać członkiem grupy.
Na przykład, jeśli podstawową grupą użytkownika jest `users` , a użytkownik jest także członkiem grup `mqm`, `groupa` i `groupb`, aby usunąć użytkownika z grupy `mqm` , używana jest następująca komenda: `usermod -G groupa,groupb` *`user-name`*, gdzie *`user-name`* jest nazwą użytkownika.

Tworzenie grup i zarządzanie nimi w systemie Linux

W systemie Linux, pod warunkiem, że nie jest używany system NIS lub NIS +, należy użyć pliku `/etc/group` do pracy z grupami.

Tworzenie grupy w systemie Linux

Utwórz grupę za pomocą komendy **groupadd** .

Procedura

Aby utworzyć nową grupę, wpisz następującą komendę: `groupadd -g` *`group-ID group-name`*
, gdzie *identyfikator-grupy* to liczbowy identyfikator grupy, a *nazwa_grupy* jest nazwą grupy.

Wyniki

Plik `/etc/group` pliku zawiera informacje o grupie.

Dodawanie użytkownika do grupy w systemie Linux

Dodaj użytkownika do grupy za pomocą komendy **usermod** .

Procedura

Aby dodać członka do grupy uzupełniającej, wykonaj komendę `usermod` i wyświetl listę grup dodatkowych, których członkiem jest aktualnie użytkownik, oraz grup dodatkowych, do których użytkownik ma zostać członkiem.
Na przykład, jeśli użytkownik jest członkiem grupy `groupa`i ma stać się członkiem `groupb` również, używana jest następująca komenda: `usermod -G groupa,groupb` *`user-name`*
, gdzie *`user-name`* jest nazwą użytkownika.

Wyświetlanie informacji o tym, kto jest w grupie w systemie Linux

Wyświetl osobę, która znajduje się w grupie, używając komendy **getent** .

Procedura

Aby wyświetlić osobę, która jest członkiem grupy, wpisz następującą komendę: `getent group` *`group-name`*
, gdzie *nazwa_grupy* jest nazwą grupy.

Usuwanie użytkownika z grupy

Usuń użytkownika z grupy za pomocą komendy **usermod** .

Procedura

Aby usunąć członka z grupy uzupełniającej, należy wykonać komendę **usermod** z listą grup dodatkowych, do których użytkownik ma pozostać członkiem grupy.
Na przykład, jeśli podstawową grupą użytkownika jest `users` , a użytkownik jest także członkiem grup `mqm`, `groupa` i `groupb`, aby usunąć użytkownika z grupy `mqm` , używana jest następująca komenda: `usermod -G groupa,groupb` *`user-name`*
, gdzie *nazwa-użytkownika* jest nazwą użytkownika.

Jak działają autoryzacje

Tabele specyfikacji autoryzacji w tematach w tej sekcji określają dokładnie, w jaki sposób działają autoryzacje i ograniczenia, które mają zastosowanie.

Tabele mają zastosowanie do następujących sytuacji:

- Aplikacje, które wywołują wywołania MQI
- Programy administracyjne, które wydają komendy MQSC, jako wyjścia z systemu PCF
- Programy administracyjne, które wydają komendy PCF

W tej sekcji informacje są prezentowane jako zestaw tabel, które określają następujące elementy:

Działanie do wykonania
Opcja MQI, komenda MQSC lub komenda PCF.

Obiekt kontroli dostępu
Kolejka, proces, menedżer kolejek, lista nazw, informacje o uwierzytelnianiu, kanał, kanał połączenia klienta, obiekt nasłuchiwania lub usługa.

Wymagane uprawnienia
Wyrażony jako stała MQZAO_.

W tabelach stałe przedrostki przedrostków MQZAO_ odpowiadają słowom kluczom z listy autoryzacji dla komendy `setmqaut` dla danej jednostki. Na przykład MQZAO_BROWSE odpowiada słowu kluczowi `+browse`, MQZAO_SET_ALL_CONTEXT odpowiada słownie kluczowi `+setall`, itd. Te stałe są zdefiniowane w pliku nagłówkowego cmqzc.hdostarczonym wraz z produktem.

Autoryzacje dla wywołań MQI

MQCONN, **MQOPEN**, **MQPUT1**i **MQCLOSE** mogą wymagać sprawdzenia autoryzacji. W tabelach w tym temacie podsumowane są autoryzacje wymagane dla każdego wywołania.

Aplikacja może wydawać określone wywołania i opcje MQI tylko wtedy, gdy identyfikator użytkownika, pod którym jest uruchomiony (lub którego autoryzacje jest w stanie przyjąć), otrzymał odpowiednie uprawnienia.

Cztery wywołania MQI mogą wymagać sprawdzenia autoryzacji: **MQCONN**, **MQOPEN**, **MQPUT1**i **MQCLOSE**.

W przypadku systemów MQOPEN i MQPUT1sprawdzanie uprawnień jest wykonywane na podstawie nazwy otwieranego obiektu, a nie nazwy lub nazw, co powoduje, że nazwa została rozstrzygnięta. Na przykład aplikacja może mieć uprawnienie do otwierania kolejki aliasowej bez uprawnienia do otwierania kolejki podstawowej, do której alias jest tłumaczona. Reguła polega na tym, że sprawdzanie jest przeprowadzane na pierwszej definicji napotkanej podczas procesu rozstrzygania nazwy, która nie jest aliasem menedżera kolejek, chyba że definicja aliasu menedżera kolejek jest otwierana bezpośrednio, to znaczy, że jej nazwa jest wyświetlana w polu *ObjectName* deskryptora obiektu. Uprawnienia są zawsze potrzebne dla otwieranego obiektu. W niektórych przypadkach wymagane jest dodatkowe uprawnienie niezależne od kolejki, które jest uzyskiwane za pomocą autoryzacji dla obiektu menedżera kolejek.

Tabela 8 na stronie 93, Tabela 9 na stronie 93, Tabela 10 na stronie 93i Tabela 11 na stronie 94 podsumowują autoryzacje wymagane dla każdego wywołania. W tabelach *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie ma znaczenia dla tej operacji; *Brak sprawdzania* oznacza, że nie jest przeprowadzane sprawdzanie autoryzacji.

Uwaga: W tych tabelach nie zostanie podana żadna wzmianka o listach nazw, kanałach, kanałach połączeń klienta, obiektach nasłuchiwania, usługach lub obiektach informacji uwierzytelniających. Wynika to z faktu, że żadne autoryzacje nie mają zastosowania do tych obiektów, z wyjątkiem MQOO_INQUIRE, dla których mają zastosowanie te same uprawnienia, jak w przypadku innych obiektów.

Specjalna autoryzacja MQZAO_ALL_MQI obejmuje wszystkie autoryzacje w tabelach, które są istotne dla danego typu obiektu, z wyjątkiem operacji MQZAO_DELETE i MQZAO_DISPLAY, które są klasowane jako autoryzacje administracyjne.

Aby zmodyfikować dowolne opcje kontekstu komunikatu, należy mieć odpowiednie autoryzacje do wystawienia połączenia. Na przykład, aby można było używać funkcji MQOO_SET_IDENTITY_CONTEXT lub MQPMO_SET_IDENTITY_CONTEXT, użytkownik musi mieć uprawnienie `+setid` .

Tabela 8. Autoryzacja zabezpieczeń wymagana dla wywołań MQCONN			
Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 94)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCONN	Nie dotyczy	Nie dotyczy	MQZAO_CONNECT

Tabela 9. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN			
Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 94)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_INQUIRE	MQZAO_ZAPYTANIE_O	MQZAO_ZAPYTANIE_O	MQZAO_ZAPYTANIE_O
MQOO_BROWSE	MQZAO_PRZEGLĄDANIE	Nie dotyczy	Brak sprawdzenia
MQOO_INPUT_ *	MQZAO_INPUT	Nie dotyczy	Brak sprawdzenia
MQOO_SAVE_ ALL_CONTEXT **(“2” na stronie 94)**	MQZAO_INPUT	Nie dotyczy	Nie dotyczy
MQOO_OUTPUT (normalna kolejka) **(“3” na stronie 94)**	MQZAO_OUTPUT	Nie dotyczy	Nie dotyczy
MQOO_PASS_ IDENTITY_CONTEXT **(“4” na stronie 94)**	MQZAO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	Nie dotyczy	Brak sprawdzenia
MQOO_PASS_ALL_ CONTEXT **(“4” na stronie 94, “5” na stronie 94)**	MQZAO_PASS _ALL_CONTEXT	Nie dotyczy	Brak sprawdzenia
MQOO_SET_ IDENTITY_CONTEXT **(“4” na stronie 94, “5” na stronie 94)**	MQZAO_SET_ KONTEKST_IDENTYFIKATORA	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **(“6” na stronie 94)**
MQOO_SET_ ALL_CONTEXT **(“4” na stronie 94, “7” na stronie 94)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **(“6” na stronie 94)**
MQOO_OUTPUT (kolejka transmisji) **(“8” na stronie 94)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **(“6” na stronie 94)**
MQOO_SET	MQZAO_SET	Nie dotyczy	Brak sprawdzenia
MQOO_ALTERNATE_ USER_AUTHORITY	**(“9” na stronie 95)**	**(“9” na stronie 95)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“9” na stronie 95, “10” na stronie 95)**

Tabela 10. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1			
Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 94)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	MQZAO_PASS_ IDENTITY_CONTEXT **(“11” na stronie 95)**	Nie dotyczy	Brak sprawdzenia

Tabela 10. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1 (kontynuacja)			
Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 94)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **(“11” na stronie 95)**	Nie dotyczy	Brak sprawdzenia
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **(“11” na stronie 95)**	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **(“6” na stronie 94)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **(“11” na stronie 95)**	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **(“6” na stronie 94)**
(Kolejka transmisji) **(“8” na stronie 94)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **(“6” na stronie 94)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**(“12” na stronie 95)**	Nie dotyczy	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” na stronie 95)**

Tabela 11. Autoryzacja zabezpieczeń wymagana dla wywołań MQCLOSE			
Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 94)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCO_DELETE	MQZAO_DELETE **(“13” na stronie 95)**	Nie dotyczy	Nie dotyczy
MQCO_DELETE _PURGE	MQZAO_DELETE **(“13” na stronie 95)**	Nie dotyczy	Nie dotyczy

Uwagi dotyczące tabel:

1. W przypadku otwierania kolejki modelowej:
   - Uprawnienie MQZAO_DISPLAY jest wymagane dla kolejki modelowej, oprócz uprawnień do otwarcia kolejki modelowej dla typu dostępu, dla którego otwierana jest kolejka modelowa.
   - Uprawnienie MQZAO_CREATE nie jest wymagane do utworzenia kolejki dynamicznej.
   - Identyfikator użytkownika używany do otwarcia kolejki modelowej jest automatycznie nadawany przez wszystkie uprawnienia specyficzne dla kolejki (równoważne MQZAO_ALL) dla utworzonej kolejki dynamicznej.
2. Parametr MQOO_INPUT_ * musi być również określony. Jest to poprawne dla kolejki lokalnej, modelu lub kolejki aliasowej.
3. To sprawdzenie jest wykonywane dla wszystkich przypadków wyjściowych, z wyjątkiem kolejek transmisji (patrz uwaga “8” na stronie 94).
4. Należy również określić parametr MQOO_OUTPUT.
5. Opcja MQOO_PASS_IDENTITY_CONTEXT jest również implikowana przez tę opcję.
6. Uprawnienie to jest wymagane zarówno dla obiektu menedżera kolejek, jak i dla konkretnej kolejki.
7. Opcja ta oznacza również parametr mqoo_pass_identity_context, mqoo_pass_all_context i MQOO_SET_IDENTITY_CONTEXT.
8. To sprawdzenie jest wykonywane dla lokalnej lub modelowej kolejki, której atrybut kolejki *Użycie* ma wartość MQUS_TRANSMISSION, i jest otwierany bezpośrednio dla danych wyjściowych. Nie ma

zastosowania, jeśli kolejka zdalna jest otwierana (przez określenie nazw zdalnego menedżera kolejek i kolejki zdalnej albo przez określenie nazwy lokalnej definicji kolejki zdalnej).

9. Należy również określić co najmniej jedną z następujących wartości: MQOO_INQUIRE (dla dowolnego typu obiektu) lub MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET (dla kolejek). Sprawdzenie przeprowadzane jest tak, jak w przypadku pozostałych określonych opcji, przy użyciu podanego identyfikatora użytkownika alternatywnego dla określonego uprawnienia do obiektu o określonej nazwie oraz bieżącego uprawnienia do aplikacji dla sprawdzania identyfikatora MQZAO_ALTERNATE_USER_IDENTIFIER.
10. Ta autoryzacja umożliwia określenie dowolnego identyfikatora *AlternateUser* .
11. Sprawdzenie MQZAO_OUTPUT jest przeprowadzane również wtedy, gdy kolejka nie ma atrybutu kolejki *Użycie* w tabeli MQUS_TRANSMISSION.
12. Przeprowadzone sprawdzenie jest tak, jak w przypadku pozostałych określonych opcji, przy użyciu podanego identyfikatora użytkownika alternatywnego dla określonego uprawnienia do kolejki, oraz bieżącego uprawnienia do aplikacji dla sprawdzania identyfikatora MQZAO_ALTERNATE_USER_IDENTIFIER.
13. Kontrola jest przeprowadzana tylko w przypadku, gdy spełnione są oba poniższe warunki:
    - Trwała kolejka dynamiczna jest zamykana i usuwana.
    - Kolejka nie została utworzona przez wywołanie MQOPEN , które zwróciło uchwyt obiektu, który jest używany.

    W przeciwnym razie nie będzie sprawdzania.

Autoryzacje dla komend MQSC w systemach PCF o zmienionym znaczeniu

Te informacje podsumowują autoryzacje wymagane dla każdej komendy MQSC zawartej w programie Escape PCF.

Nie dotyczy oznacza, że ta operacja nie ma znaczenia dla tego typu obiektu.

ID użytkownika, pod którym uruchomiony jest program uruchamiający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie MQZAO_DISPLAY w menedżerze kolejek w celu wykonania komend PCF
- Uprawnienie do wydania komendy MQSC w tekście komendy Escape PCF

ALTER *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	ZMIANA MQZAO_CHANGE
Temat	ZMIANA MQZAO_CHANGE
Proces	ZMIANA MQZAO_CHANGE
Menedżer kolejek	ZMIANA MQZAO_CHANGE
Lista nazw	ZMIANA MQZAO_CHANGE
Informacje uwierzytelniające	ZMIANA MQZAO_CHANGE
Kanał	ZMIANA MQZAO_CHANGE
Kanał połączenia klienta	ZMIANA MQZAO_CHANGE
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE
Informacje o komunikacji	ZMIANA MQZAO_CHANGE

CLEAR *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CLEAR
Temat	MQZAO_CLEAR
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	Nie dotyczy
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy
Informacje o komunikacji	Nie dotyczy

DEFINE *obiekt* NOREPLACE (“1” na stronie 100)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(“2” na stronie 100)**
Temat	MQZAO_CREATE **(“2” na stronie 100)**
Proces	MQZAO_CREATE **(“2” na stronie 100)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(“2” na stronie 100)**
Informacje uwierzytelniające	MQZAO_CREATE **(“2” na stronie 100)**
Kanał	MQZAO_CREATE **(“2” na stronie 100)**
Kanał połączenia klienta	MQZAO_CREATE **(“2” na stronie 100)**
Program nasłuchujący	MQZAO_CREATE **(“2” na stronie 100)**
Usługa	MQZAO_CREATE **(“2” na stronie 100)**
Informacje o komunikacji	MQZAO_CREATE **(“2” na stronie 100)**

DEFINE *obiekt* REPLACE (“1” na stronie 100, “3” na stronie 100)

Obiekt	Wymagane uprawnienia
Kolejka	ZMIANA MQZAO_CHANGE
Temat	ZMIANA MQZAO_CHANGE
Proces	ZMIANA MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	ZMIANA MQZAO_CHANGE
Informacje uwierzytelniające	ZMIANA MQZAO_CHANGE
Kanał	ZMIANA MQZAO_CHANGE

Obiekt	Wymagane uprawnienia
Kanał połączenia klienta	ZMIANA MQZAO_CHANGE
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE
Informacje o komunikacji	ZMIANA MQZAO_CHANGE

DELETE *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DELETE
Temat	MQZAO_DELETE
Proces	MQZAO_DELETE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_DELETE
Informacje uwierzytelniające	MQZAO_DELETE
Kanał	MQZAO_DELETE
Kanał połączenia klienta	MQZAO_DELETE
Program nasłuchujący	MQZAO_DELETE
Usługa	MQZAO_DELETE
Informacje o komunikacji	MQZAO_DELETE

DISPLAY *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DISPLAY
Temat	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
Menedżer kolejek	MQZAO_DISPLAY
Lista nazw	MQZAO_DISPLAY
Informacje uwierzytelniające	MQZAO_DISPLAY
Kanał	MQZAO_DISPLAY
Kanał połączenia klienta	MQZAO_DISPLAY
Program nasłuchujący	MQZAO_DISPLAY
Usługa	MQZAO_DISPLAY
Informacje o komunikacji	MQZAO_DISPLAY

START *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy

Obiekt	Wymagane uprawnienia
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

STOP *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

Komendy kanałów

Komenda	Obiekt	Wymagane uprawnienia
KANAŁ PING	Kanał	MQZAO_CONTROL
Resetuj kanał	Kanał	MQZAO_CONTROL_EXTENDED
Rozstrzyganie kanału	Kanał	MQZAO_CONTROL_EXTENDED

Komendy dotyczące subskrypcji

Komenda	Obiekt	Wymagane uprawnienia
ALTER SUB	Temat	MQZAO_CONTROL
DEFINE SUB	Temat	MQZAO_CONTROL
USUŃ SUB	Temat	MQZAO_CONTROL
WYŚWIETL SUB	Temat	MQZAO_DISPLAY

Komendy ochrony

Komenda	Obiekt	Wymagane uprawnienia
SET AUTHREC	Menedżer kolejek	ZMIANA MQZAO_CHANGE
USUŃ AUTHREC	Menedżer kolejek	ZMIANA MQZAO_CHANGE
DISPLAY AUTHREC	Menedżer kolejek	MQZAO_DISPLAY
DISPLAY AUTHSERV	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETLAJ ENTAUTH	Menedżer kolejek	MQZAO_DISPLAY
USTAW WARTOŚĆ CHLAUTH	Menedżer kolejek	ZMIANA MQZAO_CHANGE
WYŚWIETL CHLAUTH	Menedżer kolejek	MQZAO_DISPLAY
REFRESH SECURITY	Menedżer kolejek	ZMIANA MQZAO_CHANGE

Wyświetlanie statusu

Komenda	Obiekt	Wymagane uprawnienia
WYŚWIETL STATUS CHSTATUS	Menedżer kolejek	MQZAO_DISPLAY Należy pamiętać, że jeśli typem kanału jest CLUSSDR, w kolejce transmisji wymagane jest uprawnienie +inq (lub równoważna wartość MQZAO_INQUIRE).
WYŚWIETL STATUS LSSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL PUBSUB	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL STATUS SBSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL STATUS SVSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL STATUS TPSTATUS	Menedżer kolejek	MQZAO_DISPLAY

Komendy klastrów

Komenda	Obiekt	Wymagane uprawnienia
WYŚWIETL CLUSQMGR	Menedżer kolejek	MQZAO_DISPLAY
ODŚWIEŻ KLASTER	Wymagane jest członkostwo w grupie 'mqm'	
Resetowanie klastra	Wymagane jest członkostwo w grupie 'mqm'	
Menedżer kolejki zawieszony	Wymagane jest członkostwo w grupie 'mqm'	
WZNÓW MENEDŻERA KOLEJEK	Wymagane jest członkostwo w grupie 'mqm'	

Inne komendy administracyjne

Komenda	Obiekt	Wymagane uprawnienia
PING QMGR	Menedżer kolejek	MQZAO_DISPLAY
ODŚWIEŻ MENEDŻERA KOLEJEK	Menedżer kolejek	ZMIANA MQZAO_CHANGE

Komenda	Obiekt	Wymagane uprawnienia
RESETOWANIE MENEDŻERA KOLEJEK	Menedżer kolejek	ZMIANA MQZAO_CHANGE
WYŚWIETL KONTEKST	Menedżer kolejek	MQZAO_DISPLAY
ZATRZYMAJ CONN	Menedżer kolejek	ZMIANA MQZAO_CHANGE

Uwaga:

1. W przypadku komend DEFINE wymagane jest również uprawnienie MQZAO_DISPLAY dla obiektu LIKE, jeśli jest on określony, lub w odpowiednim SYSTEM.DEFAULT.xxx , jeśli parametr LIKE jest pominięty.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane dla wszystkich obiektów dla określonego menedżera kolejek, poprzez określenie typu obiektu QMGR w komendzie `setmqaut` .
3. Dotyczy to sytuacji, gdy obiekt, który ma zostać zastąpiony, już istnieje. Jeśli tak nie jest, sprawdzanie jest tak samo, jak dla opcji DEFINE *obiekt* NOREPLACE.

Informacje pokrewne

Technologia klastrowa: sprawdzone procedury użycia komendy REFRESH CLUSTER

Autoryzacje dla komend PCF

W tej sekcji podsumowano autoryzacje wymagane dla każdej komendy PCF.

Brak sprawdzania oznacza, że sprawdzanie autoryzacji nie jest przeprowadzane; *Nie dotyczy* oznacza, że ta operacja nie ma znaczenia dla tego typu obiektu.

ID użytkownika, pod którym uruchomiony jest program uruchamiający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie MQZAO_DISPLAY w menedżerze kolejek w celu wykonania komend PCF

Specjalna autoryzacja MQZAO_ALL_ADMIN obejmuje wszystkie autoryzacje znajdujące się na poniższej liście, które są istotne dla danego typu obiektu, z wyjątkiem MQZAO_CREATE, który nie jest specyficzny dla konkretnego obiektu lub typu obiektu.

Zmień *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	ZMIANA MQZAO_CHANGE
Temat	ZMIANA MQZAO_CHANGE
Proces	ZMIANA MQZAO_CHANGE
menedżer kolejek	ZMIANA MQZAO_CHANGE
Lista nazw	ZMIANA MQZAO_CHANGE
Informacje uwierzytelniające	ZMIANA MQZAO_CHANGE
Kanał	ZMIANA MQZAO_CHANGE
Kanał połączenia klienta	ZMIANA MQZAO_CHANGE
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE
Informacje o komunikacji	ZMIANA MQZAO_CHANGE

Wyczyść obiekt *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CLEAR
Temat	MQZAO_CLEAR
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	Nie dotyczy
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy
Informacje o komunikacji	Nie dotyczy

Skopiuj *obiekt* (bez zastępowania) (1)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(2)**
Temat	MQZAO_CREATE **(2)**
Proces	MQZAO_CREATE **(2)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(2)**
Informacje uwierzytelniające	MQZAO_CREATE **(2)**
Kanał	MQZAO_CREATE **(2)**
Kanał połączenia klienta	MQZAO_CREATE **(2)**
Program nasłuchujący	MQZAO_CREATE **(2)**
Usługa	MQZAO_CREATE **(2)**
Informacje o komunikacji	MQZAO_CREATE **(“2” na stronie 106)**

Skopiuj *obiekt* (z zastępem) (1, 4)

Obiekt	Wymagane uprawnienia
Kolejka	ZMIANA MQZAO_CHANGE
Temat	ZMIANA MQZAO_CHANGE
Proces	ZMIANA MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	ZMIANA MQZAO_CHANGE
Informacje uwierzytelniające	ZMIANA MQZAO_CHANGE
Kanał	ZMIANA MQZAO_CHANGE

Obiekt	Wymagane uprawnienia
Kanał połączenia klienta	ZMIANA MQZAO_CHANGE
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE
Informacje o komunikacji	ZMIANA MQZAO_CHANGE

Utwórz obiekt *obiekt* (bez zastępowania) (3)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(2)**
Temat	MQZAO_CREATE **(2)**
Proces	MQZAO_CREATE **(2)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(2)**
Informacje uwierzytelniające	MQZAO_CREATE **(2)**
Kanał	MQZAO_CREATE **(2)**
Kanał połączenia klienta	MQZAO_CREATE **(2)**
Program nasłuchujący	MQZAO_CREATE **(2)**
Usługa	MQZAO_CREATE **(2)**
Informacje o komunikacji	MQZAO_CREATE **(2)**

Utwórz obiekt *obiekt* (z zastępem) (3, 4)

Obiekt	Wymagane uprawnienia
Kolejka	ZMIANA MQZAO_CHANGE
Temat	ZMIANA MQZAO_CHANGE
Proces	ZMIANA MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	ZMIANA MQZAO_CHANGE
Informacje uwierzytelniające	ZMIANA MQZAO_CHANGE
Kanał	ZMIANA MQZAO_CHANGE
Kanał połączenia klienta	ZMIANA MQZAO_CHANGE
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE
Informacje o komunikacji	ZMIANA MQZAO_CHANGE

Usuń obiekt *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DELETE
Temat	MQZAO_DELETE

Obiekt	Wymagane uprawnienia
Proces	MQZAO_DELETE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_DELETE
Informacje uwierzytelniające	MQZAO_DELETE
Kanał	MQZAO_DELETE
Kanał połączenia klienta	MQZAO_DELETE
Program nasłuchujący	MQZAO_DELETE
Usługa	MQZAO_DELETE
Informacje o komunikacji	MQZAO_DELETE

Zapytaj *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DISPLAY
Temat	MQZAO_DISPLAY
Proces	MQZAO_DISPLAY
menedżer kolejek	MQZAO_DISPLAY
Lista nazw	MQZAO_DISPLAY
Informacje uwierzytelniające	MQZAO_DISPLAY
Kanał	MQZAO_DISPLAY
Kanał połączenia klienta	MQZAO_DISPLAY
Program nasłuchujący	MQZAO_DISPLAY
Usługa	MQZAO_DISPLAY
Informacje o komunikacji	MQZAO_DISPLAY

Zapytanie o nazwy *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Brak sprawdzenia
Temat	Brak sprawdzenia
Proces	Brak sprawdzenia
Menedżer kolejek	Brak sprawdzenia
Lista nazw	Brak sprawdzenia
Informacje uwierzytelniające	Brak sprawdzenia
Kanał	Brak sprawdzenia
Kanał połączenia klienta	Brak sprawdzenia
Program nasłuchujący	Brak sprawdzenia
Usługa	Brak sprawdzenia

Obiekt	Wymagane uprawnienia
Informacje o komunikacji	Brak sprawdzenia

Uruchom *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

Zatrzymaj *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

Komendy kanałów

Komenda	Obiekt	Wymagane uprawnienia
Kanał Ping	Kanał	MQZAO_CONTROL
Resetowanie kanału	Kanał	MQZAO_CONTROL_EXTENDED
Rozstrzyganie kanału	Kanał	MQZAO_CONTROL_EXTENDED

Komendy dotyczące subskrypcji

Komenda	Obiekt	Wymagane uprawnienia
Zmień subskrypcję	Temat	MQZAO_CONTROL
Utwórz subskrypcję	Temat	MQZAO_CONTROL
Usuń subskrypcję	Temat	MQZAO_CONTROL
Zapytanie o subskrypcję	Temat	MQZAO_DISPLAY

Komendy ochrony

Komenda	Obiekt	Wymagane uprawnienia
Ustaw rekord uprawnień	Menedżer kolejek	ZMIANA MQZAO_CHANGE
Usuń rekord uprawnień	Menedżer kolejek	ZMIANA MQZAO_CHANGE
Zapytanie o rekordy uprawnień	Menedżer kolejek	MQZAO_DISPLAY
Usługa InInquire Authority	Menedżer kolejek	MQZAO_DISPLAY
Obiekt Inquire Entity Authority	Menedżer kolejek	MQZAO_DISPLAY
Ustawianie rekordu uwierzytelniania kanału	Menedżer kolejek	ZMIANA MQZAO_CHANGE
Zapytanie o rekordy uwierzytelniania kanału	Menedżer kolejek	MQZAO_DISPLAY
Odśwież zabezpieczenia	Menedżer kolejek	ZMIANA MQZAO_CHANGE

Wyświetlanie statusu

Komenda	Obiekt	Wymagane uprawnienia
Status uzyskiwania informacji o statusie kanału	Menedżer kolejek	MQZAO_DISPLAY Należy pamiętać, że jeśli typem kanału jest CLUSSDR, w kolejce transmisji wymagane jest uprawnienie +inq (lub równoważna wartość MQZAO_INQUIRE).
Zapytanie o status programu nasłuchującego kanału	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status publikowania/subskrypcji	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status subskrypcji	Menedżer kolejek	MQZAO_DISPLAY
Status usługi Inquire	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status tematu	Menedżer kolejek	MQZAO_DISPLAY

Komendy klastrów

Komenda	Obiekt	Wymagane uprawnienia
Inquire Cluster Queue Manager	Menedżer kolejek	MQZAO_DISPLAY
Odśwież klaster	Wymagane jest członkostwo w grupie 'mqm'	

Komenda	Obiekt	Wymagane uprawnienia
Resetowanie klastra	Wymagane jest członkostwo w grupie 'mqm'	
Zawieś klaster menedżera kolejek	Wymagane jest członkostwo w grupie 'mqm'	
Wznów klaster menedżera kolejek	Wymagane jest członkostwo w grupie 'mqm'	

Inne komendy administracyjne

Komenda	Obiekt	Wymagane uprawnienia
Menedżer kolejek Ping	Menedżer kolejek	MQZAO_DISPLAY
Odśwież menedżer kolejek	Menedżer kolejek	ZMIANA MQZAO_CHANGE
Zresetuj menedżera kolejek	Menedżer kolejek	ZMIANA MQZAO_CHANGE
Resetuj statystyki kolejki	Kolejka	MQZAO_DISPLAY i MQZAO_CHANGE
Zapytanie o połączenie	Menedżer kolejek	MQZAO_DISPLAY
Zatrzymaj połączenie	Menedżer kolejek	ZMIANA MQZAO_CHANGE

Uwaga:

1. W przypadku komend Kopiowanie uprawnienie MQZAO_DISPLAY jest również wymagane dla obiektu From.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane dla wszystkich obiektów dla określonego menedżera kolejek, poprzez określenie typu obiektu QMGR w komendzie `setmqaut` .
3. W przypadku komend Create wymagane jest również uprawnienie MQZAO_DISPLAY dla odpowiedniego SYSTEM.DEFAULT.* .
4. Dotyczy to sytuacji, gdy obiekt, który ma zostać zastąpiony, już istnieje. Jeśli tak nie jest, sprawdzanie jest tak samo jak w przypadku kopiowania lub tworzenia bez zastępowania.

Specjalne uwagi dotyczące zabezpieczeń w systemie Windows

Niektóre funkcje zabezpieczeń zachowują się inaczej w różnych wersjach systemu Windows.

Zabezpieczenia systemu IBM WebSphere MQ są oparte na wywołaniach interfejsu API systemu operacyjnego w celu uzyskania informacji na temat autoryzacji użytkowników i przynależności do grup. Niektóre funkcje nie zachowują się identycznie jak w systemach Windows . Ta kolekcja tematów zawiera opisy sytuacji, w których różnice te mogą mieć wpływ na bezpieczeństwo systemu IBM WebSphere MQ podczas działania produktu IBM WebSphere MQ w środowisku Windows .

Program obsługi wyjścia kanału SSPI

Produkt WebSphere MQ for Windows udostępnia program obsługi wyjścia zabezpieczeń, który może być używany zarówno w kanałach komunikatów, jak i w kanałach MQI. Wyjście jest dostarczane jako kod źródłowy i obiektowy, a także udostępnia uwierzytelnianie jednokierunkowe i dwukierunkowe.

Wyjście zabezpieczeń korzysta z interfejsu SSPI (Security Support Provider Interface), który udostępnia zintegrowane zabezpieczenia na platformach Windows .

Wyjście zabezpieczeń udostępnia następujące usługi identyfikacji i uwierzytelniania:

uwierzytelnianie jednokierunkowe
W ten sposób obsługiwana jest obsługa uwierzytelniania Windows NT LAN Manager (NTLM). NTLM pozwala serwerom na uwierzytelnianie swoich klientów. Nie zezwala on klientowi na uwierzytelnienie serwera lub jednego serwera w celu uwierzytelnienia innego serwera. NTLM został zaprojektowany

dla środowiska sieciowego, w którym zakłada się, że serwery są prawdziwe. Protokół NTLM jest obsługiwany na wszystkich platformach Windows , które są obsługiwane przez produkt WebSphere MQ w wersji 7.0.

Ta usługa jest zwykle używana w kanale MQI w celu włączenia menedżera kolejek serwera w celu uwierzytelnienia aplikacji klienckiej MQI produktu WebSphere MQ . Aplikacja kliencka jest identyfikowana za pomocą ID użytkownika powiązanego z uruchomionym procesem.

Aby wykonać uwierzytelnianie, wyjście zabezpieczeń na końcu kanału klienta uzyskuje znacznik uwierzytelniania z NTLM i wysyła token w komunikacie bezpieczeństwa do jego partnera na drugim końcu kanału. Wyjście zabezpieczeń partnera przekazuje znacznik do protokołu NTLM, który sprawdza, czy znacznik jest autentyczny. Jeśli program obsługi wyjścia zabezpieczeń partnera nie jest zadowolony z autentyczności tokenu, nakazuje agentowi MCA zamknięcie kanału.

Dwa sposoby, czyli wzajemne uwierzytelnianie

Korzysta z usług uwierzytelniania Kerberos . Protokół Kerberos nie zakłada, że serwery w środowisku sieciowym są prawdziwe. Serwery mogą uwierzytelniać klientów i inne serwery, a klienci mogą uwierzytelniać serwery. Protokół Kerberos jest obsługiwany na wszystkich platformach Windows obsługiwanych przez produkt WebSphere MQ w wersji 7.0.

Ta usługa może być używana zarówno w kanałach komunikatów, jak i w kanałach MQI. W kanale komunikatów zapewnia wzajemne uwierzytelnianie dwóch menedżerów kolejek. W kanale MQI włącza menedżera kolejek serwera i aplikację kliencką MQI produktu WebSphere MQ w celu uwierzytelnienia siebie. Menedżer kolejek jest identyfikowany za pomocą nazwy poprzedzonej łańcuchem `ibmMQSeries/`. Aplikacja kliencka jest identyfikowana za pomocą ID użytkownika powiązanego z uruchomionym procesem.

Aby wykonać uwierzytelnianie wzajemne, inicjujące wyjście zabezpieczeń uzyskuje znacznik uwierzytelniania z serwera zabezpieczeń Kerberos i wysyła znacznik w komunikacie bezpieczeństwa do jego partnera. Wyjście zabezpieczeń partnera przekazuje znacznik do serwera Kerberos , który sprawdza, czy jest on autentyczny. Serwer zabezpieczeń Kerberos generuje drugi znacznik, który jest wysyłany przez partnera w komunikacie bezpieczeństwa do inicjowania wyjścia zabezpieczeń. Następnie inicjujące wyjście zabezpieczeń zwraca się do serwera Kerberos o sprawdzenie, czy drugi znacznik jest autentyczny. Podczas tej wymiany, jeśli albo wyjście zabezpieczeń nie jest spełnione z autentycznością tokenu wysłanego przez drugiego, to poleca on agentowi MCA zamknięcie kanału.

Wyjście zabezpieczeń jest dostarczane zarówno w formacie źródłowym, jak i obiektowym. Kodu źródłowego można użyć jako punktu wyjścia do zapisu własnych programów obsługi wyjścia kanału lub można użyć modułu obiektowego jako dostarczonego. Moduł obiektu ma dwa punkty wejścia, jeden dla uwierzytelniania jednego ze sposobów przy użyciu obsługi uwierzytelniania NTLM, a drugi dla uwierzytelniania dwudrożnego przy użyciu usług uwierzytelniania Kerberos .

Więcej informacji na temat sposobu działania programu obsługi wyjścia kanału SSPI oraz instrukcji implementowania zawiera sekcja Korzystanie z wyjścia zabezpieczeń SSPI w systemach Windows.

Jeśli w systemie Windows zostanie wyświetlony błąd 'group not found' (nie znaleziono grupy)

Ten problem może wystąpić, ponieważ produkt WebSphere MQ utraci dostęp do lokalnej grupy mqm, gdy serwery Windows są awansowane do kontrolerów domeny lub z nich demotowane. Aby rozwiązać ten problem, utwórz ponownie lokalną grupę mqm.

Objaw jest błędem wskazującego na brak lokalnej grupy mqm, na przykład:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

Zmiana stanu komputera między serwerem a kontrolerem domeny może mieć wpływ na działanie produktu WebSphere MQ, ponieważ produkt WebSphere MQ korzysta z lokalnie zdefiniowanej grupy mqm. Gdy serwer jest promowany jako kontroler domeny, zasięg zmienia się z poziomu lokalnego na domenę lokalną. Gdy komputer zostanie zdegradowany do serwera, wszystkie lokalne grupy domeny zostaną usunięte. Oznacza to, że zmiana komputera z serwera na kontroler domeny i z powrotem na serwer utraci dostęp do lokalnej grupy mqm.

Aby zaradzić temu problemowi, należy ponownie utworzyć lokalną grupę mqm przy użyciu standardowych narzędzi zarządzania Windows . Ponieważ wszystkie informacje o członkostwie w grupach są tracone, należy przywrócić uprzywilejowane użytkowników WebSphere MQ w nowo utworzonej lokalnej grupie mqm. Jeśli komputer jest elementem domeny, należy również dodać grupę mqm domeny do lokalnej grupy mqm, aby nadać użytkownikowi uprzywilejowanym identyfikator użytkownika WebSphere MQ , który jest wymagany przez ten poziom uprawnień.

W przypadku problemów z kontrolerami IBM WebSphere MQ i domenami w systemie Windows

Niektóre problemy mogą wystąpić z ustawieniami zabezpieczeń, gdy serwery Windows są awansowane do kontrolerów domeny.

Podczas awansowania serwerów Windows 2000, Windows 2003 lub Windows Server 2008 do kontrolerów domeny użytkownik jest prezentowany z opcją wyboru domyślnego lub innego niż domyślne ustawienia zabezpieczeń odnoszący się do uprawnień użytkownika i grupy. Ta opcja określa, czy dowolne użytkownicy mogą pobierać przypisania do grup z aktywnego katalogu. Ponieważ produkt WebSphere MQ wykorzystuje informacje o przynależności do grup w celu zaimplementowania strategii bezpieczeństwa, ważne jest, aby identyfikator użytkownika wykonujący operacje WebSphere MQ mógł określić przypisania do grup innych użytkowników.

W systemie Windows 2000, gdy domena jest tworzona przy użyciu domyślnej opcji zabezpieczeń, domyślny identyfikator użytkownika utworzony przez produkt WebSphere MQ podczas procesu instalacji może uzyskać członkostwo w grupach dla innych użytkowników, jeśli jest to wymagane. Produkt następnie instaluje się normalnie, tworząc obiekty domyślne, a menedżer kolejek może określić uprawnienia dostępu użytkowników lokalnych i domen, jeśli jest to wymagane.

W systemie Windows 2000, gdy domena jest tworzona przy użyciu opcji zabezpieczeń innej niż domyślna, lub w systemach Windows 2003 i Windows Server 2008, gdy domena jest tworzona przy użyciu opcji zabezpieczeń domyślnych, identyfikator użytkownika utworzony przez produkt WebSphere MQ podczas instalacji nie zawsze może określić wymagane przypisania do grupy. W tym przypadku należy wiedzieć:

- W jaki sposób system Windows 2000 z niedomyślnym lub Windows 2003 i serwerem Windows Server 2008 z domyślnymi uprawnieniami zabezpieczeń zachowuje się
- Jak zezwolić członkom grupy mqm domeny na odczytywanie członkostwa w grupie
- Jak skonfigurować usługę IBM WebSphere MQ Windows w taki sposób, aby była uruchamiana przez użytkownika domeny

Domena Windows 2000 z niedomyślną domeną lub domeną Windows 2003 i Windows Server 2008 z domyślnymi uprawnieniami

Instalacja produktu WebSphere MQ zachowuje się inaczej w tych systemach operacyjnych w zależności od tego, czy instalacja jest wykonywana przez użytkownika lokalnego czy użytkownika domeny.

Jeśli **lokalny** użytkownik zainstaluje produkt WebSphere MQ, kreator przygotowania produktu WebSphere MQ wykryje, że lokalny użytkownik utworzony dla usługi Windows produktu IBM WebSphere MQ może pobrać informacje o przynależności do grupy dla użytkownika instalujący. Kreator przygotowania produktu WebSphere MQ zadaje użytkownikowi pytania dotyczące konfiguracji sieci w celu określenia, czy istnieją inne konta użytkowników zdefiniowane w kontrolerach domeny działających w systemie Windows 2000 lub nowszym. W takim przypadku usługa produktu IBM WebSphere MQ Windows musi działać pod kontem użytkownika domeny z określonymi ustawieniami i uprawnieniami. Kreator przygotowania produktu WebSphere MQ prosi użytkownika o podanie szczegółów konta tego użytkownika. Jego pomoc elektroniczna zawiera szczegółowe informacje na temat wymaganego konta użytkownika domeny, które może zostać wysłane do administratora domeny.

Jeśli użytkownik **domena** zainstaluje produkt WebSphere MQ, kreator przygotowania produktu WebSphere MQ wykryje, że lokalny użytkownik utworzony dla usługi IBM WebSphere MQ Windows nie może pobrać informacji o przynależności do grupy dla użytkownika instalujący. W takim przypadku kreator przygotowania produktu WebSphere MQ zawsze prosi użytkownika o podanie szczegółów konta użytkownika domeny dla usługi IBM WebSphere MQ Windows , która ma być używana.

Jeśli usługa produktu IBM WebSphere MQ Windows musi korzystać z konta użytkownika domeny, produkt WebSphere MQ nie może działać poprawnie, dopóki nie zostanie to skonfigurowane przy użyciu kreatora przygotowania produktu WebSphere MQ . Kreator przygotowania produktu WebSphere MQ nie zezwala użytkownikowi na kontynuowanie pracy z innymi zadaniami, dopóki usługa Windows nie zostanie skonfigurowana z odpowiednim kontem.

Jeśli domena Windows 2000 została skonfigurowana z niedomyślnymi uprawnieniami zabezpieczeń, zwykle rozwiązaniem, aby produkt WebSphere MQ działał poprawnie, jest skonfigurowanie go przy użyciu odpowiedniego konta użytkownika domeny, zgodnie z opisem powyżej.

Więcej informacji na ten temat zawiera sekcja Tworzenie i konfigurowanie kont domeny dla produktu WebSphere MQ .

Konfigurowanie usług IBM WebSphere MQ do uruchamiania w ramach użytkownika domeny w systemie Windows
Użyj kreatora przygotowania IBM WebSphere MQ , aby wprowadzić szczegóły konta użytkownika domeny. Alternatywnie można użyć panelu Zarządzanie komputerem, aby zmienić szczegóły **Logowanie** dla konkretnej instalacji IBM WebSphere MQ Service.

Więcej informacji na ten temat zawiera sekcja Zmiana hasła do konta użytkownika usługi IBM WebSphere MQ Windows

Stosowanie plików szablonów zabezpieczeń w systemie Windows

Zastosowanie szablonu może mieć wpływ na ustawienia zabezpieczeń stosowane w plikach i katalogach produktu WebSphere MQ . Jeśli używany jest szablon wysoce bezpieczny, należy go zastosować przed zainstalowaniem produktu WebSphere MQ.

System Windows obsługuje tekstowe pliki szablonów zabezpieczeń, które mogą być używane do stosowania jednolitych ustawień zabezpieczeń na jednym lub wielu komputerach z przystawką konfiguracji zabezpieczeń i analizy MMC. W szczególności system Windows udostępnia kilka szablonów, które zawierają szereg ustawień zabezpieczeń, których celem jest zapewnienie konkretnych poziomów zabezpieczeń. Szablony te obejmują kompatybilność, bezpieczny i wysoce bezpieczny.

Zastosowanie jednego z tych szablonów może mieć wpływ na ustawienia zabezpieczeń stosowane w plikach i katalogach produktu WebSphere MQ . Aby użyć szablonu o wysokiej wartości Secure, należy skonfigurować komputer przed zainstalowaniem produktu WebSphere MQ.

Jeśli szablon wysoce zabezpieczony zostanie zastosowany do komputera, na którym jest już zainstalowany produkt WebSphere MQ , wszystkie uprawnienia ustawione w plikach i katalogach produktu WebSphere MQ zostaną usunięte. Ponieważ te uprawnienia są usuwane, użytkownik traci dostęp do katalogów *Administrator*, *mqm*oraz, jeśli ma to zastosowanie, do grupy *Wszyscy* w odniesieniu do katalogów błędów.

Zagnieżdżone grupy

Istnieją ograniczenia dotyczące korzystania z grup zagnieżdżonych. Wynik ten częściowo wynika z poziomu funkcjonalnego domeny, a częściowo z ograniczeń produktu WebSphere MQ .

Active Directory może obsługiwać różne typy grup w kontekście domeny w zależności od poziomu funkcjonalnego domeny. Domyślnie domeny Windows 2003 są na poziomie funkcjonalnym *mieszany Windows 2000* . (Serwer Windows 2003, Windows XP, Windows Vista i Windows Server 2008 wszystkie są zgodne z modelem domeny Windows 2003.) Poziom funkcjonalny domeny określa obsługiwane typy grup i poziom zagnieżdżenia dozwolony podczas konfigurowania identyfikatorów użytkowników w środowisku domeny. Zapoznaj się z dokumentacją Active Directory , aby uzyskać szczegółowe informacje na temat zakresu grupy i kryteriów włączania.

Oprócz wymagań dotyczących katalogu Active Directory , obowiązują dalsze ograniczenia dotyczące identyfikatorów używanych przez produkt WebSphere MQ. Sieciowe interfejsy API używane przez produkt WebSphere MQ nie obsługują wszystkich konfiguracji obsługiwanych przez poziom funkcjonalny domeny. W rezultacie produkt WebSphere MQ nie może wysłać zapytania o członkostwo w grupie wszystkich identyfikatorów domen znajdujących się w grupie lokalnej domeny, która jest następnie zagnieżdżona w grupie lokalnej. Ponadto wielokrotne zagnieżdżanie grup globalnych i uniwersalnych nie jest obsługiwane. Jednak obsługiwane są natychmiast zagnieżdżone grupy globalne lub uniwersalne.

Konfigurowanie dodatkowych uprawnień dla aplikacji Windows łączących się z produktem IBM WebSphere MQ

Konto, w ramach którego uruchomione procesy produktu IBM WebSphere MQ może wymagać dodatkowej autoryzacji przed przyznaniem dostępu SYNCHRONIZE do procesów aplikacji, może wymagać dodatkowej autoryzacji.

Problemy mogą wystąpić, jeśli używane są aplikacje Windows , na przykład strony ASP, łączące się z produktem IBM WebSphere MQ , które są skonfigurowane do uruchamiania na poziomie bezpieczeństwa wyższym niż zwykle.

Program IBM WebSphere MQ wymaga ZSYNCHRONIZOWANIA dostępu do procesów aplikacji w celu skoordynowania określonych działań. Poprawka APAR IC35116 została zmieniona IBM WebSphere MQ , tak aby określone zostały odpowiednie uprawnienia. Jednak konto, w ramach którego uruchamiane jest procesy IBM WebSphere MQ , może wymagać dodatkowej autoryzacji, zanim będzie można uzyskać dostęp do żądanego dostępu.

Gdy aplikacja serwera po raz pierwszy próbuje połączyć się z menedżerem kolejek IBM WebSphere MQ , zmodyfikuje proces, aby nadać uprawnienia SYNCHRONIZE administratorom produktu IBM WebSphere MQ . Aby skonfigurować dodatkowe uprawnienia do identyfikatora użytkownika, w ramach którego działają procesy produktu IBM WebSphere MQ , wykonaj następujące kroki:

1. Uruchom narzędzie Zasady zabezpieczeń lokalnych, a następnie kliknij opcję Ustawienia zabezpieczeń-> Zasady lokalne-> Przypisania prawym przyciskiem myszy, a następnie kliknij opcję Debuguj programy.
2. Kliknij dwukrotnie "Debuguj programy", a następnie dodaj identyfikator użytkownika IBM WebSphere MQ do listy.

Jeśli system znajduje się w domenie systemu Windows , a efektywne ustawienie strategii nadal nie jest ustawione, nawet jeśli ustawione jest ustawienie strategii lokalnej, identyfikator użytkownika musi być autoryzowany w taki sam sposób na poziomie domeny, za pomocą narzędzia Strategia bezpieczeństwa domeny.

Konfigurowanie zabezpieczeń w systemie HP Integrity NonStop Server

Zagadnienia dotyczące bezpieczeństwa specyficzne dla systemów HP Integrity NonStop Server .

Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server obsługuje zarówno protokół TLS (Transport Layer Security), jak i protokoły SSL (Secure Sockets Layer) w celu zapewnienia bezpieczeństwa na poziomie łącza podczas nawiązywania połączenia z menedżerem kolejek. Te protokoły są obsługiwane przy użyciu implementacji OpenSSL. OpenSSL wymaga podania źródła danych losowych w celu zapewnienia silnych operacji kryptograficznych.

OpenSSL

Przegląd zabezpieczeń OpenSSL dla klienta IBM WebSphere MQ dla HP Integrity NonStop Server.

Pakiet OpenSSL jest implementacją open source protokołów Secure Sockets Layer (SSL) i Transport Layer Security (TLS) w celu zapewnienia bezpiecznej komunikacji w sieci.

Pakiet jest rozwijany przez projekt OpenSSL Project. Więcej informacji na temat projektu OpenSSL zawiera sekcja https://www.openssl.org. Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server zawiera zmodyfikowane wersje bibliotek OpenSSL i **openssl** . Biblioteki i komenda **openssl** są eksportowane z biblioteki narzędziowej OpenSSL 1.0.1ci są dostarczane tylko jako kod obiektu. Nie podano kodu źródłowego.

Biblioteki OpenSSL są ładowane przez aplikacje klienckie IBM WebSphere MQ dynamicznie zgodnie z wymaganiami. Tylko biblioteki OpenSSL , które są udostępniane przez produkt IBM WebSphere MQ , są obsługiwane w aplikacjach klienckich IBM WebSphere MQ .

Komenda **openssl** , która może być używana do zarządzania certyfikatami, jest instalowana w katalogu OSS `opt_installation_path/opt/mqm/bin`.

Za pomocą komendy **openssl** można tworzyć klucze i certyfikaty cyfrowe oraz zarządzać nimi przy użyciu różnych powszechnie dostępnych formatów danych, a także wykonywać proste zadania ośrodka certyfikacji (CA).

Domyślnym formatem danych klucza i certyfikatu, który jest przetwarzany przez OpenSSL , jest format PEM (Privacy Enhanced Mail). Dane w formacie PEM to dane ASCII kodowane w formacie base64 . Dane mogą być więc przesyłane za pomocą systemów tekstowych, takich jak e-mail, i można je wyciąć i wkleić, korzystając z edytorów tekstu i przeglądarek internetowych. PEM jest standardem internetowym dla opartych na tekstyliach wymian kryptograficznych i jest określony w internetowych RFC 1421, 1422, 1423 i 1424. IBM WebSphere MQ zakłada, że plik z rozszerzeniem `.pem` zawiera dane w formacie PEM. Plik w formacie PEM może zawierać wiele certyfikatów i innych zakodowanych obiektów, a także może zawierać komentarze.

Obsługa SSL produktu IBM WebSphere MQ w innych systemach operacyjnych może wymagać, aby dane kluczy i certyfikatów w plikach były kodowane przy użyciu reguł kodowania wyróżniającego (DER). DER jest zestawem reguł kodowania dotyczących używania notacji ASN.1 w bezpiecznej komunikacji. Dane zakodowane za pomocą DER są danymi binarnymi, a format danych klucza i certyfikatu zakodowany za pomocą DER jest znany również jako PKCS#12 lub PFX. Plik zawierający te dane zwykle ma rozszerzenie `.p12` lub `.pfx`. Komenda **openssl** może zostać przekształta w formacie PEM i PKCS#12 .

demon entropii

OpenSSL wymaga podania źródła danych losowych w celu zapewnienia silnych operacji kryptograficznych. Generowanie liczb losowych to możliwość, która zwykle jest udostępniana przez system operacyjny lub przez cały proces demona. System operacyjny HP Integrity NonStop Server nie udostępnia tej możliwości w systemie operacyjnym.

W przypadku korzystania z obsługi protokołu SSL i TLS dostarczanego z klientem IBM WebSphere MQ dla produktu HP Integrity NonStop Serverproces, który jest nazywany demonem entropii, jest potrzebny do udostępnienia źródła danych losowych. Gdy uruchamiasz kanał klienta, który wymaga protokołu SSL lub TLS, OpenSSL oczekuje, że demon entropii będzie działać i będzie udostępniał swoje usługi na gnieździe w systemie plików OSS w `/etc/egd-pool`.

Demon entropii nie jest udostępniany przez klienta IBM WebSphere MQ dla produktu HP Integrity NonStop Server. Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server jest testowany z następującymi demonami entropii:

- amqjkdm0 (zgodnie z udostępnionym przez serwer IBM WebSphere MQ 5.3)
- `/usr/local/bin/prngd` (wersja 0.9.27, zgodnie z dostarczonym przez HP Integrity NonStop Server Open Source Technical Library)

Konfigurowanie zabezpieczeń klienta MQI produktu IBM WebSphere MQ

Należy wziąć pod uwagę bezpieczeństwo klienta MQI produktu IBM WebSphere MQ , dzięki czemu aplikacje klienckie nie mają nieograniczonego dostępu do zasobów na serwerze.

W przypadku uruchamiania aplikacji klienckiej nie należy uruchamiać aplikacji przy użyciu identyfikatora użytkownika, który ma więcej praw dostępu niż jest to konieczne, na przykład użytkownika w grupie `mqm` lub nawet samego użytkownika `mqm` .

Uruchamiając aplikację jako użytkownik z zbyt dużą liczbę praw dostępu, należy uruchomić ryzyko dostępu aplikacji do części menedżera kolejek i jej zmiany, albo przez przypadek, albo przez złośliwie.

Istnieją dwa aspekty zabezpieczeń między aplikacją kliencką a jej serwerem menedżera kolejek: uwierzytelnianie i kontrola dostępu.

- Uwierzytelnianie może być używane w celu zapewnienia, że aplikacja kliencka, działająca jako konkretna użytkownik, jest tym, kim się mówi. Za pomocą uwierzytelniania można uniemożliwić atakującemu uzyskanie dostępu do menedżera kolejek poprzez podszywanie się do jednej z aplikacji.

  W przypadku protokołu SSL lub TLS należy użyć uwierzytelniania wzajemnego. Więcej informacji na ten temat zawiera sekcja “Praca z protokołem SSL lub TLS” na stronie 114

- Kontroli dostępu można użyć do nadania lub usunięcia praw dostępu dla konkretnego użytkownika lub grupy użytkowników. Uruchamiając aplikację kliencką z specjalnie utworzonym użytkownikiem (lub użytkownikiem w konkretnej grupie), można użyć elementów kontroli dostępu, aby upewnić się, że aplikacja nie może uzyskać dostępu do części menedżera kolejek, do których aplikacja nie powinna.

  Podczas konfigurowania kontroli dostępu należy wziąć pod uwagę reguły uwierzytelniania kanału oraz pole MCAUSER w kanale. Obie te funkcje mają możliwość zmiany identyfikatora użytkownika, który jest używany do weryfikowania praw kontroli dostępu.

  Aby uzyskać więcej informacji na temat kontroli dostępu, patrz "Autoryzowanie dostępu do obiektów" na stronie 165.

Jeśli aplikacja kliencka została utworzona w celu nawiązania połączenia z konkretnym kanałem o ograniczonym identyfikatorze, ale w polu MCAUSER kanału ma ustawiony identyfikator administratora, to pod warunkiem, że aplikacja kliencka łączy się pomyślnie, to identyfikator administratora jest używany do sprawdzania kontroli dostępu. Oznacza to, że aplikacja kliencka będzie miała pełne prawa dostępu do menedżera kolejek.

Więcej informacji na temat atrybutu MCAUSER znajduje się w sekcji "Odwzorowywanie identyfikatora użytkownika potwierdzonego przez klienta na identyfikator użytkownika MCAUSER" na stronie 191.

Reguły uwierzytelniania kanału mogą być również używane jako metoda kontroli dostępu do menedżera kolejek, poprzez ustawienie konkretnych reguł i kryteriów dla połączenia, które ma zostać zaakceptowane.

Więcej informacji na temat reguł uwierzytelniania kanału zawiera sekcja "Rekordy uwierzytelniania kanału" na stronie 41.

Określanie, że w czasie wykonywania w kliencie MQI są używane tylko specyfikacje CipherSpecs z certyfikatem FIPS

Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi korzystać z certyfikatów CipherSpecsz certyfikatem FIPS.

Aby w czasie wykonywania był zgodny ze standardem FIPS, konieczne jest utworzenie repozytoriów kluczy i zarządzanie nim przy użyciu oprogramowania zgodnego ze standardem FIPS, takiego jak runmqakm z opcją -fips.

Użytkownik może określić, że kanał SSL lub TLS musi używać tylko certyfikatów CipherSpecs z certyfikatem FIPS na trzy sposoby, wymienionych w kolejności wykonywania następujących czynności:

1. Ustaw pole FipsRequired w strukturze MQSCO na MQSSL_FIPS_YES.
2. Ustaw zmienną środowiskową MQSSLFIPS na YES.
3. Ustaw atrybut SSLFipsRequired w pliku konfiguracyjnym klienta na YES.

Domyślnie opcja CipherSpecs z certyfikatem FIPS nie jest wymagana.

Wartości te mają takie same znaczenia, jak równoważne wartości parametrów w instrukcji ALTER QMGR SSLFIPS (patrz ALTER QMGR). Jeśli proces klienta aktualnie nie ma aktywnych połączeń SSL lub TLS, a wartość FipsRequired jest poprawnie określona w przypadku protokołu SSL MQCONNX, wszystkie kolejne połączenia SSL powiązane z tym procesem muszą używać tylko tych specyfikacji CipherSpecs powiązanych z tą wartością. Ma to zastosowanie do czasu, aż zostaną zatrzymane wszystkie połączenia SSL lub TLS. W tym momencie kolejny element MQCONNX może udostępnić nową wartość dla parametru FipsRequired.

Jeśli sprzęt szyfrujący jest obecny, moduły kryptograficzne używane przez produkt WebSphere MQ można skonfigurować w taki sposób, aby były modułami udostępnianymi przez produkt sprzętowy. Może to być zgodne ze standardem FIPS dla określonego poziomu. Konfigurowalne moduły i ich zgodność ze standardem FIPS zależą od produktu sprzętowego.

Jeśli to możliwe, jeśli skonfigurowano tylko standard FIPS (CipherSpecs), klient MQI odrzuca połączenia, które określają atrybut CipherSpec inny niż FIPS przy użyciu parametru MQRC_SSL_INITIALIZATION_ERROR. Produkt WebSphere MQ nie gwarantuje odrzucania wszystkich

takich połączeń i jest odpowiedzialny za określenie, czy konfiguracja produktu WebSphere MQ jest zgodna ze standardem FIPS.

Pojęcia pokrewne

“FIPS (Federal Information Processing Standards) dla systemów UNIX, Linuxi Windows” na stronie 27
Jeśli szyfrowanie jest wymagane w kanale SSL lub TLS w systemach Windowsi UNIX and Linux , produkt WebSphere MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach Windowsi UNIX and Linux oprogramowanie ICC przeszło program sprawdzania poprawności Cryptomodule FIPS (Federal Information Processing Standards) w Instytucie Standardów i Technologii Stanów Zjednoczonych (poziom 140-2).

Sekcja SSL pliku konfiguracyjnego klienta

Odsyłacze pokrewne

FipsRequired (MQLONG)

MQSSLFIPS

Uruchamianie aplikacji klienckich SSL lub TLS z wieloma instalacjami pakietu GSKit V8.0 w systemie AIX

Aplikacje klienckie SSL lub TLS na serwerze AIX mogą doświadczyć MQRC_CHANNEL_CONFIG_ERROR i błędów AMQ6175 podczas pracy w systemach AIX z wieloma instalacjami pakietu GSKit V8.0 .

Podczas uruchamiania aplikacji klienckich w systemie AIX z wieloma instalacjami pakietu GSKit V8.0 wywołania połączenia klienta mogą zwracać wartość MQRC_CHANNEL_CONFIG_ERROR , gdy używany jest protokół SSL lub TLS. /var/mqm/errors rejestruje błędy AMQ6175 i AMQ9220 dla niesprawnej aplikacji klienckiej, na przykład:

```
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
                    Host(machine.example.ibm.com) Installation(Installation1)
                    VRMF(7.1.0.0)
AMQ6175: The system could not dynamically load the shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so'. The system returned
error number '8' and error message 'Symbol resolution failed
for /usr/mqm/gskit8/lib64/libgsk8ssl_64.so because:
    Symbol VALUE_EC_NamedCurve_secp256r1__9GSKASNOID (number 16) is not
exported from dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
    Symbol VALUE_EC_NamedCurve_secp384r1__9GSKASNOID (number 17) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
    Symbol VALUE_EC_NamedCurve_secp521r1__9GSKASNOID (number 18) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
    Symbol VALUE_EC_ecPublicKey__9GSKASNOID (number 19) is not exported from dependent
module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
    Symbol VALUE_EC_ecdsa_with_SHA1__9GSKASNOID (number 20) is not exported from
dependent module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.
    Symbol VALUE_EC_ecdsa__9GSKASNOID (number 21) is not exported from dependent
      module /db2data/db2inst1/sqllib/lib64/libgsk8cms_64.so.'.

EXPLANATION:
This message applies to AIX systems. The shared library
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed
to load correctly due to a problem with the library.
ACTION:
Check the file access permissions and that the file has not been corrupted.
----- amqxufnx.c : 1284 ---------------------------------------------------------
09/08/11 11:16:13 - Process(24412.1) User(user) Program(example)
                    Host(machine.example.ibm.com) Installation(Installation1)
                    VRMF(7.1.0.0)
AMQ9220: The GSKit communications program could not be loaded.

EXPLANATION:
The attempt to load the GSKit library or procedure
'/usr/mqm/gskit8/lib64/libgsk8ssl_64.so' failed with error code
536895861.
ACTION:
Either the library must be installed on the system or the environment changed
to allow the program to locate it.
----- amqcgska.c : 836 ----------------------------------------------------------
```

Częstą przyczyną tego błędu jest to, że ustawienie zmiennej środowiskowej LIBPATH lub LD_LIBRARY_PATH spowodowało, że klient IBM WebSphere MQ załadował mieszany zestaw bibliotek

z dwóch różnych instalacji pakietu GSKit V8.0 . Ten błąd może być przyczyną wykonywania aplikacji klienckiej produktuIBM WebSphere MQ w środowisku Db2 .

Aby uniknąć tego błędu, należy dołączyć katalogi bibliotek produktu IBM WebSphere MQ z przodu ścieżki do biblioteki, aby mieć pierwszeństwo przed bibliotekami produktu IBM WebSphere MQ . Można to osiągnąć za pomocą komendy **setmqenv** z parametrem **-k** , na przykład:

```
. /usr/mqm/bin/setmqenv -s -k
```

Więcej informacji na temat korzystania z komendy **setmqenv** można znaleźć w sekcji setmqenv (ustawienie środowiska WebSphere MQ)

Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemach UNIX, Linux, and Windows

Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację protokołu SSL lub TLS, należy zdefiniować kanały w celu użycia protokołu SSL lub TLS. Należy także utworzyć certyfikaty cyfrowe i zarządzać nimi. W systemach UNIX, Linux i Windows można wykonać testy z samopodpisanymi certyfikatami.

Certyfikat samopodpisany nie może zostać odwołany, co może pozwolić atakującemu na łyżkę tożsamości po skompromitywaniu klucza prywatnego. CAs może odwołać skompromiowany certyfikat, co uniemożliwia jego dalsze korzystanie. Certyfikaty podpisane przez ośrodek CA są więc bezpieczniejsze w środowisku produkcyjnym, chociaż samopodpisane certyfikaty są wygodniejsze dla systemu testowego.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows” na stronie 118.

W tej kolekcji tematów przedstawiono niektóre zadania związane z konfiguroniem komunikacji SSL oraz szczegółowe informacje na temat wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalną częścią protokołów. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji IBM WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemach UNIX, Linux i Windows klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie IBM WebSphere MQ :

- W przypadku menedżera kolejek format to `ibmwebspheremq` , po którym następuje zmiana nazwy menedżera kolejek na małe litery. Na przykład: `QM1`, `ibmwebspheremqqm1`
- W przypadku klienta IBM WebSphere MQ `ibmwebspheremq` , po którym następuje zmiana identyfikatora użytkownika na małe litery, na przykład `ibmwebspheremqmyuserid`.

Produkt IBM WebSphere MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się tylko wtedy, gdy kanał działający jako serwer SSL lub TLS jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER. Więcej informacji na ten temat zawiera sekcja “Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS” na stronie 214.

Praca z protokołem SSL lub TLS

W tych tematach znajdują się instrukcje dotyczące wykonywania pojedynczych zadań związanych z używaniem protokołu SSL lub TLS z produktem IBM WebSphere MQ.

Wiele z nich jest używanych jako kroki w zadaniach wyższego poziomu opisanych w następujących sekcjach:

- “Identyfikowanie i uwierzytelnianie użytkowników” na stronie 149
- “Autoryzowanie dostępu do obiektów” na stronie 165
- “Poufność komunikatów” na stronie 213
- “Integralność danych komunikatów” na stronie 235
- “Zabezpieczanie klastrów” na stronie 253

Praca z protokołem SSL lub TLS w systemie HP Integrity NonStop Server

Opisuje implementację zabezpieczeń klienta IBM WebSphere MQ dla produktu HP Integrity NonStop Server OpenSSL , w tym usługi zabezpieczeń, komponenty, obsługiwane wersje protokołów, obsługiwane specyfikacje CipherSpecsoraz nieobsługiwane funkcje zabezpieczeń.

IBM WebSphere MQ Obsługa protokołu SSL i TLS udostępnia następujące usługi zabezpieczeń dla kanałów klienta:

- Uwierzytelnianie serwera i, opcjonalnie, uwierzytelnianie klienta.
- Szyfrowanie i deszyfrowanie danych, które przepływają przez kanał.
- Integralność sprawdza dane, które przepływają przez kanał.

Obsługa protokołu SSL i TLS dostarczana z klientem IBM WebSphere MQ dla produktu HP Integrity NonStop Server składa się z następujących komponentów:

- Biblioteki OpenSSL i komendy **openssl** .
- IBM WebSphere MQ , komenda stash, **amqrsslc**.

Następujące wymagane komponenty dla operacji kanału klienta SSL lub TLS nie są dostarczane z klientem IBM WebSphere MQ dla produktu HP Integrity NonStop Server:

- Demon entropii w celu udostępnienia źródła danych losowych dla kryptografii OpenSSL .

Obsługiwane wersje protokołów

Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server obsługuje następujące wersje protokołów:

- SSL 3.0
- TLS 1.0
- TLS 1.2

Obsługiwane CipherSpecs

Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server obsługuje następujące wersje produktu CipherSpecs :

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- RC4_SHA_US
- RC4_MD5_US
- TRIPLE_DES_SHA_US
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (nieaktualne)
- DES_SHA_EXPORT1024
- RC4_56_SHA_EXPORT1024
- RC4_MD5_EXPORT

- RC2_MD5_EXPORT
- DES_SHA_EXPORT
- TLS_RSA_WITH_DES_CBC_SHA
- NULL_SHA
- NULL_MD5
- FIPS_WITH_DES_CBC_SHA
- FIPS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384

Nieobsługiwana funkcjonalność zabezpieczeń

Klient IBM WebSphere MQ dla HP Integrity NonStop Server nie obsługuje obecnie:

- Obsługa sprzętu szyfrującego PKCS#11
- Sprawdzanie listy odwołań certyfikatów LDAP
- Sprawdzanie protokołu OCSP Online Certificate Status Protocol
- Elementy sterujące szyfru FIPS 140-2, NSA SUITE B

Zarządzanie certyfikatami

Użyj zestawu plików do przechowywania informacji o unieważnieniu certyfikatu cyfrowego i certyfikatu.

IBM WebSphere MQ Obsługa protokołu SSL i TLS korzysta z zestawu plików do przechowywania informacji o cofnięciu certyfikatu cyfrowego i certyfikatu. Pliki te znajdują się w katalogu określonym programowo za pomocą pola KeyRepository w strukturze MQSCO przekazanej w wywołaniu MQCONNX, przez zmienną środowiskową *MQSSLKEYR* lub w sekcji SSL produktu `mqclient.ini` przy użyciu atrybutu SSLKeyRepository .

Struktura MQSCO ma pierwszeństwo przed zmienną środowiskową MQSSLKEYR, która ma pierwszeństwo przed wartością sekcji pliku ini.

Ważne: Położenie repozytorium kluczy określa położenie katalogu, a nie nazwę pliku na platformie HP Integrity NonStop Server .

Klient IBM WebSphere MQ dla produktu HP Integrity NonStop Server używa następujących plików, w których rozróżniana jest wielkość liter, o nazwach plików w repozytorium kluczy:

- “Osobista baza certyfikatów” na stronie 117
- “Magazyn zaufanych certyfikatów” na stronie 117
- “Przekaż frazę pliku ukrytych haseł” na stronie 117
- “Plik listy odwołań certyfikatów” na stronie 117

Osobista baza certyfikatów
Plik bazy certyfikatów osobistych `cert.pem`.

Ten plik zawiera certyfikat osobisty i zaszyfrowany klucz prywatny dla klienta, który ma być używany w formacie PEM. Istnienie tego pliku jest opcjonalne, gdy używane są kanały SSL lub TLS, które nie wymagają uwierzytelniania klienta. Jeśli uwierzytelnianie klienta jest wymagane przez kanał, a w definicji kanału określono SSLCAUTH (REQUIRED), plik ten musi istnieć i musi zawierać zarówno certyfikat, jak i zaszyfrowany klucz prywatny.

Uprawnienia do plików muszą być ustawione w tym pliku, aby umożliwić dostęp do odczytu właścicielowi bazy certyfikatów.

Poprawnie sformatowany plik `cert.pem` musi zawierać dokładnie dwie sekcje z następującymi nagłówkami i stopkami:

```
-----BEGIN PRIVATE KEY-----
Base 64 ASCII encoded private key data here
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

Fraza hasła dla zaszyfrowanego klucza prywatnego jest przechowywana w pliku ukrytych haseł, `Stash.sth`.

Magazyn zaufanych certyfikatów
Plik zaufanych certyfikatów bazy danych `trust.pem`.

Ten plik zawiera certyfikaty, które są wymagane do sprawdzenia poprawności certyfikatów osobistych używanych przez menedżery kolejek, z którymi klient nawiązuje połączenie, w formacie PEM. Magazyn zaufanych certyfikatów jest obowiązkowy dla wszystkich kanałów klienta SSL lub TLS.

Uprawnienia do pliku muszą być ustawione w taki sposób, aby ograniczał dostęp do zapisu do tego pliku.

Poprawnie sformatowany plik `trust.pem` musi zawierać jedną lub więcej sekcji z następującymi nagłówkami i stopkami:

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

Przekaż frazę pliku ukrytych haseł
Plik ukrytych haseł, `Stash.sth`.

Ten plik jest formatem binarnym prywatnym dla programu IBM WebSphere MQ i zawiera zaszyfrowaną frazę hasła do użycia podczas uzyskiwania dostępu do klucza prywatnego znajdującego się w pliku `cert.pem` . Sam klucz prywatny jest przechowywany w bazie certyfikatów produktu `cert.pem` .

Plik ten jest tworzony lub modyfikowany za pomocą narzędzia wiersza komend IBM WebSphere MQ **amqrsslc** z parametrem **-s** . Na przykład, jeśli katalog `/home/alice` zawiera plik `cert.pem` :

```
amqrsslc -s /home/alice/cert

  Enter password for Keystore /home/alice/cert.pem :
    password

  Stashed the password in file /home/alice/Stash.sth
```

Uprawnienia do plików muszą być ustawione w tym pliku, aby umożliwić dostęp do odczytu właścicielowi powiązanej bazy certyfikatów osobistych.

Plik listy odwołań certyfikatów
Plik listy odwołań certyfikatów (`crl.pem`).

Ten plik zawiera listy odwołań certyfikatów (CRL) używane przez klienta do sprawdzania poprawności certyfikatów cyfrowych w formacie PEM. Istnienie tego pliku jest opcjonalne. Jeśli ten plik nie jest obecny, podczas sprawdzania poprawności certyfikatów nie są wykonywane żadne sprawdzenia odwołań certyfikatów.

Uprawnienia do pliku muszą być ustawione w taki sposób, aby ograniczał dostęp do zapisu do tego pliku.

Poprawnie sformatowany plik `crl.pem` musi zawierać jedną lub więcej sekcji z następującymi nagłówkami i stopkami:

```
-----BEGIN X509 CRL-----
Base 64 ASCII encoded CRL data here
-----END X509 CRL-----
```

Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows

W systemach UNIX, Linux i Windows obsługa protokołu SSL (Secure Sockets Layer) jest instalowana wraz z produktem IBM WebSphere MQ.

Więcej szczegółowych informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja Sprawdzanie poprawności certyfikatu i projekt strategii zaufania.

Korzystanie z komendy iKeyman, iKeycmd, runmqakm i runmqckm

W systemach UNIX, Linux i Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą interfejsu GUI programu iKeyman lub z poziomu wiersza komend za pomocą komendy iKeycmd lub runmqakm.

- W systemach **UNIX and Linux** :
  - Aby uruchomić interfejs GUI programu iKeyman , należy użyć komendy **strmqikm** .
  - Komenda **runmqckm** służy do wykonywania zadań za pomocą interfejsu wiersza komend iKeycmd .
  - Komenda **runmqakm** służy do wykonywania zadań za pomocą interfejsu wiersza komend runmqakm. Składnia komendy dla **runmqakm** jest taka sama, jak składnia komendy **runmqckm**.

    Jeśli konieczne jest zarządzanie certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend **runmqckm** lub **strmqikm** .

  W sekcji Zarządzanie kluczami i certyfikatami znajduje się pełny opis interfejsów wiersza komend dla komend **runmqckm** i **runmqakm** .

  Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że iKeycmd i iKeyman są programami 64-bitowymi. Moduły zewnętrzne wymagane do obsługi standardu PKCS #11 zostaną załadowane do procesu 64-bitowego. W związku z tym wymagane jest zainstalowanie 64-bitowej biblioteki PKCS #11 na potrzeby administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ programy iKeyman i iKeycmd są 32-bitowe na tych platformach.

  W przypadku następujących platform, w których środowisko JRE było 32-bitowe we wcześniejszych wersjach produktu, ale jest 64-bitowe tylko w produkcie IBM WebSphere MQ Version 7.5, może być konieczne zainstalowanie dodatkowych sterowników PKCS#11 odpowiednich dla trybu adresowania środowiska JRE **iKeyman** i **iKeycmd** . Jest to spowodowane tym, że sterownik PKCS#11 musi używać tego samego trybu adresowania co środowisko JRE. W poniższej tabeli przedstawiono tryby adresowania środowiska JRE produktu IBM WebSphere MQ Version 7.5 .

Tabela 12. IBM WebSphere MQ Version 7.5 tryby adresowania środowiska JRE

Platforma	**Tryb adresowania JRE**
Windows (wersja 32-bitowa lub 64-bitowa)	32
Linux dla 32-bitowego systemu System x	32
Linux dla 64-bitowego systemu System x	64
Linux dla System p	64

Tabela 12. IBM WebSphere MQ Version 7.5 tryby adresowania środowiska JRE (kontynuacja)	
Platforma	**Tryb adresowania JRE**
Linux dla System z	64
HP-UX	64
Solaris Sparc	64
Solaris x86-64	64
AIX	64

Przed uruchomieniem komendy **strmqikm** w celu uruchomienia interfejsu GUI programu iKeyman upewnij się, że pracujesz na komputerze, który jest w stanie uruchomić system X Window System, i wykonaj następujące czynności:

– Ustaw zmienną środowiskową DISPLAY, na przykład:

```
export DISPLAY=mypc:0
```

– Upewnij się, że zmienna środowiskowa PATH zawiera **/usr/bin** i **/bin**. Jest to również wymagane w przypadku komend **runmqckm** i **runmqakm** . Na przykład:

```
export PATH=$PATH:/usr/bin:/bin
```

- W systemach **Windows** :
  – Aby uruchomić interfejs GUI programu iKeyman , należy użyć komendy **strmqikm** .
  – Komenda **runmqckm** służy do wykonywania zadań za pomocą interfejsu wiersza komend iKeycmd .

    Jeśli konieczne jest zarządzanie certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend **runmqckm** lub **strmqikm** .

Aby zażądać śledzenia SSL w systemach UNIX, Linux lub Windows , patrz strmqtrc.

Odsyłacze pokrewne
Komendy runmqckm i runmqakm

Konfigurowanie repozytorium kluczy w systemach UNIX, Linux, and Windows

Repozytorium kluczy można skonfigurować za pomocą interfejsu użytkownika iKeyman lub za pomocą komend **iKeycmd** lub **runmqakm** .

O tym zadaniu

Połączenie SSL lub TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek produktu IBM WebSphere MQ i produkt IBM WebSphere MQ MQI client muszą mieć dostęp do repozytorium kluczy. Więcej informacji na ten temat zawiera sekcja “Repozytorium kluczy SSL lub TLS” na stronie 24.

W systemach UNIX, Linux, and Windows certyfikaty cyfrowe są przechowywane w pliku bazy danych kluczy, który jest zarządzany za pomocą interfejsu użytkownika **iKeyman** , lub za pomocą komend **iKeycmd** lub **runmqakm** . Te certyfikaty cyfrowe mają etykiety. Konkretna etykieta wiąże certyfikat osobisty z menedżerem kolejek lub IBM WebSphere MQ MQI client. Protokół SSL i TLS używają tego certyfikatu do celów uwierzytelniania. W systemach UNIX, Linux, and Windows produkt IBM WebSphere MQ używa `ibmwebspheremq` jako przedrostka etykiety, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Po przedrostku następuje nazwa menedżera kolejek lub identyfikator logowania użytkownika IBM WebSphere MQ MQI client , który został zmieniony na małe litery. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Nazwa pliku bazy danych kluczy składa się ze ścieżki i nazwy macierzystej:

- W systemach UNIX and Linux domyślną ścieżką dla menedżera kolejek (ustawionym podczas tworzenia menedżera kolejek) jest `/var/mqm/qmgrs/<queue_manager_name>/ssl`.

  W systemach Windows domyślna ścieżka to *MQ_INSTALLATION_PATH*`\Qmgrs\`*queue_manager_name*`\ssl`, gdzie *MQ_INSTALLATION_PATH* to katalog, w którym zainstalowano produkt IBM WebSphere MQ . Na przykład: `C:\program files\IBM\WebSphere MQ\Qmgrs\QM1\ssl`.

  Domyślna nazwa rdzenia to `key`. Opcjonalnie można wybrać własną ścieżkę i nazwę macierzystą, ale rozszerzenie musi mieć wartość `.kdb`.

  Jeśli wybierzesz własną ścieżkę lub nazwę pliku, ustaw uprawnienia dostępu do pliku, aby ściśle kontrolować dostęp do niego.
- W przypadku klienta WebSphere MQ nie ma domyślnej ścieżki ani nazwy macierzystej. Ściśle kontroluje dostęp do tego pliku. Rozszerzenie musi mieć wartość `.kdb`.

Nie należy tworzyć repozytoriów kluczy w systemie plików, który nie obsługuje blokad na poziomie plików, na przykład systemu NFS w wersji 2 w systemach Linux .

Więcej informacji na temat sprawdzania i określania nazwy pliku bazy danych kluczy zawiera sekcja “Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemach UNIX, Linux lub Windows” na stronie 124 . Nazwę pliku bazy danych kluczy można określić przed utworzeniem pliku bazy danych kluczy lub po jego utworzeniu.

ID użytkownika, z którego uruchamiana jest komenda **iKeyman** lub **iKeycmd** , musi mieć uprawnienia do zapisu w katalogu, w którym jest tworzony lub aktualizowany plik bazy danych kluczy. W przypadku menedżera kolejek, który używa domyślnego katalogu `ssl` , ID użytkownika, z którego uruchamiany jest produkt **iKeyman** lub **iKeycmd** , musi być członkiem grupy mqm. W przypadku IBM WebSphere MQ MQI client, jeśli produkt **iKeyman** lub **iKeycmd** jest uruchamiany z ID użytkownika innego niż ten, w którym działa klient, należy zmienić uprawnienia dostępu do pliku, aby umożliwić IBM WebSphere MQ MQI client uzyskanie dostępu do pliku bazy danych kluczy w czasie wykonywania. Aby uzyskać więcej informacji, patrz “Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemie Windows” na stronie 122 lub “Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemach UNIX and Linux” na stronie 122.

W produkcie **iKeyman** lub **iKeycmd** w wersji 7.0nowe kluczowe bazy danych są automatycznie zapełniane zestawem wstępnie zdefiniowanych certyfikatów ośrodka certyfikacji (CA). W produkcie **iKeyman** lub **iKeycmd** w wersji 8.0bazy danych kluczy nie są zapełniane automatycznie, co powoduje, że konfiguracja początkowa jest bardziej bezpieczna, ponieważ w pliku bazy danych kluczy są uwzględniane tylko te certyfikaty ośrodków CA.

Uwaga: Ze względu na tę zmianę w działaniu pakietu GSKit w wersji 8.0 , która powoduje, że certyfikaty ośrodka CA nie są już automatycznie dodawane do repozytorium, należy ręcznie dodać preferowane certyfikaty ośrodka CA. Ta zmiana sposobu działania umożliwia bardziej szczegółową kontrolę używanych certyfikatów CA. Więcej informacji zawiera sekcja “Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy w systemach UNIX, Linux, and Windows z pakietem GSKit w wersji 8.0” na stronie 123.

Bazę danych kluczy tworzy się za pomocą wiersza komend lub za pomocą interfejsu użytkownika programu **strmqikm** (iKeyman).

Uwaga: Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny z FIPS-em, należy użyć komendy **runmqakm** . Interfejs użytkownika produktu **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS.

Procedura

Utwórz bazę danych kluczy, korzystając z wiersza komend.

1. Uruchom jedną z następujących komend:

- W systemach UNIX, Linux, and Windows :

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- Za pomocą komendy runmqakm:

```
runmqakm -keydb -create -db filename -pw password -type cms
    -stash -fips -strong
```

gdzie:

-db *nazwa_pliku*
Określa pełną nazwę pliku bazy danych kluczy CMS i musi mieć rozszerzenie pliku `.kdb`.

-pw *hasło*
Określa hasło do bazy danych kluczy CMS.

-type *cms*
Określa typ bazy danych. (Dla produktu IBM WebSphere MQmusi to być wartość `cms`.)

-stash
Zapisuje hasło bazy danych kluczy w pliku.

-fips
Wyłącza korzystanie z biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Gdy w trybie FIPS komponent ICC używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

-silne
Sprawdza, czy wprowadzone hasło spełnia minimalne wymagania dotyczące siły hasła. Minimalne wymagania dotyczące hasła są następujące:

- Hasło musi mieć długość co najmniej 14 znaków.
- Hasło musi zawierać co najmniej jedno małe litery, jedną wielką literę oraz jedną cyfrę lub znak specjalny. Do znaków specjalnych należą: gwiazdka (*), znak dolara ($), znak liczby (#) i znak procentu (%). Spacja jest sklasyfikowana jako znak specjalny.
- Każdy znak może występować maksymalnie trzykrotnie w haśle.
- Maksymalnie dwa kolejne znaki w haśle mogą być identyczne.
- Wszystkie znaki znajdują się w standardowym zestawie znaków ASCII, ustawionym w zakresie od 0x20 do 0x7E.

Alternatywnie można utworzyć bazę danych kluczy za pomocą interfejsu użytkownika programu **strmqikm** (iKeyman).

2. W systemach UNIX and Linux zaloguj się jako użytkownik root. W systemach Windows zaloguj się jako administrator lub jako członek grupy MQM.
3. Uruchom interfejs użytkownika iKeyman , uruchamiając komendę **strmqikm** .
4. W menu **Plik bazy danych kluczy** kliknij opcję **Nowy**.

   Zostanie otwarte okno Nowe.
5. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
6. W polu **File Name** (Nazwa pliku) wpisz nazwę pliku.

   To pole zawiera już tekst `key.kdb`. Jeśli nazwą rdzenia jest `key`, pozostaw to pole bez zmian. Jeśli określiłeś inną nazwę rdzenia, zastąp `key` nazwą macierzystą. Nie należy jednak zmieniać rozszerzenia `.kdb` .
7. W polu **Położenie** wpisz ścieżkę.

   Na przykład:

   - W przypadku menedżera kolejek: `/var/mqm/qmgrs/QM1/ssl` (w systemach UNIX and Linux) lub `C:\Program Files\IBM\WebSphere MQ\qmgrs\QM1\ssl` (w systemach Windows).

Ścieżka musi być zgodna z wartością atrybutu **SSLKeyRepository** menedżera kolejek.

- W przypadku klienta IBM WebSphere MQ : `/var/mqm/ssl` (w systemach UNIX and Linux) lub `C:\mqm\ssl` (w systemach Windows).

8. Kliknij przycisk **Otwórz**.

   Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
9. Wpisz hasło w polu **Hasło** i wpisz je ponownie w polu **Potwierdź hasło** .
10. Zaznacz pole wyboru **Stash the password to a file** (Stash hasło do pliku).

    Uwaga: Jeśli hasło nie zostanie zeskładowane, próby uruchomienia kanałów SSL lub TLS nie powiodą się, ponieważ nie mogą uzyskać hasła wymaganego do uzyskania dostępu do pliku bazy danych kluczy.
11. Kliknij przycisk **OK**.

    Zostanie otwarte okno Certyfikaty osobiste.
12. Ustaw uprawnienia dostępu zgodnie z opisem w sekcji “Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemie Windows” na stronie 122 lub “Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemach UNIX and Linux” na stronie 122.

Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemie Windows
Pliki bazy danych kluczy mogą nie mieć odpowiednich uprawnień dostępu. Należy ustawić odpowiedni dostęp do tych plików.

Ustaw kontrolę dostępu do plików *key*.kdb, *key*.sth, *key*.crli *key*.rdb, gdzie *klucz* jest nazwą macierzystą bazy danych kluczy, aby nadać uprawnienie do ograniczonego zbioru użytkowników.

Rozważ nadanie praw dostępu w następujący sposób:

pełne uprawnienia
BUILTIN\Administrators, NT AUTHORITY\SYSTEM oraz użytkownik, który utworzył pliki bazy danych.

uprawnienie do odczytu
W przypadku menedżera kolejek tylko lokalna grupa mqm. W związku z tym założono, że agent MCA działa pod identyfikatorem użytkownika w grupie mqm.

W przypadku klienta identyfikator użytkownika, pod którym uruchomiony jest proces klienta.

Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemach UNIX and Linux
Pliki bazy danych kluczy mogą nie mieć odpowiednich uprawnień dostępu. Należy ustawić odpowiedni dostęp do tych plików.

W przypadku menedżera kolejek należy ustawić uprawnienia do plików bazy danych kluczy, tak aby menedżer kolejek i procesy kanału mogły je odczytywać, gdy jest to konieczne, ale inni użytkownicy nie mogą ich odczytywać ani modyfikować. Zwykle użytkownik mqm musi mieć uprawnienia do odczytu. Jeśli plik bazy danych kluczy został utworzony przez zalogowanie się jako użytkownik mqm, to uprawnienia są prawdopodobnie wystarczające. Jeśli użytkownik nie jest użytkownikiem mqm, ale inny użytkownik w grupie mqm, prawdopodobnie konieczne jest nadanie uprawnień do odczytu innym użytkownikom w grupie mqm.

Podobnie w przypadku klienta należy ustawić uprawnienia do plików bazy danych kluczy, tak aby procesy aplikacji klienta mogły odczytywać je w razie potrzeby, ale inni użytkownicy nie mogą ich odczytywać ani modyfikować. Zwykle użytkownik, pod którym uruchamiany jest proces klienta, wymaga uprawnień do odczytu. Jeśli plik bazy danych kluczy został utworzony przez zalogowanie się jako ten użytkownik, to uprawnienia są prawdopodobnie wystarczające. Jeśli użytkownik nie był użytkownikiem procesu klienta, ale inny użytkownik w tej grupie, prawdopodobnie musi nadać uprawnienia do odczytu innym użytkownikom w grupie.

Ustaw uprawnienia dla plików *key*.kdb, *key*.sth, *key*.crli *key*.rdb, gdzie *klucz* jest nazwą macierzystą bazy danych kluczy, do odczytu i zapisu dla właściciela pliku, oraz do odczytu dla grupy użytkowników mqm lub klienta (-rw-r -----).

Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy w systemach UNIX, Linux, and Windows z pakietem GSKit w wersji 8.0
Wykonaj tę procedurę, aby dodać jeden lub więcej domyślnych certyfikatów CA do pustego repozytorium kluczy z pakietem GSKit w wersji 8.

W pakiecie GSKit w wersji 7.0zachowanie podczas tworzenia nowego repozytorium kluczy miało być automatycznie dodawane w zestawie domyślnych certyfikatów CA dla powszechnie używanych ośrodków certyfikacji. W przypadku pakietu GSKit 8 to zachowanie zostało zmienione w taki sposób, że certyfikaty ośrodka CA nie są już automatycznie dodawane do repozytorium. Użytkownik jest teraz wymagany do ręcznego dodawania certyfikatów CA do repozytorium kluczy.

Korzystanie z programu narzędziowego iKeyman

Na komputerze, na którym chcesz dodać certyfikat CA, wykonaj następujące kroki:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** (w systemach UNIX, Linux i Windows).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy zostanie wyświetlona w polu **File Name** (Nazwa pliku).
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Signer Certificates** (Certyfikaty osoby podpisującej).
9. Kliknij opcję **Zapełnij**. Zostanie otwarte okno Dodaj certyfikat ośrodka CA.
10. Certyfikaty ośrodka CA, które są dostępne do dodania do repozytorium, są wyświetlane w hierarchicznej strukturze drzewa. Wybierz pozycję najwyższego poziomu dla organizacji, której certyfikaty CA mają być zaufane, aby wyświetlić pełną listę poprawnych certyfikatów ośrodka CA.
11. Wybierz z listy certyfikaty ośrodka CA, które chcesz ufać, a następnie kliknij przycisk **OK**. Certyfikaty są dodawane do repozytorium kluczy.

Za pomocą wiersza komend

Użyj następujących komend, aby wyświetlić listę, a następnie dodać certyfikaty ośrodka CA za pomocą komendy iKeycmd:

- Wydaj następującą komendę, aby wyświetlić listę domyślnych certyfikatów CA wraz z organizacjami, które je wystawiają:

```
runmqckm -cert -listsigners
```

- Wydaj następującą komendę, aby dodać wszystkie certyfikaty ośrodka CA dla organizacji określonej w polu *etykieta* :

```
runmqckm -cert -populate -db filename -pw password -label label
```

gdzie:

-db *filename*	to pełna nazwa ścieżki do bazy danych kluczy.
-pw *password*	to hasło do bazy danych kluczy.

`-label label` jest etykietą przyłączoną do certyfikatu.

Uwaga: Dodanie certyfikatu ośrodka CA do repozytorium kluczy powoduje, że produkt WebSphere MQ jest zaufany do wszystkich certyfikatów osobistych podpisanych przez ten certyfikat ośrodka CA. Należy dokładnie rozważyć, które ośrodki certyfikacji mają być zaufane i dodać tylko zestaw certyfikatów ośrodków CA potrzebnych do uwierzytelniania klientów i menedżerów. Nie zaleca się dodawania pełnego zestawu domyślnych certyfikatów CA, o ile nie jest to ostateczne wymaganie dotyczące strategii bezpieczeństwa.

Znajdowanie repozytorium kluczy dla menedżera kolejek w systemach UNIX, Linux, and Windows

Ta procedura służy do uzyskiwania położenia pliku bazy danych kluczy menedżera kolejek.

Procedura

1. Wyświetl atrybuty menedżera kolejek przy użyciu jednej z następujących komend MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

   Atrybuty menedżera kolejek można również wyświetlić za pomocą programu IBM WebSphere MQ Explorer lub komend PCF.
2. Sprawdź dane wyjściowe komendy dla ścieżki i nazwy macierzystej pliku bazy danych kluczy. Na przykład składnia
   a. w systemach UNIX and Linux : `/var/mqm/qmgrs/QM1/ssl/key`, gdzie `/var/mqm/qmgrs/QM1/ssl` jest ścieżką, a `key` jest nazwą rdzenia
   b. w systemie Windows: *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl\key`, gdzie *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl` jest ścieżką, a `key` jest nazwą rdzenia. *MQ_INSTALLATION_PATH* reprezentuje katalog najwyższego poziomu, w którym zainstalowany jest produkt WebSphere MQ .

Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemach UNIX, Linux lub Windows

Położenie pliku bazy danych kluczy menedżera kolejek można zmienić za pomocą różnych sposobów, w tym komendy MQSC ALTER QMGR.

Położenie pliku bazy danych kluczy menedżera kolejek można zmienić, używając komendy MQSC ALTER QMGR w celu ustawienia atrybutu repozytorium kluczy menedżera kolejek. Na przykład w systemach UNIX and Linux :

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

Plik bazy danych kluczy zawiera pełną nazwę pliku: `/var/mqm/qmgrs/QM1/ssl/MyKey.kdb`

W systemie Windows:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\Mykey')
```

Plik bazy danych kluczy zawiera pełną nazwę pliku: `C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\Mykey.kdb`

Ostrzeżenie: Upewnij się, że rozszerzenie `.kdb` nie zawiera nazwy pliku w słowie kluczowym SSLKEYR, ponieważ menedżer kolejek dołącza to rozszerzenie automatycznie.

Atrybuty menedżera kolejek można także zmienić przy użyciu programu WebSphere MQ Explorer lub komend PCF.

W przypadku zmiany położenia pliku bazy danych kluczy menedżera kolejek certyfikaty nie są przesyłane ze starego miejsca. Jeśli używany plik bazy danych kluczy jest nowym plikiem bazy danych kluczy,

należy zapełnić go certyfikatami ośrodka CA i osobistymi, które są potrzebne, zgodnie z opisem w sekcji “Importowanie certyfikatu osobistego do repozytorium kluczy w systemach UNIX, Linux, and Windows” na stronie 138.

Znajdowanie repozytorium kluczy dla klienta MQI produktu IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Położenie repozytorium kluczy jest nadawane przez zmienną MQSSLKEYR lub jest określone w wywołaniu MQCONNX.

Sprawdź zmienną środowiskową MQSSLKEYR, aby uzyskać położenie pliku bazy danych kluczy klienta MQI produktu IBM WebSphere MQ . Na przykład:

```
echo $MQSSLKEYR
```

Sprawdź również aplikację, ponieważ nazwa pliku bazy danych kluczy może być również ustawiona w wywołaniu MQCONNX, zgodnie z opisem w sekcji “Określanie położenia repozytorium kluczy dla klienta MQI produktu IBM WebSphere MQ w systemach UNIX, Linux, and Windows” na stronie 125. Wartość ustawiona w wywołaniu MQCONNX przesłania wartość MQSSLKEYR.

Określanie położenia repozytorium kluczy dla klienta MQI produktu IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Dla klienta MQI produktu IBM WebSphere MQ nie ma domyślnego repozytorium kluczy. Jego położenie można określić na jeden z dwóch sposobów. Upewnij się, że dostęp do pliku bazy danych kluczy jest możliwy tylko dla zamierzonych użytkowników lub administratorów, aby zapobiec nieautoryzowanemu kopiowaniu do innych systemów.

Położenie pliku bazy danych kluczy klienta MQI produktu IBM WebSphere MQ można określić na jeden z dwóch sposobów:

- Ustawianie zmiennej środowiskowej MQSSLKEYR. Na przykład w systemach UNIX and Linux :

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  W pliku bazy danych kluczy znajduje się pełna nazwa pliku:

  ```
  /var/mqm/ssl/key.kdb
  ```

  W systemie Windows:

  ```
  set MQSSLKEYR=C:\Program Files\IBM\WebSphere MQ\ssl\key
  ```

  W pliku bazy danych kluczy znajduje się pełna nazwa pliku:

  ```
  C:\Program Files\IBM\WebSphere MQ\ssl\key.kdb
  ```

  Uwaga: Rozszerzenie .kdb jest obowiązkową częścią nazwy pliku, ale nie jest dołączane jako część wartości zmiennej środowiskowej.
- Podanie ścieżki i nazwy macierzystej pliku bazy danych kluczy w polu *KeyRepository* struktury MQSCO, gdy aplikacja tworzy wywołanie MQCONNX. Więcej informacji na temat korzystania ze struktury MQSCO w produkcie MQCONNX zawiera sekcja Przegląd dla MQSCO .

Gdy zmiany w certyfikatach lub w bazie certyfikatów stają się skuteczne w systemach UNIX, Linux lub Windows.

W przypadku zmiany certyfikatów w bazie certyfikatów lub lokalizacji bazy certyfikatów zmiany są wprowadzane w zależności od typu kanału i sposobu działania kanału.

Zmiany w certyfikatach w pliku bazy danych kluczy i w atrybucie repozytorium kluczy stają się skuteczne w następujących sytuacjach:

- Gdy nowy proces wychodzący pojedynczego kanału jest uruchamiany jako pierwszy, uruchamiany jest kanał SSL.
- Gdy nowy przychodzący proces pojedynczego kanału TCP/IP po raz pierwszy otrzyma żądanie uruchomienia kanału SSL.
- Po wydaniu komendy MQSC REFRESH SECURITY TYPE (SSL) w celu odświeżenia środowiska SSL produktu Websphere MQ .
- W przypadku procesów aplikacji klienckich, gdy ostatnie połączenie SSL w procesie jest zamknięte. Następne połączenie SSL odbierze zmiany certyfikatu.
- W przypadku kanałów, które są uruchamiane jako wątki procesu zestawiania procesów (amqrmppa), proces zestawiania procesów jest uruchamiany lub restartowany, a najpierw uruchamia kanał SSL. Jeśli proces zestawiania procesów uruchomił już kanał SSL i chcesz, aby zmiana stała się efektywna od razu, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- W przypadku kanałów, które są uruchamiane jako wątki inicjatora kanału, gdy inicjator kanału jest uruchamiany lub restartowany, a najpierw uruchamia kanał SSL. Jeśli proces inicjatora kanału uruchomił już kanał SSL i chcesz, aby zmiana stała się efektywna natychmiast, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- W przypadku kanałów uruchamianych jako wątki programu nasłuchującego TCP/IP, gdy proces nasłuchiwania jest uruchamiany lub restartowany, a po pierwsze odbiera żądanie uruchomienia kanału SSL. Jeśli program nasłuchujący uruchomił już kanał SSL i chcesz, aby zmiana stała się efektywna od razu, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).

Można również odświeżyć środowisko SSL produktu WebSphere MQ przy użyciu programu IBM WebSphere MQ Explorer lub komend PCF.

Tworzenie samopodpisanego certyfikatu osobistego w systemach UNIX, Linux, and Windows

Certyfikat samopodpisany można utworzyć za pomocą komendy iKeyman, iKeycmdlub runmqakm.

Uwaga: Produkt IBM WebSphere MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami z rodziny SHA-2 .

Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są one skróconą formą odpowiednio SHA384WithRSA i SHA512WithRSA .

Więcej informacji o tym, dlaczego warto korzystać z certyfikatów samopodpisanych, zawiera sekcja “Korzystanie z certyfikatów samopodpisanych w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek” na stronie 214.

Nie wszystkie certyfikaty cyfrowe mogą być używane ze wszystkimi obiektami CipherSpecs. Należy się upewnić, że został utworzony certyfikat kompatybilny z CipherSpecs , który ma być używany. Produkt WebSphere MQ obsługuje trzy różne typy CipherSpec. Szczegółowe informacje na ten temat zawiera sekcja “Współdziałanie Elliptic Curve i RSA CipherSpecs” na stronie 36 w temacie “Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35 . Aby użyć typu 1 CipherSpecs (dla nazw rozpoczynających się od ECDHE_ECDSA_), należy użyć komendy **runmqakm** w celu utworzenia certyfikatu i podać parametr algorytmu podpisu ECDSA (Elliptic Curve ECDSA), na przykład **-sig_alg** EC_ecdsa_with_SHA384 .

Korzystanie z programu narzędziowego iKeyman

W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

Aby uzyskać certyfikat samopodpisany dla menedżera kolejek lub klienta MQI produktu WebSphere MQ , należy wykonać następującą procedurę:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** .
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Otwórz.
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, w którym ma zostać zapisany certyfikat, na przykład `key.kdb`.
6. Kliknij przycisk **Otwórz**. Zostanie wyświetlone okno Pytanie o hasło.
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. W menu **Create** (Utwórz) kliknij opcję **New Self-Signed Certificate**(Nowy certyfikat samopodpisany) Zostanie wyświetlone okno Tworzenie nowego samopodpisanego certyfikatu.
9. W polu **Key Label** (Etykieta klucza) wpisz:
   - W przypadku menedżera kolejek, `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek składanego na małe litery. Na przykład: `QM1`, `ibmwebspheremqqm1`lub,
   - W przypadku klienta WebSphere MQ `ibmwebspheremq` , po którym następuje identyfikator użytkownika logowania składany na małe litery, na przykład `ibmwebspheremqmyuserid` .
10. Wpisz lub wybierz wartość dla dowolnego pola w polu **Distinguished name**lub dowolnej z pól **Subject alternative name** .
11. W pozostałych polach zaakceptuj wartości domyślne lub wybierz nowe. Więcej informacji na temat nazw wyróżniających zawiera sekcja “Nazwy wyróżniające” na stronie 11.
12. Kliknij przycisk **OK**. Na liście **Personal Certificates** (Certyfikaty osobiste) wyświetlana jest etykieta samopodpisanego certyfikatu osobistego, który został utworzony.

Za pomocą wiersza komend

Aby utworzyć samopodpisany certyfikat osobisty za pomocą komendy iKeycmd lub runmqakm, należy użyć następujących komend:

- Za pomocą komendy iKeycmd w systemach UNIX, Linux i Windows :

```
runmqckm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days
 -sig_alg algorithm
```

  Zamiast produktu `-dn` *`distinguished_name`* można używać produktów `-san_dsname` *`DNS_names`* , `-san_emailaddr` *`email_addresses`* lub `-san_ipaddr` *`IP_addresses`* .

- Za pomocą komendy runmqakm:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -fips -sig_alg algorithm
```

`-db` *`filename`*	Pełna nazwa pliku bazy danych kluczy CMS.
`-pw` *`password`*	Hasło do bazy danych kluczy CMS.
`-label` *`label`*	Etykieta klucza dołączona do certyfikatu.
`-dn` *`distinguished_name`*	Nazwa wyróżniająca X.500 ujęta w podwójny cudzysłów. Wymagany jest co najmniej jeden atrybut. Można podać wiele atrybutów OU lub DC.

-size *key_size*	Wielkość klucza. W przypadku komendy iKeycmdwartość może wynosić 512 lub 1024. W przypadku komendy runmqakm wartością może być 512, 1024, 2048 lub 4096.
-x509version *version*	Wersja certyfikatu X.509 do utworzenia. Wartością może być 1, 2 lub 3. Domyślną wartością jest 3.
-expire *days*	Czas ważności (w dniach) certyfikatu. Wartość domyślna to 365 dni dla certyfikatu.
-fips	określa, że komenda jest uruchamiana w trybie FIPS. Ten tryb powoduje wyłączenie użycia biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Działając w trybie FIPS, komponent ICC korzysta z algorytmów, których poprawność została sprawdzona pod kątem standardu FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.
-sig_alg	W przypadku komendy runmqakm: algorytm kodowania mieszającego używany podczas tworzenia certyfikatu samopodpisanego. Ten algorytm kodowania mieszającego jest używany do tworzenia sygnatury powiązanej z nowo utworzonym samopodpisanym certyfikatem. Wartość ta może mieć wartość md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA , SHA_WITH_RSA, sha1, SHA1WithDSA , SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA , SHA224WithECDSA, SHA224WithRSA , sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384 , SHA384_WITH_RSA, SHA384WithECDSA , SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA , EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224 , EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 lub EC_ecdsa_with_SHA512. Wartością domyślną jest SHA1WithRSA.
-sig_alg	W przypadku komendy iKeycmd: algorytm podpisu asymetrycznego używany do tworzenia pary kluczy pozycji. Wartość ta może mieć wartość MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA , MD5WithRSA, SHA1WithDSA, SHA1WithRSA, SHA256_WITH_RSA, SHA256WithRSA , SHA2WithRSA, SHA384_WITH_RSA, SHA384WithRSA, SHA512_WITH_RSA, SHA512WithRSA, SHA_WITH_DSA, SHA_WITH_RSA , SHAWithDSA, lub SHAWithRSA. Wartością domyślną jest SHA1WithRSA.
-san_dnsname *DNS_names*	Rozdzielana przecinkami lub spacjami lista nazw DNS dla tworzonej pozycji.
-san_emailaddr *email_addresses*	Lista adresów e-mail oddzielonych przecinkami lub spacjami dla tworzonej pozycji.
-san_ipaddr *IP_addresses*	Lista adresów IP oddzielonych przecinkami lub spacjami dla tworzonej pozycji.

distributed *Żądanie certyfikatu osobistego w systemach UNIX, Linux, and Windows*

Żądanie certyfikatu osobistego można zażądać za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** lub **runmqakm** . Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

O tym zadaniu

Certyfikat osobisty można zażądać za pomocą interfejsu GUI programu iKeyman lub z poziomu wiersza komend, z uwzględnieniem następujących czynników:

- Produkt WebSphere MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami z rodziny SHA-2 .
- Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są one skróconą formą odpowiednio SHA384WithRSA i SHA512WithRSA .
- Nie wszystkie certyfikaty cyfrowe mogą być używane ze wszystkimi obiektami CipherSpecs. Należy się upewnić, że został złożony wniosek o certyfikat zgodny z CipherSpecs , który ma być używany. Produkt WebSphere MQ obsługuje trzy różne typy interfejsu CipherSpec. Szczegółowe informacje na ten temat zawiera sekcja “Współdziałanie Elliptic Curve i RSA CipherSpecs” na stronie 36 w temacie “Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35 .
- Aby użyć typu 1 CipherSpecs (z nazwami rozpoczynające się od ECDHE_ECDSA_), należy użyć komendy **runmqakm** , aby zażądać certyfikatu i podać parametr algorytmu podpisu ECDSA (Elliptic Curve ECDSA), na przykład **-sig_alg** EC_ecdsa_with_SHA384.
- Tylko komenda runmqakm udostępnia opcję zgodną ze standardem FIPS.
- Jeśli używany jest sprzęt szyfrujący, należy zapoznać się z “Żądanie certyfikatu osobistego dla sprzętu PKCS #11” na stronie 146.

Korzystanie z interfejsu użytkownika iKeyman

O tym zadaniu

W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Wykonaj następujące kroki, aby zastosować się do certyfikatu osobistego za pomocą interfejsu użytkownika iKeyman :

1. Uruchom interfejs użytkownika iKeyman za pomocą komendy **strmqikm** .
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz).

   Zostanie otwarte okno **Otwórz** .
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać wygenerowany żądanie, na przykład key . kdb.
6. Kliknij przycisk **Otwórz**.

   Zostanie otwarte okno **Pytanie o hasło** .
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**.

   Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. W menu **Utwórz** kliknij opcję **Nowe żądanie certyfikatu**. Zostanie otwarte okno **Tworzenie nowego klucza i żądania certyfikatu** .
9. W polu **Key Label** (Etykieta klucza) wprowadź następujące etykiety:
   - W przypadku menedżera kolejek wpisz ibmwebspheremq , a następnie nazwę menedżera kolejek, który zmienił się na małe litery. Na przykład w przypadku menedżera kolejek o nazwie QM1należy wprowadzić wartość ibmwebspheremqqm1.
   - W przypadku partycji IBM WebSphere MQ MQI clientwpisz ibmwebspheremq , a następnie ID użytkownika logowania, wszystkie małe litery, na przykład ibmwebspheremqmyuserid .

10. Wpisz lub wybierz wartość w dowolnym polu w polu **Nazwa wyróżniająca** lub dowolną z pól **Nazwa alternatywna podmiotu** . W pozostałych polach zaakceptuj wartości domyślne lub wybierz nowe.

    Więcej informacji na temat nazw wyróżniających zawiera sekcja “Nazwy wyróżniające” na stronie 11.
11. W polu **Wprowadź nazwę pliku, w którym zostanie zapisane żądanie certyfikatu** zaakceptuj wartość domyślną `certreq.arm`lub wpisz nową wartość z pełną ścieżką.
12. Kliknij przycisk **OK**.

    Zostanie wyświetlone okno z potwierdzeniem.
13. Kliknij przycisk **OK**.

    Na liście **Personal Certificate Requests** (Żądania certyfikatu osobistego) wyświetlana jest etykieta utworzonego żądania certyfikatu osobistego. Żądanie certyfikatu jest przechowywane w pliku, który został wybrany w kroku “11” na stronie 130.
14. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując ten plik do formularza żądania na stronie internetowej ośrodka CA.

Za pomocą wiersza komend

Procedura

Aby zażądać certyfikatu osobistego za pomocą komendy **runmqckm** lub **runmqakm** , należy użyć następujących komend:

- Korzystanie z produktu **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -sig_alg algorithm
```

  Zamiast produktu `-dn` *distinguished_name* można używać produktów `-san_dsname` *DNS_names* , `-san_emailaddr` *email_addresses* lub `-san_ipaddr` *IP_addresses* .

- Za pomocą komendy runmqakm:

```
runmqakm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -fips
        -sig_alg algorithm
```

gdzie:

-db *nazwa_pliku*
Określa pełną nazwę pliku bazy danych kluczy CMS.

-pw *hasło*
Określa hasło do bazy danych kluczy CMS.

-label *etykieta*
Określa etykietę klucza dołączoną do certyfikatu.

-dn *nazwa_wyróżniająca*
Określa nazwę wyróżniającą X.500 ujętą w podwójny cudzysłów. Wymagany jest co najmniej jeden atrybut. Można podać wiele atrybutów OU i DC.

-size *wielkość_klucza*
Określa wielkość klucza. Jeśli używany jest produkt **runmqckm** , wartość może mieć wartość 512 lub 1024. Jeśli używany jest produkt **runmqakm**, wartość może mieć wartość 512, 1024lub 2048.

-file *nazwa_pliku*
Określa nazwę pliku dla żądania certyfikatu.

-fips
określa, że komenda jest uruchamiana w trybie FIPS. Ten tryb powoduje wyłączenie użycia biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Gdy w trybie FIPS komponent ICC używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

-sig_alg
W przypadku bazy danych **runmqckm**określa algorytm podpisu asymetrycznego używany do tworzenia pary kluczy pozycji. Wartość ta może mieć wartość MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA , SHA1WithRSA, SHA256_WITH_RSA, SHA256WithRSA, SHA2WithRSA, SHA384_WITH_RSA , SHA384WithRSA, SHA512_WITH_RSA , SHA512WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, lub SHAWithRSA . Wartością domyślną jest SHA1WithRSA .

-sig_alg
W przypadku bazy danych **runmqakm**określa algorytm kodowania mieszającego używany podczas tworzenia żądania certyfikatu. Ten algorytm kodowania mieszającego jest używany do tworzenia sygnatury powiązanej z nowo utworzonym żądaniem certyfikatu. Wartość ta może mieć wartość md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA , SHA_WITH_RSA, sha1, SHA1WithDSA , SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA , SHA224WithECDSA, SHA224WithRSA , sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384 , SHA384_WITH_RSA, SHA384WithECDSA , SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA , EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224 , EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 lub EC_ecdsa_with_SHA512. Wartością domyślną jest SHA1WithRSA.

-san_dnsname *nazwy_nazw DNS*
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę nazw DNS dla tworzonej pozycji.

-san_emailaddr *adres_e-mail*
Określa rozdzielaną przecinkami lub spacjami listę adresów e-mail dla tworzonej pozycji.

-san_ipaddr *adres_IP*
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę adresów IP dla tworzonej pozycji.

Odnawianie istniejącego certyfikatu osobistego w systemach UNIX, Linux, and Windows

Certyfikat osobisty można odnowić za pomocą interfejsu użytkownika iKeyman lub za pomocą komend **iKeycmd** lub **runmqakm** .

Zanim rozpoczniesz

Jeśli wymagane jest użycie większych kluczowych wielkości dla certyfikatów osobistych, opisane poniżej kroki odnowienia nie działają, ponieważ utworzone żądanie certyfikatu zostało wygenerowane z istniejącego klucza.

Postępuj zgodnie z krokami opisanymi w sekcji “Żądanie certyfikatu osobistego w systemach UNIX, Linux, and Windows” na stronie 128 , aby utworzyć nowe żądanie certyfikatu, używając wymaganych wielkości kluczy. Ten proces zastępuje istniejący klucz.

O tym zadaniu

Certyfikat osobisty ma datę ważności, po której certyfikat nie może być już używany. W tym zadaniu wyjaśniono, jak odnowić istniejący certyfikat osobisty, zanim utraci ważność.

Korzystanie z interfejsu użytkownika iKeyman

O tym zadaniu

W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Wykonaj następujące kroki, aby zastosować się do certyfikatu osobistego za pomocą interfejsu użytkownika iKeyman :

1. Uruchom interfejs użytkownika iKeyman , korzystając z komendy **strmqikm** w systemach UNIX, Linux, and Windows .
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz).

   Zostanie otwarte okno **Otwórz** .
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać wygenerowany żądanie, na przykład `key.kdb`.
6. Kliknij przycisk **Otwórz**.

   Zostanie otwarte okno **Pytanie o hasło** .
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**.

   Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. Z menu rozwijanego menu rozwijanego wybierz opcję **Certyfikaty osobiste** , a następnie wybierz certyfikat z listy, która ma zostać odnowiona.
9. Kliknij opcję **Utwórz ponownie żądanie ...** .

   Zostanie otwarte okno, w którym można wprowadzić nazwę pliku i informacje o położeniu pliku.
10. W polu **file name**(Nazwa pliku) zaakceptuj wartość domyślną `certreq.arm`lub wpisz nową wartość, w tym pełną ścieżkę do pliku.
11. Kliknij przycisk **OK**. Żądanie certyfikatu jest zapisywane w pliku wybranym w kroku “9” na stronie 132.
12. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując ten plik do formularza żądania na stronie internetowej ośrodka CA.

Za pomocą wiersza komend

Procedura

Aby zażądać certyfikatu osobistego za pomocą komendy **iKeycmd** lub **runmqakm** , należy użyć następujących komend:

- Korzystanie z produktu **iKeycmd** w systemach UNIX, Linux, and Windows :

```
runmqckm -certreq -recreate -db filename -pw
password -label label
 -target filename
```

- Za pomocą komendy runmqakm:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
  -target filename
```

gdzie:

-db *nazwa_pliku*
Określa pełną nazwę pliku bazy danych kluczy CMS.

-pw *hasło*
Określa hasło do bazy danych kluczy CMS.

-target *nazwa_pliku*
Określa nazwę pliku dla żądania certyfikatu.

Co dalej

Po otrzymaniu od ośrodka certyfikacji podpisanego certyfikatu osobistego, można go dodać do bazy danych kluczy, wykonując kroki opisane w sekcji "Odbieranie certyfikatów osobistych do repozytorium kluczy w systemach UNIX, Linux i Windows" na stronie 133.

Odbieranie certyfikatów osobistych do repozytorium kluczy w systemach UNIX, Linux i Windows

Ta procedura umożliwia otrzymanie certyfikatu osobistego do pliku bazy danych kluczy. Repozytorium kluczy musi być tym samym repozytorium, w którym zostało utworzone żądanie certyfikatu.

Po wysłaniu przez ośrodek CA nowego certyfikatu osobistego, należy dodać go do pliku bazy danych kluczy, z którego wygenerowano nowe żądanie certyfikatu. Jeśli ośrodek CA wyśle certyfikat jako część wiadomości e-mail, skopiuj certyfikat do osobnego pliku.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Upewnij się, że plik certyfikatu, który ma być zaimportowany, ma uprawnienia do zapisu dla bieżącego użytkownika, a następnie użyj następującej procedury dla menedżera kolejek lub klienta MQI produktu WebSphere MQ , aby odebrać certyfikat osobisty do pliku bazy danych kluczy:

1. Uruchom interfejs graficzny programu iKeyman za pomocą komendy **strmqikm** (w systemie Windows UNIX and Linux).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij przycisk **Otwórz**, a następnie przycisk **OK**. Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** . Wybierz widok **Personal Certificates** (Certyfikaty osobiste).
8. Kliknij przycisk **Odbierz**. Zostanie otwarte okno Pobierz certyfikat z pliku.
9. Wpisz nazwę i położenie pliku certyfikatu dla nowego certyfikatu osobistego lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
10. Kliknij przycisk **OK**. Jeśli w bazie danych kluczy masz już certyfikat osobisty, zostanie otwarte okno z pytaniem, czy chcesz ustawić klucz, który jest dodawany jako klucz domyślny w bazie danych.
11. Kliknij przycisk **Tak** lub **Nie**. Zostanie otwarte okno Enter a Label (Wprowadzanie etykiety).
12. Kliknij przycisk **OK**. Pole **Personal Certificates** (Certyfikaty osobiste) zawiera etykietę dodanego nowego certyfikatu osobistego.

Za pomocą wiersza komend

Użyj następujących komend, aby dodać certyfikat osobisty do pliku bazy danych kluczy za pomocą komendy iKeycmd :

- W systemach UNIX, Linux i Windowswydaj następującą komendę:

```
runmqckm -cert -receive -file filename -db filename -pw
password
        -format ascii
```

gdzie:

`-file filename`	to pełna nazwa pliku zawierającego certyfikat osobisty.
`-db filename`	jest pełną nazwą pliku bazy danych kluczy CMS.
`-pw password`	jest hasłem dla bazy danych kluczy CMS.
`-format ascii`	jest formatem certyfikatu. Wartość może mieć wartość `ascii` dla Base64-encoded ASCII lub `binary` dla danych binarnych DER. Wartością domyślną jest `ascii` .

Jeśli używany jest sprzęt szyfrujący, należy zapoznać się z “Importowanie certyfikatu osobistego do sprzętu PKCS #11” na stronie 148.

Wyodrębnianie certyfikatu ośrodka CA z repozytorium kluczy

Aby wyodrębnić certyfikat ośrodka CA, należy wykonać następującą procedurę.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Wykonaj następujące kroki na komputerze, na podstawie którego ma zostać wyodrębnienie certyfikatu ośrodka CA:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **`strmqikm`** .
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać wyodrębniony, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Signer Certificates** (Certyfikaty osoby podpisującej) i wybierz certyfikat, który ma zostać wyodrębniony.
9. Kliknij opcję **Wyodrębnij**. Zostanie otwarte okno Wyodrębnianie certyfikatu do pliku.
10. Wybierz **Typ danych** certyfikatu, na przykład **Base64-encoded ASCII data** (Dane ASCII z kodowaniem Base64) dla pliku z rozszerzeniem `.arm` .
11. Wpisz nazwę i położenie pliku certyfikatu, w którym ma zostać zapisany certyfikat, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
12. Kliknij przycisk **OK**. Certyfikat jest zapisywany w podanym pliku.

Za pomocą wiersza komend

Aby wyodrębnić certyfikat ośrodka CA za pomocą komendy iKeycmd , należy użyć następujących komend:

- W systemach UNIX, Linux i Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

gdzie:

-db *filename*	to pełna ścieżka do bazy danych kluczy CMS.
-pw *password*	jest hasłem dla bazy danych kluczy CMS.
-label *label*	jest etykietą przyłączoną do certyfikatu.
-target *filename*	jest nazwą pliku docelowego.
-format *ascii*	jest formatem certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartość domyślna to `ascii`.

Wyodrębnianie publicznych części samopodpisanego certyfikatu z repozytorium kluczy w systemach UNIX, Linux i Windows

Aby wyodrębnić część publiczną samopodpisanego certyfikatu, należy wykonać następującą procedurę.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Wykonaj następujące kroki na maszynie, z której chcesz wyodrębnić część publiczną certyfikatu samopodpisanego:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** (w systemach UNIX, Linux i Windows).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać wyodrębnienie certyfikatu, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Personal Certificates** (Certyfikaty osobiste) i wybierz certyfikat.
9. Kliknij opcję **Wyodrębnij certyfikat**. Zostanie otwarte okno Wyodrębnianie certyfikatu do pliku.
10. Wybierz **Typ danych** certyfikatu, na przykład **Base64-encoded ASCII data** (Dane ASCII z kodowaniem Base64) dla pliku z rozszerzeniem `.arm` .
11. Wpisz nazwę i położenie pliku certyfikatu, w którym ma zostać zapisany certyfikat, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
12. Kliknij przycisk **OK**. Certyfikat jest zapisywany w podanym pliku. Należy zwrócić uwagę, że podczas wyodrębniania (a nie eksportowania) certyfikatu dołączana jest tylko publiczna część certyfikatu, więc hasło nie jest wymagane.

Za pomocą wiersza komend

Aby wyodrębnić część publiczną samopodpisanego certyfikatu za pomocą komendy iKeycmd lub runmqakm, należy użyć następujących komend:

- W systemach UNIX, Linux i Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Za pomocą komendy runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

gdzie:

-db *filename*	to pełna ścieżka do bazy danych kluczy CMS.
-pw *password*	jest hasłem dla bazy danych kluczy CMS.
-label *label*	jest etykietą przyłączoną do certyfikatu.
-target *filename*	jest nazwą pliku docelowego.
-format *ascii*	jest formatem certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartość domyślna to `ascii`.

Dodawanie certyfikatu ośrodka CA (lub publicznej części certyfikatu samopodpisanego) do repozytorium kluczy w systemach UNIX, Linux, and Windows

Poniższa procedura opisuje sposób dodawania certyfikatu CA lub części publicznej certyfikatu samopodpisanego do repozytorium kluczy.

Jeśli certyfikat, który ma zostać dodany, jest częścią łańcucha certyfikatów, należy również dodać wszystkie certyfikaty znajdujące się w łańcuchu powyżej tego certyfikatu. Certyfikaty należy dodawać w ściśle określonym porządku malejącym, rozpoczynając od certyfikatu głównego, po którym w łańcuchu następuje certyfikat CA znajdujący się w hierarchii bezpośrednio poniżej itd.

Poniższe instrukcje, które odnoszą się do certyfikatu CA, dotyczą również publicznej części certyfikatu samopodpisanego.

Uwaga: Jeśli certyfikat, który ma zostać dodany, jest częścią łańcucha certyfikatów, należy również dodać wszystkie certyfikaty znajdujące się w łańcuchu powyżej tego certyfikatu. Należy upewnić się, że certyfikat używa kodowania ASCII (UTF-8) lub kodowania binarnego (DER), ponieważ pakiet IBM Global Secure Toolkit (GSKit) nie obsługuje certyfikatów z innymi typami kodowania. Certyfikaty należy dodawać w ściśle określonym porządku malejącym, rozpoczynając od certyfikatu głównego, po którym następuje certyfikat ośrodka CA znajdujący się w łańcuchu bezpośrednio poniżej.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Na komputerze, na którym chcesz dodać certyfikat CA, wykonaj następujące kroki:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** (w systemach UNIX, Linux i Windows).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).

4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy zostanie wyświetlona w polu **File Name** (Nazwa pliku).
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Signer Certificates** (Certyfikaty osoby podpisującej).
9. Kliknij przycisk **Dodaj**. Zostanie otwarte okno Add CA's Certificate from a File (Dodawanie certyfikatu CA z pliku).
10. Wpisz nazwę pliku certyfikatu i miejsce, w którym jest zapisany, lub kliknij przycisk **Browse** (Przeglądaj), aby wybrać nazwę i położenie.
11. Kliknij przycisk **OK**. Zostanie otwarte okno Enter a Label (Wprowadzanie etykiety).
12. W oknie Enter a Label (Wprowadzanie etykiety) wpisz nazwę certyfikatu.
13. Kliknij przycisk **OK**. Certyfikat zostanie dodany do bazy danych kluczy.

Za pomocą wiersza komend

W celu dodania certyfikatu CA za pomocą narzędzia iKeycmd wykonaj następujące komendy:

- W systemach UNIX, Linux i Windowswydaj następującą komendę:

```
runmqckm -cert -add -db filename -pw password -label label -file filename
        -format ascii
```

gdzie:

`-db` *`filename`*	jest nazwą pełnej ścieżki do bazy danych kluczy CMS.
`-pw` *`password`*	jest hasłem dla bazy danych kluczy CMS.
`-label` *`label`*	jest etykietą przyłączoną do certyfikatu.
`-file` *`filename`*	jest nazwą pliku zawierającego certyfikat.
`-format` *`ascii`*	jest formatem certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartość domyślna to `ascii`.

Eksportowanie certyfikatu osobistego z repozytorium kluczy

Aby wyeksportować certyfikat osobisty, należy wykonać następującą procedurę.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Wykonaj następujące kroki na komputerze, z którego ma zostać wyeksportowany certyfikat osobisty:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **`strmqikm`** (w systemie Windows UNIX and Linux).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać wyeksportowany certyfikat, na przykład `key.kdb`.

6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Personal Certificates** (Certyfikaty osobiste) i wybierz certyfikat, który chcesz wyeksportować.
9. Kliknij opcję **Eksportuj/importuj**. Zostanie otwarte okno dialogowe Eksportuj/importuj.
10. Wybierz opcję **Eksportuj klucz**.
11. Wybierz opcję **Typ pliku kluczy** certyfikatu, który ma zostać wyeksportowany, na przykład **PKCS12**.
12. Wpisz nazwę i położenie pliku, do którego certyfikat ma zostać wyeksportowany, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
13. Kliknij przycisk **OK**. Zostanie otwarte okno Password Prompt (Zapytanie o hasło). Należy zwrócić uwagę, że podczas eksportowania (a nie wyodrębniania) certyfikatu dołączane są zarówno publiczne, jak i prywatne części certyfikatu. Z tego powodu wyeksportowany plik jest chroniony hasłem. Po wyodrębnienia certyfikatu dołączana jest tylko publiczna część certyfikatu, więc hasło nie jest wymagane.
14. Wpisz hasło w polu **Hasło** i wpisz je ponownie w polu **Potwierdź hasło** .
15. Kliknij przycisk **OK**. Certyfikat jest eksportowany do pliku określonego przez użytkownika.

Za pomocą wiersza komend

Aby wyeksportować certyfikat osobisty za pomocą komendy iKeycmd, należy użyć następujących komend:

- W systemach UNIX, Linux i Windows:

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

gdzie:

`-db` *filename*	jest nazwą pełnej ścieżki do bazy danych kluczy CMS.
`-pw` *password*	jest hasłem dla bazy danych kluczy CMS.
`-label` *label*	jest etykietą przyłączoną do certyfikatu.
`-type` *cms*	jest typem bazy danych.
`-target` *filename*	to pełna ścieżka do pliku docelowego.
`-target_pw` *password*	to hasło do szyfrowania certyfikatu.
`-target_type` *pkcs12*	to typ certyfikatu.

Importowanie certyfikatu osobistego do repozytorium kluczy w systemach UNIX, Linux, and Windows

Wykonaj tę procedurę, aby zaimportować certyfikat osobisty.

Przed zaimportowaniem certyfikatu osobistego w formacie PKCS #12 do pliku bazy danych kluczy należy najpierw dodać pełny poprawny łańcuch wystawiających certyfikaty ośrodka CA do pliku bazy danych kluczy (patrz sekcja “Dodawanie certyfikatu ośrodka CA (lub publicznej części certyfikatu samopodpisanego) do repozytorium kluczy w systemach UNIX, Linux, and Windows” na stronie 136).

Pliki PKCS #12 powinny być uważane za tymczasowe i usunięte po użyciu.

Korzystanie z programu narzędziowego iKeyman

Jeśli wymagane jest zarządzanie certyfikatami SSL w sposób zgodny z FIPS-em, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

Wykonaj następujące kroki na komputerze, do którego ma zostać zaimportowany certyfikat osobisty:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** .
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Otwórz.
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij przycisk **Otwórz**. Zostanie wyświetlone okno Pytanie o hasło.
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy zostanie wyświetlona w polu **File Name** (Nazwa pliku).
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz **Personal Certificates**(Certyfikaty osobiste).
9. Jeśli w widoku Certyfikaty osobiste znajdują się certyfikaty, wykonaj następujące kroki:
   a. Kliknij opcję **Eksportuj/importuj**. Zostanie wyświetlone okno dialogowe Eksport/Import.
   b. Wybierz opcję **Importuj klucz**.
10. Jeśli w widoku Certyfikaty osobiste nie ma żadnych certyfikatów, kliknij przycisk **Importuj**.
11. W polu **Key file type** (Typ pliku kluczy) wybierz certyfikat, który ma zostać zaimportowany, na przykład PKCS12.
12. Wpisz nazwę pliku certyfikatu i miejsce, w którym jest zapisany, lub kliknij przycisk **Browse** (Przeglądaj), aby wybrać nazwę i położenie.
13. Kliknij przycisk **OK**. Zostanie wyświetlone okno Pytanie o hasło.
14. W polu **Hasło** wpisz hasło, które jest używane podczas eksportowania certyfikatu.
15. Kliknij przycisk **OK**. Zostanie wyświetlone okno Zmień etykiety. To okno pozwala na zmianę etykiet importowanych certyfikatów, jeśli na przykład w docelowej bazie danych istnieje już certyfikat o takiej samej etykiecie. Zmiana etykiet certyfikatów nie ma wpływu na sprawdzanie poprawności łańcucha certyfikatów. Można go użyć do zmiany etykiety certyfikatu osobistego na wymagany przez produkt WebSphere MQ w celu powiązania certyfikatu z określonym menedżerem kolejek lub klientem (na przykład`ibmwebspheremqqm1`).
16. Aby zmienić etykietę, wybierz wymaganą etykietę z listy **Wybierz etykietę do zmiany** . Etykieta jest kopiowana do pola wprowadzania **Enter a new label** . Zastąp tekst etykiety nową etykietą i kliknij przycisk **Zastosuj**.
17. Tekst w polu **Wprowadź nową etykietę** jest kopiowany z powrotem do pola **Wybierz etykietę do zmiany** , zastępując oryginalnie wybraną etykietę, a następnie ponownie etykietowanie odpowiedniego certyfikatu.
18. Po zmianie wszystkich etykiet, które mają zostać zmienione, kliknij przycisk **OK**. Okno Zmień etykiety zostanie zamknięte, a oryginalne okno IBM Key Management zostanie ponownie wyświetlone razem z polami **Personal Certificates** (Certyfikaty osobiste) i **Signer Certificates** (Certyfikaty osób podpisującego) zaktualizowanymi certyfikatami poprawnie.
19. Certyfikat jest importowany do docelowej bazy danych kluczy.

Za pomocą wiersza komend

Aby zaimportować certyfikat osobisty za pomocą komendy iKeycmd, należy użyć następujących komend:

- W systemach UNIX, Linux i Windows:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

gdzie:

-file *filename*	to pełna nazwa pliku zawierającego certyfikat PKCS #12 .
-pw *password*	to hasło do certyfikatu PKCS #12 .
-type *pkcs12*	jest typem pliku.
-target *filename*	jest nazwą docelowej bazy danych kluczy CMS.
-target_pw *password*	jest hasłem dla bazy danych kluczy CMS.
-target_type *cms*	jest typem bazy danych określonej przez parametr -target
-label *label*	jest etykietą certyfikatu do zaimportowania z bazy danych kluczy źródłowych.
-new_label *label*	to etykieta, do której certyfikat zostanie przypisany w docelowej bazie danych. Jeśli opcja -new_label zostanie pominięta, wartością domyślną będzie użycie tej samej wartości, co opcja -label .

Komenda iKeycmd nie udostępnia komendy do bezpośredniej zmiany etykiet certyfikatów. Aby zmienić etykietę certyfikatu, wykonaj następujące kroki:

1. Wyeksportuj certyfikat do pliku #12 PKCS za pomocą komendy **-cert -export** . Podaj istniejącą etykietę certyfikatu dla opcji -label .
2. Za pomocą komendy **-cert -delete** usuń istniejącą kopię certyfikatu z oryginalnej bazy danych kluczy.
3. Zaimportuj certyfikat z pliku PKCS #12 za pomocą komendy **-cert -import** . Podaj starą etykietę dla opcji -label i wymaganą nową etykietę dla opcji -new_label . Certyfikat zostanie zaimportowany z powrotem do bazy danych kluczy z wymaganą etykietą.

Importowanie z pliku Microsoft .pfx

Należy wykonać tę procedurę w celu mportu z pliku Microsoft .pfx za pomocą programu iKeyman. Nie można użyć komendy runmqakm do zaimportowania pliku .pfx.

Plik .pfx może zawierać dwa certyfikaty odnoszące się do tego samego klucza. Jednym z nich jest certyfikat osobisty lub ośrodek (zawierający klucz publiczny i prywatny). Drugi to certyfikat ośrodka CA (osoba podpisująca) (zawierający tylko klucz publiczny). Te certyfikaty nie mogą współistnieć w tym samym pliku bazy danych kluczy CMS, więc tylko jeden z nich może być importowany. Ponadto "przyjazna nazwa" lub etykieta jest dołączona tylko do certyfikatu osoby podpisującej.

Certyfikat osobisty jest identyfikowany przez wygenerowany przez system unikalny identyfikator użytkownika (UUID). W tej sekcji przedstawiono import certyfikatu osobistego z pliku pfx podczas etykietowania go z nazwą przyjazną poprzednio przypisaną do certyfikatu ośrodka CA (osoby podpisującej). Wystawianie certyfikatów CA (osoby podpisującej) powinno już zostać dodane do docelowej bazy danych kluczy. Należy pamiętać, że pliki PKCS#12 powinny być uważane za tymczasowe i usunięte po użyciu.

Aby zaimportować certyfikat osobisty ze źródłowej bazy danych pfx, wykonaj następujące kroki:

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** (w systemach Linux, UNIX lub Windows). Zostanie wyświetlone okno narzędzia IBM Key Management.
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Otwórz.
3. Wybierz typ bazy danych kluczy **PKCS12**.
4. **Przed wykonaniem tego kroku zalecane jest wykonanie kopii zapasowej bazy danych pfx.** Wybierz bazę danych kluczy pfx, która ma zostać zaimporta. Kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Podaj hasło.
5. Wprowadź hasło bazy danych kluczy i kliknij przycisk **OK**. Zostanie wyświetlone okno narzędzia IBM Key Management. Na pasku tytułu wyświetlana jest nazwa wybranego pliku bazy danych kluczy pfx, który wskazuje, że plik jest otwarty i gotowy.

6. Z listy wybierz pozycję **Certyfikaty osób podpisującego** . "przyjazna nazwa" wymaganego certyfikatu jest wyświetlana jako etykieta w panelu Certyfikaty osób podpisującego.
7. Wybierz pozycję etykiety i kliknij przycisk **Usuń** , aby usunąć certyfikat osoby podpisującej. Zostanie wyświetlone okno Potwierdź.
8. Kliknij przycisk **Tak**. Wybrana etykieta nie jest już wyświetlana w panelu Certyfikaty podpisującego.
9. Powtórz kroki 6, 7 i 8 dla wszystkich certyfikatów osoby podpisującej.
10. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Otwórz.
11. Wybierz docelową bazę danych CMS, do której importowany jest plik pfx. Kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Podaj hasło.
12. Wprowadź hasło bazy danych kluczy i kliknij przycisk **OK**. Zostanie wyświetlone okno narzędzia IBM Key Management. Na pasku tytułu wyświetlana jest nazwa wybranego pliku bazy danych kluczy, który wskazuje, że plik jest otwarty i gotowy.
13. Z listy wybierz pozycję **Personal Certificates** (Certyfikaty osobiste).
14. Jeśli w widoku Certyfikaty osobiste znajdują się certyfikaty, wykonaj następujące kroki:
    a. Kliknij opcję **Eksportuj/importuj klucz**. Zostanie wyświetlone okno dialogowe Eksport/Import.
    b. Wybierz opcję **Importuj** z menu Wybierz typ działania.
15. Jeśli w widoku Certyfikaty osobiste nie ma żadnych certyfikatów, kliknij przycisk **Importuj**.
16. Wybierz plik PKCS12 .
17. Wprowadź nazwę pliku pfx, który został użyty w kroku 4. Kliknij przycisk **OK**. Zostanie wyświetlone okno Podaj hasło.
18. Podaj to samo hasło, które zostało określone podczas usuwania certyfikatu osoby podpisującej. Kliknij przycisk **OK**.
19. Zostanie wyświetlone okno Zmień etykiety (tak, jak powinno być tylko jeden certyfikat dostępny do zaimportowania). Etykieta certyfikatu powinna być identyfikatorem UUID, który ma format `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.
20. Aby zmienić etykietę, wybierz identyfikator UUID z panelu **Wybierz etykietę do zmiany:** . Etykieta zostanie zreplikowana w polu **Wprowadź nową etykietę:** . Zastąp tekst etykiety nazwą przyjazną, która została usunięta w kroku 7, a następnie kliknij przycisk **Zastosuj**. Nazwa przyjazna musi mieć postać `ibmwebspheremq`, po której następuje nazwa menedżera kolejek lub identyfikator logowania użytkownika klienta MQI produktu WebSphere MQ , który jest zapisany małymi literami.
21. Kliknij przycisk **OK**. Okno Zmień etykiety zostanie teraz usunięte, a oryginalne okno IBM Key Management zostanie ponownie wyświetlone razem z panelami Certyfikaty osobiste i Certyfikaty osób podpisanych zaktualizowanymi poprawnie z etykietą certyfikatu osobistego.
22. Certyfikat osobisty pfx jest teraz importowany do bazy danych (docelowej) bazy danych.

Zmiana etykiety certyfikatu za pomocą komendy iKeycmd

Importowanie z pliku #7 PKCS

Narzędzia iKeyman i iKeycmd nie obsługują plików PKCS #7 (.p7b). Użyj narzędzia runmqckm, aby zaimportować certyfikaty z pliku #7 PKCS.

Aby dodać certyfikat CA z pliku PKCS #7 , należy użyć następującej komendy:

```
runmqckm -cert -add -db filename -pw password -type cms -file filename
-label label
```

`-db` *`filename`*	jest pełną nazwą pliku bazy danych kluczy CMS.
`-pw` *`password`*	to hasło do bazy danych kluczy.
`-type` *`cms`*	to typ bazy danych kluczy.
`-file` *`filename`*	jest nazwą pliku #7 PKCS.

`-label` *label*	to etykieta, do której certyfikat jest przypisany w docelowej bazie danych. Pierwszy certyfikat przyjmuje podaną etykietę. Wszystkie pozostałe certyfikaty, jeśli są obecne, mają etykietę z nazwą ich podmiotu.

Aby zaimportować certyfikat osobisty z pliku PKCS #7 , należy użyć następującej komendy:

```
runmqckm -cert -import -db filename -pw password -type pkcs7 -target filename
-target_pw password -target_type cms -label label -new_label label
```

`-db` *filename*	to pełna nazwa pliku zawierającego certyfikat PKCS #7 .
`-pw` *password*	to hasło do certyfikatu PKCS #7 .
`-type` *pkcs7*	jest typem pliku.
`-target` *filename*	jest nazwą docelowej bazy danych kluczy.
`-target_pw` *password*	jest hasłem dla docelowej bazy danych kluczy.
`-target_type` *cms*	jest typem bazy danych określonej przez parametr `-target`
`-label` *label*	jest etykietą certyfikatu, który ma zostać zaimportowany.
`-new_label` *label*	to etykieta, do której certyfikat zostanie przypisany w docelowej bazie danych. Jeśli opcja `-new_label` zostanie pominięta, wartością domyślną będzie użycie tej samej wartości, co opcja `-label` .

Usuwanie certyfikatu z repozytorium kluczy w systemach UNIX, Linux, and Windows

Ta procedura służy do usuwania certyfikatów osobistych lub certyfikatów CA.

Korzystanie z programu narzędziowego iKeyman

Aby zarządzać certyfikatami SSL w sposób zgodny ze standardem FIPS, należy użyć komendy runmqakm. W programie narzędziowym iKeyman nie jest dostępna opcja zgodna ze standardem FIPS.

1. Uruchom interfejs GUI programu iKeyman za pomocą komendy **strmqikm** (w systemach UNIX, Linux i Windows).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Open (Otwieranie).
3. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **CMS** (Certificate Management System - system zarządzania certyfikatami).
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, z którego ma zostać usunięty certyfikat, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy jest wyświetlana w polu **Nazwa pliku** .
8. Z listy rozwijanej wybierz opcję **Certyfikaty osobiste** lub **Certyfikaty osób podpisującego** .
9. Wybierz certyfikat, który chcesz usunąć.
10. Jeśli nie masz jeszcze kopii certyfikatu i chcesz go zapisać, kliknij opcję **Export/Import** (Eksportuj/importuj) i wyeksportuj go (patrz sekcja “Eksportowanie certyfikatu osobistego z repozytorium kluczy” na stronie 137).
11. Po wybraniu certyfikatu kliknij opcję **Usuń**. Zostanie otwarte okno Potwierdź.
12. Kliknij przycisk **Tak**. W polu **Personal Certificates** (Certyfikaty osobiste) nie jest już wyświetlana etykieta certyfikatu, który został usunięty.

Za pomocą wiersza komend

Aby usunąć certyfikat za pomocą komendy iKeycmd lub runmqakm, należy użyć następujących komend:

- W systemach UNIX, Linux i Windows:

```
runmqckm -cert -delete -db filename -pw password -label label
```

gdzie:

-db *filename*	jest pełną nazwą pliku bazy danych kluczy CMS.
-pw *password*	jest hasłem dla bazy danych kluczy CMS.
-label *label*	jest etykietą dołączoną do certyfikatu osobistego.
-fips	określa, że komenda jest uruchamiana w trybie FIPS. Ten tryb powoduje wyłączenie użycia biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Działając w trybie FIPS, komponent ICC korzysta z algorytmów, których poprawność została sprawdzona pod kątem standardu FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

Generowanie silnych haseł dla ochrony repozytorium kluczy

Za pomocą komendy **runmqakm** można generować silne hasła dla ochrony repozytorium kluczy.

Aby wygenerować silne hasło, można użyć komendy **runmqakm** z następującymi parametrami:

```
runmqakm -random -create -length 14 -strong -fips
```

W przypadku używania wygenerowanego hasła w parametrze **-pw** w kolejnych komendach administracyjnych certyfikatu należy zawsze umieszczać znaki cudzysłowu wokół hasła. W systemach UNIX and Linux należy również użyć znaku ukośnika odwrotnego w celu zmiany znaczenia następujących znaków, jeśli są one wyświetlane w łańcuchu hasła:

```
!   \   "    '
```

Podczas wprowadzania hasła w odpowiedzi na pytanie **runmqckm**, **runmqakm** lub iKeyman interfejs GUI nie jest konieczne, aby zacytować hasło ani go uniknąć. Nie jest to konieczne, ponieważ powłoki systemu operacyjnego nie mają wpływu na wprowadzanie danych w tych przypadkach.

Konfigurowanie sprzętu szyfrującego w systemach UNIX, Linux, and Windows

Sprzęt szyfrujący dla menedżera kolejek lub klienta można skonfigurować na wiele sposobów.

Sprzęt szyfrujący dla menedżera kolejek można skonfigurować w systemach UNIX, Linux lub Windows , korzystając z jednej z następujących metod:

- Użyj komendy ALTER QMGR MQSC z parametrem SSLCRYP, zgodnie z opisem w sekcji ALTER QMGR.
- Za pomocą programu IBM WebSphere MQ Explorer można skonfigurować sprzęt szyfrujący w systemie UNIX, Linux lub Windows . Więcej informacji na ten temat zawiera pomoc elektroniczna.

Sprzęt szyfrujący dla klienta WebSphere MQ można skonfigurować w systemach UNIX, Linux lub Windows przy użyciu jednej z następujących metod:

- Ustaw zmienną środowiskową MQSSLCRYP. Dozwolone wartości parametru MQSSLCRYP są takie same, jak w przypadku parametru SSLCRYP, zgodnie z opisem w sekcji ALTER QMGR. Jeśli używana jest wersja GSK_PCS11 parametru SSLCRYP, etykieta znacznika PKCS #11 musi być określona w całości w dolnej części sprawy.
- Ustaw pole **CryptoHardware** struktury opcji konfiguracji protokołu SSL (MQSCO) w wywołaniu MQCONNX. Więcej informacji na ten temat zawiera sekcja Przegląd produktu MQSCO.

Jeśli skonfigurowano sprzęt szyfrujący, który korzysta z interfejsu PKCS #11 przy użyciu dowolnej z tych metod, należy zapisać certyfikat osobisty używany na kanałach w pliku bazy danych kluczy dla skonfigurowanego znacznika szyfrującego. Jest to opisane w sekcji "Zarządzanie certyfikatami na sprzęcie PKCS #11" na stronie 144.

Zarządzanie certyfikatami na sprzęcie PKCS #11
Istnieje możliwość zarządzania certyfikatami cyfrowymi na sprzęcie szyfrującym, który obsługuje interfejs PKCS #11 .

O tym zadaniu

Bazę danych kluczy należy utworzyć w celu przygotowania środowiska produktu IBM WebSphere MQ , nawet jeśli użytkownik nie zamierza przechowywać w nim certyfikatów ośrodka certyfikacji (CA), ale będzie przechowywać wszystkie certyfikaty na sprzęcie kryptograficznym. Baza danych kluczy jest niezbędna dla menedżera kolejek w celu odwołania się do jego pola SSLKEYR lub dla aplikacji klienckiej do odwołania się w zmiennej środowiskowej MQSSLKEYR. Ta baza danych kluczy jest również wymagana, jeśli tworzone jest żądanie certyfikatu.

Bazę danych kluczy tworzy się za pomocą wiersza komend lub za pomocą interfejsu użytkownika programu **strmqikm** (iKeyman).

Procedura

Utwórz bazę danych kluczy, korzystając z wiersza komend.

1. Uruchom jedną z następujących komend:
   - W systemach UNIX, Linux, and Windows :

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Za pomocą komendy runmqakm:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
         -stash -fips -strong
     ```

   gdzie:

   -db *nazwa_pliku*
   Określa pełną nazwę pliku bazy danych kluczy CMS i musi mieć rozszerzenie pliku .kdb.

   -pw *hasło*
   Określa hasło do bazy danych kluczy CMS.

   -type *cms*
   Określa typ bazy danych. (Dla produktu IBM WebSphere MQmusi to być wartość cms.)

   -stash
   Zapisuje hasło bazy danych kluczy w pliku.

   -fips
   Wyłącza korzystanie z biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Gdy w trybie FIPS komponent ICC używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

   -silne
   Sprawdza, czy wprowadzone hasło spełnia minimalne wymagania dotyczące siły hasła. Minimalne wymagania dotyczące hasła są następujące:

   - Hasło musi mieć długość co najmniej 14 znaków.
   - Hasło musi zawierać co najmniej jedno małe litery, jedną wielką literę oraz jedną cyfrę lub znak specjalny. Do znaków specjalnych należą: gwiazdka (*), znak dolara ($), znak liczby (#) i znak procentu (%). Spacja jest sklasyfikowana jako znak specjalny.
   - Każdy znak może występować maksymalnie trzykrotnie w haśle.

- Maksymalnie dwa kolejne znaki w haśle mogą być identyczne.
- Wszystkie znaki znajdują się w standardowym zestawie znaków ASCII, ustawionym w zakresie od 0x20 do 0x7E.

Alternatywnie można utworzyć bazę danych kluczy za pomocą interfejsu użytkownika programu **strmqikm** (iKeyman).

2. W systemach UNIX and Linux zaloguj się jako użytkownik root. W systemach Windows zaloguj się jako administrator lub jako członek grupy MQM.
3. Uruchom interfejs użytkownika iKeyman , uruchamiając komendę **strmqikm** .
4. Kliknij opcję **Plik bazy danych kluczy** > **Otwórz**.
5. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **PKCS11Direct**.
6. W polu **File Name** (Nazwa pliku) wpisz nazwę modułu do zarządzania sprzętem szyfrującym, na przykład PKCS11_API.so.

   Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że iKeycmd i iKeyman są programami 64-bitowymi. Moduły zewnętrzne wymagane do obsługi standardu PKCS #11 zostaną załadowane do procesu 64-bitowego. W związku z tym wymagane jest zainstalowanie 64-bitowej biblioteki PKCS #11 na potrzeby administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ programy iKeyman i iKeycmd są 32-bitowe na tych platformach.
7. W polu **Położenie** wprowadź ścieżkę:
   - W systemach UNIX and Linux może to być na przykład /usr/lib/pksc11.
   - W systemach Windows można wpisać nazwę biblioteki, na przykład cryptoki.

   Kliknij przycisk **OK**. Zostanie otwarte okno Otwórz token szyfrujący.
8. W polu **Hasło tokenu szyfrującego** wpisz hasło, które zostało ustawione podczas konfigurowania sprzętu szyfrującego.
9. Jeśli sprzęt szyfrujący ma zdolność do przechowywania certyfikatów osoby podpisującej wymaganych do odebrania lub zaimportowania certyfikatu osobistego, należy usunąć zaznaczenie obu pól wyboru bazy danych kluczy drugorzędnych i przejść z kroku “13” na stronie 146.

   Jeśli do przechowywania certyfikatów osób podpisujących wymagana jest dodatkowa baza danych kluczy CMS, wybierz opcję **Otwórz istniejący plik bazy danych kluczy drugorzędnych** lub **Utwórz nowy plik bazy danych kluczy dodatkowych**.
10. W polu **File Name** (Nazwa pliku) wpisz nazwę pliku. To pole zawiera już tekst key.kdb. Jeśli nazwą rdzenia jest key, pozostaw to pole bez zmian. Jeśli określiłeś inną nazwę rdzenia, zastąp key nazwą macierzystą. Nie wolno zmieniać przyrostka .kdb .
11. W polu **Położenie** wpisz ścieżkę, na przykład:
    - Dla menedżera kolejek: /var/mqm/qmgrs/QM1/ssl
    - Dla klienta MQI produktu IBM WebSphere MQ : /var/mqm/ssl

    Kliknij przycisk **OK**. Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
12. Wprowadź hasło.

    Jeśli w kroku “9” na stronie 145wybrano opcję **Otwórz istniejący plik bazy danych kluczy drugorzędnych** , wpisz hasło w polu **Hasło** .

    Jeśli w kroku “9” na stronie 145wybrano opcję **Utwórz nowy plik bazy danych kluczy drugorzędnych** , wykonaj następujące kroki podrzędne:

    a) Wpisz hasło w polu **Hasło** i wpisz je ponownie w polu **Potwierdź hasło** .

    b) Wybierz opcję **Stash hasło to a file**. Należy zwrócić uwagę, że jeśli hasło nie zostanie zeskładowane, próby uruchomienia kanałów SSL nie powiodą się, ponieważ nie będą mogły uzyskać hasła wymaganego do uzyskania dostępu do pliku bazy danych kluczy.

    c) Kliknij przycisk **OK**. Zostanie otwarte okno z potwierdzeniem, że hasło znajduje się w pliku key.sth (chyba że podano inną nazwę rdzenia).

13. Kliknij przycisk **OK**. Zostanie wyświetlona ramka treści bazy danych kluczy.

Żądanie certyfikatu osobistego dla sprzętu PKCS #11
Za pomocą tej procedury można użyć menedżera kolejek lub klienta MQI produktu IBM WebSphere MQ do żądania certyfikatu osobistego dla sprzętu szyfrującego.

Korzystanie z interfejsu użytkownika iKeyman

O tym zadaniu

Uwaga: Produkt WebSphere MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami z rodziny SHA-2 .

Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są one skróconą formą odpowiednio SHA384WithRSA i SHA512WithRSA .

Procedura

Aby zażądać certyfikatu osobistego z interfejsu użytkownika iKeyman , wykonaj następujące kroki:

1. Wykonaj kroki, które należy wykonać, aby pracować ze sprzętem szyfrującym. Patrz “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 144.
2. W menu **Utwórz** kliknij opcję **Nowe żądanie certyfikatu**.

   Zostanie otwarte okno Tworzenie nowego klucza i żądania certyfikatu.
3. W polu **Key Label** (Etykieta klucza) wprowadź następujące etykiety:
   - W przypadku menedżera kolejek wpisz `ibmwebspheremq` , a następnie nazwę menedżera kolejek, który zmienił się na małe litery. Na przykład w przypadku menedżera kolejek o nazwie `QM1`należy wprowadzić wartość `ibmwebspheremqqm1`.
   - W przypadku partycji IBM WebSphere MQ MQI clientwpisz `ibmwebspheremq` , a następnie ID użytkownika logowania, wszystkie małe litery, na przykład `ibmwebspheremqmyuserid` .
4. Wprowadź wartości w polu **Nazwa zwykła** i **Organizacja**, a następnie wybierz opcję **Kraj** .
   W przypadku pozostałych pól opcjonalnych zaakceptuj wartości domyślne lub wpisz lub wybierz nowe wartości.

   Należy pamiętać, że w polu **Jednostka organizacyjna** można podać tylko jedną nazwę. Aby uzyskać więcej informacji na temat tych pól, zobacz: “Nazwy wyróżniające” na stronie 11.
5. W polu **Wprowadź nazwę pliku, w którym zostanie zapisane żądanie certyfikatu** zaakceptuj wartość domyślną `certreq.arm`lub wpisz nową wartość z pełną ścieżką.
6. Kliknij przycisk **OK**.

   Zostanie wyświetlone okno potwierdzenia.
7. Kliknij przycisk **OK**.

   Na liście **Personal Certificate Requests** (Żądania certyfikatu osobistego) wyświetlana jest etykieta utworzonego żądania certyfikatu osobistego. Żądanie certyfikatu jest przechowywane w pliku, który został wybrany w kroku “5” na stronie 146.
8. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując ten plik do formularza żądania na stronie internetowej ośrodka CA.

Za pomocą wiersza komend

Procedura

Aby zażądać certyfikatu osobistego za pomocą komendy **runmqckm** lub **runmqakm** , należy użyć następujących komend:

- Korzystanie z produktu **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -sig_alg algorithm
```

Zamiast produktu -dn *distinguished_name* można używać produktów -san_dsname *DNS_names* , -san_emailaddr *email_addresses* lub -san_ipaddr *IP_addresses* .

- Za pomocą komendy runmqakm:

```
runmqakm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -fips
        -sig_alg algorithm
```

gdzie:

-db *nazwa_pliku*
Określa pełną nazwę pliku bazy danych kluczy CMS.

-pw *hasło*
Określa hasło do bazy danych kluczy CMS.

-label *etykieta*
Określa etykietę klucza dołączoną do certyfikatu.

-dn *nazwa_wyróżniająca*
Określa nazwę wyróżniającą X.500 ujętą w podwójny cudzysłów. Wymagany jest co najmniej jeden atrybut. Można podać wiele atrybutów OU i DC.

-size *wielkość_klucza*
Określa wielkość klucza. Jeśli używany jest produkt **runmqckm** , wartość może mieć wartość 512 lub 1024. Jeśli używany jest produkt **runmqakm**, wartość może mieć wartość 512, 1024lub 2048.

-file *nazwa_pliku*
Określa nazwę pliku dla żądania certyfikatu.

-fips
określa, że komenda jest uruchamiana w trybie FIPS. Ten tryb powoduje wyłączenie użycia biblioteki kryptograficznej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Gdy w trybie FIPS komponent ICC używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

-sig_alg
W przypadku bazy danych **runmqckm**określa algorytm podpisu asymetrycznego używany do tworzenia pary kluczy pozycji. Wartość ta może mieć wartość MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA , SHA1WithRSA, SHA256_WITH_RSA, SHA256WithRSA, SHA2WithRSA, SHA384_WITH_RSA , SHA384WithRSA, SHA512_WITH_RSA , SHA512WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, lub SHAWithRSA . Wartością domyślną jest SHA1WithRSA .

-sig_alg
W przypadku bazy danych **runmqakm**określa algorytm kodowania mieszającego używany podczas tworzenia żądania certyfikatu. Ten algorytm kodowania mieszającego jest używany do tworzenia sygnatury powiązanej z nowo utworzonym żądaniem certyfikatu. Wartość ta może mieć wartość md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA , SHA_WITH_RSA, sha1, SHA1WithDSA , SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA , SHA224WithECDSA, SHA224WithRSA , sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384 , SHA384_WITH_RSA, SHA384WithECDSA , SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA , EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224 , EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 lub EC_ecdsa_with_SHA512. Wartością domyślną jest SHA1WithRSA.

-san_dnsname ***nazwy_nazw DNS***
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę nazw DNS dla tworzonej pozycji.

-san_emailaddr ***adres_e-mail***
Określa rozdzielaną przecinkami lub spacjami listę adresów e-mail dla tworzonej pozycji.

-san_ipaddr ***adres_IP***
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę adresów IP dla tworzonej pozycji.

Importowanie certyfikatu osobistego do sprzętu PKCS #11
Tej procedury należy użyć dla menedżera kolejek lub klienta MQI produktu IBM WebSphere MQ w celu zaimportowania certyfikatu osobistego do sprzętu szyfrującego.

Korzystanie z programu narzędziowego iKeyman

Procedura

Aby zażądać certyfikatu osobistego z interfejsu użytkownika iKeyman , wykonaj następujące kroki:

1. Wykonaj kroki, które należy wykonać, aby pracować ze sprzętem szyfrującym. Patrz “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 144.
2. Kliknij opcję **Odbierz**. Zostanie otwarte okno Pobierz certyfikat z pliku.
3. Wybierz opcję **Typ danych** nowego certyfikatu osobistego, na przykład `Base64-encoded ASCII data` , dla pliku z rozszerzeniem `.arm` .
4. Wpisz nazwę i położenie pliku certyfikatu dla nowego certyfikatu osobistego lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
5. Kliknij przycisk **OK**. Jeśli w bazie danych kluczy znajduje się już certyfikat osobisty, zostanie wyświetlone okno z zapytaniem o to, czy ma zostać ustawiony klucz dodawany jako klucz domyślny w bazie danych.
6. Kliknij przycisk **Tak** lub **Nie**. Zostanie otwarte okno Enter a Label (Wprowadzanie etykiety).
7. Wpisz etykietę.

   Na przykład, można użyć tej samej etykiety, co w przypadku zażądania certyfikatu osobistego. Należy pamiętać, że etykieta musi być w poprawnym formacie IBM WebSphere MQ :

   - W przypadku menedżera kolejek `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek przy użyciu małych liter. Na przykład dla menedżera kolejek o nazwie QM1etykieta będzie mieć następującą wartość: `ibmwebspheremqqm1`.
   - W przypadku klienta MQI produktu IBM WebSphere MQ `ibmwebspheremq` , a po nim identyfikator użytkownika logowania, małe litery. Na przykład dla ID użytkownika `MyUserID`etykieta będzie następująca: `ibmwebspheremqmyuserid`.
8. Kliknij przycisk **OK**. Na liście **Personal Certificates** (Certyfikaty osobiste) jest wyświetlana etykieta nowego certyfikatu osobistego, który został dodany. Etykieta ta jest tworzona przez dodanie etykiety znacznika szyfrującego przed podaną etykietą.

Za pomocą wiersza komend

Procedura

Aby zażądać certyfikatu osobistego z wiersza komend, wykonaj następujące kroki:

1. Otwórz okno komend, które jest skonfigurowane dla danego środowiska.
2. Wprowadź odpowiednią komendę dla systemu operacyjnego i konfiguracji:

   - W systemach Windowsi UNIX and Linux należy użyć jednej z następujących komend:

     ```
     runmqckm -cert -receive -file filename -crypto path
     -tokenlabel hardware_token -pw hardware_password -format cert_format
     ```

     ```
     runmqakm -cert -receive -file filename -crypto path
     ```

```
-tokenlabel hardware_token -pw hardware_password -format cert_format -fips
```

gdzie:

-file *nazwa_pliku*
Określa pełną nazwę pliku zawierającego certyfikat osobisty.

-crypto *ścieżka*
Określa pełną ścieżkę do biblioteki PKCS #11 dostarczonej wraz ze sprzętem.

-tokenlabel *znacznik_hardware_token*
Określa etykietę podaną jako część pamięci masowej sprzętu szyfrującego podczas instalacji.

-pw *hasło_magazynej_hardware_hasło*
Określa hasło dostępu do sprzętu.

-format *format_cert*
Określa format certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartością domyślną jest ASCII.

-fips
Określa, że komenda jest uruchamiana w trybie FIPS. Ten tryb wyłącza korzystanie z biblioteki szyfrującej BSafe. Używany jest tylko komponent ICC. Komponent ten musi zostać pomyślnie zainicjowany w trybie FIPS. Gdy w trybie FIPS komponent ICC używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, komenda **runmqakm** nie powiedzie się.

Identyfikowanie i uwierzytelnianie użytkowników

Użytkownik może zidentyfikować i uwierzytelnić użytkowników przy użyciu struktury MQCSP lub w kilku typach programów użytkownika obsługi wyjścia.

Korzystanie ze struktury MQCSP

Strukturę parametrów zabezpieczeń połączenia MQCSP określa się w wywołaniu MQCONNX. Struktura ta zawiera identyfikator użytkownika i hasło. Jeśli jest to konieczne, można zmienić protokół MQCSP w wyjściu zabezpieczeń.

Uwaga: Menedżer uprawnień do obiektu (Object Authority Manager-OAM) nie używa hasła. Jednak OAM wykonuje pewną ograniczoną pracę z identyfikatorem użytkownika, co może być uznane za trywialną formę uwierzytelniania. Te kontrole zatrzymują przyjęcie innego ID użytkownika, jeśli używane są te parametry w aplikacjach.

Implementowanie identyfikacji i uwierzytelniania w wyjściach zabezpieczeń

Podstawowym celem wyjścia zabezpieczeń jest włączenie agenta MCA na każdym końcu kanału w celu uwierzytelnienia jego partnera. Na każdym końcu kanału komunikatów i na końcu kanału MQI, agent MCA zwykle działa w imieniu menedżera kolejek, z którym jest połączony. Na końcu kanału MQI klienta agent MCA zwykle działa w imieniu użytkownika aplikacji klienckiej WebSphere MQ . W takiej sytuacji uwierzytelnianie wzajemne ma miejsce między dwoma menedżerami kolejek lub między menedżerem kolejek a użytkownikiem aplikacji klienckiej MQI produktu WebSphere MQ .

Dostarczone wyjście zabezpieczeń (wyjście kanału SSPI) ilustruje sposób implementowania wzajemnego uwierzytelniania przez wymianę tokenów uwierzytelniania, które są generowane, a następnie sprawdzane przez zaufany serwer uwierzytelniania, taki jak Kerberos. Szczegółowe informacje na ten temat zawiera sekcja “Program obsługi wyjścia kanału SSPI” na stronie 106.

Wzajemne uwierzytelnianie może być również realizowane za pomocą technologii Public Key Infrastructure (PKI). Każde wyjście zabezpieczeń generuje niektóre dane losowe, podpisuje je za pomocą klucza prywatnego menedżera kolejek lub użytkownika, które reprezentuje, a następnie wysyła podpisane dane do jego partnera w komunikacie bezpieczeństwa. Wyjście zabezpieczeń partnera wykonuje uwierzytelnianie, sprawdzając podpis cyfrowy przy użyciu klucza publicznego menedżera kolejek lub użytkownika. Przed wymianą podpisów cyfrowych, wyjścia zabezpieczeń mogą wymagać

uzgodnienia algorytmu generowania streszczenia komunikatów, jeśli do użycia jest dostępny więcej niż jeden algorytm.

Gdy wyjście zabezpieczeń wysyła podpisane dane do jego partnera, musi on również wysłać kilka sposobów identyfikowania menedżera kolejek lub użytkownika, który jest reprezentowany. Może to być nazwa wyróżniająca (Distinguished Name), a nawet certyfikat cyfrowy. Jeśli zostanie wysłany certyfikat cyfrowy, wyjście zabezpieczeń partnera może sprawdzić poprawność certyfikatu, pracując przez łańcuch certyfikatów w certyfikacie głównego ośrodka CA. Zapewnia to prawo własności klucza publicznego, który jest używany do sprawdzania podpisu cyfrowego.

Wyjście zabezpieczeń partnera może sprawdzać poprawność certyfikatu cyfrowego tylko wtedy, gdy ma dostęp do repozytorium kluczy, które zawiera pozostałe certyfikaty w łańcuchu certyfikatów. Jeśli certyfikat cyfrowy dla menedżera kolejek lub użytkownika nie jest wysyłany, musi być on dostępny w repozytorium kluczy, do którego ma dostęp wyjście zabezpieczeń partnera. Wyjście zabezpieczeń partnera nie może sprawdzić podpisu cyfrowego, chyba że może znaleźć klucz publiczny osoby podpisującej.

Protokół SSL (Secure Sockets Layer) i TLS (Transport Layer Security) korzystają z technik PKI, takich jak te, które zostały opisane. Więcej informacji na temat sposobu uwierzytelniania SSL i TLS można znaleźć w sekcji “Pojęcia związane z protokołem SSL (Secure Sockets Layer) i TLS (Transport Layer Security)” na stronie 15.

Jeśli zaufany serwer uwierzytelniania lub obsługa PKI nie są dostępne, można użyć innych technik. Wspólną techniką, która może być zaimplementowana w wyjściach bezpieczeństwa, używa symetryczny algorytm klucza.

Jedno z wyjść bezpieczeństwa, wyjście A, generuje losową liczbę i wysyła je w wiadomości bezpieczeństwa do swojego partnera wyjścia bezpieczeństwa, zjazd B. Wyjście B szyfruje liczbę za pomocą jej kopii klucza, który jest znany tylko z dwóch wyjść zabezpieczeń. Wyjście B wysyła zaszyfrowaną liczbę do wyjścia A w komunikacie bezpieczeństwa z drugą liczbą losową, która została wygenerowana przez wyjście B. Program obsługi wyjścia A sprawdza, czy pierwsza liczba losowa została poprawnie zaszyfrowana, szyfruje drugą liczbę losową za pomocą jej kopii klucza, a następnie wysyła zaszyfrowaną liczbę do wyjścia B w komunikacie bezpieczeństwa. Wyjdź z B, a następnie sprawdza, czy drugi losowy numer został poprawnie zaszyfrowany. Podczas tej wymiany, jeśli albo wyjście bezpieczeństwa nie jest zadowolone z autentyczności drugiego, może poinstruować agenta MCA, aby zamknie kanał.

Zaletą tej techniki jest to, że podczas wymiany nie jest wysyłany żaden klucz ani hasło. Wadą jest to, że nie stanowi on rozwiązania problemu dystrybucji klucza współużytkowanego w bezpieczny sposób. Jedno rozwiązanie tego problemu zostało opisane w sekcji “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 233. Podobną technikę używa się w SNA do wzajemnego uwierzytelniania dwóch jednostek logicznych, gdy wiążą się one z formularzem sesji. Technika ta jest opisana w podręczniku “Uwierzytelnianie na poziomie sesji” na stronie 77.

Wszystkie poprzednie techniki uwierzytelniania wzajemnego mogą być dostosowane tak, aby zapewniły uwierzytelnianie jednokierunkowe.

Implementowanie identyfikacji i uwierzytelniania w wyjściach komunikatów

Gdy aplikacja umieszcza komunikat w kolejce, pole *UserIdentifier* w deskryptorze komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Jednak nie ma danych, które mogą być używane do uwierzytelniania ID użytkownika. Dane te mogą być dodawane przez wyjście komunikatów na wysyłającym końcu kanału i sprawdzane przez wyjście komunikatu na odbierającym końcu kanału. Dane uwierzytelniające mogą być szyfrowanym hasłem lub podpisem cyfrowym, np.

Ta usługa może być bardziej efektywna, jeśli jest zaimplementowana na poziomie aplikacji. Podstawowym wymaganiem jest podanie przez użytkownika aplikacji, która odbiera komunikat, aby mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała ten komunikat. Dlatego też naturalnym jest rozważenie wdrożenia tej usługi na poziomie aplikacji. Więcej informacji na ten temat zawiera sekcja “Odwzorowywanie tożsamości w wyjściu API i wyjście funkcji API” na stronie 154.

Implementowanie identyfikacji i uwierzytelniania w wyjściu API i wyjście funkcji API

Na poziomie pojedynczego komunikatu identyfikacja i uwierzytelnianie to usługa, która obejmuje dwóch użytkowników-nadawcę i odbiorcę wiadomości. Podstawowym wymaganiem jest podanie przez użytkownika aplikacji, która odbiera komunikat, aby mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała ten komunikat. Należy pamiętać, że wymaganie dotyczy jednego sposobu, a nie dwóch sposobów uwierzytelniania.

W zależności od tego, w jaki sposób jest on zaimplementowany, użytkownicy i ich aplikacje mogą wymagać interfejsu, a nawet interakcji z usługą. Ponadto, kiedy i w jaki sposób usługa jest używana, może zależeć od tego, gdzie znajdują się użytkownicy i ich aplikacje, a także na samej naturze samych aplikacji. Dlatego też naturalnym jest rozważenie wdrożenia usługi na poziomie aplikacji, a nie na poziomie łącza.

Jeśli rozważana jest implementacja tej usługi na poziomie łącza, może być konieczne rozwiązanie takich problemów, jak:

- W przypadku kanału komunikatów, w jaki sposób można zastosować usługę tylko do tych komunikatów, które tego wymagają?
- W jaki sposób użytkownicy i ich aplikacje mogą korzystać z interfejsu lub interakcji z usługą, jeśli jest to wymaganie?
- W przypadku sytuacji w wielu przeskokach, gdzie komunikat jest wysyłany przez więcej niż jeden kanał komunikatów w drodze do miejsca docelowego, gdzie są wywoływane komponenty usługi?

Poniżej przedstawiono kilka przykładów, w jaki sposób można zaimplementować usługę identyfikacji i uwierzytelniania na poziomie aplikacji. Termin *wyjście funkcji API* oznacza wyjście funkcji API lub wyjście funkcji API.

- Gdy aplikacja umieszcza komunikat w kolejce, wyjście interfejsu API może uzyskać znacznik uwierzytelniania z zaufanego serwera uwierzytelniającego, takiego jak Kerberos. Wyjście interfejsu API może dodać ten znacznik do danych aplikacji w komunikacie. Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może poprosić serwer uwierzytelniający o uwierzytelnienie nadawcy, sprawdzając znacznik.
- Gdy aplikacja umieszcza komunikat w kolejce, wyjście interfejsu API może dopisać następujące elementy do danych aplikacji w komunikacie:
  - Certyfikat cyfrowy nadawcy
  - Podpis cyfrowy nadawcy

  Jeśli do użycia są różne algorytmy generowania streszczenia komunikatów, wyjście interfejsu API może zawierać nazwę używanego algorytmu.

  Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może wykonać następujące operacje sprawdzania:

  - Program obsługi wyjścia funkcji API może sprawdzić poprawność certyfikatu cyfrowego poprzez pracę z użyciem łańcucha certyfikatów do głównego certyfikatu ośrodka CA. Aby to zrobić, wyjście interfejsu API musi mieć dostęp do repozytorium kluczy, które zawiera pozostałe certyfikaty w łańcuchu certyfikatów. To sprawdzenie zapewnia, że nadawca, identyfikowany przez nazwę wyróżniającą, jest rzeczywistym właścicielem klucza publicznego zawartego w certyfikacie.
  - Wyjście funkcji API może sprawdzić podpis cyfrowy, korzystając z klucza publicznego zawartego w certyfikacie. To sprawdzenie uwierzytelnia nadawcę.

  Nazwa wyróżniająca nadawcy może zostać wysłana zamiast całego certyfikatu cyfrowego. W takim przypadku repozytorium kluczy musi zawierać certyfikat nadawcy, dzięki czemu drugie wyjście funkcji API może znaleźć klucz publiczny nadawcy. Inną możliwością jest wysłanie wszystkich certyfikatów w łańcuchu certyfikatów.
- Gdy aplikacja umieszcza komunikat w kolejce, pole *UserIdentifier* w deskryptorze komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Identyfikator użytkownika może być używany do identyfikowania nadawcy. Aby włączyć uwierzytelnianie, wyjście interfejsu API może dopisać niektóre

dane, takie jak zaszyfrowane hasło, do danych aplikacji w komunikacie. Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może uwierzytelnić identyfikator użytkownika przy użyciu danych, które zostały przejechanie z komunikatem.

Technika ta może być uznana za wystarczającą dla komunikatów pochodzących z kontrolowanego i zaufanego środowiska oraz w sytuacji, gdy zaufany serwer uwierzytelniania lub obsługa PKI nie jest dostępna.

Użytkownicy uprzywilejowani

Użytkownik uprzywilejowany jest użytkownikiem, który ma pełne uprawnienia administracyjne dla produktu WebSphere MQ.

Oprócz użytkowników wymienionych w poniższej tabeli, członkowie dowolnej grupy z uprawnieniem `+crt` do kolejek są pośrednio administratorami. Podobnie, każdy użytkownik, który ma uprawnienia `+set` w menedżerze kolejek, a uprawnienia `+put` w kolejce komend to administrator.

Nie należy nadawać tych uprawnień zwykłym użytkownikom i aplikacjom.

Tabela 13. Użytkownicy uprzywilejowani według platformy.

Tabela uprzywilejowanych użytkowników. W systemie Windows, SYSTEM, wszyscy członkowie grupy mqm i wszyscy członkowie grupy Administratorzy są użytkownikami uprzywilejowanymi. W systemach UNIX and Linux wszyscy członkowie grupy mqm są użytkownikami uprzywilejowanymi. W produkcie IBM iprofile (użytkownicy) qmqm i qmqmadm, wszyscy członkowie grupy qmqmadm oraz wszyscy użytkownicy zdefiniowani z ustawieniem *ALLOBJ, są użytkownikami uprzywilejowanymi.

Platforma	**Użytkownicy uprzywilejowani**
Systemy Windows	• SYSTEM • Członkowie grupy mqm • Członkowie grupy Administratorzy
Systemy UNIX and Linux	• Członkowie grupy mqm

Identyfikowanie i uwierzytelnianie użytkowników przy użyciu struktury MQCSP

W wywołaniu MQCONNX można określić strukturę parametrów zabezpieczeń połączenia MQCSP.

Struktura parametrów zabezpieczeń połączenia MQCSP zawiera identyfikator użytkownika i hasło, których usługa autoryzacji może używać do identyfikowania i uwierzytelniania użytkownika.

Komponent usługi autoryzacji dostarczany z produktem IBM WebSphere MQ jest nazywany menedżerem uprawnień do obiektów (Object Authority Manager-OAM). OAM autoryzuje użytkowników w oparciu o identyfikator zawarty w module MQCSP, ale nie sprawdza poprawności hasła. Możliwe jest zaimplementowanie sprawdzania poprawności hasła w usłudze autoryzacji za pomocą połączonych wyjść z OAM lub poprzez wymianę OAM z alternatywną usługą autoryzacji.

Protokół MQCSP można zmienić w wyjściu zabezpieczeń.

Implementowanie identyfikacji i uwierzytelniania w wyjściach zabezpieczeń

W celu zaimplementowania jednokierunkowego lub wzajemnego uwierzytelniania można użyć wyjścia zabezpieczeń.

Podstawowym celem wyjścia zabezpieczeń jest włączenie agenta MCA na każdym końcu kanału w celu uwierzytelnienia jego partnera. Na każdym końcu kanału komunikatów i na końcu kanału MQI, agent MCA zwykle działa w imieniu menedżera kolejek, z którym jest połączony. Na końcu kanału MQI klienta agent MCA zwykle działa w imieniu użytkownika aplikacji klienckiej MQI produktu WebSphere MQ .

W takiej sytuacji uwierzytelnianie wzajemne ma miejsce między dwoma menedżerami kolejek lub między menedżerem kolejek a użytkownikiem aplikacji klienckiej MQI produktu WebSphere MQ .

Dostarczone wyjście zabezpieczeń (wyjście kanału SSPI) ilustruje sposób implementowania wzajemnego uwierzytelniania przez wymianę tokenów uwierzytelniania, które są generowane, a następnie sprawdzane przez zaufany serwer uwierzytelniania, taki jak Kerberos. Szczegółowe informacje na ten temat zawiera sekcja “Program obsługi wyjścia kanału SSPI” na stronie 106.

Wzajemne uwierzytelnianie może być również realizowane za pomocą technologii Public Key Infrastructure (PKI). Każde wyjście zabezpieczeń generuje niektóre dane losowe, podpisuje je za pomocą klucza prywatnego menedżera kolejek lub użytkownika, które reprezentuje, a następnie wysyła podpisane dane do jego partnera w komunikacie bezpieczeństwa. Wyjście zabezpieczeń partnera wykonuje uwierzytelnianie, sprawdzając podpis cyfrowy przy użyciu klucza publicznego menedżera kolejek lub użytkownika. Przed wymianą podpisów cyfrowych, wyjścia zabezpieczeń mogą wymagać uzgodnienia algorytmu generowania streszczenia komunikatów, jeśli do użycia jest dostępny więcej niż jeden algorytm.

Gdy wyjście zabezpieczeń wysyła podpisane dane do jego partnera, musi on również wysłać kilka sposobów identyfikowania menedżera kolejek lub użytkownika, który jest reprezentowany. Może to być nazwa wyróżniająca (Distinguished Name), a nawet certyfikat cyfrowy. Jeśli zostanie wysłany certyfikat cyfrowy, wyjście zabezpieczeń partnera może sprawdzić poprawność certyfikatu, pracując przez łańcuch certyfikatów w certyfikacie głównego ośrodka CA. Zapewnia to prawo własności klucza publicznego, który jest używany do sprawdzania podpisu cyfrowego.

Wyjście zabezpieczeń partnera może sprawdzać poprawność certyfikatu cyfrowego tylko wtedy, gdy ma dostęp do repozytorium kluczy, które zawiera pozostałe certyfikaty w łańcuchu certyfikatów. Jeśli certyfikat cyfrowy dla menedżera kolejek lub użytkownika nie jest wysyłany, musi być on dostępny w repozytorium kluczy, do którego ma dostęp wyjście zabezpieczeń partnera. Wyjście zabezpieczeń partnera nie może sprawdzić podpisu cyfrowego, chyba że może znaleźć klucz publiczny osoby podpisującej.

Protokół SSL (Secure Sockets Layer) i TLS (Transport Layer Security) korzystają z technik PKI, takich jak te, które zostały opisane. Więcej informacji na temat sposobu uwierzytelniania przez Secure Sockets Layer zawiera sekcja “Pojęcia związane z protokołem SSL (Secure Sockets Layer) i TLS (Transport Layer Security)” na stronie 15.

Jeśli zaufany serwer uwierzytelniania lub obsługa PKI nie są dostępne, można użyć innych technik. Wspólną techniką, która może być zaimplementowana w wyjściach bezpieczeństwa, używa symetryczny algorytm klucza.

Jedno z wyjść bezpieczeństwa, wyjście A, generuje losową liczbę i wysyła je w wiadomości bezpieczeństwa do swojego partnera wyjścia bezpieczeństwa, zjazd B. Wyjście B szyfruje liczbę za pomocą jej kopii klucza, który jest znany tylko z dwóch wyjść zabezpieczeń. Wyjście B wysyła zaszyfrowaną liczbę do wyjścia A w komunikacie bezpieczeństwa z drugą liczbą losową, która została wygenerowana przez wyjście B. Program obsługi wyjścia A sprawdza, czy pierwsza liczba losowa została poprawnie zaszyfrowana, szyfruje drugą liczbę losową za pomocą jej kopii klucza, a następnie wysyła zaszyfrowaną liczbę do wyjścia B w komunikacie bezpieczeństwa. Wyjdź z B, a następnie sprawdza, czy drugi losowy numer został poprawnie zaszyfrowany. Podczas tej wymiany, jeśli albo wyjście bezpieczeństwa nie jest zadowolone z autentyczności drugiego, może poinstruować agenta MCA, aby zamknie kanał.

Zaletą tej techniki jest to, że podczas wymiany nie jest wysyłany żaden klucz ani hasło. Wadą jest to, że nie stanowi on rozwiązania problemu dystrybucji klucza współużytkowanego w bezpieczny sposób. Jedno rozwiązanie tego problemu zostało opisane w sekcji “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 233. Podobną technikę używa się w SNA do wzajemnego uwierzytelniania dwóch jednostek logicznych, gdy wiążą się one z formularzem sesji. Technika ta jest opisana w podręczniku “Uwierzytelnianie na poziomie sesji” na stronie 77.

Wszystkie poprzednie techniki uwierzytelniania wzajemnego mogą być dostosowane tak, aby zapewniły uwierzytelnianie jednokierunkowe.

Odwzorowywanie tożsamości w wyjściach komunikatów

Istnieje możliwość użycia wyjść komunikatów do przetwarzania informacji w celu uwierzytelnienia identyfikatora użytkownika, ale może być lepiej zaimplementowanie uwierzytelniania na poziomie aplikacji.

Gdy aplikacja umieszcza komunikat w kolejce, pole *UserIdentifier* w deskryptorze komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Jednak nie ma danych, które mogą być używane do uwierzytelniania ID użytkownika. Dane te mogą być dodawane przez wyjście komunikatów na wysyłającym końcu kanału i sprawdzane przez wyjście komunikatu na odbierającym końcu kanału. Dane uwierzytelniające mogą być szyfrowanym hasłem lub podpisem cyfrowym, np.

Ta usługa może być bardziej efektywna, jeśli jest zaimplementowana na poziomie aplikacji. Podstawowym wymaganiem jest podanie przez użytkownika aplikacji, która odbiera komunikat, aby mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała ten komunikat. Dlatego też naturalnym jest rozważenie wdrożenia tej usługi na poziomie aplikacji. Więcej informacji na ten temat zawiera sekcja “Odwzorowywanie tożsamości w wyjściu API i wyjście funkcji API” na stronie 154.

Odwzorowywanie tożsamości w wyjściu API i wyjście funkcji API

Aplikacja, która odbiera komunikat, musi być w stanie zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała ten komunikat. Ta usługa jest zwykle najlepiej zaimplementowana na poziomie aplikacji. Wyjścia funkcji API mogą implementować usługę na wiele sposobów.

Na poziomie pojedynczego komunikatu identyfikacja i uwierzytelnianie to usługa, która obejmuje dwóch użytkowników-nadawcę i odbiorcę wiadomości. Podstawowym wymaganiem jest podanie przez użytkownika aplikacji, która odbiera komunikat, aby mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała ten komunikat. Należy pamiętać, że wymaganie dotyczy jednego sposobu, a nie dwóch sposobów uwierzytelniania.

W zależności od tego, w jaki sposób jest on zaimplementowany, użytkownicy i ich aplikacje mogą wymagać interfejsu, a nawet interakcji z usługą. Ponadto, kiedy i w jaki sposób usługa jest używana, może zależeć od tego, gdzie znajdują się użytkownicy i ich aplikacje, a także na samej naturze samych aplikacji. Dlatego też naturalnym jest rozważenie wdrożenia usługi na poziomie aplikacji, a nie na poziomie łącza.

Jeśli rozważana jest implementacja tej usługi na poziomie łącza, może być konieczne rozwiązanie takich problemów, jak:

- W przypadku kanału komunikatów, w jaki sposób można zastosować usługę tylko do tych komunikatów, które tego wymagają?
- W jaki sposób użytkownicy i ich aplikacje mogą korzystać z interfejsu lub interakcji z usługą, jeśli jest to wymaganie?
- W przypadku sytuacji w wielu przeskokach, gdzie komunikat jest wysyłany przez więcej niż jeden kanał komunikatów w drodze do miejsca docelowego, gdzie są wywoływane komponenty usługi?

Poniżej przedstawiono kilka przykładów, w jaki sposób można zaimplementować usługę identyfikacji i uwierzytelniania na poziomie aplikacji. Termin *wyjście funkcji API* oznacza wyjście funkcji API lub wyjście funkcji API.

- Gdy aplikacja umieszcza komunikat w kolejce, wyjście interfejsu API może uzyskać znacznik uwierzytelniania z zaufanego serwera uwierzytelniającego, takiego jak Kerberos. Wyjście interfejsu API może dodać ten znacznik do danych aplikacji w komunikacie. Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może poprosić serwer uwierzytelniający o uwierzytelnienie nadawcy, sprawdzając znacznik.
- Gdy aplikacja umieszcza komunikat w kolejce, wyjście interfejsu API może dopisać następujące elementy do danych aplikacji w komunikacie:
  - Certyfikat cyfrowy nadawcy
  - Podpis cyfrowy nadawcy

Jeśli do użycia są różne algorytmy generowania streszczenia komunikatów, wyjście interfejsu API może zawierać nazwę używanego algorytmu.

Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może wykonać następujące operacje sprawdzania:

- Program obsługi wyjścia funkcji API może sprawdzić poprawność certyfikatu cyfrowego poprzez pracę z użyciem łańcucha certyfikatów do głównego certyfikatu ośrodka CA. Aby to zrobić, wyjście interfejsu API musi mieć dostęp do repozytorium kluczy, które zawiera pozostałe certyfikaty w łańcuchu certyfikatów. To sprawdzenie zapewnia, że nadawca, identyfikowany przez nazwę wyróżniającą, jest rzeczywistym właścicielem klucza publicznego zawartego w certyfikacie.
- Wyjście funkcji API może sprawdzić podpis cyfrowy, korzystając z klucza publicznego zawartego w certyfikacie. To sprawdzenie uwierzytelnia nadawcę.

Nazwa wyróżniająca nadawcy może zostać wysłana zamiast całego certyfikatu cyfrowego. W takim przypadku repozytorium kluczy musi zawierać certyfikat nadawcy, dzięki czemu drugie wyjście funkcji API może znaleźć klucz publiczny nadawcy. Inną możliwością jest wysłanie wszystkich certyfikatów w łańcuchu certyfikatów.

- Gdy aplikacja umieszcza komunikat w kolejce, pole *UserIdentifier* w deskryptorze komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Identyfikator użytkownika może być używany do identyfikowania nadawcy. Aby włączyć uwierzytelnianie, wyjście interfejsu API może dopisać niektóre dane, takie jak zaszyfrowane hasło, do danych aplikacji w komunikacie. Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może uwierzytelnić identyfikator użytkownika przy użyciu danych, które zostały przejechanie z komunikatem.

  Technika ta może być uznana za wystarczającą dla komunikatów pochodzących z kontrolowanego i zaufanego środowiska oraz w sytuacji, gdy zaufany serwer uwierzytelniania lub obsługa PKI nie jest dostępna.

Praca z odwołanymi certyfikatami

Certyfikaty cyfrowe mogą zostać odwołane przez ośrodki certyfikacji. Status unieważnienia certyfikatów można sprawdzić za pomocą protokołu OCSP lub listy CRL na serwerach LDAP, w zależności od platformy.

Podczas uzgadniania protokołu SSL komunikujący się partnerzy uwierzytelniają się nawzajem za pomocą certyfikatów cyfrowych. Uwierzytelnianie może obejmować również sprawdzanie, czy otrzymany certyfikat nadal jest zaufany. Ośrodek certyfikacji (CAs) unieważnia certyfikaty z różnych powodów, w tym:

- Właściciel przeniósł się do innej organizacji
- Klucz prywatny nie jest już niejawny

CAs publikuje unieważnione certyfikaty osobiste na liście CRL (Certificate Revocation List). Certyfikaty ośrodka CA, które zostały odwołane, są publikowane na liście odwołań do uprawnień (Authority Revocation List-ARL).

W systemach UNIX, Linux i Windows produkt WebSphere MQ SSL obsługuje sprawdzanie unieważnionych certyfikatów przy użyciu protokołu OCSP (Online Certificate Status Protocol) lub przy użyciu list CRL i ARL na serwerach LDAP (Lightweight Directory Access Protocol). Preferowaną metodą jest użycie protokołu OCSP. IBM WebSphere MQ classes for Java i IBM WebSphere MQ classes for JMS nie mogą korzystać z informacji OCSP w pliku tabeli definicji kanału klienta. Można jednak skonfigurować protokół OCSP w sposób opisany w sekcji Korzystanie z protokołu Online Certificate Protocol.

W przypadku operacji z/Os i IBM i WebSphere MQ obsługa SSL sprawdza odwołane certyfikaty, korzystając tylko z list CRL i ARL tylko na serwerach LDAP.

Więcej informacji na temat certyfikatu

Uprawnienia, patrz “certyfikaty cyfrowe” na stronie 9.

Unieważnione certyfikaty i protokół OCSP

Produkt IBM WebSphere MQ określa, który program odpowiadający OCSP (Online Certificate Status Protocol) zostanie użyty i obsługuje odebraną odpowiedź. Udostępnienie programu odpowiadającego OCSP może wymagać wykonania odpowiednich czynności.

Uwaga: Te informacje odnoszą się tylko do produktu WebSphere MQ w systemach Windows i UNIX and Linux.

Aby sprawdzić status unieważnienia certyfikatu cyfrowego za pomocą protokołu OCSP, produkt WebSphere MQ może użyć dwóch metod pozwalających na określenie modułu odpowiadającego OCSP, z którym należy się skontaktować:

- Przy użyciu rozszerzenia certyfikatu AIA (AuthorityInfoAccess) w certyfikacie, który ma zostać sprawdzony.
- Przy użyciu adresu URL określonego w obiekcie informacji uwierzytelniającej lub określonego przez aplikację kliencką.

Adres URL określony w obiekcie informacji uwierzytelniającej lub przez aplikację kliencką ma priorytet nad adresem URL w rozszerzeniu certyfikatu AIA.

Adres URL modułu odpowiadającego OCSP może wskazywać położenie znajdujące się poza firewallem. W takim przypadku należy zmienić konfigurację firewalla, aby moduł odpowiadający OCSP był dostępny, lub skonfigurować serwer proxy OCSP. Należy określić nazwę serwera proxy przy użyciu zmiennej SSLHTTPProxyName w sekcji SSL. W systemach klienckich nazwę serwera proxy można także określić, używając zmiennej środowiskowej MQSSLPROXY. Więcej szczegółów można znaleźć w informacjach pokrewnych.

Jeśli nie jest ważne, czy certyfikaty TLS lub SSL zostały odwołane (na przykład w przypadku środowiska testowego), można ustawić zmienną OCSPCheckExtensions na wartość NO w sekcji SSL. Po ustawieniu tej zmiennej wszystkie rozszerzenia certyfikatu AIA są ignorowane. To rozwiązanie raczej nie jest dopuszczalne w środowisku produkcyjnym, w którym zazwyczaj nie umożliwia się dostępu użytkownikom przedstawiającym odwołane certyfikaty.

Wywołanie mające na celu uzyskanie dostępu do modułu odpowiadającego OCSP może zwrócić jeden z następujących trzech wyników:

Dobrze
Certyfikat jest poprawny.

Odwołany
Certyfikat jest odwołany.

Nieznany
Powodem zwrócenia tego wyniku może być jedna z trzech przyczyn:

- Produkt IBM WebSphere MQ nie może uzyskać dostępu do programu odpowiadającego OCSP.
- Program odpowiadający OCSP wysłał odpowiedź, lecz produkt WebSphere MQ nie może zweryfikować podpisu cyfrowego odpowiedzi.
- Program odpowiadający OCSP wysłał odpowiedź, która wskazuje, że nie ma danych odwołania dla certyfikatu.

Jeśli produkt IBM WebSphere MQ odbierze wynik OCSP `Nieznany`, jego zachowanie zależy od ustawienia atrybutu OCSPAuthentication. W przypadku menedżerów kolejek ten atrybut znajduje się w sekcji SSL pliku `qm.ini` w systemach UNIX and Linux lub w rejestrze Windows. Można go ustawić za pomocą programu IBM WebSphere MQ Explorer. W przypadku klientów ten atrybut znajduje się w sekcji SSL pliku konfiguracyjnego klienta.

Jeśli zostanie odebrany wynik `Nieznany` i atrybut OCSPAuthentication jest ustawiony na wartość REQUIRED (domyślną), produkt WebSphere MQ odrzuci połączenie i zgłosi komunikat o błędzie typu AMQ9716. Jeśli komunikaty zdarzeń SSL w menedżerze kolejek są włączone, generowany jest komunikat zdarzenia SSL typu MQRC_CHANNEL_SSL_ERROR z opcją ReasonQualifier ustawioną na wartość MQRQ_SSL_HANDSHAKE_ERROR.

Jeśli zostanie odebrany wynik `Nieznany` i atrybut OCSPAuthentication jest ustawiony na wartość OPTIONAL, produkt WebSphere MQ zezwoli na uruchomienie kanału SSL i nie zostaną wygenerowane ostrzeżenia ani komunikaty zdarzeń SSL.

Jeśli zostanie odebrany wynik `Nieznany` i atrybut OCSPAuthentication ma ustawioną wartość WARN, kanał SSL zostanie uruchomiony, ale produkt IBM WebSphere MQ zgłosi komunikat ostrzegawczy typu AMQ9717 w dzienniku błędów. Jeśli komunikaty zdarzeń SSL w menedżerze kolejek są włączone, generowany jest komunikat zdarzenia SSL typu MQRC_CHANNEL_SSL_WARNING z opcją ReasonQualifier ustawioną na wartość MQRQ_SSL_UNKNOWN_REVOCATION.

Podpisywanie cyfrowe odpowiedzi OCSP

Moduł odpowiadający OCSP może podpisać swoje odpowiedzi, używając jednej z trzech metod. Program odpowiadający informuje o użytej metodzie.

- Odpowiedź OCSP może być podpisana cyfrowo przy użyciu tego samego certyfikatu CA, przy użyciu którego wystawiono sprawdzany certyfikat. W tym przypadku konfigurowanie dodatkowego certyfikatu nie jest wymagane. Kroki wykonane w celu nawiązania połączenia SSL wystarczają do sprawdzenia odpowiedzi OCSP.
- Odpowiedź OCSP może być podpisana cyfrowo przy użyciu innego certyfikatu podpisanego przez ten sam ośrodek certyfikacji (CA), który wystawił sprawdzany certyfikat. Certyfikat podpisujący jest w tym przypadku wysyłany razem z odpowiedzią OCSP. Certyfikat wprowadzony przez moduł odpowiadający OCSP musi mieć opcję Extended Key Usage Extension (rozszerzenie rozszerzonego użycia klucza) ustawioną na wartość `id-kp-OCSPSigning`, co umożliwia traktowanie go jako zaufanego na potrzeby tego zastosowania. Ponieważ odpowiedź OCSP jest wysyłana z certyfikatem, przy użyciu którego ją podpisano (i ten certyfikat jest podpisany przez ośrodek CA, który jest zaufany na potrzeby połączenia SSL), nie jest wymagana dodatkowa konfiguracja certyfikatu.
- Odpowiedź OCSP może być podpisana cyfrowo przy użyciu innego certyfikatu, który nie jest bezpośrednio powiązany ze sprawdzanym certyfikatem. W takim przypadku odpowiedź OCSP jest podpisana przy użyciu certyfikatu wystawionego przez sam moduł odpowiadający OCSP. Należy dodać kopię certyfikatu modułu odpowiadającego OCSP do bazy danych kluczy klienta lub menedżera kolejek, który wykonuje sprawdzenie OCSP. Patrz sekcja “Dodawanie certyfikatu ośrodka CA (lub publicznej części certyfikatu samopodpisanego) do repozytorium kluczy w systemach UNIX, Linux, and Windows” na stronie 136. Certyfikat CA jest domyślnie dodawany jako zaufany certyfikat główny, co jest ustawieniem wymaganym w tym kontekście. Jeśli ten certyfikat nie zostanie dodany, produkt WebSphere MQ nie może sprawdzić podpisu cyfrowego odpowiedzi OCSP i sprawdzenie OCSP daje wynik Nieznany, co może spowodować zamknięcie kanału przez produkt IBM WebSphere MQ w zależności od wartości atrybutu OCSPAuthentication.

Protokół Online Certificate Status Protocol (OCSP) w aplikacjach klienckich Java JMS

Z powodu ograniczeń dotyczących funkcji API języka Java produkt WebSphere MQ może używać sprawdzania unieważnienia certyfikatu przez protokół OCSP (Online Certificate Status Protocol) dla bezpiecznych gniazd SSL i TLS tylko wtedy, gdy protokół OCSP jest włączony dla całego procesu maszyny JVM. Istnieją dwa sposoby włączenia protokołu OCSP dla wszystkich bezpiecznych gniazd w maszynie JVM:

- Wprowadzenie zmian w pliku java.security środowiska JRE w celu włączenia do niego ustawień konfiguracyjnych protokołu OCSP pokazanych w tabeli 1 i zrestartowanie aplikacji.
- Użycie funkcji API java.security.Security.setProperty() podporządkowanej dowolnej obowiązującej strategii menedżera zabezpieczeń Java.

Minimalnie należy określić jedną z dwóch wartości ocsp.enable lub ocsp.responderURL.

Nazwa właściwości	Opis
ocsp.enable	Ta właściwość ma wartość `true` (prawda) lub `false` (fałsz). Jeśli właściwość ma wartość `true` (prawda), podczas sprawdzania unieważnień certyfikatu sprawdzanie OCSP jest włączone. Jeśli

Nazwa właściwości	Opis
	właściwość ma wartość `false` (fałsz) lub nie jest ustawiona, sprawdzanie OCSP jest wyłączone.
ocsp.responderURL	Wartość tej właściwości określa adres URL identyfikujący położenie modułu odpowiadającego OCSP. Poniżej przedstawiono przykład: `ocsp.responderURL=http://ocsp.example.net:80`. Domyślnie położenie modułu odpowiadającego OCSP jest określane w sposób niejawny na podstawie certyfikatu, którego poprawność jest sprawdzana. Ta właściwość jest używana w przypadku braku w certyfikacie rozszerzenia Authority Information Access (zdefiniowanego w dokumencie RFC 3280) lub wtedy, gdy wymaga ono zastąpienia.
ocsp.responderCertSubjectName	Wartość tej właściwości jest nazwą podmiotu certyfikatu modułu odpowiadającego OCSP. Poniżej przedstawiono przykład: `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Domyślnie certyfikat modułu odpowiadającego OCSP jest certyfikatem wystawcy certyfikatu, którego poprawność jest sprawdzana. Ta właściwość określa certyfikat modułu odpowiadającego OCSP, gdy wartość domyślna nie ma zastosowania. Wartością jest nazwa wyróżniająca w postaci łańcucha (zdefiniowana w dokumencie RFC 2253), która identyfikuje certyfikat w zestawie certyfikatów dostarczonych podczas sprawdzania poprawności ścieżki certyfikatu. W przypadku, gdy sama nazwa podmiotu nie jest wystarczająca do jednoznacznego zidentyfikowania certyfikatu, zamiast tej właściwości należy użyć obu właściwości ocsp.responderCertIssuerName i ocsp.responderCertSerialNumber. Gdy ta właściwość jest ustawiona, właściwości ocsp.responderCertIssuerName i ocsp.responderCertSerialNumber są ignorowane.
ocsp.responderCertIssuerName	Wartość tej właściwości jest nazwą wystawcy certyfikatu modułu odpowiadającego OCSP. Poniżej przedstawiono przykład: `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Domyślnie certyfikat modułu odpowiadającego OCSP jest certyfikatem wystawcy certyfikatu, którego poprawność jest sprawdzana. Ta właściwość określa certyfikat modułu odpowiadającego OCSP, gdy wartość domyślna nie ma zastosowania. Wartością jest nazwa wyróżniająca w postaci łańcucha (zdefiniowana w dokumencie RFC 2253), która identyfikuje certyfikat w zestawie certyfikatów dostarczonych podczas sprawdzania poprawności ścieżki certyfikatu. Jeśli ta właściwość jest ustawiona, musi być również ustawiona właściwość ocsp.responderCertSerialNumber. Gdy ustawiona jest właściwość ocsp.responderCertSubjectName, ta właściwość jest ignorowana.
ocsp.responderCertSerialNumber	Wartość tej właściwości jest numerem seryjnym certyfikatu modułu odpowiadającego OCSP. Poniżej przedstawiono przykład: `ocsp.responderCertSerialNumber=2A:FF:00`. Domyślnie certyfikat modułu odpowiadającego OCSP jest certyfikatem wystawcy certyfikatu, którego poprawność jest sprawdzana. Ta właściwość określa certyfikat modułu odpowiadającego OCSP, gdy wartość domyślna nie ma zastosowania. Wartość to jest łańcuchem cyfr szesnastkowych (jako separatory dozwolone są dwukropki i spacje) identyfikującym certyfikat w zestawie certyfikatów dostarczonych podczas sprawdzania poprawności ścieżki certyfikatów. Jeśli ta właściwość jest ustawiona, musi

Nazwa właściwości	Opis
	być również ustawiona właściwość ocsp.responderCertIssuerName. Gdy ustawiona jest właściwość ocsp.responderCertSubjectName, ta właściwość jest ignorowana.

Przed włączeniem protokołu OCSP w przedstawiony sposób należy wziąć pod uwagę następujące zagadnienia:

- Ustawienie konfiguracji OCSP ma wpływ na wszystkie bezpieczne gniazda w procesie maszyny JVM. W niektórych przypadkach ta konfiguracja może mieć niepożądane efekty uboczne, gdy maszyna JVM jest współużytkowana z kodem innej aplikacji korzystającym z bezpiecznych gniazd SSL lub TLS. Należy upewnić się, że wybrana konfiguracja OCSP jest odpowiednia dla wszystkich aplikacji działających na tej samej maszynie JVM.
- Podczas konserwacji środowiska JRE plik java.security może zostać nadpisany. Należy uważać podczas stosowania poprawek tymczasowych i konserwacji produktu, aby nie dopuścić do nadpisania pliku java.security. Może być konieczne ponowne wprowadzenie zmian w pliku java.security po zastosowaniu konserwacji. Z tej przyczyny można rozważyć ustawienie konfiguracji protokołu OCSP za pomocą funkcji API java.security.Security.setProperty().
- Włączenie sprawdzania OCSP ma zastosowanie tylko wtedy, gdy włączone jest również sprawdzanie unieważniania. Sprawdzanie unieważniania jest włączane za pomocą metody `PKIXParameters.setRevocationEnabled()`.
- W przypadku używania opisanego w sekcji Włączanie sprawdzania OCSP w przechwytywaczach rodzimych przechwytywacza języka Java produktu AMS należy unikać używania konfiguracji OCSP java.security, która powoduje konflikt z konfiguracją OCSP produktu AMS w pliku konfiguracyjnym magazynu kluczy.

Praca z listami odwołań certyfikatów i listami odwołań uprawnień

WebSphere MQ's support for CRLs and ARLs varies by platform.

Obsługa CRL i ARL na każdej platformie jest następująca:

- W systemie z/OSSystem SSL obsługuje listy CRL i ARL przechowywane na serwerach LDAP przez produkt Tivoli Public Key Infrastructure.
- Na innych platformach obsługa CRL i ARL jest zgodna z rekomendacjami profilu CRL PKIX X.509 V2 .

Produkt WebSphere MQ obsługuje pamięć podręczną list CRL i ARL, do których dostęp uzyskano w ciągu ostatnich 12 godzin.

Gdy menedżer kolejek lub klient MQI produktu WebSphere MQ odbiera certyfikat, sprawdza listę CRL, aby potwierdzić, że certyfikat jest nadal ważny. Produkt WebSphere MQ sprawdza najpierw w pamięci podręcznej, jeśli istnieje pamięć podręczna. Jeśli lista CRL nie znajduje się w pamięci podręcznej, produkt WebSphere MQ interroguje położenia serwera CRL LDAP w kolejności, w jakiej występują na liście nazw obiektów informacji uwierzytelniających określonych za pomocą atrybutu *SSLCRLNamelist* , do momentu znalezienia przez produkt WebSphere MQ dostępnej listy CRL. Jeśli lista nazw nie jest określona lub jest określona z pustą wartością, listy CRL nie są sprawdzane.

Więcej informacji na temat protokołu LDAP zawiera sekcja Korzystanie z usług protokołu dostępu do katalogu uproszczonego w produkcie WebSphere MQ dla systemu Windows.

Konfigurowanie serwerów LDAP

Skonfiguruj strukturę drzewa informacji katalogu LDAP w taki sposób, aby odzwierciedlała hierarchię nazw wyróżniających CAs. W tym celu należy użyć plików LDAP Data Interchange Format.

Skonfiguruj strukturę drzewa informacji katalogu LDAP (DIT) w taki sposób, aby używała hierarchii odpowiadającej nazwie wyróżniającej CAs, które wystawiają certyfikaty i listy CRL. Strukturę DIT można skonfigurować przy użyciu pliku, który korzysta z formatu LDIF (LDAP Data Interchange Format). W celu zaktualizowania katalogu można również użyć plików LDIF.

Pliki LDIF to pliki tekstowe ASCII, które zawierają informacje wymagane do zdefiniowania obiektów w katalogu LDAP. Pliki LDIF zawierają co najmniej jeden wpis, z których każdy składa się z nazwy wyróżniającej, co najmniej jednej definicji klasy obiektu oraz, opcjonalnie, wielu definicji atrybutów.

Atrybut `certificateRevocationList;binary` zawiera listę, w postaci binarnej, unieważnionych certyfikatów użytkownika. Atrybut `authorityRevocationList;binary` zawiera binarną listę certyfikatów CA, które zostały odwołane. W przypadku korzystania z protokołu SSL w produkcie WebSphere MQ dane binarne dla tych atrybutów muszą być zgodne z formatem DER (Definite Encoding Rules-Definitowe reguły kodowania). Więcej informacji na temat plików LDIF znajduje się w dokumentacji dostarczonej wraz z serwerem LDAP.

Rysunek 12 na stronie 160 przedstawia przykładowy plik LDIF, który można utworzyć jako dane wejściowe dla serwera LDAP w celu załadowania list CRL i ARL wydawanych przez CA1, który jest wyimaginowanym Certyfikatem Ośrodka o nazwie wyróżniającej "CN=CA1, OU=Test, O=IBM, C=GB", utworzonego przez organizację testową w IBM.

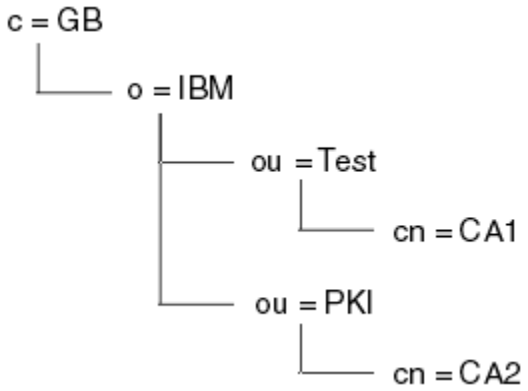
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

dn: ou=Test, o=IBM, c=GB
ou: Test
objectclass: organizationalUnit

dn: cn=CA1, ou=Test, o=IBM, c=GB
cn: CA1
objectclass: cRLDistributionPoint
objectclass: certificateAuthority
authorityRevocationList;binary:: (DER format data)
certificateRevocationList;binary:: (DER format data)
caCertificate;binary:: (DER format data)
```

Rysunek 12. Przykładowy plik LDIF dla ośrodka certyfikacji. Może to różnić się od implementacji do implementacji.

Rysunek 13 na stronie 160 przedstawia strukturę DIT, która jest tworzona przez serwer LDAP podczas ładowania przykładowego pliku LDIF, który jest wyświetlany w programie Rysunek 12 na stronie 160 , razem z podobnym plikiem dla CA2, wyimaginowanym uprawnionym certyfikatem ustawionym przez organizację PKI, także w IBM.



Rysunek 13. Przykład struktury drzewa informacji katalogu LDAP

Produkt WebSphere MQ sprawdza zarówno listy CRL, jak i listy ARL.

Uwaga: Upewnij się, że lista kontroli dostępu dla serwera LDAP pozwala autoryzowanym użytkownikom na odczytywanie, wyszukiwanie i porównywanie pozycji, które przechowują listy CRL i ARL. Produkt WebSphere MQ uzyskuje dostęp do serwera LDAP przy użyciu właściwości LDAPUSER i LDAPPWD obiektu AUTHINFO.

Konfigurowanie i aktualizowanie serwerów LDAP
Ta procedura służy do konfigurowania lub aktualizowania serwera LDAP.

1. Uzyskaj listy CRL i ARL w formacie DER z poziomu ośrodka certyfikacji lub uprawnień.
2. Za pomocą edytora tekstu lub narzędzia udostępnionego wraz z serwerem LDAP należy utworzyć jeden lub więcej plików LDIF, które zawierają nazwę wyróżniającą ośrodka CA i wymagane definicje klas obiektów. Skopiuj dane formatu DER do pliku LDIF jako wartości atrybutu `certificateRevocationList;binary` dla list CRL, atrybutu `authorityRevocationList;binary` dla list ARL lub obu tych wartości.
3. Uruchom serwer LDAP.
4. Dodaj wpisy z pliku LDIF lub plików utworzonych w kroku “2” na stronie 161.

Po skonfigurowaniu serwera CRL LDAP należy sprawdzić, czy jest on poprawnie skonfigurowany. Najpierw spróbuj użyć certyfikatu, który nie jest odwołany w kanale, i sprawdź, czy kanał jest uruchamiany poprawnie. Następnie należy użyć certyfikatu, który został unieważniony, i sprawdzić, czy uruchomienie kanału nie powiodło się.

Należy często uzyskiwać zaktualizowane listy CRL z ośrodków certyfikacji. Co 12 godzin należy rozważyć wykonanie tego działania na serwerach LDAP.

Uzyskiwanie dostępu do list CRL i ARL z menedżerem kolejek

Menedżer kolejek jest powiązany z jednym lub większą liczbę obiektów informacji uwierzytelniających, które przechowują adres serwera CRL LDAP.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation Lists-CRL) mają zastosowanie także do list odwołań uprawnień (Authority Revocation Lists-ARL).

Menedżer kolejek określa sposób uzyskiwania dostępu do list CRL przez podanie menedżera kolejek z obiektami informacji uwierzytelniających, z których każdy zawiera adres serwera CRL LDAP. Obiekty informacji uwierzytelniającej znajdują się na liście nazw, która jest określona w atrybucie menedżera kolejek *SSLCRLNamelist* .

W poniższym przykładzie do określenia parametrów używany jest program MQSC:

1. Zdefiniuj obiekty informacji uwierzytelniających za pomocą komendy MQSC DEFINE AUTHINFO z parametrem AUTHTYPE ustawionym na CRLLDAP.

   Wartość CRLLDAP dla parametru AUTHTYPE wskazuje, że dostęp do list CRL jest uzyskiwany na serwerach LDAP. Każdy obiekt informacji uwierzytelniającej o typie CRLLDAP, który jest tworzony, przechowuje adres serwera LDAP. Jeśli istnieje więcej niż jeden obiekt informacji uwierzytelniających, serwery LDAP, do których one wskazują *muszą* , zawierają identyczne informacje. Zapewnia to ciągłość usługi, jeśli jeden lub więcej serwerów LDAP nie powiedzie się.

   Na wszystkich platformach identyfikator użytkownika i hasło są wysyłane do serwera LDAP bez szyfrowania.
2. Korzystając z komendy MQSC DEFINE NAMELIST, zdefiniuj listę nazw dla nazw obiektów informacji uwierzytelniających.
3. Używając komendy ALTER QMGR MQSC, podaj listę nazw do menedżera kolejek. Na przykład:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   gdzie `sslcrlnlname` to lista nazw obiektów informacji uwierzytelniającej.

   Ta komenda ustawia atrybut menedżera kolejek o nazwie *SSLCRLNamelist*. Wartość początkowa menedżera kolejek dla tego atrybutu jest pusta.

Do listy nazw można dodać maksymalnie 10 połączeń z alternatywnymi serwerami LDAP, aby zapewnić ciągłość usługi, jeśli jeden lub więcej serwerów LDAP ulegnie awarii. Należy pamiętać, że serwery LDAP *muszą* zawierać identyczne informacje.

Uzyskiwanie dostępu do list CRL i ARL za pomocą programu IBM WebSphere MQ Explorer
Za pomocą programu IBM WebSphere MQ Explorer można określić, w jaki sposób menedżer kolejek ma dostęp do list CRL.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation Lists-CRL) mają zastosowanie także do list odwołań uprawnień (Authority Revocation Lists-ARL).

Aby skonfigurować połączenie LDAP do listy CRL, należy wykonać następującą procedurę:

1. Upewnij się, że menedżer kolejek został uruchomiony.
2. Kliknij prawym przyciskiem myszy folder **Informacje o uwierzytelnianiu** , a następnie kliknij opcję **Nowy-> Informacje o uwierzytelnianiu**. W arkuszu właściwości, który jest otwierany:
   a. Na pierwszej stronie **Create Authentication Information** (Utwórz informacje o uwierzytelnianiu) wprowadź nazwę dla obiektu CRL (LDAP).
   b. Na stronie **Ogólne** w obszarze **Zmień właściwości**wybierz typ połączenia. Opcjonalnie można wprowadzić opis.
   c. Wybierz stronę **CRL (LDAP)** (CRL) w obszarze **Change Properties**(Zmień właściwości).
   d. Wprowadź nazwę serwera LDAP jako nazwę sieciową lub adres IP.
   e. Jeśli serwer wymaga podania danych logowania, podaj identyfikator użytkownika i, jeśli to konieczne, hasło.
   f. Kliknij przycisk **OK**.
3. Kliknij prawym przyciskiem myszy folder **Listy nazw** , a następnie kliknij opcję **Nowy-> Lista nazw** . W arkuszu właściwości, który jest otwierany:
   a. Wpisz nazwę listy nazw.
   b. Dodaj nazwę obiektu CRL (LDAP) (z kroku “2.a” na stronie 162) do listy.
   c. Kliknij przycisk **OK**.
4. Kliknij prawym przyciskiem myszy menedżer kolejek, wybierz opcję **Właściwości**, a następnie wybierz stronę **SSL** :
   a. Zaznacz pole wyboru **Sprawdź certyfikaty odebrane przez tego menedżera kolejek na podstawie list odwołań certyfikatów** .
   b. W polu **Lista nazw CRL** wpisz nazwę listy nazw (z kroku “3.a” na stronie 162).

Uzyskiwanie dostępu do list CRL i ARL za pomocą klienta MQI produktu IBM WebSphere MQ
Dostępne są trzy opcje określania serwerów LDAP, które przechowują listy CRL w celu sprawdzenia przez klienta MQI produktu IBM WebSphere MQ .

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation Lists-CRL) mają zastosowanie także do list odwołań uprawnień (Authority Revocation Lists-ARL).

Następujące trzy sposoby określania serwerów LDAP są następujące:

- Korzystanie z tabeli definicji kanału
- Korzystanie z struktury opcji konfiguracji protokołu SSL, MQSCO, w wywołaniu MQCONNX
- Korzystanie z Active Directory (w systemach Windows z obsługą Active Directory)

Więcej szczegółowych informacji można znaleźć w sekcji informacji pokrewnych.

Można uwzględnić maksymalnie 10 połączeń z alternatywnymi serwerami LDAP, aby zapewnić ciągłość usługi, jeśli jeden lub więcej serwerów LDAP ulegnie awarii. Należy pamiętać, że serwery LDAP *muszą* zawierać identyczne informacje.

Nie można uzyskać dostępu do list CRL LDAP z kanału klienta MQI produktu WebSphere MQ działającego na serwerze Linux (platforma zSeries).

Położenie respondera OCSP i serwerów LDAP, które przechowują listy CRL
W systemie klienta MQI produktu IBM WebSphere MQ można określić położenie respondera OCSP oraz serwerów LDAP (Lightweight Directory Access Protocol), które przechowują listy odwołań certyfikatów (CRL).

Te lokalizacje można określić na trzy sposoby, wymienione tutaj, w kolejności malejącej kolejności wykonywania.

Gdy aplikacja kliencka MQI produktu WebSphere MQ wysyła wywołanie MQCONNX

Istnieje możliwość określenia modułu odpowiadającego OCSP lub serwera LDAP, który posiada listy CRL w wywołaniu **MQCONNX** .

W wywołaniu **MQCONNX** struktura opcji łączenia, MQCNO, może odwoływać się do struktury opcji konfiguracji protokołu SSL, MQSCO. Z kolei struktura MQSCO może odwoływać się do jednej lub większej liczby struktur rekordu informacji uwierzytelniających, MQAIR. Każda struktura MQAIR zawiera wszystkie informacje, których klient MQI produktu WebSphere MQ wymaga uzyskania dostępu do programu odpowiadającego OCSP lub serwera LDAP, który posiada listy CRL. Na przykład jednym z pól w strukturze MQAIR jest adres URL, z którym można skontaktować się z responderem. Więcej informacji na temat struktury MQAIR zawiera sekcja MQAIR-rekord informacji o uwierzytelnianiu.

Korzystanie z tabeli definicji kanału klienta (ccdt) w celu uzyskania dostępu do serwerów odpowiadających za pomocą protokołu OCSP lub serwera LDAP

Aby klient MQI produktu WebSphere MQ mógł uzyskać dostęp do serwerów odpowiadających za pomocą protokołu OCSP lub serwera LDAP, w których znajdują się listy CRL, należy dołączyć atrybuty jednego lub większej liczby obiektów informacji uwierzytelniających w tabeli definicji kanału klienta.

W menedżerze kolejek serwera można zdefiniować jeden lub więcej obiektów informacji uwierzytelniających. Atrybuty obiektu uwierzytelniającego zawierają wszystkie informacje wymagane do uzyskania dostępu do modułu odpowiadającego OCSP (na platformach, na których jest obsługiwany protokół OCSP) lub serwera LDAP, który zawiera listy CRL. Jeden z atrybutów określa adres URL programu odpowiadającego OCSP, inny określa adres hosta lub adres IP systemu, na którym działa serwer LDAP.

Obiekt informacji uwierzytelniającej o typie AUTHTYPE (OCSP) nie jest stosowany do użycia w menedżerach kolejek systemu IBM i lub z/OS , ale można go określić na tych platformach, które mają być skopiowane do tabeli definicji kanału klienta (CCDT) w celu użycia klienta.

Aby umożliwić klientowi MQI produktu WebSphere MQ dostęp do serwerów odpowiadających za pomocą protokołu OCSP lub serwera LDAP, w których są przechowywane listy CRL, atrybuty jednego lub większej liczby obiektów informacji uwierzytelniających mogą być zawarte w tabeli definicji kanału klienta. Istnieje możliwość uwzględnienia takich atrybutów w jeden z następujących sposobów:

Na platformach serwerowych AIX, HP-UX, Linux, Solaris i Windows

Istnieje możliwość zdefiniowania listy nazw zawierającej nazwy jednego lub większej liczby obiektów informacji uwierzytelniających. Następnie można ustawić atrybut menedżera kolejek (**SSLCRLNameList**) na nazwę tej listy nazw.

Jeśli używane są listy CRL, można skonfigurować więcej niż jeden serwer LDAP, aby zapewnić wyższą dostępność. Zamiarem jest to, że każdy serwer LDAP przechowuje te same listy CRL. Jeśli jeden serwer LDAP nie jest dostępny, jeśli jest wymagany, klient MQI produktu WebSphere MQ może podjąć próbę uzyskania dostępu do innego serwera.

Atrybuty obiektów informacji uwierzytelniających identyfikowanych przez listę nazw są określane wspólnie tutaj jako *położenie odwołania certyfikatu*. Po ustawieniu atrybutu menedżera kolejek, **SSLCRLNameList**, na nazwę listy nazw, położenie odwołania certyfikatu jest kopiowane do tabeli definicji kanału klienta powiązanej z menedżerem kolejek. Jeśli dostęp do tabeli CCDT można uzyskać z systemu klienta jako współużytkowanego pliku lub jeśli w systemie klienta jest kopiowana aplikacja CCDT, klient MQI produktu WebSphere MQ w tym systemie może użyć położenia odwołania do certyfikatu w tabeli definicji kanału klienta w celu uzyskania dostępu do serwerów odpowiadających za pomocą protokołu OCSP lub serwera LDAP, które zawierają listy CRL.

Jeśli położenie odwołania do certyfikatu menedżera kolejek zostanie później zmienione, zmiana zostanie odzwierciedlona w tabeli definicji kanału klienta powiązanej z menedżerem kolejek. Jeśli atrybut menedżera kolejek **SSLCRLNameList**jest ustawiony na wartość pustą, położenie odwołania do certyfikatu jest usuwane z tabeli definicji kanału klienta. Zmiany te nie są odzwierciedlane w żadnej kopii tabeli w systemie klienckim.

Jeśli wymagane jest, aby położenie odwołania certyfikatu na kliencie i na serwerze końców kanału MQI było inne, a menedżer kolejek serwera jest tym, który jest używany do tworzenia położenia odwołania certyfikatu, można wykonać następujące czynności:

1. W menedżerze kolejek serwera utwórz położenie odwołania do certyfikatu, które ma być używane w systemie klienckim.
2. Skopiuj tabelę CCDT zawierającą położenie odwołania certyfikatu do systemu klienta.
3. W menedżerze kolejek serwera zmień położenie odwołania certyfikatu na wartość wymaganą na końcu serwera kanału MQI.

Korzystanie z Active Directory w systemie Windows

W systemach Windows można użyć komendy sterującej **setmqcrl** w celu opublikowania informacji o bieżącej liście CRL w Active Directory.

Komenda **setmqcrl** nie publikuje informacji OCSP.

Więcej informacji na temat tej komendy i jej składni zawiera sekcja setmqcrl.

Uzyskiwanie dostępu do list CRL i ARL z klasami produktu IBM WebSphere MQ dla klas Java i IBM WebSphere MQ dla usługi JMS

Klasy IBM WebSphere MQ classes for Java i IBM WebSphere MQ classes for JMS uzyskują dostęp do list CRL w inny sposób niż w przypadku innych platform.

Informacje na temat pracy z listami CRL i ARL z klasami IBM WebSphere MQ dla języka Java zawiera sekcja Korzystanie z list odwołań certyfikatów.

Więcej informacji na temat pracy z listami CRL i ARL z klasami IBM WebSphere MQ dla usługi JMS zawiera sekcja Właściwość obiektu SSLCERTSTORES.

Manipulowanie obiektami informacji uwierzytelniających

Obiekty informacji uwierzytelniających można manipulować za pomocą komend MQSC lub PCF, lub IBM WebSphere MQ Explorer.

Następujące komendy MQSC działają na obiektach informacji uwierzytelniających:

- DEFINE AUTHINFO
- ALTER AUTHINFO
- USUŃ INFORMACJE O AUTORYZACJI
- WYŚWIETLENIE INFORMACJI UWIERZYTELNIAJĄCYCH

Pełny opis tych komend można znaleźć w sekcji Komendy skryptowe (MQSC) .

Następujące komendy programu Programmable Command Format (PCF) działają na obiektach informacji uwierzytelniających:

- Tworzenie informacji uwierzytelniających
- Kopiowanie informacji uwierzytelniających
- Zmień informacje uwierzytelniające
- Usuń informacje uwierzytelniające
- Sprawdzanie informacji uwierzytelniających
- Sprawdź nazwy informacji uwierzytelniających

Pełny opis tych komend znajduje się w sekcji Definicje formatów komend programowalnych .

Na platformach, na których jest ona dostępna, można również użyć programu WebSphere MQ Explorer.

Autoryzowanie dostępu do obiektów

Ta sekcja zawiera informacje na temat korzystania z menedżera uprawnień do obiektów i programów obsługi wyjścia kanału w celu kontrolowania dostępu do obiektów.

W systemach UNIX, Linux, and Windows . sterowanie dostępem do obiektów za pomocą menedżera uprawnień do obiektów (Object Authority Manager-OAM). Ta kolekcja tematów zawiera informacje na temat korzystania z interfejsu komend do OAM. Zawiera on również listę kontrolną, której można użyć do określenia zadań, które należy wykonać w celu zastosowania zabezpieczeń w systemie, a także uwagi dotyczące nadawania użytkownikom uprawnień do administrowania produktem IBM WebSphere MQ oraz do pracy z obiektami IBM WebSphere MQ . Jeśli dostarczone mechanizmy bezpieczeństwa nie spełniają Twoich potrzeb, można opracować własne programy obsługi wyjścia kanału.

Sterowanie dostępem do obiektów za pomocą OAM w systemach UNIX, Linux i Windows

Menedżer uprawnień do obiektów (Object Authority Manager-OAM) udostępnia interfejs komend do nadawania i odwoływania uprawnień do obiektów WebSphere MQ .

Użytkownik musi mieć odpowiednie uprawnienia do korzystania z tych komend, zgodnie z opisem w sekcji “Uprawnienie do administrowania produktem IBM WebSphere MQ w systemach UNIX, Linux, and Windows” na stronie 204. Identyfikatory użytkowników, którzy są uprawnieni do administrowania produktem WebSphere MQ , mają uprawnienia *super user* do menedżera kolejek, co oznacza, że nie trzeba nadawać im dalszych uprawnień do wydawania żadnych żądań MQI lub komend.

Nadawanie dostępu do obiektu IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Aby nadać użytkownikom i grupom użytkowników dostęp do obiektów produktu IBM WebSphere MQ , należy użyć komendy sterującej **setmqaut** lub komendy PCF produktu **MQCMD_SET_AUTH_REC** .

Pełną definicję komendy sterującej **setmqaut** i jej składnię można znaleźć w sekcji setmqaut, a w celu uzyskania pełnej definicji komendy **MQCMD_SET_AUTH_REC** PCF i jej składni można znaleźć w sekcji Ustawianie rekordu uprawnień.

Aby można było użyć tej komendy, menedżer kolejek musi być uruchomiony. Po zmianie dostępu do nazwy użytkownika zmiany są uwzględniane natychmiast przez OAM.

Aby nadać użytkownikom dostęp do obiektu, należy określić:

- Nazwa menedżera kolejek, który jest właścicielem obiektów, z którymi pracuje użytkownik. Jeśli nie zostanie określona nazwa menedżera kolejek, zostanie przyjęty domyślny menedżer kolejek.
- Nazwa i typ obiektu (w celu jednoznacznego zidentyfikowania obiektu). Nazwę należy określić jako *profil*. Jest to jawna nazwa obiektu lub nazwa ogólna, w tym znaki wieloznaczne. Szczegółowy opis ogólnych profili oraz użycie znaków wieloznacznych w tych profilach zawiera sekcja “Korzystanie z profili ogólnych OAM w systemach UNIX, Linux, and Windows” na stronie 166.
- Jeden lub większa liczba nazw użytkowników i grup, do których ma zastosowanie uprawnienie.

  Jeśli ID użytkownika zawiera spacje, należy go ująć w znaki cudzysłowu przy użyciu tej komendy. W systemach Windows użytkownik może kwalifikować się do identyfikatora użytkownika z nazwą domeny. Jeśli rzeczywisty identyfikator użytkownika zawiera symbol at (@), zastąp go znakiem @ @, aby pokazać, że jest to część identyfikatora użytkownika, a nie ogranicznik między identyfikatorem użytkownika i nazwą domeny.
- Lista autoryzacji. Każdy element na liście określa typ dostępu, który ma zostać nadany temu obiektowi (lub odebrany z niego). Każda autoryzacja na liście jest określona jako słowo kluczowe, poprzedzona znakiem plus (+) lub znakiem minus (-). Użyj znaku plus, aby dodać określoną autoryzację, oraz

znak minus, aby usunąć autoryzację. Między znakiem + lub-znakiem i słowem kluczowym nie może występować spacje.

W jednej komendzie można określić dowolną liczbę autoryzacji. Na przykład lista autoryzacji zezwalających użytkownikowi lub grupie na umieszczanie komunikatów w kolejce i przeglądanie ich, ale w celu odebrania dostępu do pobierania komunikatów jest następująca:

```
    +browse -get +put
```

Przykłady użycia komendy setmqaut

W poniższych przykładach przedstawiono sposób użycia komendy `setmqaut` do nadawania i odbierania uprawnień do korzystania z obiektu:

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
         -g groupa +browse -get +put
```

W tym przykładzie:

- `saturn.queue.manager` jest nazwą menedżera kolejek
- `queue` jest typem obiektu
- `RED.LOCAL.QUEUE` jest nazwą obiektu
- `groupa` to identyfikator grupy z autoryzacjami, które mają zostać zmienione.
- `+browse -get +put` to lista autoryzacji dla podanej kolejki.
  - Program `+browse` dodaje autoryzację do przeglądania komunikatów w kolejce (do wydania **MQGET** za pomocą opcji przeglądania)
  - `-get` usuwa autoryzację do pobierania komunikatów (**MQGET**) z kolejki.
  - `+put` dodaje autoryzację do umieszczania (**MQPUT**) komunikatów w kolejce.

Poniższa komenda odbiera uprawnienie do umieszczania w kolejce MyQueue z głównego użytkownika fvuser oraz z grup groupa i groupb. W systemach UNIX and Linux ta komenda odbiera także uprawnienia do umieszczania uprawnień dla wszystkich użytkowników w tej samej grupie podstawowej, co użytkownik fvuser.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
         -g groupa -g groupb -put
```

Korzystanie z komendy z inną usługą autoryzacji

Jeśli korzystasz z własnej usługi autoryzacji zamiast OAM, możesz podać nazwę tej usługi w komendzie **setmqaut** , aby skierować komendę do tej usługi. Ten parametr należy określić, jeśli w tym samym czasie jest uruchomionych wiele instalowalnych komponentów. Jeśli nie, aktualizacja zostanie wykonana do pierwszego instalowalnego komponentu dla usługi autoryzacji. Domyślnie jest to dostarczany OAM.

Korzystanie z profili ogólnych OAM w systemach UNIX, Linux, and Windows

Profile ogólne OAM umożliwiają ustawienie uprawnień użytkownika do wielu obiektów jednocześnie, a nie konieczności wydawania osobnych komend **setmqaut** dla każdego pojedynczego obiektu po jego utworzeniu.

Użycie profili ogólnych w komendzie **setmqaut** umożliwia ustawienie uprawnień ogólnych dla wszystkich obiektów, które pasują do tego profilu.

Ta kolekcja tematów zawiera bardziej szczegółowe informacje na temat korzystania z profili ogólnych.

Korzystanie ze znaków wieloznacznych w profilach OAM

Nazwa ogólna profilu to użycie znaków specjalnych (znaków wieloznacznych) w nazwie profilu. Na przykład znak wieloznaczny znaku zapytania (?) zastępuje dowolny pojedynczy znak w nazwie. Dlatego jeśli zostanie określona opcja ABC.?EF, autoryzacja, którą podasz temu profilowi, będzie dotyczyć wszystkich obiektów o nazwach ABC.DEF , ABC.CEF, ABC.BEFitd.

Dostępne są następujące znaki wieloznaczne:

?

Znak zapytania (?) zastępuje pojedynczy znak. Na przykład AB.?D ma zastosowanie do obiektów AB.CD , AB.EDi AB.FD.

*****

Użyj gwiazdki (*) jako:

- *Kwalifikator* w nazwie profilu, który będzie zgodny z dowolnym kwalifikatorem w nazwie obiektu. Kwalifikator stanowi część nazwy obiektu oddzieloną za pomocą kropki. Na przykład w produkcie ABC.DEF.GHIkwalifikatory to: ABC, DEFi GHI .

  Na przykład ABC.*.JKL ma zastosowanie do obiektów ABC.DEF.JKLi ABC.GHI.JKL. (Należy zwrócić uwagę, że **nie** ma zastosowania do produktu ABC.JKL; * używany w tym kontekście zawsze wskazuje jeden kwalifikator.)
- Znak w kwalifikatorze w nazwie profilu w celu dopasowania do zera lub większej liczby znaków w kwalifikatorze w nazwie obiektu.

  Na przykład ABC.DE*.JKL ma zastosowanie do obiektów ABC.DE.JKL, ABC.DEF.JKLi ABC.DEGH.JKL .

******

Użyj dwukrotnego znaku gwiazdki (**) **raz** w nazwie profilu jako:

- Nazwa całego profilu, która będzie zgodna ze wszystkimi nazwami obiektów. Jeśli na przykład w celu identyfikowania procesów używany jest produkt `-t prcs` , to jako nazwę profilu należy użyć wartości **, a następnie należy zmienić autoryzacje dla wszystkich procesów.
- Jako kwalifikator początkowy, środkowy lub końcowy w nazwie profilu w celu dopasowania do zera lub większej liczby kwalifikatorów w nazwie obiektu. Na przykład: **.ABC identyfikuje wszystkie obiekty z kwalifikatorem końcowym ABC.

Uwaga: Jeśli w systemach UNIX and Linux używane są znaki wieloznaczne, **należy** umieścić nazwę profilu w pojedynczych znakach cudzysłowu.

Priorytety profilu

Ważnym punktem, który należy zrozumieć, gdy używane są profile ogólne, jest priorytet, który profile są nadawane podczas decydowania o tym, jakie uprawnienia mają być stosowane do tworzonego obiektu. Na przykład załóżmy, że wydałeś komendy:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

Pierwsza z nich daje uprawnienia do umieszczania wszystkich kolejek dla głównego freda o nazwach zgodnych z profilem AB. *; Drugie daje uprawnienie do uzyskania uprawnień do tego samego typu kolejki, które są zgodne z profilem AB.C*.

Załóżmy, że teraz tworzona jest kolejka o nazwie AB.CD. Zgodnie z regułami dopasowywania znaków wieloznacznych do tej kolejki można zastosować setmqaut. Więc, czy to ma włożyć lub uzyskać autorytet?

Aby znaleźć odpowiedź, należy zastosować regułę, która w każdym przypadku, gdy wiele profili może dotyczyć obiektu, **tylko najbardziej konkretne zastosowanie**. Sposób stosowania tej reguły polega na porównywaniu nazw profili z lewej do prawej. Wszędzie tam, gdzie się różnią, znak inny niż ogólny jest bardziej specyficzny niż ogólny znak. Tak więc w powyższym przykładzie kolejka AB.CD ma uprawnienie **get** (AB.C* jest bardziej konkretny niż AB. *).

Jeśli porównywane są znaki ogólne, kolejność *specyficzności* jest następująca:

1. ?
2. *
3. **

Zrzut ustawień profilu

Pełną definicję komendy sterującej **dmpmqaut** i jej składnię można znaleźć w sekcji dmpmqaut, a w celu uzyskania pełnej definicji komendy **MQCMD_INQUIRE_AUTH_RECS** PCF i jej składni można znaleźć w sekcji Inquire Authority Records (zapytanie o rekordy uprawnień).

W poniższych przykładach przedstawiono sposób użycia komendy sterującej **dmpmqaut** w celu zrzutu rekordów uprawnień dla profili ogólnych:

1. W tym przykładzie zrzuty wszystkie rekordy uprawnień z profilem, który jest zgodny z kolejką a.b.c dla użytkownika user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Wynikowy zrzut wygląda następująco:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Uwaga: Chociaż użytkownicy produktu UNIX and Linux mogą używać opcji `-p` dla komendy **dmpmqaut** , podczas definiowania autoryzacji muszą one korzystać z produktu `-g groupname` .
2. W tym przykładzie zrzuca się wszystkie rekordy uprawnień z profilem, który jest zgodny z kolejką a.b.c.

   ```
   dmpmqaut -m qmgr1 -n a.b.c -t q
   ```

   Wynikowy zrzut wygląda następująco:

   ```
   profile:     a.b.c
   object type: queue
   entity:      Administrator
   type:        principal
   authority:   all
   - - - - - - - - - - - - - - - -
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   - - - - - - - - - - - - - - - -
   profile:     a.**
   object type: queue
   entity:      group1
   type:        group
   authority:   get
   ```
3. W tym przykładzie zrzuty są wszystkie rekordy uprawnień dla profilu a.b. *, kolejki typu.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Wynikowy zrzut wygląda następująco:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

4. W tym przykładzie zrzuty wszystkie rekordy uprawnień dla menedżera kolejek qmX.

```
dmpmqaut -m qmX
```

   Wynikowy zrzut wygląda następująco:

```
profile:     q1
object type: queue
entity:      Administrator
type:        principal
authority:   all
- - - - - - - - - - - - - - - -
profile:     q*
object type: queue
entity:      user1
type:        principal
authority:   get, browse
- - - - - - - - - - - - - - - -
profile:     name.*
object type: namelist
entity:      user2
type:        principal
authority:   get
- - - - - - - - - - - - - - - -
profile:     pr1
object type: process
entity:      group1
type:        group
authority:   get
```

5. W tym przykładzie zrzuca się wszystkie nazwy profili i typy obiektów dla menedżera kolejek qmX.

```
dmpmqaut -m qmX -l
```

   Wynikowy zrzut wygląda następująco:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Uwaga: Tylko w przypadku produktu WebSphere MQ for Windows wyświetlane są wszystkie elementy główne, na przykład informacje o domenie:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

Korzystanie ze znaków wieloznacznych w profilach OAM

Użyj znaków wieloznacznych w nazwie profilu menedżera uprawnień do obiektów (OAM), aby ten profil miał zastosowanie do więcej niż jednego obiektu.

Nazwa ogólna profilu to użycie znaków specjalnych (znaków wieloznacznych) w nazwie profilu. Na przykład znak wieloznaczny znaku zapytania (?) zastępuje dowolny pojedynczy znak w nazwie. Dlatego jeśli zostanie określona opcja `ABC.?EF`, autoryzacja, którą podasz temu profilowi, będzie dotyczyć wszystkich obiektów o nazwach `ABC.DEF`, `ABC.CEF`, `ABC.BEF`itd.

Dostępne są następujące znaki wieloznaczne:

?

Znak zapytania (?) zastępuje pojedynczy znak. Na przykład `AB.?D` ma zastosowanie do obiektów `AB.CD`, `AB.ED`i `AB.FD`.

*****

Użyj gwiazdki (*) jako:

- *Kwalifikator* w nazwie profilu, który będzie zgodny z dowolnym kwalifikatorem w nazwie obiektu. Kwalifikator stanowi część nazwy obiektu oddzieloną za pomocą kropki. Na przykład w nazwie `ABC.DEF.GHI` kwalifikatorami są `ABC`, `DEF` oraz `GHI`.

  Na przykład `ABC.*.JKL` ma zastosowanie do obiektów `ABC.DEF.JKL`i `ABC.GHI.JKL`. (Należy zwrócić uwagę, że **nie** ma zastosowania do produktu `ABC.JKL`; * używany w tym kontekście zawsze wskazuje jeden kwalifikator.)
- Znak w kwalifikatorze w nazwie profilu w celu dopasowania do zera lub większej liczby znaków w kwalifikatorze w nazwie obiektu.

  Na przykład `ABC.DE*.JKL` ma zastosowanie do obiektów `ABC.DE.JKL`, `ABC.DEF.JKL`i `ABC.DEGH.JKL`.

******

Użyj dwukrotnego znaku gwiazdki (**) **raz** w nazwie profilu jako:

- Nazwa całego profilu, która będzie zgodna ze wszystkimi nazwami obiektów. Jeśli na przykład w celu identyfikowania procesów używany jest produkt `-t prcs` , to jako nazwę profilu należy użyć wartości **, a następnie należy zmienić autoryzacje dla wszystkich procesów.
- Jako kwalifikator początkowy, środkowy lub końcowy w nazwie profilu w celu dopasowania do zera lub większej liczby kwalifikatorów w nazwie obiektu. Na przykład: `**.ABC` identyfikuje wszystkie obiekty z kwalifikatorem końcowym ABC.

Uwaga: Jeśli w systemach UNIX and Linux używane są znaki wieloznaczne, **należy** umieścić nazwę profilu w pojedynczych znakach cudzysłowu.

Priorytety profilu

Do pojedynczego obiektu można zastosować więcej niż jeden profil ogólny. W takim przypadku zastosowanie ma najbardziej konkretna reguła.

Ważnym punktem, który należy zrozumieć, gdy używane są profile ogólne, jest priorytet, który profile są nadawane podczas decydowania o tym, jakie uprawnienia mają być stosowane do tworzonego obiektu. Na przykład załóżmy, że wydałeś komendy:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

Pierwsza z nich daje uprawnienia do umieszczania wszystkich kolejek dla głównego freda o nazwach zgodnych z profilem AB. *; Drugie daje uprawnienie do uzyskania uprawnień do tego samego typu kolejki, które są zgodne z profilem AB.C*.

Załóżmy, że teraz tworzona jest kolejka o nazwie AB.CD. Zgodnie z regułami dopasowywania znaków wieloznacznych do tej kolejki można zastosować setmqaut. Więc, czy to ma włożyć lub uzyskać autorytet?

Aby znaleźć odpowiedź, należy zastosować regułę, która w każdym przypadku, gdy wiele profili może dotyczyć obiektu, **tylko najbardziej konkretne zastosowanie**. Sposób stosowania tej reguły polega na porównywaniu nazw profili z lewej do prawej. Wszędzie tam, gdzie się różnią, znak inny niż ogólny jest bardziej specyficzny niż ogólny znak. Tak więc w powyższym przykładzie kolejka AB.CD ma uprawnienie **get** (AB.C* jest bardziej konkretny niż AB. *).

Jeśli porównywane są znaki ogólne, kolejność *specyficzności* jest następująca:

1. ?
2. *
3. **

Zrzut ustawień profilu

Aby wykonać zrzut bieżących autoryzacji powiązanych z określonym profilem, należy użyć komendy sterującej **dmpmqaut** lub komendy PCF produktu **MQCMD_INQUIRE_AUTH_RECS** .

Pełną definicję komendy sterującej **dmpmqaut** i jej składnię można znaleźć w sekcji dmpmqaut, a w celu uzyskania pełnej definicji komendy **MQCMD_INQUIRE_AUTH_RECS** PCF i jej składni można znaleźć w sekcji Inquire Authority Records(zapytanie o rekordy uprawnień).

W poniższych przykładach przedstawiono sposób użycia komendy sterującej **dmpmqaut** w celu zrzutu rekordów uprawnień dla profili ogólnych:

1. W tym przykładzie zrzuty wszystkie rekordy uprawnień z profilem, który jest zgodny z kolejką a.b.c dla użytkownika user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Wynikowy zrzut wygląda podobnie jak w poniższym przykładzie:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Uwaga: Użytkownicy programu UNIX and Linux nie mogą korzystać z opcji `-p` . Zamiast tego muszą używać produktu `-g groupname` .
2. W tym przykładzie zrzuca się wszystkie rekordy uprawnień z profilem, który jest zgodny z kolejką a.b.c.

   ```
   dmpmqaut -m qmgr1 -n a.b.c -t q
   ```

   Wynikowy zrzut wygląda podobnie jak w poniższym przykładzie:

   ```
   profile:     a.b.c
   object type: queue
   entity:      Administrator
   type:        principal
   authority:   all
   - - - - - - - - - - - - - - - -
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   - - - - - - - - - - - - - - - -
   profile:     a.**
   object type: queue
   entity:      group1
   type:        group
   authority:   get
   ```
3. W tym przykładzie zrzuty są wszystkie rekordy uprawnień dla profilu a.b. *, kolejki typu.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Wynikowy zrzut wygląda podobnie jak w poniższym przykładzie:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```
4. W tym przykładzie zrzuty wszystkie rekordy uprawnień dla menedżera kolejek qmX.

   ```
   dmpmqaut -m qmX
   ```

   Wynikowy zrzut wygląda podobnie jak w poniższym przykładzie:

   ```
   profile:     q1
   object type: queue
   entity:      Administrator
   type:        principal
   authority:   all
   - - - - - - - - - - - - - - - -
   profile:     q*
   ```

```
object type: queue
entity:      user1
type:        principal
authority:   get, browse
- - - - - - - - - - - - - - - -
profile:     name.*
object type: namelist
entity:      user2
type:        principal
authority:   get
- - - - - - - - - - - - - - - -
profile:     pr1
object type: process
entity:      group1
type:        group
authority:   get
```

5. W tym przykładzie zrzuca się wszystkie nazwy profili i typy obiektów dla menedżera kolejek qmX.

   ```
   dmpmqaut -m qmX -l
   ```

   Wynikowy zrzut wygląda podobnie jak w poniższym przykładzie:

   ```
   profile: q1, type: queue
   profile: q*, type: queue
   profile: name.*, type: namelist
   profile: pr1, type: process
   ```

Uwaga: Tylko w przypadku produktu WebSphere MQ for Windows wyświetlane są wszystkie elementy główne, na przykład informacje o domenie:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

Wyświetlanie ustawień dostępu

Użyj komendy sterującej **dspmqaut** lub komendy **MQCMD_INQUIRE_ENTITY_AUTH** PCF, aby wyświetlić autoryzacje, które konkretna jednostka główna lub grupa ma dla danego obiektu.

Aby można było użyć tej komendy, menedżer kolejek musi być uruchomiony. Po zmianie dostępu do nazwy użytkownika zmiany są uwzględniane natychmiast przez OAM. Autoryzacja może być wyświetlana tylko dla jednej grupy lub nazwy użytkownika jednocześnie. Pełną definicję komendy sterującej **dmpmqaut** i jej składnię można znaleźć w sekcji dmpmqaut, a w celu uzyskania pełnej definicji komendy **MQCMD_INQUIRE_ENTITY_AUTH** PCF i jej składni można znaleźć w sekcji Inquire Entity Authority.

W poniższym przykładzie przedstawiono użycie komendy sterującej **dspmqaut** w celu wyświetlenia autoryzacji, które grupa GpAdmin ma do definicji procesu o nazwie Annuities , która znajduje się w menedżerze kolejek QueueMan1.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

Zmiana i odebranie dostępu do obiektu IBM WebSphere MQ

Aby zmienić poziom dostępu użytkownika lub grupy do obiektu, należy użyć komendy **setmqaut** . Aby odwołać dostęp konkretnego użytkownika, który jest członkiem grupy, która ma uprawnienia, należy usunąć użytkownika z grupy.

Proces usuwania użytkownika z grupy jest opisany w sekcji:

- “Tworzenie grup i zarządzanie nimi w systemie Windows” na stronie 85
- “Tworzenie grup w systemie HP-UX i zarządzanie nimi” na stronie 88
- “Tworzenie grup i zarządzanie nimi w systemie AIX” na stronie 89
- “Tworzenie grup i zarządzanie nimi w systemie Solaris” na stronie 90

- “Tworzenie grup i zarządzanie nimi w systemie Linux” na stronie 91

.

Identyfikator użytkownika, który tworzy obiekt IBM WebSphere MQ , ma nadane pełne uprawnienia kontrolne do tego obiektu. Jeśli ten identyfikator użytkownika zostanie usunięty z lokalnej grupy mqm (lub z grupy Administratorzy w systemach Windows), uprawnienia te nie zostaną odebrane. Użyj komendy sterującej **setmqaut** lub komendy **MQCMD_DELETE_AUTH_REC** PCF, aby odebrać uprawnienia dostępu do obiektu dla ID użytkownika, który go utworzył, po usunięciu go z grupy mqm lub Administratorzy. Pełną definicję komendy sterującą setmqaut i jej składnię można znaleźć w sekcji setmqaut, a w celu uzyskania pełnej definicji komendy **MQCMD_INQUIRE_ENTITY_AUTH** PCF i jej składni można znaleźć w sekcji Inquire Entity Authority.

W systemie Windowsusuń pozycje OAM odpowiadające konkretnym kontem użytkownika systemu Windows przed usunięciem profilu użytkownika. Usunięcie pozycji OAM nie jest możliwe po usunięciu konta użytkownika.

Zapobieganie sprawdzom dostępu do zabezpieczeń w systemach UNIX, Linux, and Windows

Aby wyłączyć wszystkie sprawdzanie zabezpieczeń, można wyłączyć OAM. Może to być odpowiednie dla środowiska testowego. Po wyłączeniu lub usunięciu OAM nie można dodać OAM do istniejącego menedżera kolejek.

Jeśli użytkownik zdecyduje, że nie chce przeprowadzać kontroli zabezpieczeń (na przykład w środowisku testowym), może wyłączyć OAM na jeden z dwóch sposobów:

- Przed utworzeniem menedżera kolejek należy ustawić zmienną środowiskową MQSNOAUT systemu operacyjnego (jeśli to zrobisz, nie będzie można dodać później OAM):

  Więcej informacji na temat implikacji ustawienia zmiennej MQSNOAUT zawiera sekcja Zmienne środowiskowe .
- Edytuj plik konfiguracyjny menedżera kolejek, aby usunąć usługę. (Jeśli to zrobisz, nie możesz dodać OAM później.)

W przypadku użycia komendy setmqaut lub dspmqaut podczas gdy OAM jest wyłączony, należy zwrócić uwagę na następujące punkty:

- OAM nie sprawdza poprawności podanej nazwy użytkownika lub grupy, co oznacza, że komenda może akceptować niepoprawne wartości .
- OAM nie wykonuje sprawdzania zabezpieczeń i wskazuje, że wszystkie jednostki główne i grupy są autoryzowane do wykonywania wszystkich odpowiednich operacji na obiekcie.

Ostrzeżenie: Gdy OAM jest usuwany, nie można go ponownie umieścić w istniejącym menedżerze kolejek. To jest spowodowane tym, że OAM musi być na miejscu w czasie tworzenia obiektu. Aby ponownie użyć programu WebSphere MQ OAM po jego usunięciu, menedżer kolejek musi zostać odbudowany.

Pojęcia pokrewne

Usługi instalowalne

Nadawanie wymaganego dostępu do zasobów

W tym temacie opisano czynności, które należy wykonać w celu zastosowania zabezpieczeń w systemie WebSphere MQ .

O tym zadaniu

Podczas wykonywania tej czynności użytkownik decyduje, jakie czynności są niezbędne do zastosowania odpowiedniego poziomu zabezpieczeń do elementów instalacji produktu WebSphere MQ . Każde pojedyncze zadanie, do którego się odwołuje, zawiera instrukcje krok po kroku dla wszystkich platform.

Procedura

1. Czy konieczne jest ograniczenie dostępu do menedżera kolejek do określonych użytkowników?
   a) Nie: nie podejmuje dalszych działań.
   b) Tak: Przejdź do następnego pytania.
2. Czy ci użytkownicy potrzebują częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: patrz sekcja "Nadawanie częściowemu dostępowi administracyjnie do podzbioru zasobów menedżera kolejek" na stronie 174.
3. Czy ci użytkownicy potrzebują pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: patrz sekcja "Nadawanie pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek" na stronie 180.
4. Czy ci użytkownicy muszą mieć dostęp tylko do odczytu do wszystkich zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: patrz sekcja "Nadawanie dostępu tylko do odczytu do wszystkich zasobów w menedżerze kolejek" na stronie 184.
5. Czy ci użytkownicy potrzebują pełnego dostępu administracyjnego do wszystkich zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: patrz sekcja "Nadawanie pełnego dostępu administracyjnego do wszystkich zasobów w menedżerze kolejek" na stronie 185.
6. Czy potrzebne są aplikacje użytkownika do nawiązywania połączenia z menedżerem kolejek?
   a) Nie: Wyłącz połączenia, zgodnie z opisem w sekcji "Usuwanie połączeń z menedżerem kolejek" na stronie 186
   b) Tak: patrz sekcja "Zezwalanie aplikacjom użytkownika na łączenie się z menedżerem kolejek" na stronie 187.

Nadawanie częściowemu dostępowi administracyjnie do podzbioru zasobów menedżera kolejek

Niektórym użytkownikom należy nadać częściowy dostęp administracyjny do niektórych, ale nie wszystkich, zasobów menedżera kolejek. Ta tabela służy do określania działań, które należy wykonać.

Tabela 14. Przyznawanie częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek

Użytkownicy muszą administrować obiektami tego typu.	**Wykonaj to działanie**
Kolejki	Przyznaj częściowy dostęp administracyjny do wymaganych kolejek zgodnie z opisem w sekcji "Udzielanie ograniczonego dostępu administracyjnego do niektórych kolejek" na stronie 175
Tematy	Przyznaj częściowy dostęp administracyjny do wymaganych tematów, zgodnie z opisem w sekcji "Ograniczanie dostępu administracyjnego do niektórych tematów" na stronie 176

Tabela 14. Przyznawanie częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek (kontynuacja)	
Użytkownicy muszą administrować obiektami tego typu.	**Wykonaj to działanie**
Kanały	Przyznaj częściowy dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji “Przyznawanie niektórych kanałów ograniczonego dostępu administracyjnego” na stronie 176
Menedżer kolejek	Przyznaj częściowy dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji “Nadawanie ograniczonego dostępu administracyjnego do menedżera kolejek” na stronie 177
Procesy	Przyznaj częściowy dostęp administracyjny do wymaganych procesów, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego niektórym procesom” na stronie 178
Listy nazw	Przyznaj częściowy dostęp administracyjny do wymaganych list nazw, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych list nazw” na stronie 178
Usługi	Przyznaj częściowy dostęp administracyjny do wymaganych usług, zgodnie z opisem w sekcji “Ograniczanie dostępu administracyjnego do niektórych usług” na stronie 179

Udzielanie ograniczonego dostępu administracyjnego do niektórych kolejek

Przydziel częściowy dostęp administracyjny do niektórych kolejek w menedżerze kolejek, do każdej grupy użytkowników z potrzebą biznesową dla tej grupy.

O tym zadaniu

Aby nadać ograniczony dostęp administracyjny niektórym kolejkom dla niektórych działań, należy użyć odpowiednich komend dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
```

- Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

  ReqdAction
  Działanie, które zostanie podjęte przez grupę, jest następujące:

– W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + dlt, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Uwaga: Nadawanie + crt dla kolejek pośrednio sprawia, że użytkownik lub grupa jest administratorem. Nie używaj uprawnienia + crt, aby przyznać ograniczony dostęp administracyjny do niektórych kolejek.

QTYPE

W przypadku komendy DISPLAY, jedna z wartości QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE lub QCLUSTER.

Dla innych wartości parametru *ReqdAction*należy użyć jednej z wartości: QLOCAL, QALIAS, QMODEL lub QREMOTE.

Ograniczanie dostępu administracyjnego do niektórych tematów

Przyznaj częściowy dostęp administracyjny do niektórych tematów w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby przyznać ograniczony dostęp administracyjny do niektórych tematów w niektórych działaniach, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
```

- Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

ReqdAction
Działanie, które zostanie podjęte przez grupę, jest następujące:

– W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Przyznawanie niektórych kanałów ograniczonego dostępu administracyjnego

Przydziel częściowy dostęp administracyjny do niektórych kanałów w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niego biznesowe potrzeby.

O tym zadaniu

Aby przyznać ograniczony dostęp administracyjny do niektórych kanałów dla niektórych działań, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

ReqdAction
Działanie, które zostanie podjęte przez grupę, jest następujące:

– W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Nadawanie ograniczonego dostępu administracyjnego do menedżera kolejek

Przyznaj częściowy dostęp administracyjny do menedżera kolejek, do każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać ograniczony dostęp administracyjny do wykonywania niektórych działań w menedżerze kolejek, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Wyniki

Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w menedżerze kolejek, należy wprowadzić następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName.ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName.ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby zezwolić użytkownikowi na użycie komendy DISPLAY QMGR, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

ReqdAction
Działanie, które zostanie podjęte przez grupę, jest następujące:

- W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

  Chociaż zestaw + jest autoryzacją MQI i nie jest zwykle uznawany za administracyjny, nadanie + ustawienie menedżera kolejek może pośrednio prowadzić do pełnej władzy administracyjnej. Nie przyznaj wartości + ustawionym dla zwykłych użytkowników i aplikacji.

Przyznawanie ograniczonego dostępu administracyjnego niektórym procesom

Przydziel częściowy dostęp administracyjny do niektórych procesów w menedżerze kolejek, do każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać ograniczony dostęp administracyjny niektórym procesom dla niektórych działań, należy użyć odpowiednich komend dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
```

- Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

  ReqdAction
  Działanie, które zostanie podjęte przez grupę, jest następujące:

  – W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych list nazw

Przydziel częściowy dostęp administracyjny do niektórych list nazw w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać ograniczony dostęp administracyjny do niektórych list nazw dla niektórych działań, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

ReqdAction
Działanie, które zostanie podjęte przez grupę, jest następujące:

– W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Ograniczanie dostępu administracyjnego do niektórych usług

Przyznaj częściowy dostęp administracyjny do niektórych usług w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby przyznać ograniczony dostęp administracyjny do niektórych usług dla niektórych działań, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Uwaga: Obiekty usług nie istnieją w produkcie z/OS.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Wyniki

Te komendy nadają dostęp do określonej usługi. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w usłudze, należy wprowadzić następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName.ReqdAction.SERVICE UACC(NONE)
PERMIT QMgrName.ReqdAction.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby zezwolić użytkownikowi na użycie komendy DISPLAY SERVICE, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.SERVICE UACC(NONE)
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

ReqdAction
Działanie, które zostanie podjęte przez grupę, jest następujące:

- W systemach UNIX, Linux i Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

Nadawanie pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek

Niektórym użytkownikom należy nadać pełny dostęp administracyjny do niektórych, ale nie wszystkich, zasobów menedżera kolejek. Te tabele umożliwiają określenie działań, które należy wykonać.

Tabela 15. Nadawanie pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek

Użytkownicy muszą administrować obiektami tego typu.	**Wykonaj to działanie**
Kolejki	Nadaj pełny dostęp administracyjny do wymaganych kolejek zgodnie z opisem w sekcji “Nadawanie pełnych uprawnień administracyjnych do niektórych kolejek” na stronie 180
Tematy	Nadaj pełny dostęp administracyjny do wymaganych tematów, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego niektórych tematów” na stronie 181
Kanały	Nadaj pełny dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego niektórym kanałom” na stronie 181
Menedżer kolejek	Nadaj pełny dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do menedżera kolejek” na stronie 182
Procesy	Nadaj pełny dostęp administracyjny do wymaganych procesów, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego niektórym procesom” na stronie 183
Listy nazw	Nadaj pełny dostęp administracyjny do wymaganych list nazw, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego niektórych list nazw” na stronie 183
Usługi	Należy nadać pełny dostęp administracyjny do wymaganych usług zgodnie z opisem w sekcji “Zapewnienie pełnego dostępu administracyjnego do niektórych usług” na stronie 184

Nadawanie pełnych uprawnień administracyjnych do niektórych kolejek

Należy nadać pełny dostęp administracyjny do niektórych kolejek w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niego dostęp biznesowy.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych kolejek, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.QUEUE.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego niektórych tematów

Należy nadać pełny dostęp administracyjny do niektórych tematów w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych tematów w niektórych działaniach, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM)
MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.TOPIC.ObjectProfile UACC(NONE)
PERMIT QMgrName.TOPIC.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego niektórym kanałom

Nadaj pełnemu administracyjnemu dostępowi do niektórych kanałów menedżera kolejek, każdemu grupie użytkowników, którzy muszą mieć do niego dostęp.

O tym zadaniu

Aby przyznać pełny dostęp administracyjny do niektórych kanałów, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.CHANNEL.ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego do menedżera kolejek

Nadaj menedżerowi kolejek pełny dostęp administracyjny do każdej grupy użytkowników, którzy muszą mieć do niego dostęp w firmie.

O tym zadaniu

Aby nadać menedżerowi kolejek pełny dostęp administracyjny, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego niektórym procesom

Należy nadać pełny dostęp administracyjny do niektórych procesów w menedżerze kolejek, do każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych procesów, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.CHANNEL.ObjectProfile UACC(NONE)
PERMIT QMgrName.PROCESS.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego niektórych list nazw

Należy nadać pełny dostęp administracyjny do niektórych list nazw w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych list nazw, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM)
MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.NAMELIST.ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

  Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Zapewnienie pełnego dostępu administracyjnego do niektórych usług

Należy nadać pełny dostęp administracyjny do niektórych usług w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych usług, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.SERVICE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie dostępu tylko do odczytu do wszystkich zasobów w menedżerze kolejek

Nadaj dostęp tylko do odczytu wszystkim zasobom w menedżerze kolejek, każdemu użytkownikowi lub grupie użytkowników, którzy muszą mieć do niego dostęp biznesowy.

O tym zadaniu

Użyj kreatora dodawania uprawnień opartych na rolach lub odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- Za pomocą kreatora:
  a) W panelu Navigator programu WebSphere MQ Explorer kliknij prawym przyciskiem myszy menedżer kolejek, a następnie kliknij opcję **Uprawnienia do obiektu** > **Dodaj uprawnienia oparte na rolach** .

Zostanie otwarty kreator dodawania uprawnień opartych na rolach.

- W systemach UNIX i Windows wprowadź następujące komendy:

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +inq
setmqaut -m QMgrName -n ** -t clntconn -g GroupName +dsp
setmqaut -m QMgrName -n ** -t authinfo -g GroupName +dsp
setmqaut -m QMgrName -n ** -t listener -g GroupName +dsp
setmqaut -m QMgrName -n ** -t namelist -g GroupName +dsp
setmqaut -m QMgrName -n ** -t process -g GroupName +dsp
setmqaut -m QMgrName -n ** -t service -g GroupName +dsp
setmqaut -m QMgrName -t qmgr -g GroupName +dsp +inq +connect
```

Uprawnienia szczegółowe do systemu SYSTEM.ADMIN.COMMAND.QUEUE i SYSTEM.MQEXPLORER.REPLY.MODEL jest wymagany tylko wtedy, gdy ma być używany program MQ Explorer.

- W przypadku produktu IBM inaleźy wprowadzić następujące komendy:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*Q) USER('GroupName') AUT(*ADMDSP *BROWSE) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*TOPIC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CHL) USER('GroupName') AUT(*ADMDSP *INQ) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*CLTCN) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*AUTHINFO) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*LSR) USER('GroupName') AUT(*ADMDSP)MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*NMLIST) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ(*ALL) OBJTYPE(*SVC) USER('GroupName') AUT(*ADMDSP) MQMNAME('QMgrName')
GRTMQMAUT OBJ('object-name') OBJTYPE(*MQM)  USER('GroupName') AUT(*ADMDSP *CONNECT *INQ)
MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MQTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie pełnego dostępu administracyjnego do wszystkich zasobów w menedżerze kolejek

Należy nadać pełny dostęp administracyjny do wszystkich zasobów w menedżerze kolejek, każdemu użytkownikowi lub grupie użytkowników, którzy muszą mieć do niego dostęp w firmie.

O tym zadaniu

Użyj kreatora dodawania uprawnień opartych na rolach lub odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- Za pomocą kreatora:

  a) W panelu Navigator programu WebSphere MQ Explorer kliknij prawym przyciskiem myszy menedżer kolejek, a następnie kliknij opcję **Uprawnienia do obiektu** > **Dodaj uprawnienia oparte na rolach** .

  Zostanie otwarty kreator dodawania uprawnień opartych na rolach.

- W przypadku systemów UNIX and Linux należy wprowadzić następujące komendy:

```
setmqaut -m QMgrName -n '**' -t queue -g GroupName +alladm +browse
setmqaut -m QMgrName -n @class -t queue -g GroupName +crt
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.QUEUE -t queue -g GroupName +dsp +inq +get
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +conn
```

- W systemach Windows należy wydać te same komendy, co w przypadku systemów UNIX and Linux , ale zamiast @classnależy użyć nazwy profilu @CLASS .
- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER('GroupName') AUT(*ALLADM) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Usuwanie połączeń z menedżerem kolejek

Jeśli nie chcesz, aby aplikacje użytkownika nawiązały połączenie z menedżerem kolejek, usuń ich uprawnienia, aby połączyć się z nim.

O tym zadaniu

Odbierz uprawnienia wszystkich użytkowników do łączenia się z menedżerem kolejek przy użyciu odpowiedniej komendy dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- W systemie IBM iwykonaj następującą komendę:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

Nie należy wydawać żadnych komend PERMIT.

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

GroupName
Nazwa grupy, do której ma zostać odmówiony dostęp.

Zezwalanie aplikacjom użytkownika na łączenie się z menedżerem kolejek

Użytkownik chce zezwolić aplikacji użytkownika na łączenie się z menedżerem kolejek. Tabele znajdujące się w tym temacie umożliwiają określenie działań, które należy wykonać.

Najpierw należy określić, czy aplikacje klienckie będą łączyć się z menedżerem kolejek.

Jeśli żadna z aplikacji, które nie połączą się z menedżerem kolejek, nie jest aplikacją kliencką, należy wyłączyć zdalny dostęp zgodnie z opisem w sekcji “Wyłączanie zdalnego dostępu do menedżera kolejek” na stronie 194.

Jeśli co najmniej jedna z aplikacji, które nawiąże połączenie z menedżerem kolejek, są aplikacjami kliencką, należy zabezpieczyć zdalne połączenia w sposób opisany w sekcji “Zabezpieczanie zdalnych połączeń z menedżerem kolejek” na stronie 187.

W obu przypadkach skonfiguruj zabezpieczenia połączenia zgodnie z opisem w sekcji “Konfigurowanie zabezpieczeń połączenia” na stronie 195 .

Jeśli chcesz sterować dostępem do zasobów dla każdego użytkownika łączącego się z menedżerem kolejek, zapoznaj się z poniższą tabelą. Jeśli instrukcja w pierwszej kolumnie jest prawdziwa, należy wykonać działanie wymienione w drugiej kolumnie.

instrukcja	Podejmij to działanie
Istnieją aplikacje, które korzystają z kolejek	Więcej informacji znajduje się w sekcji “Kontrolowanie dostępu użytkowników do kolejek” na stronie 195
Dostępne są aplikacje, które korzystają z tematów	Patrz sekcja “Kontrolowanie dostępu użytkowników do tematów” na stronie 200.
Istnieją aplikacje, które zapytują się w obiekcie menedżera kolejek	Patrz sekcja “Nadawanie uprawnień do uzyskiwania informacji o menedżerze kolejek” na stronie 202.
Istnieją aplikacje, które używają obiektów procesu	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do procesów dostępu” na stronie 202
Istnieją aplikacje, które korzystają z list nazw	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do dostępu do list nazw” na stronie 203

Zabezpieczanie zdalnych połączeń z menedżerem kolejek

Istnieje możliwość zabezpieczenia połączeń zdalnych z menedżerem kolejek przy użyciu protokołu SSL lub TLS, wyjścia zabezpieczeń, rekordów uwierzytelniania kanału lub kombinacji tych metod.

O tym zadaniu

Klient łączy się z menedżerem kolejek przy użyciu kanału połączenia klienckiego na stacji roboczej klienta i kanału połączenia z serwerem na serwerze. Należy zabezpieczyć takie połączenia w jeden z następujących sposobów.

Procedura

1. Używanie protokołu SSL lub TLS z rekordami uwierzytelniania kanału:
   a) Przed otwarciem kanału należy uniemożliwić dowolną nazwę wyróżniającą (DN), korzystając z rekordu uwierzytelniania kanału SSLPEERMAP w celu odwzorowania wszystkich nazw wyróżniających na USERSRC (NOACCESS).
   b) Zezwól na otwarcie kanału za pomocą rekordu uwierzytelniania kanału SSLPEERMAP w celu odwzorowania ich na użytkownika USERSRC (CHANNEL), aby zezwolić na otwarcie określonych nazw wyróżniających lub zestawów nazw wyróżniających.
2. Korzystanie z protokołu SSL lub TLS z wyjściem zabezpieczeń:
   a) Ustaw wartość MCAUSER na kanale połączenia z serwerem na identyfikator użytkownika bez uprawnień.
   b) Zapisz wyjście zabezpieczeń, aby przypisać wartość MCAUSER w zależności od wartości nazwy wyróżniającej SSL, którą otrzymuje w polach SSLPeerNamePtr i SSLPeerName, które zostały przekazane do wyjścia w strukturze MQCD.
3. Używanie protokołu SSL lub TLS z wartościami definicji kanału stałego:
   a) Ustaw wartość SSLPEER w kanale połączenia z serwerem, aby określić konkretną wartość lub zawężający zakres wartości.
   b) Ustaw wartość MCAUSER na kanale połączenia serwera z identyfikatorem użytkownika, z którym powinien być uruchamiany kanał.
4. Przy użyciu rekordów uwierzytelniania kanału w kanałach, które nie używają protokołu SSL lub TLS:
   a) Przed otwarciem kanałów nie należy otwierać żadnych adresów IP, korzystając z rekordu uwierzytelniania kanału odwzorowania adresu z parametrem ADDRESS (*) i USERSRC (NOACCESS).
   b) Zezwól na otwieranie konkretnych adresów IP kanałami, korzystając z rekordów uwierzytelniania kanału odwzorowującego adres dla tych adresów z użyciem parametru USERSRC (CHANNEL).
5. Korzystanie z wyjścia zabezpieczeń:
   a) Napisz wyjście zabezpieczeń, aby autoryzować połączenia na podstawie dowolnej właściwości wybranej, na przykład, adresu źródłowego adresu IP.
6. Możliwe jest również użycie rekordów uwierzytelniania kanału przy użyciu wyjścia zabezpieczeń lub użycie wszystkich trzech metod, jeśli wymagają tego konkretne okoliczności.

Blokowanie konkretnych adresów IP

Można zapobiec akceptowaniu przez konkretny kanał połączenia przychodzącego z adresu IP lub uniemożliwić temu menedżerowi kolejek zezwalanie na dostęp z adresu IP przy użyciu rekordu uwierzytelniania kanału.

Zanim rozpoczniesz

Włącz rekordy uwierzytelniania kanału, uruchamiając następującą komendę:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Aby nie dopuścić do akceptowania połączenia przychodzącego przez określone kanały i upewnić się, że połączenia są akceptowane tylko wtedy, gdy używana jest poprawna nazwa kanału, do blokowania adresów IP można użyć jednego typu reguły. Aby nie zezwalać na dostęp do całego menedżera kolejek przez adres IP, zwykle jest używany firewall w celu trwałego zablokowania tego menedżera kolejek.

Można jednak użyć innego typu reguły, aby zezwolić na tymczasowe blokowanie kilku adresów, na przykład podczas oczekiwania na aktualizację firewalla.

Procedura

- Aby zablokować adresy IP przy użyciu konkretnego kanału, należy ustawić rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

Do komendy dostępne są trzy części:

SET CHLAUTH (*nazwa-kanału-ogólnego*)
Za pomocą tej części komendy można sterować tym, czy połączenie ma być blokowe dla całego menedżera kolejek, pojedynczego kanału czy zakresu kanałów. To, co tu wkładasz, określa, które obszary są przykryte.

Na przykład:

- SET CHLAUTH('*') -blokuje każdy kanał w menedżerze kolejek, to znaczy cały menedżer kolejek
- SET CHLAUTH ('SYSTEM. *')-blokuje każdy kanał, który zaczyna się od systemu SYSTEM.
- SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-blokuje kanał SYSTEM.DEF.SVRCONN

Typ reguły CHLAUTH
Użyj tej części komendy, aby określić typ komendy i określić, czy ma być podany pojedynczy adres, czy lista adresów.

Na przykład:

- TYPE(ADDRESSMAP) -Użyj komendy ADDRESSMAP, jeśli chcesz podać pojedynczy adres lub adres zastępczy. Na przykład program ADDRESS('192.168.*') blokuje wszystkie połączenia przychodzące z adresu IP, począwszy od 192.168.

  Więcej informacji na temat filtrowania adresów IP za pomocą wzorców znajduje się w sekcji Ogólne adresy IP.
- TYPE(BLOCKADDR) -Należy użyć komendy BLOCKADDR, jeśli ma zostać dostarczona lista adresów do zablokowania.

Parametry dodatkowe
Parametry te są zależne od typu reguły używanej w drugiej części komendy:

- W przypadku produktu TYPE(ADDRESSMAP) należy użyć adresu
- W przypadku systemu TYPE(BLOCKADDR) należy użyć komendy ADDRLIST.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH

Tymczasowe blokowanie konkretnych adresów IP, jeśli menedżer kolejek nie jest uruchomiony
Użytkownik może zablokować określone adresy IP lub zakresy adresów, gdy menedżer kolejek nie jest uruchomiony i dlatego nie można wydać komend MQSC. Modyfikując plik `blockaddr.ini` , można tymczasowo zablokować adresy IP w wyjątkowych sytuacjach.

O tym zadaniu

Plik `blockaddr.ini` zawiera kopię definicji BLOCKADDR, które są używane przez menedżer kolejek. Ten plik jest odczytyany przez program nasłuchujący, jeśli program nasłuchujący został uruchomiony przed menedżerem kolejek. W tych okolicznościach program nasłuchujący korzysta z dowolnych wartości, które zostały ręcznie dodane do pliku `blockaddr.ini` .

Należy jednak pamiętać o tym, że po uruchomieniu menedżera kolejek zapisuje zestaw definicji BLOCKADDR do pliku `blockaddr.ini` , nadpisując ręczne edytowanie, które można było wykonać. Podobnie, za każdym razem, gdy definicja BLOCKADDR zostanie dodana lub usunięta za pomocą komendy **SET CHLAUTH** , plik `blockaddr.ini` zostanie zaktualizowany. W związku z tym można wprowadzać trwałe zmiany w definicjach BLOCKADDR tylko za pomocą komendy **SET CHLAUTH** , gdy menedżer kolejek jest uruchomiony.

Procedura

1. Otwórz plik `blockaddr.ini` w edytorze tekstu.
   Plik ten znajduje się w katalogu danych menedżera kolejek.
2. Dodaj adresy IP jako proste pary klucz-wartość, gdzie słowo kluczowe to `Addr`.
   Więcej informacji na temat filtrowania adresów IP z wzorcami zawiera sekcja Ogólne adresy IP.
   Na przykład:

```
Addr = 192.0.2.0
Addr = 192.0.*
Addr = 192.0.2.1-8
```

Zadania pokrewne

“Blokowanie konkretnych adresów IP” na stronie 188
Można zapobiec akceptowaniu przez konkretny kanał połączenia przychodzącego z adresu IP lub uniemożliwić temu menedżerowi kolejek zezwalanie na dostęp z adresu IP przy użyciu rekordu uwierzytelniania kanału.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Blokowanie konkretnych ID użytkowników
Można uniemożliwić konkretnym użytkownikom korzystanie z kanału poprzez określenie identyfikatorów użytkowników, które, jeśli są aserowane, powodują zakończenie kanału. W tym celu należy ustawić rekord uwierzytelniania kanału.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.
Lista użytkowników podana w produkcie `TYPE(BLOCKUSER)` ma zastosowanie tylko do kanałów SVRCONN, a nie do kanałów menedżera kolejek.
userID1 i *userID2* to każdy identyfikator użytkownika, który ma zostać uniemożliwił korzystanie z kanału. Można również określić wartość specjalną `*MQADMIN` , która ma odwoływać się do uprawnionych użytkowników administracyjnych. Więcej informacji na temat użytkowników uprzywilejowanych zawiera sekcja “Użytkownicy uprzywilejowani” na stronie 152. Więcej informacji na temat produktu `*MQADMIN`zawiera sekcja SET CHLAUTH.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Odwzorowywanie zdalnego menedżera kolejek na identyfikator użytkownika MCAUSER
Za pomocą rekordu uwierzytelniania kanału można ustawić atrybut MCAUSER kanału zgodnie z menedżerem kolejek, z którego łączy się kanał.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Opcjonalnie można ograniczyć adresy IP, do których ma zastosowanie reguła.

Należy zauważyć, że ta technika nie ma zastosowania do kanałów połączenia z serwerem. Jeśli w poniższych komendach zostanie podana nazwa kanału połączenia z serwerem, nie będzie to miało żadnego wpływu na działanie.

Procedura

- Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

  ```
  SET CHLAUTH('generic-channel-name') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user)
  ```

  nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.
  generic-partner-qmgr-name to nazwa menedżera kolejek lub wzorzec zawierający symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą menedżera kolejek.
  użytkownik to identyfikator użytkownika, który ma być używany dla wszystkich połączeń z określonego menedżera kolejek.
- Aby ograniczyć tę komendę do określonych adresów IP, należy podać parametr **ADDRESS** w następujący sposób:

  ```
  SET CHLAUTH('generic-channel-name') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user) ADDRESS(
  generic-ip-address)
  ```

  nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.
  generic-ip-address to pojedynczy adres lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny lub łącznik (-) w celu wskazania zakresu, który jest zgodny z adresem. Więcej informacji na temat ogólnych adresów IP znajduje się w sekcji Ogólne adresy IP .

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH

Odwzorowywanie identyfikatora użytkownika potwierdzonego przez klienta na identyfikator użytkownika MCAUSER
Za pomocą rekordu uwierzytelniania kanału można zmienić atrybut MCAUSER kanału połączenia z serwerem, zgodnie z oryginalnym identyfikatorem użytkownika otrzymanego od klienta.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Należy pamiętać, że ta technika ma zastosowanie tylko do kanałów połączenia z serwerem. Nie ma on wpływu na inne typy kanałów.

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record** . Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.
nazwa-użytkownika-klienta to identyfikator użytkownika, który został sprawdzony przez klienta.
użytkownik to identyfikator użytkownika, który ma być używany zamiast nazwy użytkownika klienta.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH

Odwzorowywanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER
Za pomocą rekordu uwierzytelniania kanału można ustawić atrybut MCAUSER kanału, zgodnie z odebraną nazwą wyróżniającą (DN).

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP) SSLPEER(generic-ssl-peer-name
) USERSRC(MAP) MCAUSER(user)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.
generic-ssl-peer-name jest łańcuchem, który jest następujący po standardowych regułach programu IBM WebSphere MQ dla wartości SSLPEER. Patrz Reguły WebSphere MQ dla wartości SSLPEER.
użytkownik jest identyfikatorem użytkownika, który ma być używany dla wszystkich połączeń korzystających z określonej nazwy wyróżniającej.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH

Blokowanie dostępu ze zdalnego menedżera kolejek
Za pomocą rekordu uwierzytelniania kanału można zapobiec uruchamianiu zdalnych kanałów przez zdalny menedżer kolejek.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Należy zauważyć, że ta technika nie ma zastosowania do kanałów połączenia z serwerem. Jeśli nazwa kanału połączenia z serwerem zostanie określona w poniższej komendzie, nie będzie ona miała żadnego wpływu.

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(QMGRMAP) QMNAME('generic-partner-qmgr-name')
USERSRC(NOACCESS)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.

generic-partner-qmgr-name to nazwa menedżera kolejek lub wzorzec zawierający symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą menedżera kolejek.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Blokowanie dostępu dla ID użytkownika potwierdzonego przez klienta

Istnieje możliwość użycia rekordu uwierzytelniania kanału w celu uniknięcia uruchamiania przez klient ID użytkownika z kanałów startowych.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Należy pamiętać, że ta technika ma zastosowanie tylko do kanałów połączenia z serwerem. Nie ma on wpływu na inne typy kanałów.

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(USERMAP) CLNTUSER('client-user-name') USERSRC(NOACCESS)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.

nazwa-użytkownika-klienta to identyfikator użytkownika, który został sprawdzony przez klienta.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Blokowanie dostępu dla nazwy wyróżniającej SSL

Za pomocą rekordu uwierzytelniania kanału można zapobiec uruchamianiu kanałów wyjściowych nazwy wyróżniającej SSL.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP) SSLPEER('generic-ssl-peer-name')
USERSRC(NOACCESS)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.

generic-ssl-peer-name jest łańcuchem, który jest następujący po standardowych regułach programu IBM WebSphere MQ dla wartości SSLPEER. Patrz Reguły WebSphere MQ dla wartości SSLPEER.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Odwzorowywanie adresu IP na identyfikator użytkownika MCAUSER

Za pomocą rekordu uwierzytelniania kanału można ustawić atrybut MCAUSER kanału, zgodnie z adresem IP, z którego połączenie jest odbierane.

Zanim rozpoczniesz

Upewnij się, że rekordy uwierzytelniania kanału są włączone w następujący sposób:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedura

Ustaw rekord uwierzytelniania kanału za pomocą komendy MQSC **SET CHLAUTH**lub komendy PCF **Set Channel Authentication Record**. Na przykład można wydać komendę MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(ADDRESSMAP) ADDRESS('generic-ip-address') USERSRC(MAP)
MCAUSER(user)
```

nazwa-kanału-ogólnego to nazwa kanału, do którego ma być sterowanie dostępem, lub wzorzec, w tym symbol gwiazdki (*) jako znak wieloznaczny zgodny z nazwą kanału.

użytkownik jest identyfikatorem użytkownika, który ma być używany dla wszystkich połączeń korzystających z określonej nazwy wyróżniającej.

generic-ip-address to adres, z którego nawiąże połączenie, lub wzorzec zawierający gwiazdkę (*) jako znak wieloznaczny lub łącznik (-) w celu wskazania zakresu, który jest zgodny z adresem.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH

Wyłączanie zdalnego dostępu do menedżera kolejek

Jeśli nie chcesz, aby aplikacje klienckie łączyły się z menedżerem kolejek, wyłącz zdalny dostęp do tego menedżera kolejek.

O tym zadaniu

Zapobiegaj łączeniu aplikacji klienckich z menedżerem kolejek w jeden z następujących sposobów:

Procedura

- Usuń wszystkie kanały połączenia z serwerem za pomocą komendy MQSC **DELETE CHANNEL**.
- Ustaw identyfikator użytkownika agenta kanału komunikatów (MCAUSER) kanału na identyfikator użytkownika bez praw dostępu, za pomocą komendy MQSC **ALTER CHANNEL**.

Konfigurowanie zabezpieczeń połączenia

Nadaj uprawnienie do łączenia się z menedżerem kolejek dla każdego użytkownika lub grupy użytkowników, którzy mają do tego celu biznesowe.

O tym zadaniu

Aby skonfigurować zabezpieczenia połączenia, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM)  USER('GroupName') AUT(*CONNECT)
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

  Te komendy umożliwiają nawiązanie połączenia dla zadań wsadowych, CICS, IMS i inicjatora kanału (CHIN). Jeśli nie jest używany konkretny typ połączenia, pomiń odpowiednie komendy.

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Kontrolowanie dostępu użytkowników do kolejek

Użytkownik chce kontrolować dostęp aplikacji do kolejek. W tym temacie opisano działania, które należy wykonać.

Dla każdej prawdziwej instrukcji w pierwszej kolumnie należy wykonać działanie wskazane w drugiej kolumnie.

instrukcja	Działanie
Aplikacja pobiera komunikaty z kolejki	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do pobierania komunikatów z kolejek” na stronie 196
Kontekst zbiorów aplikacji	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do ustawiania kontekstu” na stronie 196
Kontekst przekazuje kontekst	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do przekazywania kontekstu” na stronie 197

instrukcja	Działanie
Aplikacja umieszcza komunikaty w kolejce klastrowej	Więcej informacji znajduje się w sekcji “Autoryzowanie umieszczania komunikatów w kolejkach klastra zdalnego” na stronie 254
Aplikacja umieszcza komunikaty w kolejce lokalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 198
Aplikacja umieszcza komunikaty w kolejce modelowej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce modelowej” na stronie 199
Aplikacja umieszcza komunikaty w kolejce zdalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra” na stronie 199

Nadawanie uprawnień do pobierania komunikatów z kolejek
Nadanie uprawnień do pobierania komunikatów z kolejki lub zestawu kolejek do każdej grupy użytkowników z potrzebą biznesową dla danej kolejki.

O tym zadaniu

Aby nadać uprawnienia do pobierania komunikatów z niektórych kolejek, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do ustawiania kontekstu
Nadanie uprawnień do ustawiania kontekstu dla umieszczanego komunikatu, dla każdej grupy użytkowników z potrzebą biznesową dla danej grupy.

O tym zadaniu

Aby nadać uprawnienia do ustawiania kontekstu w niektórych kolejkach, należy użyć odpowiednich komend dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows należy wprowadzić jedną z następujących komend:
  - Aby ustawić tylko kontekst tożsamości:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
    ```

  - Aby ustawić cały kontekst:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
    ```

- W przypadku produktu IBM iwprowadź jedną z następujących komend:
  - Aby ustawić tylko kontekst tożsamości:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('QMgrName')
    ```

  - Aby ustawić cały kontekst:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL)
    MQMNAME('QMgrName')
    ```

- W systemie z/OSnależy wprowadzić jeden z następujących zestawów komend:
  - Aby ustawić tylko kontekst tożsamości:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
    ```

  - Aby ustawić cały kontekst:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
    ```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do przekazywania kontekstu
Nadanie uprawnień do przekazywania kontekstu z pobranego komunikatu do jednego, który jest umieszczany, do każdej grupy użytkowników z potrzebą biznesową dla danej grupy.

O tym zadaniu

Aby nadać uprawnienia do przekazywania kontekstu w niektórych kolejkach, należy użyć odpowiednich komend dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows należy wprowadzić jedną z następujących komend:
  - Aby przekazać tylko kontekst tożsamości:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Aby przekazać cały kontekst:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
```

- W przypadku produktu IBM iwprowadź jedną z następujących komend:
  - Aby przekazać tylko kontekst tożsamości:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID)
    MQMNAME('QMgrName')
    ```

  - Aby przekazać cały kontekst:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL)
    MQMNAME('QMgrName')
    ```

- W systemie z/OSwprowadź następujące komendy, aby przekazać kontekst tożsamości lub cały kontekst:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej
Nadanie uprawnień do umieszczania komunikatów w kolejce lokalnej lub w kolejce, do każdej grupy użytkowników z potrzebą biznesową dla danej grupy.

O tym zadaniu

Aby nadać uprawnienia do umieszczania komunikatów w niektórych kolejkach lokalnych, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
  ```

- W systemie IBM iwykonaj następującą komendę:

  ```
  GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
  ```

- W systemie z/OSwprowadź następujące komendy:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w kolejce modelowej
Nadanie uprawnień do umieszczania komunikatów w kolejce modelowej lub w zestawie kolejek modelowych, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp biznesowy.

O tym zadaniu

Kolejki modelowe są używane do tworzenia kolejek dynamicznych. Dlatego należy nadać uprawnienia zarówno do kolejek modelowych, jak i dynamicznych. Aby nadać te uprawnienia, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows należy wprowadzić następujące komendy:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- W przypadku produktu IBM inależy wprowadzić następujące komendy:

```
GRTMQMAUT OBJ('ModelQueueName') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQQUEUE QMgrName.ModelQueueName UACC(NONE)
PERMIT QMgrName.ModelQueueName CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  Nazwa ModelQueue
  Nazwa kolejki modelowej, na której oparte są kolejki dynamiczne.

  ObjectProfile
  Nazwa kolejki dynamicznej lub profilu ogólnego, dla której mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra
Nadanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra lub zestawie kolejek do każdej grupy użytkowników z potrzebą biznesową dla danej grupy.

O tym zadaniu

Aby umieścić komunikat w zdalnej kolejce klastra, można umieścić go w lokalnej definicji kolejki zdalnej lub w pełnej kolejce zdalnej. Jeśli używana jest lokalna definicja kolejki zdalnej, wymagane są uprawnienia do umieszczenia w obiekcie lokalnym: patrz sekcja “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 198. Jeśli używana jest pełna kolejka zdalna, wymagane są uprawnienia do umieszczenia w kolejce zdalnej. Należy nadać temu uprawnienia, korzystając z odpowiednich komend dla używanego systemu operacyjnego.

Domyślnym zachowaniem jest wykonanie kontroli dostępu w stosunku do SYSTEM.CLUSTER.TRANSMIT.QUEUE. Należy pamiętać, że to zachowanie jest stosowane, nawet jeśli używane jest wiele kolejek transmisji.

Konkretne zachowanie opisane w tym temacie ma zastosowanie tylko wtedy, gdy atrybut **ClusterQueueAccessControl** w pliku qm.ini ma wartość *RQMName*, zgodnie z opisem w sekcji Sekcja zabezpieczeń , a następnie zrestartowany menedżer kolejek.

W systemach UNIX, Linuxi Windows można również użyć komendy SET AUTHREC.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

  Należy pamiętać, że można użyć obiektu *rqmname* tylko w przypadku zdalnych kolejek klastra.

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

  Należy pamiętać, że można użyć obiektu RMTMQMNAME tylko dla kolejek klastra zdalnego.

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQQUEUE  QMgrNameObjectProfile UACC(NONE)
PERMIT QMgrNameObjectProfile CLASS(MQADMIN)
ID(GroupName) ACCESS(UPDATE)
```

  Należy pamiętać, że można użyć nazwy zdalnego menedżera kolejek (lub grupy współużytkowania kolejek) tylko w przypadku zdalnych kolejek klastra.

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa zdalnego menedżera kolejek lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Kontrolowanie dostępu użytkowników do tematów

Użytkownik musi kontrolować dostęp aplikacji do tematów. W tym temacie opisano działania, które należy wykonać.

Dla każdej prawdziwej instrukcji w pierwszej kolumnie należy wykonać działanie wskazane w drugiej kolumnie.

Tabela 16. Kontrolowanie dostępu użytkowników do tematów

instrukcja	**Działanie**
Aplikacja publikuje komunikaty w temacie	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do publikowania komunikatów w temacie” na stronie 201
Aplikacja subskrybuje temat	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do subskrybowania tematów” na stronie 201

Nadawanie uprawnień do publikowania komunikatów w temacie
Nadanie uprawnień do publikowania komunikatów w temacie lub zestawie tematów do każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać uprawnienia do publikowania komunikatów w niektórych tematach, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do subskrybowania tematów
Nadanie uprawnień do subskrybowania tematu lub zestawu tematów do każdej grupy użytkowników, którzy muszą mieć do niej dostęp w firmie.

O tym zadaniu

Aby nadać uprawnienia do subskrybowania niektórych tematów, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

  Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do uzyskiwania informacji o menedżerze kolejek

Nadaj uprawnienia do tworzenia zapytań w menedżerze kolejek, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać uprawnienia do uzyskiwania informacji o menedżerze kolejek, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName ObjectProfile CLASS(MQCMDS) ID(GroupName ) ACCESS(READ)
```

Te komendy nadają dostęp do określonego menedżera kolejek. Aby zezwolić użytkownikowi na użycie komendy MQINQ, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.MQINQ.QMGR UACC(NONE)
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do procesów dostępu

Nadaj uprawnienia dostępu do procesu lub zestawu procesów, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp.

O tym zadaniu

Aby nadać uprawnienia dostępu do niektórych procesów, należy użyć odpowiednich komend dla używanego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME('QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Nadawanie uprawnień do dostępu do list nazw

Nadaj uprawnienie dostępu do listy nazw lub zestawu list nazw, do każdej grupy użytkowników, którzy muszą mieć do niej dostęp biznesowy.

O tym zadaniu

Aby nadać uprawnienia do dostępu do niektórych list nazw, należy użyć odpowiednich komend dla danego systemu operacyjnego.

Procedura

- W przypadku systemów UNIX, Linux i Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
 +all
```

- W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- W systemie z/OSwprowadź następujące komendy:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
 CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, do której ma zostać przyznany dostęp.

Uprawnienie do administrowania produktem IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Administratorzy produktu IBM WebSphere MQ mogą używać wszystkich komend produktu IBM WebSphere MQ i nadawania uprawnień innym użytkownikom. Gdy administratorzy wydadzą komendy do zdalnych menedżerów kolejek, muszą mieć wymagane uprawnienia w zdalnym menedżerze kolejek. Dodatkowe uwagi dotyczą systemów Windows .

Administratorzy produktu IBM WebSphere MQ mają uprawnienia do używania wszystkich komend produktu WebSphere MQ (w tym komend do nadawania uprawnień WebSphere MQ dla innych użytkowników).

Aby być administratorem produktu IBM WebSphere MQ , użytkownik musi być członkiem specjalnej grupy o nazwie *mqm* (lub członkiem grupy Administratorzy w systemach Windows). Grupa mqm jest tworzona automatycznie, gdy zainstalowany jest produkt WebSphere MQ . Do grupy należy dodać kolejnych użytkowników, aby umożliwić im administrowanie. Wszyscy członkowie tej grupy mają dostęp do wszystkich zasobów. Ten dostęp może zostać odwołany tylko przez usunięcie użytkownika z grupy mqm i wydanie komendy REFRESH SECURITY. Administratorzy mogą używać komend sterujących do administrowania produktem WebSphere MQ. Jedną z tych komend sterujących jest **setmqaut**, która jest używana do nadawania uprawnień innym użytkownikom w celu umożliwienia im dostępu do zasobów WebSphere MQ lub sterowania nimi. Komendy PCF służące do zarządzania rekordami uprawnień są dostępne dla użytkowników niebędących administratorami, którym przyznano uprawnienia dsp i chg w menedżerze kolejek. Więcej informacji na temat zarządzania uprawnieniami za pomocą komend PCF zawiera sekcja Programmable Command Formats(Formaty komend programowalnych).

Administratorzy mogą używać komendy sterującej **runmqsc** do wydawania komend IBM WebSphere MQ Script (MQSC). Gdy produkt **runmqsc** jest używany w trybie pośrednim do wysyłania komend MQSC do zdalnego menedżera kolejek, każda komenda MQSC jest hermetyzowana w ramach komendy Escape PCF. Administratorzy muszą mieć wymagane uprawnienia dla komend MQSC, które mają być przetwarzane przez zdalny menedżer kolejek. Program WebSphere MQ Explorer wydaje komendy PCF w celu wykonywania zadań administracyjnych. Administratorzy nie wymagają dodatkowych uprawnień do korzystania z programu WebSphere MQ Explorer w celu administrowania menedżerem kolejek w systemie lokalnym. Gdy program IBM WebSphere MQ Explorer jest używany do administrowania menedżerem kolejek w innym systemie, administratorzy muszą mieć wymagane uprawnienia do komend PCF, które mają być przetwarzane przez zdalny menedżer kolejek.

Więcej informacji na temat sprawdzania uprawnień w przypadku przetwarzania komend PCF i MQSC zawierają następujące tematy:

- Informacje o komendach PCF, które działają w menedżerach kolejek, kolejkach, procesach, listach nazw i obiektach informacji uwierzytelniających, zawiera sekcja Uprawnienia do pracy z obiektami produktu WebSphere MQ. W tej sekcji znajdują się informacje o równoważnych komendach MQSC hermetyzowanych w komendach Escape PCF.
- Informacje o komendach PCF, które działają na kanałach, inicjatorach kanałów, nasłuchiwaniach i klastrach, znajdują się w sekcji Zabezpieczenia kanału.
- Informacje o komendach PCF, które działają na rekordach uprawnień, zawiera sekcja Sprawdzanie uprawnień dla komend PCF .

Dodatkowo, w systemach Windows , konto SYSTEM ma pełny dostęp do zasobów WebSphere MQ .

Na platformach UNIX and Linux tworzony jest również specjalny identyfikator użytkownika mqm, który może być używany tylko przez produkt. Nigdy nie może być ona dostępna dla użytkowników nieuprzywilejowanych. Wszystkie obiekty produktu WebSphere MQ należą do użytkownika o identyfikatorze mqm.

W systemach Windows członkowie grupy Administratorzy mogą również administrować dowolnym menedżerem kolejek, tak jak to może być kontem SYSTEM. Można również utworzyć grupę mqm domeny w kontrolerze domeny, która zawiera wszystkie identyfikatory użytkowników uprzywilejowanych aktywnych w domenie, a następnie dodać je do lokalnej grupy mqm. Niektóre komendy, na przykład **crtmqm**, manipulują uprawnieniami do obiektów IBM WebSphere MQ i dlatego potrzebują uprawnień do pracy z tymi obiektami (zgodnie z opisem podanym w poniższych sekcjach). Członkowie grupy mqm mają

uprawnienia do pracy ze wszystkimi obiektami, ale mogą wystąpić okoliczności w systemach Windows , gdy odmówiono uprawnienia, jeśli użytkownik ma użytkownika lokalnego i użytkownika uwierzytelnianego domeną o tej samej nazwie. Jest to opisane w sekcji “Jednostki główne i grupy” na stronie 208.

Wersje systemu Windows z funkcją Kontrola konta użytkownika (User Account Control-UAC) ograniczają działania użytkowników, które mogą być wykonywane w niektórych obiektach systemu operacyjnego, nawet jeśli są członkami grupy Administratorzy. Jeśli identyfikator użytkownika znajduje się w grupie Administratorzy, ale nie jest to grupa mqm, należy użyć wiersza komend z podniesionym poziomem uprawnień do wydania komend administracyjnych produktu WebSphere MQ , takich jak **crtmqm**, w przeciwnym razie zostanie wygenerowany błąd "AMQ7077: Nie masz uprawnień do wykonania żądanej operacji". Aby otworzyć wiersz komend z podniesionym poziomem uprawnień, należy kliknąć prawym przyciskiem myszy pozycję menu Start lub ikonę, a następnie wybrać opcję Uruchom jako administrator.

Nie ma potrzeby należeć do grupy mqm, aby wykonać następujące czynności:

- Wydaj komendy z programu użytkowego, które wydało komendy PCF lub komendy MQSC w ramach komendy Escape PCF, chyba że komendy manipulują inicjatorami kanału. (Te komendy są opisane w sekcji “Ochrona definicji inicjatora kanału” na stronie 74).
- Wywołaj wywołania MQI z programu użytkowego (chyba że wymagane jest użycie powiązań krótkiej ścieżki w wywołaniu MQCONNX).
- Użyj komendy `crtmqcvx` , aby utworzyć fragment kodu, który wykonuje konwersję danych dla struktur typów danych.
- Aby wyświetlić menedżery kolejek, należy użyć komendy `dspmq` .
- Użyj komendy `dspmqtrc` , aby wyświetlić dane wyjściowe śledzenia sformatowanego produktu WebSphere MQ .

Ograniczenie o 12 znaków dotyczy zarówno identyfikatorów grup, jak i użytkowników.

Platformy UNIX and Linux zwykle ograniczają długość identyfikatora użytkownika do 12 znaków. Produkt AIX , wersja 5.3 , podniósł ten limit, ale produkt WebSphere MQ nadal obserwuje ograniczenie 12 znaków na wszystkich platformach UNIX and Linux . Jeśli używany jest identyfikator użytkownika o długości większej niż 12 znaków, produkt WebSphere MQ zastąpi go wartością `UNKNOWN`. Nie należy definiować ID użytkownika o wartości `UNKNOWN`.

Zarządzanie grupą mqm

Użytkownicy należący do grupy mqm mają nadane pełne uprawnienia administracyjne w produkcie WebSphere MQ. Z tego powodu nie należy rejestrowywać aplikacji ani zwykłych użytkowników w grupie mqm. Grupa mqm powinna zawierać tylko konta administratorów produktu WebSphere MQ .

Zadania te są opisane w:

- Tworzenie grup i zarządzanie nimi w systemie Windows
- Tworzenie grup w systemie HP-UXi zarządzanie nimi
- Tworzenie grup i zarządzanie nimi w systemie AIX
- Tworzenie grup i zarządzanie nimi w systemie Solaris
- Tworzenie grup i zarządzanie nimi w systemie Linux

Jeśli kontroler domeny działa w systemie Windows 2000 lub Windows 2003, administrator domeny może skonfigurować specjalne konto dla produktu WebSphere MQ , które ma być używane. Jest to opisane w sekcji Konfigurowanie kont produktu WebSphere MQ.

Uprawnienia do pracy z obiektami IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Wszystkie obiekty są chronione przez program IBM WebSphere MQ, a nazwy użytkowników muszą mieć odpowiednie uprawnienia umożliwiające im dostęp do nich. Różne nazwy użytkowników wymagają różnych praw dostępu do różnych obiektów.

Wszystkie aplikacje, które używają wywołań MQI lub komend PCF, są dostępne dla menedżerów kolejek, kolejek, definicji procesów, list nazw, kanałów, kanałów połączeń klienta, programów nasłuchujących, usług i obiektów informacji uwierzytelniających. Wszystkie te zasoby są chronione przez produkt WebSphere MQ, a aplikacje muszą mieć uprawnienia dostępu do tych zasobów. Jednostką udostępniające żądanie może być użytkownik, program użytkowy, który wydaje wywołanie MQI, lub program administracyjny, który wydaje komendę PCF. Identyfikator requestera jest określany jako *nazwa użytkownika*.

Różne grupy użytkowników mogą być nadawane różnym typom uprawnień dostępu do tego samego obiektu. Na przykład dla określonej kolejki może być dozwolone wykonanie jednej grupy w celu wykonania operacji put i get; inna grupa może być dozwolona tylko w celu przeglądania kolejki (MQGET z opcją przeglądania). Podobnie niektóre grupy mogły umieścić i uzyskać uprawnienia do kolejki, ale nie mogą zmieniać atrybutów kolejki ani usuwać jej.

Niektóre operacje są szczególnie wrażliwe i powinny być ograniczone do użytkowników uprzywilejowanych. Na przykład:

- Dostęp do niektórych kolejek specjalnych, takich jak kolejki transmisji lub kolejka komend SYSTEM.ADMIN.COMMAND.QUEUE
- Uruchamianie programów, które używają pełnych opcji kontekstu MQI
- Tworzenie i usuwanie kolejek aplikacji

Pełne uprawnienia dostępu do obiektu są automatycznie nadawane identyfikatorowi użytkownika, który utworzył obiekt, oraz wszystkim członkom grupy mqm (oraz członkom lokalnej grupy Administratorzy w systemach Windows).

Pojęcia pokrewne

“Uprawnienie do administrowania produktem IBM WebSphere MQ w systemach UNIX, Linux, and Windows” na stronie 204
Administratorzy produktu IBM WebSphere MQ mogą używać wszystkich komend produktu IBM WebSphere MQ i nadawania uprawnień innym użytkownikom. Gdy administratorzy wydadzą komendy do zdalnych menedżerów kolejek, muszą mieć wymagane uprawnienia w zdalnym menedżerze kolejek. Dodatkowe uwagi dotyczą systemów Windows .

Podczas sprawdzania zabezpieczeń w systemach UNIX, Linux, and Windows

Operacje sprawdzania zabezpieczeń są zwykle wykonywane podczas łączenia się z menedżerem kolejek, otwierania lub zamykania obiektów oraz umieszczania lub pobierania komunikatów.

Sprawdzenia zabezpieczeń wprowadzone dla typowego zastosowania są następujące:

Nawiąże połączenie z menedżerem kolejek (wywołania MQCONN lub MQCONNX)
Jest to pierwszy raz, gdy aplikacja jest powiązana z określonym menedżerem kolejek. Menedżer kolejek interroguje środowisko operacyjne w celu wykrycia identyfikatora użytkownika powiązanego z aplikacją. Produkt WebSphere MQ sprawdza, czy ID użytkownika jest uprawniony do łączenia się z menedżerem kolejek i zachowuje ID użytkownika w celu przeprowadzenia przyszłych kontroli.

Użytkownicy nie muszą logować się do produktu WebSphere MQ; WebSphere MQ zakłada, że użytkownicy zapisali się do bazowego systemu operacyjnego i zostali uwierzytelnieni przez ten system.

Otwieranie obiektu (wywołania MQOPEN lub MQPUT1)
Dostęp do obiektów WebSphere MQ można uzyskać, otwierając obiekt i wydając mu komendy. Wszystkie operacje sprawdzania zasobów są wykonywane po otwarciu obiektu, a nie podczas uzyskiwania dostępu do niego. Oznacza to, że żądanie **MQOPEN** musi określać typ wymaganego dostępu (na przykład, czy użytkownik chce tylko przeglądać obiekt, czy też wykonać aktualizację, taką jak umieszczanie komunikatów w kolejce).

Produkt WebSphere MQ sprawdza zasób o nazwie określonej w żądaniu **MQOPEN** . W przypadku aliasu lub obiektu kolejki zdalnej używana jest autoryzacja samego obiektu, a nie kolejki, do której jest tłumaczona alias lub kolejka zdalna. Oznacza to, że użytkownik nie potrzebuje uprawnień dostępu do niego. Ogranicz uprawnienia do tworzenia kolejek do użytkowników uprzywilejowanych. Jeśli nie,

użytkownicy mogą ominąć zwykłą kontrolę dostępu po prostu przez utworzenie aliasu. Jeśli kolejka zdalna jest przywołana jawnie przy użyciu nazw kolejek i menedżerów kolejek, sprawdzana jest kolejka transmisji powiązana ze zdalnym menedżerem kolejek.

Uprawnienie do kolejki dynamicznej jest oparte na tej kolejce modelowej, z której pochodzi, ale niekoniecznie jest taka sama. Jest to opisane w uwadze “1” na stronie 94.

ID użytkownika używany przez menedżera kolejek w celu sprawdzenia dostępu jest identyfikatorem użytkownika uzyskanym ze środowiska operacyjnego aplikacji połączonej z menedżerem kolejek. Odpowiednio autoryzowana aplikacja może wywołać wywołanie **MQOPEN** , określając alternatywny ID użytkownika. Następnie zostaną przeprowadzone sprawdzenia kontroli dostępu na alternatywnym identyfikatorze użytkownika. Nie powoduje to zmiany identyfikatora użytkownika powiązanego z aplikacją, który jest używany tylko do sprawdzania kontroli dostępu.

Umieszczanie i pobieranie komunikatów (wywołania MQPUT lub MQGET)
Nie są wykonywane żadne sprawdzenia kontroli dostępu.

Zamykanie obiektu (MQCLOSE)
Nie są wykonywane żadne sprawdzenia kontroli dostępu, o ile **MQCLOSE** nie powoduje usunięcia kolejki dynamicznej. W tym przypadku istnieje sprawdzenie, czy ID użytkownika jest uprawniony do usunięcia kolejki.

Subskrybowanie tematu (MQSUB)
Gdy aplikacja subskrybuje temat, określa on typ operacji, którą musi wykonać. Jest to albo tworzenie nowej subskrypcji, zmiana istniejącej subskrypcji, albo wznawianie istniejącej subskrypcji bez jej zmiany. Dla każdego typu operacji menedżer kolejek sprawdza, czy identyfikator użytkownika powiązany z aplikacją ma uprawnienia do wykonania operacji.

Gdy aplikacja subskrybuje temat, sprawdzane są uprawnienia dotyczące obiektów tematu, które znajdują się w drzewie tematów, lub powyżej, punkt w drzewie tematów, w którym aplikacja została zasubskrybowana. Sprawdzanie uprawnień może obejmować sprawdzenie więcej niż jednego obiektu tematu.

Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest identyfikatorem użytkownika uzyskanym z systemu operacyjnego, gdy aplikacja łączy się z menedżerem kolejek.

Menedżer kolejek wykonuje sprawdzanie uprawnień w kolejkach subskrybenta, ale nie w kolejkach zarządzanych.

Sposób implementowania kontroli dostępu przez program IBM WebSphere MQ w systemach UNIX, Linux, and Windows

Produkt IBM WebSphere MQ korzysta z usług zabezpieczeń udostępnianych przez bazowy system operacyjny, korzystając z menedżera uprawnień do obiektów. Produkt IBM WebSphere MQ udostępnia komendy służące do tworzenia i obsługi list kontroli dostępu.

Interfejs kontroli dostępu o nazwie Interfejs usługi autoryzacji jest częścią produktu WebSphere MQ. Produkt WebSphere MQ udostępnia implementację menedżera kontroli dostępu (zgodnego z interfejsem usługi autoryzacji), który jest znany jako *menedżer uprawnień do obiektów (OAM)*. Jest on automatycznie instalowany i włączany dla każdego menedżera kolejek, który został utworzony, chyba że określono inaczej (zgodnie z opisem w sekcji “Zapobieganie sprawdzom dostępu do zabezpieczeń w systemach UNIX, Linux, and Windows” na stronie 173). OAM może zostać zastąpiony przez dowolny komponent napisany przez użytkownika lub dostawcę, który jest zgodny z interfejsem usługi autoryzacji.

OAM wykorzystuje funkcje bezpieczeństwa bazowego systemu operacyjnego, korzystając z identyfikatorów użytkowników i grup systemu operacyjnego. Użytkownicy mogą uzyskiwać dostęp do obiektów WebSphere MQ tylko wtedy, gdy mają one odpowiednie uprawnienia. “Sterowanie dostępem do obiektów za pomocą OAM w systemach UNIX, Linux i Windows” na stronie 165 opisuje sposób nadawania i odbierania tego uprawnienia.

OAM przechowuje listę kontroli dostępu (ACL) dla każdego zasobu, który steruje. Dane autoryzacji są przechowywane w lokalnej kolejce o nazwie SYSTEM.AUTH.DATA.QUEUE. Dostęp do tej kolejki jest ograniczony do użytkowników w grupie mqm, a dodatkowo w systemie Windows, do użytkowników

z grupy Administratorzy oraz do użytkowników zalogowanych przy użyciu identyfikatora SYSTEM. Nie można zmienić dostępu użytkownika do kolejki.

Produkt WebSphere MQ udostępnia komendy służące do tworzenia i obsługi list kontroli dostępu. Więcej informacji na temat tych komend zawiera sekcja “Sterowanie dostępem do obiektów za pomocą OAM w systemach UNIX, Linux i Windows” na stronie 165.

Produkt WebSphere MQ przekazuje żądanie OAM zawierające nazwę użytkownika, nazwę zasobu i typ dostępu. OAM nadaje lub odrzuca dostęp na podstawie listy ACL, którą utrzymuje. Produkt WebSphere MQ jest zgodny z decyzją OAM; jeśli OAM nie może podjąć decyzji, produkt WebSphere MQ nie zezwala na dostęp.

Identyfikowanie identyfikatora użytkownika w systemach UNIX, Linux, and Windows

Menedżer uprawnień do obiektów identyfikuje nazwę użytkownika, który żąda dostępu do zasobu. Identyfikator użytkownika używany jako nazwa użytkownika różni się w zależności od kontekstu.

Menedżer uprawnień do obiektu (Object Authority Manager-OAM) musi być w stanie zidentyfikować, kto żąda dostępu do określonego zasobu. Produkt IBM WebSphere MQ używa terminu *principal* do odwołania się do tego identyfikatora. Nazwa użytkownika jest ustanawiana, gdy aplikacja najpierw łączy się z menedżerem kolejek. Jest ona określana przez menedżer kolejek na podstawie identyfikatora użytkownika powiązanego z aplikacją nawiązują połączenie. (Jeśli aplikacja wysyła wywołania XA bez nawiązywania połączenia z menedżerem kolejek, to identyfikator użytkownika powiązany z aplikacją, która wydaje wywołanie xa_open, jest używany do sprawdzania uprawnień przez menedżer kolejek).

W systemach UNIX and Linux procedury autoryzacji sprawdzają rzeczywisty identyfikator użytkownika (logged-in) lub efektywny identyfikator użytkownika powiązany z aplikacją. Sprawdzany identyfikator użytkownika może być zależny od typu powiązania, aby uzyskać szczegółowe informacje na ten temat w sekcji Usługi instalowalne.

Program IBM WebSphere MQ propaguje odebrany identyfikator użytkownika z systemu w nagłówku komunikatu (struktura MQMD) każdego komunikatu jako identyfikacja użytkownika. Ten identyfikator jest częścią informacji o kontekście komunikatu i jest opisany w sekcji “Uprawnienia kontekstu w systemach UNIX, Linux i Windows” na stronie 210. Aplikacje nie mogą zmieniać tych informacji, jeśli nie zostały autoryzowane do zmiany informacji o kontekście.

Jednostki główne i grupy

Jednostki główne mogą należeć do grup. Istnieje możliwość nadania dostępu do określonego zasobu grupom, a nie osobom fizycznym, w celu zmniejszenia wymaganej liczby wymaganych czynności administracyjnych. W systemach UNIX and Linux wszystkie listy kontroli dostępu (ACL) są oparte na grupach, ale w systemach Windows ACLS jest oparte na identyfikatorach i grupach użytkowników.

Na przykład można zdefiniować grupę składającą się z użytkowników, którzy chcą uruchomić określoną aplikację. Inni użytkownicy mogą mieć dostęp do wszystkich zasobów, których wymagają, dodając identyfikator użytkownika do odpowiedniej grupy. Proces ten jest opisany w:

- Tworzenie grup i zarządzanie nimi w systemie Windows
- Tworzenie grup w systemie HP-UXi zarządzanie nimi
- Tworzenie grup i zarządzanie nimi w systemie AIX
- Tworzenie grup i zarządzanie nimi w systemie Solaris
- Tworzenie grup i zarządzanie nimi w systemie Linux

Jednostka główna może należeć do więcej niż jednej grupy (jej zestawu grup). Ma on agregat wszystkich uprawnień przyznanych każdej grupie w zestawie grup. Te uprawnienia są buforowane, więc wszelkie zmiany wprowadzane do grupy w nazwie głównej nie są rozpoznawane do momentu zrestartowania menedżera kolejek, chyba że zostanie wydana komenda MQSC REFRESH SECURITY (lub odpowiednik PCF).

Systemy UNIX and Linux

Wszystkie listy ACL są oparte na grupach. Gdy użytkownik ma nadany dostęp do określonego zasobu, grupa podstawowa ID użytkownika jest dołączana do listy ACL. Indywidualny identyfikator użytkownika nie jest uwzględniany, a uprawnienia są nadawane wszystkim członkom tej grupy. Z tego powodu należy pamiętać, że można nieumyślnie zmienić uprawnienia użytkownika, zmieniając uprawnienia innego użytkownika w tej samej grupie. Wszyscy użytkownicy są przypisani do domyślnej grupy użytkowników *nobody* , a domyślnie do tej grupy nie są nadawane żadne autoryzacje. Istnieje możliwość zmiany autoryzacji w grupie *nobody* w celu nadania użytkownikom dostępu do zasobów produktu WebSphere MQ bez konkretnych autoryzacji.

Nie definiuj ID użytkownika o wartości "UNKNOWN". Wartość "UNKNOWN" jest używana, gdy ID użytkownika jest zbyt długi, więc dowolne identyfikatory użytkowników będą korzystały z uprawnień dostępu UNKNOWN.

Identyfikatory użytkowników mogą zawierać do 12 znaków i nazw grup do 12 znaków.

Systemy Windows

Listy ACL są oparte na identyfikatorach użytkowników i grupach. Kontrole są takie same, jak w przypadku systemów UNIX , z tą różnicą, że poszczególne identyfikatory użytkowników mogą być również wyświetlane na liście ACL. Z tym samym identyfikatorem użytkownika można mieć różnych użytkowników w różnych domenach. Produkt WebSphere MQ umożliwia kwalifikowanie identyfikatorów użytkowników za pomocą nazwy domeny, dzięki czemu użytkownicy mogą mieć dostęp do różnych poziomów dostępu.

Nazwa grupy może opcjonalnie zawierać nazwę domeny, która jest określona w następujących formatach:

```
GroupName@domain
domain\GroupName
```

Grupy globalne są sprawdzane przez OAM tylko w dwóch przypadkach:

1. Sekcja zabezpieczeń menedżera kolejek zawiera następujące ustawienie: `GroupModel=GlobalGroups`; patrz Zabezpieczenia.
2. Menedżer kolejek korzysta z alternatywnej grupy dostępu do zabezpieczeń; patrz **crtmqm**.

Identyfikatory użytkowników mogą zawierać do 20 znaków, nazw domen o długości do 15 znaków oraz nazw grup o długości do 64 znaków.

OAM najpierw sprawdza lokalną bazę danych zabezpieczeń, a następnie bazę danych domeny podstawowej, a w końcu bazę danych wszystkich zaufanych domen. Pierwszy napotkany identyfikator użytkownika jest używany przez OAM do sprawdzania. Każdy z tych identyfikatorów użytkowników może mieć różne przypisania do grup na danym komputerze.

Niektóre komendy sterujące (na przykład `crtmqm`) zmieniają uprawnienia do obiektów WebSphere MQ za pomocą menedżera uprawnień do obiektów (Object Authority Manager-OAM). OAM przeszukuje bazy danych zabezpieczeń w kolejności podanej w poprzednim akapicie, aby określić uprawnienia dla konkretnego identyfikatora użytkownika. W wyniku tego uprawnienia określone przez OAM mogą przesłonić fakt, że ID użytkownika jest członkiem lokalnej grupy mqm. Jeśli na przykład komenda `crtmqm` zostanie wydana z ID użytkownika uwierzytelnionego przez kontroler domeny, który ma przypisanie do lokalnej grupy mqm za pośrednictwem grupy globalnej, wykonanie komendy nie powiedzie się, jeśli w systemie istnieje użytkownik lokalny o tej samej nazwie, który nie znajduje się w lokalnej grupie mqm.

Identyfikatory zabezpieczeń systemu Windows (SID)

Produkt WebSphere MQ w systemie Windows korzysta z identyfikatora SID, w którym jest dostępny. Jeśli identyfikator SID systemu Windows nie zostanie dostarczony z żądaniem autoryzacji, produkt WebSphere MQ identyfikuje użytkownika w oparciu o samą nazwę użytkownika, ale może to spowodować, że nadawany jest niepoprawny organ.

W systemach Windows identyfikator zabezpieczeń (SID) jest używany do uzupełnienia identyfikatora użytkownika. Identyfikator SID zawiera informacje identyfikujące pełne szczegóły konta użytkownika

w bazie danych SAM (Security account manager-SAM) systemu Windows , w której zdefiniowany jest użytkownik. Gdy komunikat jest tworzony w produkcie WebSphere MQ for Windows, produkt WebSphere MQ zapisuje identyfikator SID w deskryptorze komunikatu. Gdy produkt WebSphere MQ w systemie Windows wykonuje sprawdzenia autoryzacji, używa identyfikatora SID do wysyłania zapytań do pełnych informacji z bazy danych SAM. (Baza danych SAM, w której zdefiniowany jest użytkownik, musi być dostępna dla tego zapytania, aby powiodło się).

Domyślnie, jeśli identyfikator SID systemu Windows nie jest dostarczony z żądaniem autoryzacji, produkt WebSphere MQ identyfikuje użytkownika w oparciu o samą nazwę użytkownika. W tym celu przeszukując bazy danych zabezpieczeń w następującej kolejności:

1. Lokalna baza danych zabezpieczeń
2. Baza danych zabezpieczeń domeny podstawowej
3. Baza danych zabezpieczeń dla zaufanych domen

Jeśli nazwa użytkownika nie jest unikalna, mogą zostać nadane niepoprawne uprawnienia produktu WebSphere MQ . Aby zapobiec temu problemowi, należy dołączyć identyfikator SID w każdym żądaniu autoryzacji. Identyfikator SID jest używany przez produkt WebSphere MQ w celu ustanowienia referencji użytkownika.

Aby określić, że wszystkie żądania autoryzacji muszą zawierać identyfikator SID, należy użyć komendy `regedit`. Ustaw parametr SecurityPolicy na wartość NTSIDsRequired.

Uprawnienia użytkownika alternatywnego w systemach UNIX, Linux i Windows

Użytkownik może określić, że ID użytkownika może korzystać z uprawnień innego użytkownika podczas uzyskiwania dostępu do obiektu WebSphere MQ . Jest to nazywane *uprawnieniem alternatywnym użytkownika*i można go używać w dowolnym obiekcie WebSphere MQ .

Uprawnienie użytkownika alternatywnego jest niezbędne, gdy serwer odbiera żądania od programu i chce upewnić się, że program ma wymagane uprawnienia do żądania. Serwer może mieć wymagane uprawnienia, ale musi wiedzieć, czy program ma uprawnienia do działań, o które się zażądano.

Na przykład załóżmy, że program serwera działający pod ID użytkownika PAYSERV pobiera komunikat żądania z kolejki umieszczonej w kolejce przez użytkownika o identyfikatorze USER1. Gdy program serwera pobiera komunikat z żądaniem, przetwarza żądanie i umieszcza odpowiedź z powrotem w kolejce odpowiedzi określonej za pomocą komunikatu żądania. Zamiast używać własnego ID użytkownika (PAYSERV) do autoryzowania otwarcia kolejki odpowiedzi, serwer może określić inny ID użytkownika, w tym przypadku USER1. W tym przykładzie można użyć uprawnień użytkownika alternatywnego do określenia, czy program PAYSERV ma uprawnienia do określania wartości USER1 jako identyfikatora użytkownika alternatywnego podczas otwierania kolejki zwrotnej.

Identyfikator użytkownika alternatywnego jest określony w polu **`AlternateUserId`** deskryptora obiektu.

Uprawnienia kontekstu w systemach UNIX, Linux i Windows

Kontekst to informacja, która odnosi się do konkretnego komunikatu i jest zawarta w deskryptorze komunikatu, MQMD, który jest częścią komunikatu. Aplikacje mogą określać dane kontekstu, gdy zostanie wykonane wywołanie programu `MQOPEN` lub `MQPUT` .

Informacje o kontekście są wyświetlane w dwóch sekcjach:

Sekcja Tożsamość
Z kim pochodzi wiadomość. Składa się on z pól `UserIdentifier`, `AccountingTokeni` `ApplIdentityData` .

Sekcja Pochodzenie
Miejsce, z którego pochodzi komunikat, a po umieszczonym w kolejce. Składa się on z pól `PutApplType`, `PutApplName`, `PutDate`, `PutTimei` `ApplOriginData` .

Aplikacje mogą określać dane kontekstu, gdy zostanie wykonane wywołanie programu `MQOPEN` lub `MQPUT` . Dane te mogą być generowane przez aplikację, przekazywane z innego komunikatu lub przez

domyślnie wygenerowane przez menedżer kolejek. Na przykład, dane kontekstowe mogą być używane przez programy serwera do sprawdzania tożsamości requestera, sprawdzania, czy komunikat pochodzi z aplikacji działającej pod autoryzowanym ID użytkownika.

Program serwera może użyć `UserIdentifier` do określenia identyfikatora użytkownika alternatywnego. Za pomocą autoryzacji kontekstowej można określić, czy użytkownik może określić dowolne opcje kontekstu w dowolnym wywołaniu programu `MQOPEN` lub `MQPUT1` .

Informacje na temat opcji kontekstu oraz opis pól deskryptora komunikatu związanych z kontekstem zawiera sekcja Kontrolowanie informacji o kontekście w celu uzyskania informacji na temat opcji kontekstu oraz Przegląd dla deskryptora MQMD .

Implementowanie kontroli dostępu w wyjściach zabezpieczeń

Istnieje możliwość zaimplementowania kontroli dostępu w wyjściu zabezpieczeń przy użyciu identyfikatora MCAUserIdentifier lub menedżera uprawnień do obiektów.

MCAUserIdentifier

Każda instancja bieżącego kanału ma powiązaną strukturę definicji kanału, MQCD. Wartości początkowe pól w tabeli MQCD są określane przez definicję kanału, która jest tworzona przez administratora produktu WebSphere MQ . W szczególności wartość początkowa jednego z pól, *MCAUserIdentifier*, jest określana na podstawie wartości parametru MCAUSER komendy DEFINE CHANNEL lub przez odpowiednik parametru MCAUSER, jeśli definicja kanału jest tworzona w inny sposób. *MCAUserIdentifier* zawiera pierwsze 12 bajtów identyfikatora użytkownika MCA. Jeśli identyfikator użytkownika MCA nie jest pusty, określa on identyfikator użytkownika, który ma być używany przez agenta kanału komunikatów do autoryzacji w celu uzyskania dostępu do zasobów MQ . Upewnij się, że wartość parametru MCAUSER jest mniejsza niż 12 znaków na platformie Windows.

Struktura MQCD jest przekazywana do programu obsługi wyjścia kanału, gdy jest wywoływana przez agenta MCA. Gdy wyjście zabezpieczeń jest wywoływane przez agenta MCA, wyjście zabezpieczeń może zmienić wartość parametru *MCAUserIdentifier*, zastępując dowolną wartość określoną w definicji kanału.

W systemach IBM i, UNIX, Linux i Windows , jeśli wartość parametru *MCAUserIdentifier* nie jest pusta, menedżer kolejek używa wartości *MCAUserIdentifier* jako identyfikatora użytkownika dla sprawdzania uprawnień, gdy agent MCA próbuje uzyskać dostęp do zasobów menedżera kolejek po nawiązaniu połączenia z menedżerem kolejek. Jeśli wartość parametru *MCAUserIdentifier* jest pusta, menedżer kolejek używa domyślnego ID użytkownika agenta MCA. Ma to zastosowanie do kanałów RCVR, RQSTR, CLUSRCVR i SVRCONN. W przypadku wysyłania MCAs domyślny identyfikator użytkownika jest zawsze używany do sprawdzania uprawnień, nawet jeśli wartość parametru *MCAUserIdentifier* nie jest pusta.

W systemie z/OSmenedżer kolejek może używać wartości *MCAUserIdentifier* do sprawdzania uprawnień, pod warunkiem, że nie jest on pusty. W przypadku odbierania MCA i połączenia z serwerem MCAs, czy menedżer kolejek używa wartości *MCAUserIdentifier* dla sprawdzania uprawnień, zależy od:

- Wartość parametru PUTAUT w definicji kanału
- Profil RACF używany do sprawdzania
- Poziom dostępu identyfikatora użytkownika przestrzeni adresowej inicjatora kanału do profilu RESLEVEL.

W przypadku wysyłania MCAs zależy to od:

- Określa, czy wysyłający agent MCA jest programem wywołującym, czy odpowiadającego
- Poziom dostępu identyfikatora użytkownika przestrzeni adresowej inicjatora kanału do profilu RESLEVEL.

Identyfikator użytkownika, którego sklepy wyjścia zabezpieczeń w katalogu *MCAUserIdentifier* mogą być nabywane na różne sposoby. Poniżej przedstawiono kilka przykładów:

- Jeśli na końcu kanału MQI kanału MQI nie ma wyjścia zabezpieczeń, identyfikator użytkownika powiązany z przepływami aplikacji klienta WebSphere MQ z połączenia klienckiego MCA z agentem MCA połączenia z serwerem, gdy aplikacja kliencka zgłasza wywołanie MQCONN.Agent MCA połączenia

serwera przechowuje ten identyfikator użytkownika w polu *RemoteUserIdentifier* w strukturze definicji kanału, MQCD. Jeśli wartość parametru *MCAUserIdentifier* jest w tym momencie pusta, agent MCA przechowuje ten sam identyfikator użytkownika w katalogu *MCAUserIdentifier*. Jeśli agent MCA nie przechowuje identyfikatora użytkownika w polu *MCAUserIdentifier*, wyjście zabezpieczeń może go później wykonać, ustawiając wartość *MCAUserIdentifier* na wartość *RemoteUser*.

Jeśli ID użytkownika, który przepływa z systemu klienckiego, wprowadza nową domenę zabezpieczeń i nie jest poprawny w systemie serwera, wyjście zabezpieczeń może zastąpić identyfikator użytkownika, który jest poprawny, i zapisać podstawiony identyfikator użytkownika w polu *MCAUserIdentifier*.

- Identyfikator użytkownika może zostać wysłany przez wyjście zabezpieczeń partnera w komunikacie bezpieczeństwa.

  W kanale komunikatów wyjście zabezpieczeń wywoływane przez wysyłający agent MCA może wysłać ID użytkownika, pod którym działa wysyłający agent MCA. Wyjście zabezpieczeń wywoływane przez odbierający agent MCA może następnie zapisać identyfikator użytkownika w polu *MCAUserIdentifier*. Podobnie, w przypadku kanału MQI wyjście zabezpieczeń na końcu kanału klienta może wysłać identyfikator użytkownika powiązany z aplikacją kliencką MQI produktu WebSphere MQ . Wyjście zabezpieczeń na końcu kanału serwera może następnie przechowywać identyfikator użytkownika w polu *MCAUserIdentifier*. Podobnie jak w poprzednim przykładzie, jeśli ID użytkownika nie jest poprawny w systemie docelowym, wyjście zabezpieczeń może zastąpić identyfikator użytkownika, który jest poprawny, i zapisać podstawiony identyfikator użytkownika w polu *MCAUserIdentifier*.

  Jeśli certyfikat cyfrowy jest odbierany jako część usługi identyfikacji i uwierzytelniania, wyjście zabezpieczeń może odwzorować nazwę wyróżniającą w certyfikacie na ID użytkownika, który jest poprawny w systemie docelowym. Następnie może on przechowywać identyfikator użytkownika w polu *MCAUserIdentifier*.
- Jeśli protokół SSL jest używany w kanale, nazwa wyróżniająca partnera jest przekazywana do wyjścia w polu SSLPeerNamew tabeli MQCD, a nazwa wyróżniająca wystawcy tego certyfikatu jest przekazywana do wyjścia w polu SSLRemCertIssNamePtr w MQCXP.

Więcej informacji na temat pola *MCAUserIdentifier* , struktury definicji kanału, MQCD i struktury parametru wyjścia kanału (MQCXP) zawiera sekcja Wywołania obsługi wyjścia kanału i struktury danych. Więcej informacji na temat identyfikatora użytkownika, który przepływa z systemu klienckiego w kanale MQI, zawiera sekcja Kontrola dostępu.

Uwaga: Aplikacje wyjścia zabezpieczeń utworzone przed wydaniem produktu WebSphere MQ v7.1 mogą wymagać aktualizacji. Więcej informacji na ten temat zawiera sekcja Programy obsługi wyjścia zabezpieczeń kanału.

Uwierzytelnianie użytkownika menedżera uprawnień do obiektów WebSphere MQ

W przypadku połączeń klienta MQI produktu WebSphere MQ wyjścia zabezpieczeń mogą być używane do modyfikowania lub tworzenia struktury MQCSP używanej w uwierzytelnianiu użytkownika OAM (Object Authority Manager). Jest to opisane w sekcji Programy obsługi wyjścia kanału dla kanałów przesyłania komunikatów .

Implementowanie kontroli dostępu w wyjściach komunikatów

Może być konieczne użycie wyjścia komunikatu w celu zastąpienia jednego identyfikatora użytkownika innym.

Rozważmy aplikację kliencką, która wysyła komunikat do aplikacji serwera. Aplikacja serwera może wyodrębnić identyfikator użytkownika z pola *UserIdentifier* w deskryptorze komunikatu i pod warunkiem, że ma on alternatywne uprawnienia użytkownika, poproś menedżera kolejek o użycie tego identyfikatora użytkownika do sprawdzania uprawnień podczas uzyskiwania dostępu do zasobów produktu WebSphere MQ w imieniu klienta.

Jeśli parametr PUTAUT jest ustawiony na CTX (lub ALTMCA w systemie z/OS) w definicji kanału, identyfikator użytkownika w polu *UserIdentifier* każdego komunikatu przychodzącego jest używany do sprawdzania uprawnień, gdy agent MCA otworzy kolejkę docelową.

W pewnych okolicznościach, gdy generowany jest komunikat raportu, jest on umieszczany przy użyciu uprawnień identyfikatora użytkownika w polu *UserIdentifier* komunikatu, który powoduje zgłoszenie raportu. W szczególności raporty z potwierdzeniem odbioru (COD) i raporty o utracie ważności są zawsze umieszczane z tym uprawnieniem.

Ze względu na te sytuacje konieczne może być zastąpienie jednego identyfikatora użytkownika w polu *UserIdentifier* jako komunikatu wprowadzanego do nowej domeny zabezpieczeń. Może to być wykonane przez wyjście komunikatu na odbierającym końcu kanału. Alternatywnie można się upewnić, że identyfikator użytkownika w polu *UserIdentifier* komunikatu przychodzącego jest zdefiniowany w nowej domenie zabezpieczeń.

Jeśli komunikat przychodzący zawiera certyfikat cyfrowy dla użytkownika aplikacji, który wysłał komunikat, program obsługi wyjścia komunikatów może sprawdzić poprawność certyfikatu i odwzorować nazwę wyróżniającą w certyfikacie na identyfikator użytkownika, który jest poprawny w systemie odbierającym. Następnie można ustawić wartość pola *UserIdentifier* w deskryptorze komunikatu na ten identyfikator użytkownika.

Jeśli konieczne jest wyjście komunikatu w celu zmiany wartości pola *UserIdentifier* w komunikacie przychodzącym, może być ono odpowiednie dla wyjścia komunikatu w celu uwierzytelnienia nadawcy komunikatu w tym samym czasie. Szczegółowe informacje na ten temat zawiera sekcja “Odwzorowywanie tożsamości w wyjściach komunikatów” na stronie 154.

Implementowanie kontroli dostępu w wyjściu API i interfejsie wyjścia funkcji API

Wyjście interfejsu API lub wyjścia funkcji API może zapewnić dostęp do elementów sterujących w celu uzupełnienia tych udostępnionych przez produkt WebSphere MQ. W szczególności wyjście może zapewnić kontrolę dostępu na poziomie komunikatu. Wyjście może zapewnić, że aplikacja umieszcza w kolejce lub pobiera z kolejki tylko te komunikaty, które spełniają określone kryteria.

Rozważmy następujące przykłady:

- Komunikat zawiera informacje o zamówieniu. Gdy aplikacja próbuje umieścić komunikat w kolejce, interfejs API lub wyjście funkcji API może sprawdzić, czy łączna wartość zamówienia jest mniejsza niż określona wartość graniczna.
- Komunikaty docierają do kolejki docelowej ze zdalnych menedżerów kolejek. Gdy aplikacja próbuje pobrać komunikat z kolejki, interfejs API lub wyjście funkcji API może sprawdzić, czy nadawca komunikatu jest uprawniony do wysłania komunikatu do kolejki.

Poufność komunikatów

Aby zachować poufność, należy zaszyfrować komunikaty. W zależności od potrzeb dostępne są różne metody szyfrowania komunikatów w produkcie WebSphere MQ .

Wybór opcji CipherSpec określa, jaki poziom poufności ma być używany.

Jeśli wymagany jest poziom aplikacji, kompleksowa ochrona danych dla infrastruktury przesyłania komunikatów z punktu do punktu, można użyć produktu WebSphere MQ Advanced Message Security w celu zaszyfrowania komunikatów lub napisania własnego wyjścia funkcji API lub wyjścia funkcji API-przejście.

Jeśli wymagane jest szyfrowanie wiadomości tylko wtedy, gdy są one transportowane przez kanał, ponieważ użytkownik ma odpowiednie zabezpieczenia w menedżerach kolejek, może użyć protokołu SSL lub TLS lub można napisać własne wyjście zabezpieczeń, wyjście komunikatów lub programy obsługi wyjścia wysyłania i odbierania.

Więcej informacji na temat produktu WebSphere MQ Advanced Message Securityzawiera sekcja “Planowanie dla produktu Advanced Message Security” na stronie 66.Korzystanie z protokołu SSL i TLS z produktem WebSphere MQ jest opisane w sekcji “Obsługa protokołu SSL i TLS w produkcie IBM WebSphere MQ” na stronie 24. Korzystanie z programów obsługi wyjścia w szyfrowaniu komunikatów jest

opisane w sekcji “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 233.

Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS

Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację protokołu SSL lub TLS, należy zdefiniować kanały w celu użycia protokołu SSL lub TLS. Należy również uzyskać certyfikaty cyfrowe i zarządzać nimi. W systemie testowym można użyć samopodpisanych certyfikatów lub certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA). W systemie produkcyjnym nie należy używać certyfikatów samopodpisanych. Więcej informacji na ten temat zawiera sekcja ..//zs14140_.dita.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows” na stronie 118.

W tej kolekcji tematów przedstawiono zadania związane z konfigurowaniem komunikacji SSL oraz szczegółowe informacje na temat wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalną częścią protokołów. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji produktu WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

Uwagi:

1. W tym kontekście klient SSL odwołuje się do połączenia inicjującego uzgadnianie.
2. Więcej informacji na ten temat zawiera Glosariusz .

W systemach UNIX, Linux i Windows klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie WebSphere MQ , co oznacza `ibmwebspheremq` , po którym następuje zmiana nazwy menedżera kolejek na małe litery. Na przykład: `QM1`, `ibmwebspheremqqm1`.

Produkt WebSphere MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się tylko wtedy, gdy koniec kanału, który działa jako serwer SSL lub TLS, jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER. Więcej informacji na temat anonimowego połączenia z menedżerem kolejek, czyli gdy klient SSL lub TLS nie wysyła certyfikatu, zawiera sekcja “Łączenie dwóch menedżerów kolejek przy użyciu jednokierunkowego uwierzytelniania” na stronie 218.

Korzystanie z certyfikatów samopodpisanych w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek

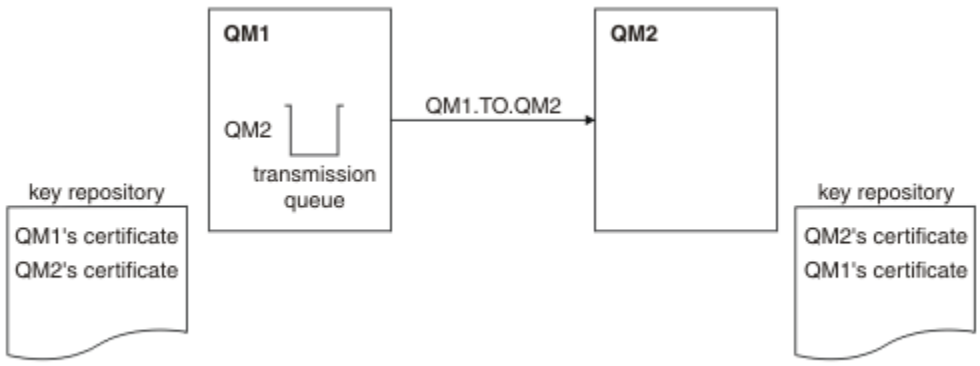
Wykonaj poniższe przykładowe instrukcje, aby zaimplementować wzajemne uwierzytelnianie między dwoma menedżerami kolejek przy użyciu samopodpisanych certyfikatów SSL lub TLS.

O tym zadaniu

Scenariusz:

- Istnieją dwa menedżery kolejek: QM1 i QM2, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między QM1 i QM2.
- Zdecydowałeś się przetestować bezpieczną komunikację przy użyciu samopodpisanych certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 14. Konfiguracja wynikający z tego zadania

W programie Rysunek 14 na stronie 215repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat publiczny z QM2. Repozytorium kluczy dla QM2 zawiera certyfikat dla QM2 i certyfikat publiczny z QM1.

Procedura

1. Przygotuj repozytorium kluczy dla każdego menedżera kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Utwórz samopodpisany certyfikat dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
3. Wyodrębnij kopię każdego certyfikatu:
   - W systemach UNIX, Linuxi Windows.
4. Prześlij publiczną część certyfikatu QM1 do systemu QM2 i odwrotnie, korzystając z programu narzędziowego, takiego jak FTP.
5. Dodaj certyfikat partnera do repozytorium kluczy dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
6. W przypadku QM1zdefiniuj kanał nadawczy i powiązaną kolejkę transmisji, wydając komendy, takie jak w poniższym przykładzie:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   W tym przykładzie użyto komendy CipherSpec RC4_MD5. Specyfikacje CipherSpecs na każdym końcu kanału muszą być takie same.
7. W systemie QM2zdefiniuj kanał odbiorczy, wydając komendę, tak jak w poniższym przykładzie:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
   ```

   Kanał musi mieć taką samą nazwę, jak kanał nadawczy zdefiniowany w kroku 6, i użyć tej samej wartości CipherSpec.
8. Uruchom kanał.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 14 na stronie 215 .

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do tych przedstawionych w poniższych przykładach.

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

W menedżerze kolejek QM2wprowadź następującą komendę:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

W każdym przypadku wartość parametru SSLPEER musi być zgodna z nazwą DN w certyfikacie partnera, który został utworzony w kroku 2. Nazwa emitentów jest zgodna z nazwą węzła sieci, ponieważ certyfikat jest samopodpisany.

Parametr SSLPEER jest opcjonalny. Jeśli ta wartość jest określona, należy ustawić jej wartość tak, aby nazwa wyróżniająca w certyfikacie partnerskim (utworzonym w kroku 2) była dozwolona. Więcej informacji na temat korzystania z funkcji SSLPEER zawiera sekcja Reguły WebSphere MQ dla wartości SSLPEER .

Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek

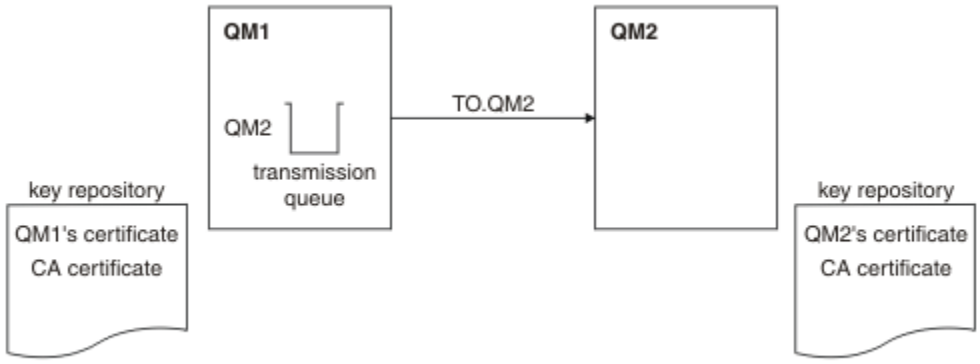
Wykonaj poniższe przykładowe instrukcje, aby zaimplementować wzajemne uwierzytelnianie między dwoma menedżerami kolejek przy użyciu certyfikatów SSL podpisanych przez ośrodek CA lub TLS.

O tym zadaniu

Scenariusz:

- Istnieją dwa menedżery kolejek o nazwach QMA i QMB, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnienie między QMA a QMB.
- W przyszłości planujesz korzystać z tej sieci w środowisku produkcyjnym, dlatego od początku zdecydowałeś się na korzystanie z podpisanych przez CA certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 15. Konfiguracja wynikający z tego zadania

W programie Rysunek 15 na stronie 217repozytorium kluczy dla QMA zawiera certyfikat QMA i certyfikat ośrodka CA. Repozytorium kluczy QMB zawiera certyfikat QMB i certyfikat CA. W tym przykładzie zarówno certyfikat QMA, jak i certyfikat QMB zostały wydane przez ten sam ośrodek CA. Jeśli certyfikat QMA i certyfikat QMB zostały wydane przez różne ośrodki certyfikacji (CA), repozytoria kluczy dla QMA i QMB muszą zawierać oba certyfikaty ośrodka CA.

Procedura

1. Przygotuj repozytorium kluczy dla każdego menedżera kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Zażądaj certyfikatu podpisanego przez ośrodek CA dla każdego menedżera kolejek.

   Dla dwóch menedżerów kolejek mogą być używane różne wartości CAs.
   - W systemach UNIX, Linuxi Windows.
3. Dodaj certyfikat ośrodka certyfikacji do repozytorium kluczy dla każdego menedżera kolejek:

   Jeśli menedżery kolejek korzystają z różnych ośrodków certyfikacji, to certyfikat ośrodka certyfikacji dla każdego ośrodka certyfikacji musi być dodany do obu repozytoriów kluczy.
   - W systemach UNIX, Linuxi Windows.
4. Dodaj certyfikat podpisany przez ośrodek CA do repozytorium kluczy dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
5. W systemie QMA zdefiniuj kanał nadawczy i powiązaną kolejkę transmisji, wydając komendy, takie jak w poniższym przykładzie:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   W tym przykładzie użyto komendy CipherSpec RC4_MD5. Specyfikacje CipherSpecs na każdym końcu kanału muszą być takie same.
6. W QMB zdefiniuj kanał odbiorczy, wydając komendę, tak jak w poniższym przykładzie:

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
   ```

   Kanał musi mieć taką samą nazwę, jak kanał nadawczy zdefiniowany w kroku 6, i użyć tej samej wartości CipherSpec.
7. Uruchom kanał:

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 15 na stronie 217.

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do przedstawionych w poniższych przykładach.

W menedżerze kolejek QMA wprowadź następującą komendę:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

W menedżerze kolejek QMB wpisz następującą komendę:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

W każdym przypadku wartość parametru SSLPEER musi być zgodna z nazwą wyróżniającą (DN) w certyfikacie partnera, który został utworzony w kroku 2. Nazwa wystawcy jest zgodna z nazwą wyróżniającą podmiotu certyfikatu ośrodka CA, który podpisał certyfikat osobisty dodany w kroku 4.

Łączenie dwóch menedżerów kolejek przy użyciu jednokierunkowego uwierzytelniania

Wykonaj poniższe przykładowe instrukcje, aby zmodyfikować system z wzajemnym uwierzytelnianiem, aby umożliwić menedżerowi kolejek nawiązanie połączenia przy użyciu jednokierunkowego uwierzytelniania. Jest to, gdy klient SSL lub TLS nie wysyła certyfikatu.

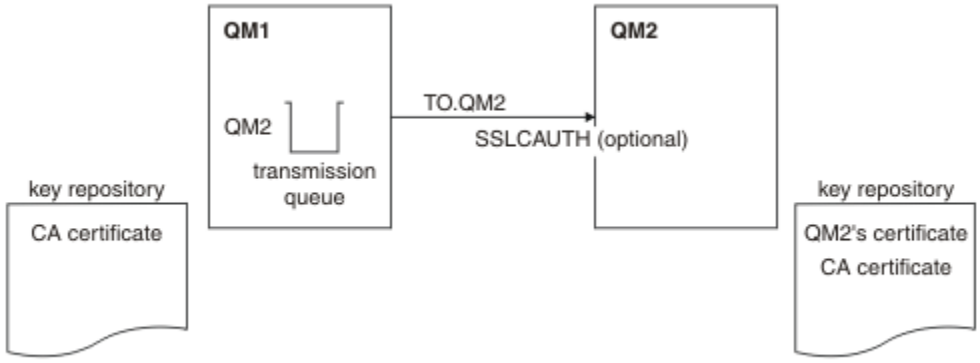
O tym zadaniu

Scenariusz:

- Dwa menedżery kolejek (QM1 i QM2) zostały skonfigurowane tak, jak w programie “Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek” na stronie 216.

- Użytkownik chce zmienić wartość QM1 , tak aby łączyła się z uwierzytelnianiem jednokierunkową na QM2.

Wynikowa konfiguracja wygląda następująco:



Rysunek 16. Menedżery kolejek zezwalające na uwierzytelnianie jednokierunkowe

Procedura

1. Usuń certyfikat osobisty QM1ze swojego repozytorium kluczy, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows. Certyfikat jest oznaczony w następujący sposób:
     - `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek składanego na małe litery. Na przykład: `QM1` , `ibmwebspheremqqm1`.
2. Opcjonalne: Jeśli w menedżerze kolejek QM1zostały wcześniej uruchomione jakiekolwiek kanały SSL lub TLS, odśwież środowisko SSL lub TLS.
3. Zezwalaj na anonimowe połączenia z odbiornikiem.

Wyniki

Repozytoria kluczy i kanały są zmieniane w sposób ilustrowany w programie Rysunek 16 na stronie 219 .

Co dalej

Jeśli kanał nadawczy był uruchomiony, a użytkownik wydał komendę REFRESH SECURITY TYPE (SSL) (w kroku 2), kanał zostanie zrestartowany automatycznie. Jeśli kanał nadawczy nie był uruchomiony, uruchom go.

Po zakończeniu działania kanału na serwerze, wartość parametru nazwy węzła na ekranie statusu kanału wskazuje, że wystąpił certyfikat klienta.

Sprawdź, czy zadanie zostało pomyślnie zakończone, wydając niektóre komendy DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowa wartość wyjściowa jest podobna do przedstawionej w poniższych przykładach:

Z poziomu menedżera kolejek QM1 wprowadź następującą komendę:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
```

```
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                          SUBSTATE(MQGET)
   XMITQ(QM2)
```

Z poziomu menedżera kolejek QM2 wprowadź następującą komendę:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                          CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                      CURRENT
   RQMNAME(QMA)                             SSLCERTI( )
   SSLPEER( )                               STATUS(RUNNING)
   SUBSTATE(RECEIVE)                        XMITQ( )
```

W przypadku QM2pole SSLPEER jest puste, co oznacza, że QM1 nie wysyłało certyfikatu. W przypadku QM1wartość SSLPEER jest zgodna z nazwą wyróżniającą (DN) w certyfikacie osobistym QM2.

Bezpieczne podłączanie klienta do menedżera kolejek

Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację protokołu SSL lub TLS, należy zdefiniować kanały w celu użycia protokołu SSL lub TLS. Należy również uzyskać certyfikaty cyfrowe i zarządzać nimi. W systemie testowym można użyć samopodpisanych certyfikatów lub certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA). W systemie produkcyjnym nie należy używać certyfikatów samopodpisanych. Więcej informacji na ten temat zawiera sekcja ..//zs14140_.dita.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows” na stronie 118.

W tej kolekcji tematów przedstawiono zadania związane z konfigurowaniem komunikacji SSL oraz szczegółowe informacje na temat wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalną częścią protokołów. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji produktu WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemach UNIX, Linux, and Windows klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie WebSphere MQ , czyli `ibmwebspheremq` , po której następuje zmiana ID użytkownika logowania na małe litery, na przykład `ibmwebspheremqmyuserid`.

Produkt WebSphere MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się tylko wtedy, gdy koniec kanału, który działa jako serwer SSL lub TLS, jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER. Więcej informacji na temat anonimowego połączenia menedżera kolejek zawiera sekcja “Anonimowo połączenie klienta z menedżerem kolejek” na stronie 224.

Korzystanie z certyfikatów samopodpisanych na potrzeby wzajemnego uwierzytelniania klienta i menedżera kolejek

Aby zaimplementować wzajemne uwierzytelnianie między klientem a menedżerem kolejek, należy postępować zgodnie z tymi przykładowymi instrukcjami, korzystając z samopodpisanych certyfikatów SSL lub TLS.

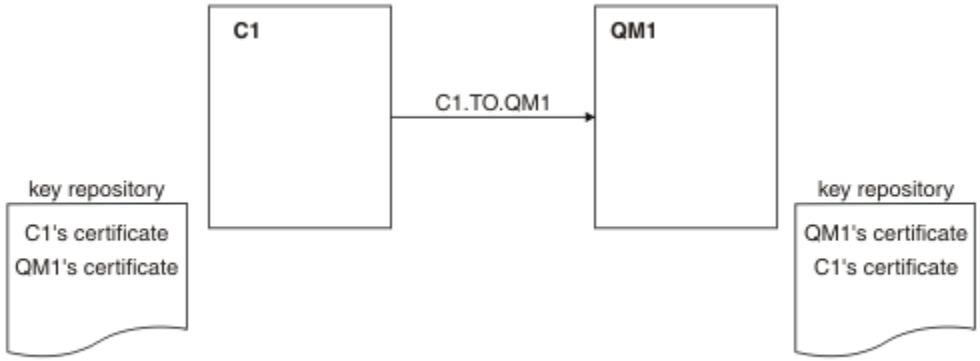
O tym zadaniu

Scenariusz:

- Istnieje klient C1i menedżer kolejek QM1, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między C1 i QM1.
- Zdecydowałeś się przetestować bezpieczną komunikację za pomocą samopodpisanych certyfikatów.

Program DCM w systemie IBM i nie obsługuje certyfikatów samopodpisanych, dlatego to zadanie nie ma zastosowania w systemach IBM i .

Wynikowa konfiguracja wygląda następująco:



Rysunek 17. Konfiguracja wynikający z tego zadania

W programie Rysunek 17 na stronie 221repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat publiczny z C1. Repozytorium kluczy dla C1 zawiera certyfikat dla C1 i certyfikat publiczny z QM1.

Procedura

1. Przygotuj repozytorium kluczy na kliencie i menedżerze kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Utwórz certyfikaty samopodpisane dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
3. Wyodrębnij kopię każdego certyfikatu:
   - W systemach UNIX, Linuxi Windows.
4. Prześlij publiczną część certyfikatu C1 do systemu QM1 i odwrotnie, korzystając z programu narzędziowego, takiego jak FTP.
5. Dodaj certyfikat partnera do repozytorium kluczy dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
6. Wydaj komendę REFRESH SECURITY TYPE (SSL) w menedżerze kolejek.
7. Zdefiniuj kanał połączenia klienckiego w jeden z następujących sposobów:

- Przy użyciu wywołania MQCONNX ze strukturą MQSCO na C1, zgodnie z opisem w sekcji Tworzenie kanału połączenia klienckiego w kliencie MQI produktu WebSphere MQ.
- Korzystanie z tabeli definicji kanału klienta zgodnie z opisem w sekcji Tworzenie definicji połączeń z serwerem i połączenia klienckiego na serwerze .

8. Na serwerze QM1zdefiniuj kanał połączenia z serwerem, wydając komendę taką jak w następującym przykładzie:

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
```

   Kanał musi mieć taką samą nazwę, jak kanał połączenia klienckiego, który został zdefiniowany w kroku 6, i musi używać tej samej wartości CipherSpec.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 17 na stronie 221 .

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do wyników przedstawionych w poniższym przykładzie.

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Ustawienie atrybutu filtru SSLPEER dla definicji kanału jest opcjonalne. Jeśli ustawiono definicję kanału SSLPEER, jego wartość musi być zgodna z nazwą wyróżniającą podmiotu w certyfikacie partnera, który został utworzony w kroku 2. Po pomyślnym nawiązaniu połączenia, pole SSLPEER w danych wyjściowych DISPLAY CHSTATUS zawiera nazwę wyróżniającą podmiotu certyfikatu klienta zdalnego.

Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania klienta i menedżera kolejek

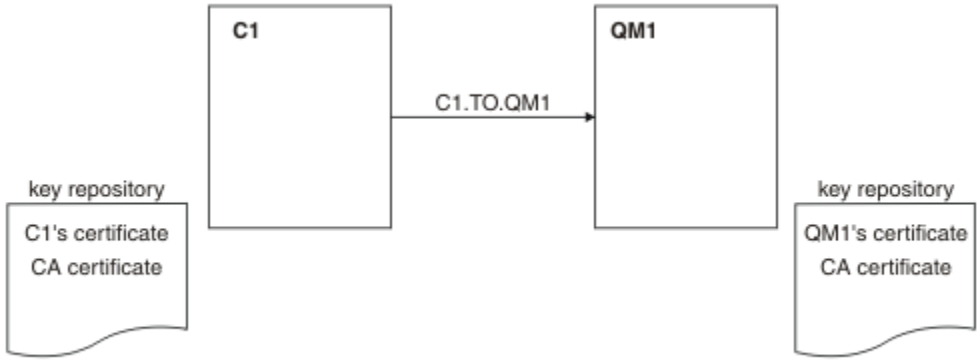
Aby zaimplementować wzajemne uwierzytelnianie między klientem a menedżerem kolejek, należy postępować zgodnie z tymi przykładowymi instrukcjami, korzystając z certyfikatów SSL podpisanych przez ośrodek CA lub TLS.

O tym zadaniu

Scenariusz:

- Istnieje klient C1i menedżer kolejek QM1, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między C1 i QM1.
- W przyszłości planujesz korzystać z tej sieci w środowisku produkcyjnym, dlatego od początku zdecydowałeś się na korzystanie z podpisanych przez CA certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 18. Konfiguracja wynikający z tego zadania

W programie Rysunek 18 na stronie 223repozytorium kluczy dla C1 zawiera certyfikat dla C1 i certyfikat ośrodka CA. Repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat ośrodka CA. W tym przykładzie zarówno certyfikat C1, jak i certyfikat QM1zostały wydane przez ten sam ośrodek CA. Jeśli certyfikat C1i certyfikat QM1zostały wydane przez różne ośrodki CA, repozytoria kluczy dla C1 i QM1 muszą zawierać oba certyfikaty ośrodka CA.

Procedura

1. Przygotuj repozytorium kluczy na kliencie i menedżerze kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Zażądaj certyfikatu podpisanego przez ośrodek CA dla klienta i menedżera kolejek.
   Dla klienta i menedżera kolejek mogą być używane różne usługi CAs.
   - W systemach UNIX, Linuxi Windows.
3. Dodaj certyfikat ośrodka certyfikacji do repozytorium kluczy dla klienta i menedżera kolejek.
   Jeśli klient i menedżer kolejek używają różnych ośrodków certyfikacji, to certyfikat ośrodka certyfikacji dla każdego ośrodka certyfikacji musi być dodany do obu repozytoriów kluczy.
   - W systemach UNIX, Linuxi Windows.
4. Dodaj certyfikat podpisany przez ośrodek CA do repozytorium kluczy dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
5. Zdefiniuj kanał połączenia klienckiego w jeden z następujących sposobów:
   - Przy użyciu wywołania MQCONNX ze strukturą MQSCO na C1, zgodnie z opisem w sekcji Tworzenie kanału połączenia klienckiego w kliencie MQI produktu WebSphere MQ.
   - Korzystanie z tabeli definicji kanału klienta zgodnie z opisem w sekcji Tworzenie definicji połączeń z serwerem i połączenia klienckiego na serwerze .
6. Na serwerze QM1zdefiniuj kanał połączenia z serwerem, wydając komendę taką jak w następującym przykładzie:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanał musi mieć taką samą nazwę, jak kanał połączenia klienckiego, który został zdefiniowany w kroku 6, i musi używać tej samej wartości CipherSpec.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 18 na stronie 223.

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do przedstawionych w poniższym przykładzie.

Z poziomu menedżera kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Pole SSLPEER w danych wyjściowych DISPLAY CHSTATUS zawiera nazwę wyróżniającą podmiotu certyfikatu klienta zdalnego, który został utworzony w kroku 2. Nazwa wystawcy jest zgodna z nazwą wyróżniającą podmiotu certyfikatu ośrodka CA, który podpisał certyfikat osobisty dodany w kroku 4.

Anonimowo połączenie klienta z menedżerem kolejek

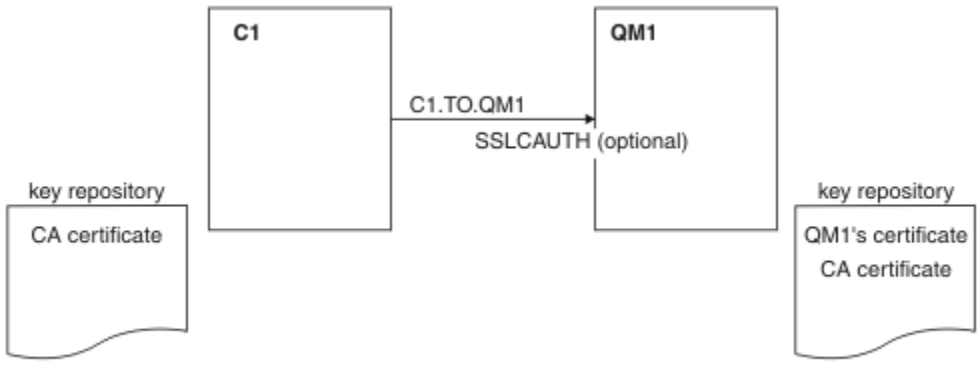
Wykonaj poniższe przykładowe instrukcje, aby zmodyfikować system z wzajemnym uwierzytelnianiem, aby umożliwić menedżerowi kolejek nawiązanie połączenia anonimowo z innym.

O tym zadaniu

Scenariusz:

- Menedżer kolejek i klient (QM1 i C1) zostały skonfigurowane w sposób opisany w sekcji “Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania klienta i menedżera kolejek” na stronie 222.
- Użytkownik chce zmienić C1 tak, aby łączył się z nim anonimowo z QM1.

Wynikowa konfiguracja wygląda następująco:



Rysunek 19. Klient i menedżer kolejek zezwalający na anonimowe połączenie

Procedura

1. Usuń certyfikat osobisty z repozytorium kluczy dla C1, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows. Certyfikat jest oznaczony w następujący sposób:

- ibmwebspheremq , a po nim identyfikator użytkownika logowania złożony z małych liter, na przykład ibmwebspheremqmyuserid.

2. Zrestartuj aplikację kliencką lub aplikację kliencką, aby zamknąć i ponownie otworzyć wszystkie połączenia SSL lub TLS.
3. Zezwalaj na anonimowe połączenia z menedżerem kolejek, wydając następującą komendę:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Wyniki

Repozytoria kluczy i kanały są zmieniane w sposób ilustrowany w programie Rysunek 19 na stronie 224 .

Co dalej

Po zakończeniu działania kanału na serwerze, wartość parametru nazwy węzła na ekranie statusu kanału wskazuje, że wystąpił certyfikat klienta.

Sprawdź, czy zadanie zostało pomyślnie zakończone, wydając niektóre komendy DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowa wartość wyjściowa jest podobna do przedstawionej w poniższym przykładzie:

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

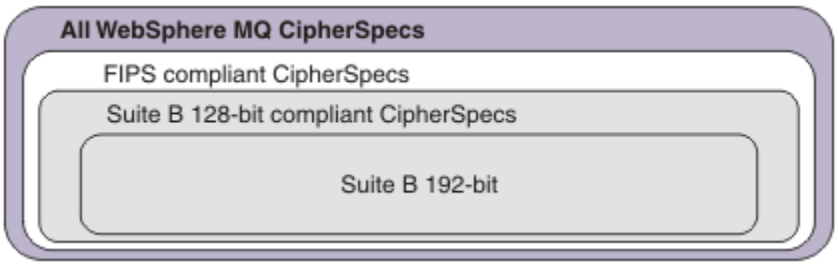
Pola SSLCERTI i SSLPEER są puste, co oznacza, że C1 nie wysłał certyfikatu.

Określanie CipherSpecs

Określ parametr CipherSpec za pomocą parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** MQSC lub **ALTER CHANNEL** MQSC.

Niektóre CipherSpecs , których można użyć z produktem IBM WebSphere MQ , są zgodne ze standardem FIPS. Inne, takie jak NULL_MD5, nie są. Podobnie niektóre CipherSpecs zgodne ze standardem FIPS są również zgodne ze standardem Suite B, chociaż inne nie są zgodne. Wszystkie CipherSpecs zgodne ze standardem Suite B są również zgodne ze standardem FIPS. Wszystkie CipherSpecs zgodne ze standardem Suite B dzielą się na dwie grupy: 128 bitów (na przykład ECDHE_ECDSA_AES_128_GCM_SHA256) i 192 bity (na przykład ECDHE_ECDSA_AES_256_GCM_SHA384).

Na poniższym diagramie przedstawiono relacje między tymi podzbiorami:



W poniższej tabeli przedstawiono specyfikacje szyfrów, których można używać z obsługą protokołów SSL i TLS produktu IBM WebSphere MQ . Jeśli żądasz certyfikatu osobistego, należy podać wielkość klucza dla pary kluczy publicznego i prywatnego. Wielkość klucza używanego podczas uzgadniania SSL jest wielkością zapisaną w certyfikacie, chyba że jest ona określona w specyfikacji szyfrowania CipherSpec(zgodnie z opisem w tabeli).

Nazwa specyfikacji szyfrowania	**Używany protokół**	**Algorytm MAC**	**Algorytm szyfrowania**	**Bity szyfrowania**	**FIPS[1]**	**Suite B 128-bitowy**	**Suite B 192-bitowy**
NULL_MD5 [a]	SSL 3.0	MD5	Brak	0	Nie	Nie	Nie
NULL_SHA [a]	SSL 3.0	SHA-1	Brak	0	Nie	Nie	Nie
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Nie	Nie	Nie
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Nie	Nie	Nie
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Nie	Nie	Nie
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Nie	Nie	Nie
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Nie	Nie	Nie
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Nie	Nie	Nie
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Nie	Nie	Nie
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Nie [5]	Nie	Nie
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Nie [6]	Nie	Nie
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Tak	Nie	Nie
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Nie	Nie	Nie
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Nie	Nie	Nie
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Tak	Nie	Nie
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Tak	Nie	Nie
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Tak	Nie

Nazwa specyfikacji szyfrowania	Używany protokół	Algorytm MAC	Algorytm szyfrowania	Bity szyfrowania	FIPS[1]	Suite B 128-bitowy	Suite B 192-bitowy
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Tak
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Nie	Nie
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Brak	0	Nie	Nie	Nie
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Brak	0	Nie	Nie	Nie
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Brak	0	Nie	Nie	Nie
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Brak	Brak	0	Nie	Nie	Nie
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Nie	Nie	Nie

Uwagi:

1. Wskazuje, czy specyfikacja szyfrowania ma certyfikat FIPS na platformie z certyfikatem FIPS. Więcej informacji na temat standardu FIPS zawiera sekcja Standard FIPS (Federal Information Processing Standard).
2. Maksymalna wielkość klucza uzgadniania to 512 bitów. Jeśli którykolwiek z certyfikatów wymienianych podczas uzgadniania SSL ma klucz większy niż 512 bitowy, na potrzeby uzgadniania generowany jest tymczasowy klucz 512-bitowy.
3. Wielkość klucza uzgadniania to 1024 bity.
4. Tej specyfikacji szyfrowania CipherSpec nie można użyć do zabezpieczenia połączenia programu WebSphere MQ Explorer z menedżerem kolejek, chyba że do środowiska JRE używanego przez program Explorer zastosowano odpowiednie nieograniczone pliki strategii.
5. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007.
6. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007. Nazwa FIPS_WITH_DES_CBC_SHA jest historyczna i odzwierciedla fakt, że wartość specyfikacji szyfrowania była poprzednio (ale już nie jest) zgodna ze standardem FIPS. Ta specyfikacja szyfrowania jest nieaktualna i jej użycie nie jest zalecane.
7. Ta specyfikacja szyfrowania może zostać użyta do przesłania maksymalnie 32 GB danych. Po przekroczeniu tej wartości połączenie zostanie przerwane i zostanie wyświetlony komunikat o błędzie AMQ9288. Aby uniknąć tego błędu, należy unikać używania algorytmu szyfrowania DES lub włączyć resetowanie klucza tajnego, gdy jest używana ta specyfikacja szyfrowania.

Obsługa platformy:

- a Dostępne na wszystkich obsługiwanych platformach.
- b Dostępne tylko na platformach UNIX, Linux, and Windows .

Pojęcia pokrewne

“Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35

Ten temat zawiera informacje na temat sposobu wyboru odpowiednich specyfikacji CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa, poprzez wykreślenie relacji między CipherSpecs a certyfikatami cyfrowymi w produkcie IBM WebSphere MQ.

Odsyłacze pokrewne

Zdefiniowanie kanału

ZMIEŃ KANAŁ

Nieaktualne CipherSpecs

Lista nieaktualnych specyfikacji CipherSpecs , które są w stanie używać z produktem WebSphere MQ (jeśli jest to konieczne).

Więcej informacji na temat włączania nieaktualnych specyfikacji CipherSpecszawiera sekcja “Wartości CipherSpec obsługiwane w produkcie IBM WebSphere MQ” na stronie 40 .

Nieaktualne CipherSpecs , które mogą być używane z obsługą protokołu WebSphere MQ TLS, są wymienione w poniższej tabeli:

Obsługa platformy “1” na stronie 230	Nazwa specyfikacji szyfrowania	Używany protokół	Integralność danych	Algorytm szyfrowania	Bity szyfrowania	FIPS “2” na stronie 230	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Wszystkie	DES_SHA_EXPORT“3” na stronie 230	SSL 3.0	SHA-1	DES	56	Nie	Nie	7.5.0.6
Windows UNIX Linux	DES_SHA_EXPORT1024“4” na stronie 230	SSL 3.0	SHA-1	DES	56	Nie	Nie	7.5.0.6
Windows UNIX Linux	FIPS_WITH_DES_CBC_SHA	SSL 3.0	SHA-1	DES	56	nie“6” na stronie 230	Nie	7.5.0.6
Windows UNIX Linux	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	SHA-1	3DES	168	nie“7” na stronie 230	Nie	7.5.0.8
Wszystkie	NULL_MD5	SSL 3.0	MD5	Brak	0	Nie	Nie	7.5.0.6
Wszystkie	NULL_SHA	SSL 3.0	SHA-1	Brak	0	Nie	Nie	7.5.0.6
Wszystkie	RC2_MD5_EXPORT“3” na stronie 230	SSL 3.0	MD5	RC2	40	Nie	Nie	7.5.0.7
Wszystkie	RC4_MD5_EXPORT“3” na stronie 230	SSL 3.0	MD5	RC4	40	Nie	Nie	7.5.0.7
Wszystkie	RC4_MD5_US	SSL 3.0	MD5	RC4	128	Nie	Nie	7.5.0.7
Wszystkie	RC4_SHA_US	SSL 3.0	SHA-1	RC4	128	Nie	Nie	7.5.0.7

Obsługa platformy "1" na stronie 230	Nazwa specyfikacji szyfrowania	Używany protokół	Integralność danych	Algorytm szyfrowania	Bity szyfrowania	FIPS "2" na stronie 230	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Windows UNIX Linux	RC4_56_SHA_EXPORT1024"4" na stronie 230	SSL 3.0	SHA-1	RC4	56	Nie	Nie	7.5.0.7
Wszystkie	TRIPLE_DES_SHA_US	SSL 3.0	SHA-1	3DES	168	Nie	Nie	7.5.0.8
Wszystkie	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	SHA-1	DES	56	nie"5" na stronie 230	Nie	7.5.0.6
Windows UNIX Linux	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	SHA-1	Brak	0	Nie	Nie	7.5.0.6
Windows UNIX Linux	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Nie	Nie	7.5.0.7
Windows UNIX Linux	ECDHE_RSA_NULL_SHA256	TLS 1.2	SHA-1	Brak	0	Nie	Nie	7.5.0.6
Windows UNIX Linux	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Nie	Nie	7.5.0.7
Windows UNIX Linux	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Brak	Brak	0	Nie	Nie	7.5.0.6
Wszystkie	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	SHA-256	Brak	0	Nie	Nie	7.5.0.6
Windows UNIX Linux	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Nie	Nie	7.5.0.7
Wszystkie	TLS_RSA_WITH_3DES_EDE_CBC_SHA"8" na stronie 230	TLS 1.0	SHA-1	3DES	168	Tak	Nie	7.5.0.8
Windows UNIX Linux	ECDHE_ECDSA_3DES_EDE_CBC_SHA256"8" na stronie 230	TLS 1.2	SHA-1	3DES	168	Tak	Nie	7.5.0.8
Windows UNIX Linux	ECDHE_RSA_3DES_EDE_CBC_SHA256"8" na stronie 230	TLS 1.2	SHA-1	3DES	168	Tak	Nie	7.5.0.8

Obsługa platformy "1" na stronie 230	Nazwa specyfikacji szyfrowania	Używany protokół	Integralność danych	Algorytm szyfrowania	Bity szyfrowania	FIPS "2" na stronie 230	Suite B	Aktualizacja, w której uznano ją za nieaktualną

Uwagi:

1. Jeśli nie wskazano konkretnej platformy, specyfikacja szyfrowania jest dostępna na wszystkich platformach.
2. Wskazuje, czy specyfikacja szyfrowania ma certyfikat FIPS na platformie z certyfikatem FIPS. Więcej informacji na temat standardu FIPS zawiera sekcja Standard FIPS (Federal Information Processing Standard).
3. Maksymalna wielkość klucza uzgadniania to 512 bitów. Jeśli którykolwiek z certyfikatów wymienianych podczas uzgadniania SSL ma klucz większy niż 512 bitowy, na potrzeby uzgadniania generowany jest tymczasowy klucz 512-bitowy.
4. Wielkość klucza uzgadniania to 1024 bity.
5. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007.
6. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007. Nazwa `FIPS_WITH_DES_CBC_SHA` jest historyczna i odzwierciedla fakt, że specyfikacja szyfrowania była wcześniej zgodna ze standardem FIPS (ale już nie jest). Ta specyfikacja szyfrowania jest nieaktualna i jej użycie nie jest zalecane.
7. Nazwa `FIPS_WITH_3DES_EDE_CBC_SHA` jest historyczna i odzwierciedla fakt, że specyfikacja szyfrowania była wcześniej zgodna ze standardem FIPS (ale już nie jest). Ta specyfikacja szyfrowania jest nieaktualna.
8. Ta specyfikacja szyfrowania może zostać użyta do przesłania maksymalnie 32 GB danych. Po przekroczeniu tej wartości połączenie zostanie przerwane i zostanie wyświetlony komunikat o błędzie AMQ9288. Aby uniknąć tego błędu, należy unikać używania algorytmu szyfrowania DES lub włączyć resetowanie klucza tajnego, gdy jest używana ta specyfikacja szyfrowania.

Uzyskiwanie informacji o specyfikacji CipherSpecs przy użyciu produktu IBM WebSphere MQ Explorer

Za pomocą programu IBM WebSphere MQ Explorer można wyświetlać opisy specyfikacji CipherSpecs.

Aby uzyskać informacje na temat specyfikacji CipherSpecs w produkcie "Określanie CipherSpecs" na stronie 225, należy wykonać następującą procedurę:

1. Otwórz program **IBM WebSphere MQ Explorer** i rozwiń folder **Menedżery kolejek** .
2. Upewnij się, że menedżer kolejek został uruchomiony.
3. Wybierz menedżer kolejek, z którym chcesz pracować, a następnie kliknij opcję **Kanały**.
4. Kliknij prawym przyciskiem myszy kanał, z którym chcesz pracować, i wybierz opcję **Właściwości**.
5. Wybierz stronę właściwości **SSL** .
6. Wybierz z listy opcję CipherSpec , z którą chcesz pracować. Opis jest wyświetlany w oknie znajdującym się poniżej listy.

Alternatywy dla opcji CipherSpecs

W przypadku platform, w których system operacyjny udostępnia obsługę protokołu SSL, system może obsługiwać nowe specyfikacje CipherSpecs. Nową specyfikację CipherSpec można określić za pomocą parametru SSLCIPH, ale wartość, którą należy podać, zależy od używanej platformy.

Uwaga: Ta sekcja nie dotyczy systemów UNIX, Linux i Windows , ponieważ specyfikacje CipherSpecs są dostarczane z produktem WebSphere MQ , dlatego nowe specyfikacje CipherSpecs nie są dostępne po wysyłce.

W przypadku platform, w których system operacyjny udostępnia obsługę protokołu SSL, system może obsługiwać nowe specyfikacje CipherSpecs , które nie są dołączone do produktu “Określanie CipherSpecs” na stronie 225. Nową specyfikację CipherSpec można określić za pomocą parametru SSLCIPH, ale wartość, którą należy podać, zależy od używanej platformy. We wszystkich przypadkach specyfikacja *musi* odpowiadać specyfikacji SSL CipherSpec , która jest poprawna i obsługiwana przez wersję protokołu SSL, w którym działa system.

IBM i

Dwuznakowy łańcuch reprezentujący wartość szesnastkową.

Więcej informacji na temat dozwolonych wartości znajduje się w odpowiedniej dokumentacji produktu (wyszukaj *cipher_spec* w dokumentacji produktu IBM i).

Aby określić wartość, można użyć komendy CHGMQMCHL lub komendy CRTMQMCHL, na przykład:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Aby ustawić parametr SSLCIPH , można również użyć komendy ALTER QMGR MQSC.

z/OS

Dwuznakowy łańcuch reprezentujący wartość szesnastkową. Kody szesnastkowe odpowiadają wartościom zdefiniowanym w protokole SSL.

Więcej informacji na ten temat zawiera opis funkcji gsk_environment_open () w rozdziale referencyjnym API w podręczniku *z/OS Cryptographic Services System SSL Programming*, SC24-5901, gdzie znajduje się lista wszystkich obsługiwanych specyfikacji szyfrów SSL V3.0 i TLS V1.0 w postaci dwucyfrowych kodów szesnastkowych.

Uwagi dotyczące klastrów produktu WebSphere MQ

W przypadku klastrów WebSphere MQ najbezpieczniej jest używać nazw CipherSpec w produkcie “Określanie CipherSpecs” na stronie 225. Jeśli używana jest specyfikacja alternatywna, należy pamiętać, że specyfikacja może nie być poprawna na innych platformach. Więcej informacji zawiera sekcja “SSL i klastry” na stronie 257.

Określanie specyfikacji CipherSpec dla klienta MQI produktu IBM WebSphere MQ

Dostępne są trzy opcje określania wartości CipherSpec dla klienta MQI produktu IBM WebSphere MQ .

Są to następujące opcje:

- Korzystanie z tabeli definicji kanału
- Przy użyciu pola SSLCipherSpec w strukturze MQCD, MQCD_VERSION_7 lub wyższej, w wywołaniu MQCONNX.
- Korzystanie z Active Directory (w systemach Windows z obsługą Active Directory)

Określanie pakietu CipherSuite z klasami produktu IBM WebSphere MQ dla klas Java i IBM WebSphere MQ dla usługi JMS

Klasy IBM WebSphere MQ classes for Java i IBM WebSphere MQ classes for JMS określają CipherSuites w inny sposób niż inne platformy.

Więcej informacji na temat określania pakietu CipherSuite z klasami produktu IBM WebSphere MQ dla języka Java zawiera sekcja Obsługa protokołu SSL (Secure Sockets Layer).

Informacje na temat określania pakietu CipherSuite z klasami IBM WebSphere MQ dla usługi JMS zawiera sekcja Korzystanie z protokołu SSL (Secure Sockets Layer) z klasami produktu WebSphere MQ dla usługi JMS.

Resetowanie kluczy tajnych SSL i TLS

Produkt IBM WebSphere MQ obsługuje resetowanie kluczy tajnych w menedżerach kolejek i klientach.

Klucze tajne są resetowane po upływie określonej liczby zaszyfrowanych bajtów danych w kanale lub po bezczynnym bezczynności kanału przez pewien czas.

Wartość resetowania klucza jest zawsze ustawiana przez stronę inicjujące kanału MQ .

Menedżer kolejek

W przypadku menedżera kolejek należy użyć komendy **ALTER QMGR** z parametrem **SSLRKEYC** , aby ustawić wartości używane podczas renegocjacji klucza.

MQI client

Klienty MQI domyślnie nie renegocjują klucza tajnego. Klient MQI może renegocjować klucz w dowolny z trzech sposobów. Na poniższej liście metody są wyświetlane w kolejności priorytetów. Jeśli zostanie określona wiele wartości, zostanie użyta najwyższa wartość priorytetu.

1. Za pomocą pola Licznik KeyResetw strukturze MQSCO w wywołaniu MQCONNX
2. Przy użyciu zmiennej środowiskowej MQSSLRESET
3. Przez ustawienie atrybutu Licznik SSLKeyResetw pliku konfiguracyjnym klienta MQI

Te zmienne mogą być ustawione na liczbę całkowitą z zakresu od 0 do 999 999 999, która reprezentuje liczbę niezaszyfrowanych bajtów wysłanych i odebranych w ramach konwersacji SSL lub TLS przed ponownym negocjacją klucza tajnego SSL lub TLS. Podanie wartości 0 oznacza, że klucze tajne SSL lub TLS nigdy nie są ponownie negocjowane. W przypadku określenia wartości resetowania klucza tajnego SSL lub TLS w zakresie od 1 bajtu do 32 kB, w kanałach SSL lub TLS zostanie użyta wartość klucza tajnego resetowania klucza o wielkości 32 kB. Ma to na celu uniknięcie nadmiernych resetów klawiszy, które mogą wystąpić w przypadku małych wartości resetowania klucza tajnego SSL lub TLS.

Jeśli określono wartość większą niż zero, a pulsy kanału są włączone dla kanału, klucz tajny jest również renegocjowany, zanim dane komunikatu zostaną wysłane lub odebrane po pulsie kanału.

Liczba bajtów do czasu zresetowania następnej operacji renegocjacji klucza tajnego po każdej pomyślnej renegocjacji.

Szczegółowe informacje na temat struktury MQSCO można znaleźć w sekcji KeyResetCount (MQLONG). Szczegółowe informacje na temat komendy MQSSLRESET zawiera sekcja MQSSLRESET. Więcej informacji na temat korzystania z protokołu SSL lub TLS w pliku konfiguracyjnym klienta zawiera sekcja Sekcja SSL pliku konfiguracyjnego klienta.

Java

W przypadku IBM WebSphere MQ classes for Javaaplikacja może zresetować klucz tajny w jeden z następujących sposobów:

- W tym celu należy ustawić pole sslResetCount w klasie MQEnvironment.
- Ustawiając właściwość środowiska MQC.SSL_RESET_COUNT_PROPERTY w obiekcie Hashtable. Następnie aplikacja przypisuje tabelę mieszającą do pola `properties` w klasie MQEnvironment lub przekazuje tabelę mieszającą do obiektu MQQueueManager na jego konstruktorze.

Jeśli aplikacja używa więcej niż jednego z tych sposobów, stosowane są zwykłe reguły pierwszeństwa. Reguły kolejności wykonywania można znaleźć w sekcji Klasa com.ibm.mq.MQEnvironment .

Wartość pola licznika sslResetlub właściwości środowiska MQC.SSL_RESET_COUNT_PROPERTY reprezentuje łączną liczbę bajtów wysłanych i odebranych przez klasy produktu WebSphere MQ dla kodu

klienta Java, zanim klucz tajny zostanie ponownie wynegocjowany. Liczba wysłanych bajtów jest liczbą przed zaszyfrowaniem, a liczba odebranych bajtów jest liczbą po deszyfrowaniu. Liczba bajtów obejmuje również informacje sterujące wysłane i odebrane przez klasy produktu WebSphere MQ dla klienta Java.

Jeśli wartość licznika resetowania wynosi zero, co jest wartością domyślną, klucz tajny nigdy nie będzie ponownie negocjowany. Licznik resetowania jest ignorowany, jeśli nie zostanie podany parametr CipherSuite .

JMS

W przypadku systemu IBM WebSphere MQ classes for JMSwłaściwość SSLRESETCOUNT reprezentuje łączną liczbę bajtów wysłanych i odebranych przez połączenie, zanim klucz tajny używany do szyfrowania jest ponownie negocjowany. Liczba wysłanych bajtów jest liczbą przed zaszyfrowaniem, a liczba odebranych bajtów jest liczbą po deszyfrowaniu. Liczba bajtów obejmuje również informacje sterujące wysłane i odebrane przez program IBM WebSphere MQ classes for JMS. Na przykład, aby skonfigurować obiekt ConnectionFactory , którego można użyć do utworzenia połączenia przez kanał MQI z włączoną obsługą protokołu SSL lub TLS z kluczem tajnym, który podlega renegocjacji po upływie 4 MB danych, należy wprowadzić następującą komendę do obiektu JMSAdmin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Jeśli wartość atrybutu SSLRESETCOUNT wynosi zero, co jest wartością domyślną, klucz tajny nigdy nie będzie ponownie negocjowany. Właściwość SSLRESETCOUNT jest ignorowana, jeśli właściwość SSLCIPHERSUITE nie jest ustawiona.

.NET

W przypadku niezarządzanych klientów .NET właściwość Liczba całkowita SSLKeyResetLiczba wskazuje liczbę niezaszyfrowanych bajtów wysłanych i odebranych w ramach konwersacji SSL lub TLS przed ponownym negocjacją klucza tajnego.

Więcej informacji na temat korzystania z właściwości obiektu w klasach produktu IBM WebSphere MQ dla platformy .NET zawiera sekcja Pobieranie i ustawianie wartości atrybutów.

XMS .NET

W przypadku niezarządzanych klientów XMS .NET należy zapoznać się z sekcji Bezpieczne połączenia z menedżerem kolejek produktu IBM WebSphere MQ.

Odsyłacze pokrewne
ALTER QMGR
WYŚWIETL QMGR

Implementowanie poufności w programach obsługi wyjścia użytkownika

Implementowanie poufności w wyjściach zabezpieczeń

Wyjścia zabezpieczeń mogą pełnić rolę w usłudze poufności, generując i rozdzielając klucz symetryczny w celu szyfrowania i deszyfrowania danych, które przepływają na kanał. Powszechną techniką wykonywania tej technologii jest technologia PKI.

Jedno wyjście zabezpieczeń generuje losową wartość danych, szyfruje je za pomocą klucza publicznego menedżera kolejek lub użytkownika, który reprezentuje wyjście zabezpieczeń partnera, a następnie wysyła zaszyfrowane dane do partnera w komunikacie bezpieczeństwa. Wyjście zabezpieczeń partnera deszyfruje losową wartość danych za pomocą klucza prywatnego menedżera kolejek lub użytkownika, który jest reprezentowany. Każde wyjście zabezpieczeń może teraz korzystać z wartości danych losowych w celu uzyskania klucza symetrycznego niezależnie od drugiego za pomocą algorytmu znanego obu z nich. Alternatywnie, mogą one używać wartości danych losowych jako klucza.

Jeśli pierwsze wyjście zabezpieczeń nie uwierzytelnił swojego partnera o tej godzinie, następny komunikat o zabezpieczeniu wysłany przez partnera może zawierać oczekiwaną wartość zaszyfrowaną za pomocą klucza symetrycznego. Pierwsze wyjście zabezpieczeń może teraz uwierzytelnić swojego partnera, sprawdzając, czy program obsługi wyjścia zabezpieczeń partnera był w stanie poprawnie zaszyfrować oczekiwaną wartość.

Wyjścia zabezpieczeń mogą również skorzystać z tej możliwości, aby uzgodnić algorytm szyfrowania i deszyfrowania danych, które przepływają na kanale, jeśli do użycia jest dostępnych więcej niż jeden algorytm.

Implementowanie poufności w wyjściach komunikatów

Wyjście komunikatu przy wysyłającym końcu kanału może szyfrować dane aplikacji w komunikacie, a inne wyjście komunikatu na odbierającym końcu kanału może deszyfrować dane. Ze względu na wydajność algorytm klucza symetrycznego jest zwykle używany do tego celu. Więcej informacji o tym, w jaki sposób klucz symetryczny może być generowany i dystrybuowany, zawiera sekcja “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 233.

Nagłówki w komunikacie, takie jak nagłówek kolejki transmisji, MQXQH, w tym osadzony deskryptor komunikatu, nie mogą być szyfrowane przy użyciu wyjścia komunikatu. Dzieje się tak dlatego, że konwersja danych nagłówków komunikatów ma miejsce po wywołaniu wyjścia komunikatu w wysyłającym zakończeniu lub przed wywołaniem wyjścia komunikatu na końcu odbierającym. Jeśli nagłówki są szyfrowane, konwersja danych nie powiedzie się, a kanał zostanie zatrzymany.

Implementowanie poufności w wyjściach wysyłania i odbierania

Wyjścia wysyłania i odbierania mogą być używane do szyfrowania i deszyfrowania danych, które przepływają w kanale. Są one bardziej odpowiednie niż wyjścia komunikatów w celu udostępnienia tej usługi z następujących powodów:

- W kanale komunikatów nagłówki komunikatów mogą być szyfrowane, a także dane aplikacji w komunikatach.
- Wyjścia wysyłania i odbierania mogą być używane w kanałach MQI, a także w kanałach komunikatów. Parametry w wywołaniach MQI mogą zawierać poufne dane aplikacji, które muszą być chronione podczas przepływu w kanale MQI. Dlatego można używać tych samych wyjść nadawanych i odbierających na obu rodzajach kanałów.

Implementowanie poufności w wyjściu API i wyjście funkcji API

Dane aplikacji w komunikacie mogą być szyfrowane przez interfejs API lub wyjście funkcji API, gdy komunikat jest umieszczany przez aplikację wysyłający i zdeszyfrowany przez drugie wyjście, gdy komunikat jest pobierany przez aplikację odbierającą. Ze względu na wydajność algorytm klucza symetrycznego jest zwykle używany do tego celu. Jednak na poziomie aplikacji, w którym wielu użytkowników może wysyłać do siebie komunikaty, problem polega na tym, w jaki sposób zapewnić, że tylko zamierzony odbiorca wiadomości będzie w stanie odszyfrować wiadomość. Jednym z rozwiązań jest użycie innego klucza symetrycznego dla każdej pary użytkowników, którzy wysyłają komunikaty do siebie nawzajem. Rozwiązanie to może być jednak trudne i czasochłonne w administrowaniu, szczególnie jeśli użytkownicy należą do różnych organizacji. Standardowy sposób rozwiązania tego problemu jest znany jako *koperta cyfrowa* i wykorzystuje technologię PKI.

Gdy aplikacja umieszcza komunikat w kolejce, funkcja API lub wyjście funkcji API generuje losowy klucz symetryczny i korzysta z klucza do zaszyfrowania danych aplikacji w komunikacie. Wyjście szyfruje klucz symetryczny przy użyciu klucza publicznego zamierzonego odbiorcy. Następnie zastępuje on dane aplikacji w komunikacie zaszyfrowanymi danymi aplikacji i zaszyfrowanym kluczem symetrycznym. W ten sposób tylko zamierzony odbiorca może zdeszyfrować klucz symetryczny, a tym samym dane aplikacji. Jeśli zaszyfrowany komunikat ma więcej niż jeden możliwy odbiornik, wyjście może zaszyfrować kopię klucza symetrycznego dla każdego zamierzonego odbiornika.

Jeśli dostępne są różne algorytmy szyfrowania i deszyfrowania danych aplikacji, wyjście może zawierać nazwę algorytmu, który był używany.

Integralność danych komunikatów

Aby zachować integralność danych, można użyć różnych typów programów obsługi wyjścia użytkownika w celu udostępnienia skrótów komunikatów lub podpisów cyfrowych dla komunikatów.

Integralność danych

Implementowanie integralności danych w komunikatach

Jeśli używany jest protokół SSL lub TLS, wybór opcji CipherSpec określa poziom integralności danych w przedsiębiorstwie. Jeśli używany jest produkt WebSphere MQ Advanced Message Service (AMS), można określić integralność dla unikalnego komunikatu.

Implementowanie integralności danych w wyjściach komunikatów

Komunikat może zostać podpisany cyfrowo przez wyjście komunikatu na wysyłającym końcu kanału. Podpis cyfrowy może być następnie sprawdzany przez wyjście komunikatu na końcu odbierającego kanału w celu wykrycia, czy komunikat został celowo zmodyfikowany.

Niektóre zabezpieczenia można uzyskać, używając skrótu komunikatu zamiast podpisu cyfrowego. Streszczenie komunikatu może być skuteczne w przypadku niezmiennego lub bezdyskryminacyjnego manipulowania, ale nie przeszkadza temu, aby bardziej poinformowani osoby dokonali zmiany lub wymiany wiadomości, generując dla niego zupełnie nowy skrót. Jest to szczególnie prawdziwe, jeśli algorytm używany do generowania streszczenia komunikatów jest dobrze znany.

Implementowanie integralności danych w wyjściach wysyłania i odbierania

W przypadku kanału komunikatów wyjścia komunikatów są bardziej odpowiednie do udostępniania tej usługi, ponieważ wyjście komunikatu ma dostęp do całego komunikatu. W przypadku kanału MQI parametry w wywołaniach MQI mogą zawierać dane aplikacji, które muszą być chronione, a wyjścia wysyłania i odbierania mogą zapewnić tę ochronę.

Implementowanie integralności danych w wyjściu funkcji API lub w wyjściu funkcji API

Komunikat może zostać podpisany cyfrowo przez wyjście funkcji API lub wyjścia funkcji API, gdy komunikat jest umieszczany w aplikacji wysyłającej. Podpis cyfrowy może następnie zostać sprawdzony przez drugie wyjście, gdy komunikat jest pobierany przez aplikację odbierającą w celu wykrycia, czy komunikat został celowo zmodyfikowany.

Niektóre zabezpieczenia można uzyskać, używając skrótu komunikatu zamiast podpisu cyfrowego. Streszczenie komunikatu może być skuteczne w przypadku niezmiennego lub bezdyskryminacyjnego manipulowania, ale nie przeszkadza temu, aby bardziej poinformowani osoby dokonali zmiany lub wymiany wiadomości, generując dla niego zupełnie nowy skrót. Jest to szczególnie prawdziwe, jeśli algorytm, który jest używany do generowania skrótu wiadomości, jest dobrze znany,

Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS

Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację protokołu SSL lub TLS, należy zdefiniować kanały w celu użycia protokołu SSL lub TLS. Należy również uzyskać certyfikaty cyfrowe i zarządzać nimi. W systemie testowym można użyć samopodpisanych certyfikatów lub certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA). W systemie produkcyjnym nie należy używać certyfikatów samopodpisanych. Więcej informacji na ten temat zawiera sekcja ../zs14140_.dita.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows” na stronie 118.

W tej kolekcji tematów przedstawiono zadania związane z konfigurowaniem komunikacji SSL oraz szczegółowe informacje na temat wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalną częścią protokołów. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza

poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji produktu WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

Uwagi:

1. W tym kontekście klient SSL odwołuje się do połączenia inicjującego uzgadnianie.
2. Więcej informacji na ten temat zawiera Glosariusz .

W systemach UNIX, Linux i Windows klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie WebSphere MQ , co oznacza `ibmwebspheremq` , po którym następuje zmiana nazwy menedżera kolejek na małe litery. Na przykład: `QM1`, `ibmwebspheremqqm1`.

Produkt WebSphere MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się tylko wtedy, gdy koniec kanału, który działa jako serwer SSL lub TLS, jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER. Więcej informacji na temat anonimowego połączenia z menedżerem kolejek, czyli gdy klient SSL lub TLS nie wysyła certyfikatu, zawiera sekcja “Łączenie dwóch menedżerów kolejek przy użyciu jednokierunkowego uwierzytelniania” na stronie 218.

Cyfrowe etykiety certyfikatów, zrozumienie wymagań

Podczas konfigurowania protokołu SSL i TLS do korzystania z certyfikatów cyfrowych mogą istnieć określone wymagania dotyczące etykiet, które należy spełnić, w zależności od używanej platformy i metody używanej do nawiązywania połączenia.

O tym zadaniu

Jaka jest etykieta certyfikatu?

Etykieta certyfikatu jest unikalnym identyfikatorem reprezentującym certyfikat cyfrowy przechowywanego w repozytorium kluczy i zapewnia wygodną nazwę czytelną dla człowieka, z którą można odwoływać się do konkretnego certyfikatu podczas wykonywania funkcji zarządzania kluczami. Etykieta certyfikatu jest przypisana podczas dodawania certyfikatu do repozytorium kluczy po raz pierwszy.

Etykieta certyfikatu jest oddzielona od pól *Nazwa wyróżniająca podmiotu* certyfikatu lub *Nazwa zwykła podmiotu* . Należy zauważyć, że pola *Nazwa wyróżniająca podmiotu* i *Nazwa zwykła podmiotu* są polami w samym certyfikacie. Są one definiowane podczas tworzenia certyfikatu i nie można ich zmieniać. Jeśli jest to konieczne, można jednak zmienić etykietę powiązaną z certyfikatem cyfrowym.

W jaki sposób używana jest etykieta certyfikatu?

Produkt IBM WebSphere MQ używa etykiet certyfikatów w celu znalezienia certyfikatu osobistego, który jest wysyłany podczas uzgadniania SSL. Eliminuje to niejednoznaczność, jeśli w repozytorium kluczy istnieje więcej niż jeden certyfikat osobisty.

Etykiety certyfikatów są zgodne z konwencją nazewnictwa. W tym celu należy upewnić się, że używana jest poprawna konwencja nazewnictwa etykiet odpowiadająca używanej platformie.

W tym kontekście klient SSL lub TLS odwołuje się do partnera połączenia inicjującego uzgadnianie, które może być klientem IBM WebSphere MQ lub innym menedżerem kolejek.

Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji IBM WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta, a klient zawsze udostępnia certyfikat serwerowi, jeśli zostanie znaleziony. Jeśli klient nie może znaleźć certyfikatu osobistego, klient wysyła odpowiedź no `certificate` na serwer.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się, jeśli koniec kanału, który działa jako

serwer SSL lub TLS, jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER.

Więcej informacji na temat nawiązywania połączenia z menedżerem kolejek przy użyciu uwierzytelniania jednokierunkowego, czyli gdy klient SSL lub TLS nie wysyła certyfikatu, zawiera sekcja “Łączenie dwóch menedżerów kolejek przy użyciu jednokierunkowego uwierzytelniania” na stronie 218.

Systemy , UNIX, Linux, and Windows

O tym zadaniu

W systemach , UNIX, Linux, and Windows , serwer SSL lub TLS wysyła certyfikat do klienta tylko wtedy, gdy serwer znajduje się na etykiecie w poprawnym formacie IBM WebSphere MQ . W tych systemach poprawnym formatem jest `ibmwebspheremq`, a po nim nazwa menedżera kolejek została zmieniona na małe.

Na przykład dla menedżera kolejek o nazwie `QM1`, wymaganie etykiety certyfikatu to:

```
ibmwebspheremqqm1
```

Jeśli w repozytorium kluczy menedżera kolejek nie znaleziono żadnego certyfikatu pasującego do wymaganej etykiety w poprawnym przypadku i w poprawnym formacie, wystąpi błąd, a uzgadnianie SSL lub TLS nie powiedzie się.

IBM WebSphere MQ klient

O tym zadaniu

Podczas nawiązywania połączenia z aplikacją kliencką IBM WebSphere MQ klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma jeden certyfikat z etykietą w formacie `ibmwebspheremq`, po którym następuje nazwa użytkownika uruchomionego przez użytkownika procesu aplikacji klienckiej.

Na przykład dla nazwy użytkownika `wasadmin`wymagane jest, aby etykieta certyfikatu była tak pokazana, jak mała:

```
   ibmwebspheremqwasadmin
```

Powyższy wymóg etykiety dotyczy klientów usługi komunikatów dla C, C + + i .NET.

Klient JMS produktu IBM WebSphere MQ Java lub IBM WebSphere MQ

O tym zadaniu

Klienty IBM WebSphere MQ Java lub IBM WebSphere MQ JMS korzystają z infrastruktury dostawcy JSSE (Java Secure Socket Extension) w celu wybrania certyfikatu osobistego podczas uzgadniania SSL lub TLS i dlatego nie podlegają wymaganiom etykiety certyfikatu.

Domyślne działanie polega na tym, że klient JSSE iteruje certyfikaty w repozytorium kluczy, wybierając pierwszy akceptowany certyfikat osobisty. To zachowanie jest jednak tylko domyślne i jest zależne od implementacji dostawcy JSSE.

Ponadto interfejs JSSE jest wysoce konfigurowalny poprzez konfigurację i bezpośredni dostęp w czasie wykonywania przez aplikację. Szczegółowe informacje można znaleźć w dokumentacji dostarczonej przez dostawcę JSSE.

Aby uzyskać informacje na temat rozwiązywania problemów lub lepiej zrozumieć uzgadnianie wykonywane przez aplikację kliencką Java produktu IBM WebSphere MQ w połączeniu z konkretnym dostawcą JSSE, można włączyć debugowanie, ustawiając

```
javax.net.debug=ssl
```

w środowisku JVM.

`-Djavax.net.debug=ssl` można użyć w wierszu komend lub ustawić zmienną w aplikacji lub za pomocą konfiguracji.

Pojęcia pokrewne

“Importowanie certyfikatu osobistego do repozytorium kluczy w systemach UNIX, Linux, and Windows” na stronie 138
Wykonaj tę procedurę, aby zaimportować certyfikat osobisty.

Korzystanie z certyfikatów samopodpisanych w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek

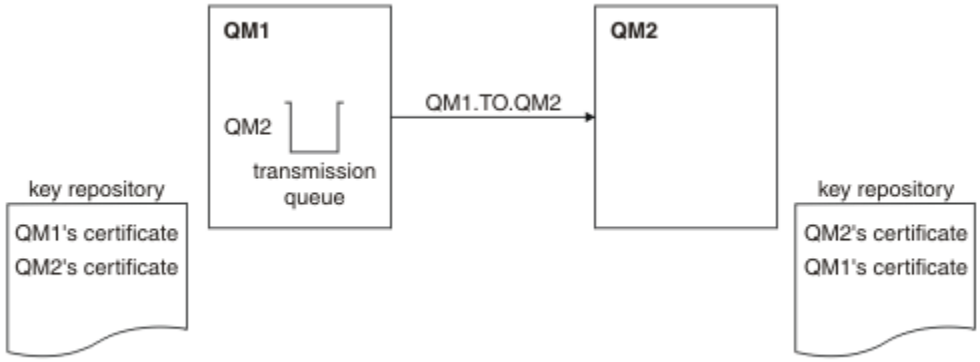
Wykonaj poniższe przykładowe instrukcje, aby zaimplementować wzajemne uwierzytelnianie między dwoma menedżerami kolejek przy użyciu samopodpisanych certyfikatów SSL lub TLS.

O tym zadaniu

Scenariusz:

- Istnieją dwa menedżery kolejek: QM1 i QM2, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między QM1 i QM2.
- Zdecydowałeś się przetestować bezpieczną komunikację przy użyciu samopodpisanych certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 20. Konfiguracja wynikający z tego zadania

W programie Rysunek 14 na stronie 215repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat publiczny z QM2. Repozytorium kluczy dla QM2 zawiera certyfikat dla QM2 i certyfikat publiczny z QM1.

Procedura

1. Przygotuj repozytorium kluczy dla każdego menedżera kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Utwórz samopodpisany certyfikat dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
3. Wyodrębnij kopię każdego certyfikatu:
   - W systemach UNIX, Linuxi Windows.
4. Prześlij publiczną część certyfikatu QM1 do systemu QM2 i odwrotnie, korzystając z programu narzędziowego, takiego jak FTP.
5. Dodaj certyfikat partnera do repozytorium kluczy dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.

6. W przypadku QM1zdefiniuj kanał nadawczy i powiązaną kolejkę transmisji, wydając komendy, takie jak w poniższym przykładzie:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

   W tym przykładzie użyto komendy CipherSpec RC4_MD5. Specyfikacje CipherSpecs na każdym końcu kanału muszą być takie same.
7. W systemie QM2zdefiniuj kanał odbiorczy, wydając komendę, tak jak w poniższym przykładzie:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
```

   Kanał musi mieć taką samą nazwę, jak kanał nadawczy zdefiniowany w kroku 6, i użyć tej samej wartości CipherSpec.
8. Uruchom kanał.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 14 na stronie 215 .

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do tych przedstawionych w poniższych przykładach.

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

W menedżerze kolejek QM2wprowadź następującą komendę:

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

W każdym przypadku wartość parametru SSLPEER musi być zgodna z nazwą DN w certyfikacie partnera, który został utworzony w kroku 2. Nazwa emitentów jest zgodna z nazwą węzła sieci, ponieważ certyfikat jest samopodpisany.

Parametr SSLPEER jest opcjonalny. Jeśli ta wartość jest określona, należy ustawić jej wartość tak, aby nazwa wyróżniająca w certyfikacie partnerskim (utworzonym w kroku 2) była dozwolona. Więcej informacji na temat korzystania z funkcji SSLPEER zawiera sekcja Reguły WebSphere MQ dla wartości SSLPEER .

Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek

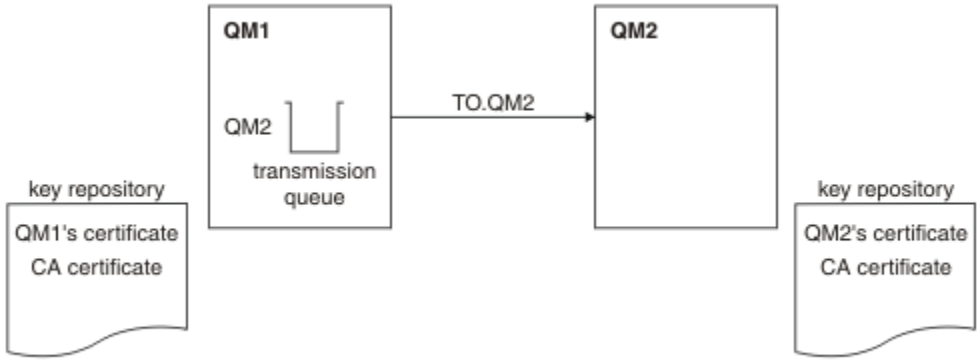
Wykonaj poniższe przykładowe instrukcje, aby zaimplementować wzajemne uwierzytelnianie między dwoma menedżerami kolejek przy użyciu certyfikatów SSL podpisanych przez ośrodek CA lub TLS.

O tym zadaniu

Scenariusz:

- Istnieją dwa menedżery kolejek o nazwach QMA i QMB, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnienie między QMA a QMB.
- W przyszłości planujesz korzystać z tej sieci w środowisku produkcyjnym, dlatego od początku zdecydowałeś się na korzystanie z podpisanych przez CA certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 21. Konfiguracja wynikający z tego zadania

W programie Rysunek 15 na stronie 217repozytorium kluczy dla QMA zawiera certyfikat QMA i certyfikat ośrodka CA. Repozytorium kluczy QMB zawiera certyfikat QMB i certyfikat CA. W tym przykładzie zarówno certyfikat QMA, jak i certyfikat QMB zostały wydane przez ten sam ośrodek CA. Jeśli certyfikat QMA i certyfikat QMB zostały wydane przez różne ośrodki certyfikacji (CA), repozytoria kluczy dla QMA i QMB muszą zawierać oba certyfikaty ośrodka CA.

Procedura

1. Przygotuj repozytorium kluczy dla każdego menedżera kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Zażądaj certyfikatu podpisanego przez ośrodek CA dla każdego menedżera kolejek.
   Dla dwóch menedżerów kolejek mogą być używane różne wartości CAs.
   - W systemach UNIX, Linuxi Windows.
3. Dodaj certyfikat ośrodka certyfikacji do repozytorium kluczy dla każdego menedżera kolejek:

Jeśli menedżery kolejek korzystają z różnych ośrodków certyfikacji, to certyfikat ośrodka certyfikacji dla każdego ośrodka certyfikacji musi być dodany do obu repozytoriów kluczy.

- W systemach UNIX, Linuxi Windows.

4. Dodaj certyfikat podpisany przez ośrodek CA do repozytorium kluczy dla każdego menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
5. W systemie QMA zdefiniuj kanał nadawczy i powiązaną kolejkę transmisji, wydając komendy, takie jak w poniższym przykładzie:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

   W tym przykładzie użyto komendy CipherSpec RC4_MD5. Specyfikacje CipherSpecs na każdym końcu kanału muszą być takie same.
6. W QMB zdefiniuj kanał odbiorczy, wydając komendę, tak jak w poniższym przykładzie:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
```

   Kanał musi mieć taką samą nazwę, jak kanał nadawczy zdefiniowany w kroku 6, i użyć tej samej wartości CipherSpec.
7. Uruchom kanał:

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 15 na stronie 217.

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do przedstawionych w poniższych przykładach.

W menedżerze kolejek QMA wprowadź następującą komendę:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

W menedżerze kolejek QMB wpisz następującą komendę:

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
```

```
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                          SUBSTATE(RECEIVE)
   XMITQ( )
```

W każdym przypadku wartość parametru SSLPEER musi być zgodna z nazwą wyróżniającą (DN) w certyfikacie partnera, który został utworzony w kroku 2. Nazwa wystawcy jest zgodna z nazwą wyróżniającą podmiotu certyfikatu ośrodka CA, który podpisał certyfikat osobisty dodany w kroku 4.

Łączenie dwóch menedżerów kolejek przy użyciu jednokierunkowego uwierzytelniania

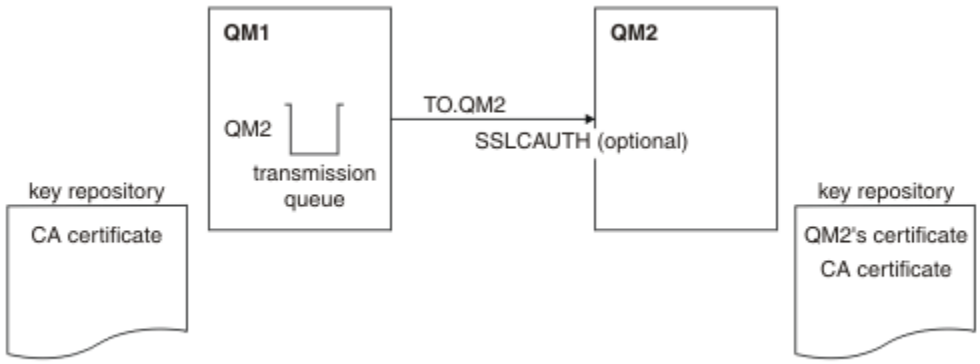
Wykonaj poniższe przykładowe instrukcje, aby zmodyfikować system z wzajemnym uwierzytelnianiem, aby umożliwić menedżerowi kolejek nawiązanie połączenia przy użyciu jednokierunkowego uwierzytelniania. Jest to, gdy klient SSL lub TLS nie wysyła certyfikatu.

O tym zadaniu

Scenariusz:

- Dwa menedżery kolejek (QM1 i QM2) zostały skonfigurowane tak, jak w programie “Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania dwóch menedżerów kolejek” na stronie 216.
- Użytkownik chce zmienić wartość QM1 , tak aby łączyła się z uwierzytelnianiem jednokierunkową na QM2.

Wynikowa konfiguracja wygląda następująco:



Rysunek 22. Menedżery kolejek zezwalające na uwierzytelnianie jednokierunkowe

Procedura

1. Usuń certyfikat osobisty QM1ze swojego repozytorium kluczy, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows. Certyfikat jest oznaczony w następujący sposób:
     - `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek składanego na małe litery. Na przykład: `QM1` , `ibmwebspheremqqm1`.
2. Opcjonalne: Jeśli w menedżerze kolejek QM1zostały wcześniej uruchomione jakiekolwiek kanały SSL lub TLS, odśwież środowisko SSL lub TLS.
3. Zezwalaj na anonimowe połączenia z odbiornikiem.

Wyniki

Repozytoria kluczy i kanały są zmieniane w sposób ilustrowany w programie Rysunek 16 na stronie 219 .

Co dalej

Jeśli kanał nadawczy był uruchomiony, a użytkownik wydał komendę REFRESH SECURITY TYPE (SSL) (w kroku 2), kanał zostanie zrestartowany automatycznie. Jeśli kanał nadawczy nie był uruchomiony, uruchom go.

Po zakończeniu działania kanału na serwerze, wartość parametru nazwy węzła na ekranie statusu kanału wskazuje, że wystąpił certyfikat klienta.

Sprawdź, czy zadanie zostało pomyślnie zakończone, wydając niektóre komendy DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowa wartość wyjściowa jest podobna do przedstawionej w poniższych przykładach:

Z poziomu menedżera kolejek QM1 wprowadź następującą komendę:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

Z poziomu menedżera kolejek QM2 wprowadź następującą komendę:

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

W przypadku QM2pole SSLPEER jest puste, co oznacza, że QM1 nie wysyłało certyfikatu. W przypadku QM1wartość SSLPEER jest zgodna z nazwą wyróżniającą (DN) w certyfikacie osobistym QM2.

Bezpieczne podłączanie klienta do menedżera kolejek

Bezpieczna komunikacja korzystająca z protokołów zabezpieczeń szyfrujących SSL lub TLS obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację protokołu SSL lub TLS, należy zdefiniować kanały w celu użycia protokołu SSL lub TLS. Należy również uzyskać certyfikaty cyfrowe i zarządzać nimi. W systemie testowym można użyć samopodpisanych certyfikatów lub certyfikatów wystawionych przez lokalny ośrodek certyfikacji (CA). W systemie produkcyjnym nie należy używać certyfikatów samopodpisanych. Więcej informacji na ten temat zawiera sekcja ../zs14140_.dita.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL lub TLS w systemach UNIX, Linux, and Windows” na stronie 118.

W tej kolekcji tematów przedstawiono zadania związane z konfigurowaniem komunikacji SSL oraz szczegółowe informacje na temat wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalną częścią protokołów. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji produktu WebSphere MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemach UNIX, Linux, and Windows klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie WebSphere MQ , czyli `ibmwebspheremq` , po której następuje zmiana ID użytkownika logowania na małe litery, na przykład `ibmwebspheremqmyuserid`.

Produkt WebSphere MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów. Upewnij się, że cała etykieta certyfikatu została podana małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie nie powiedzie się tylko wtedy, gdy koniec kanału, który działa jako serwer SSL lub TLS, jest zdefiniowany z parametrem SSLCAUTH ustawionym na REQUIRED lub zestawem wartości parametru SSLPEER. Więcej informacji na temat anonimowego połączenia menedżera kolejek zawiera sekcja “Anonimowo połączenie klienta z menedżerem kolejek” na stronie 224.

Korzystanie z certyfikatów samopodpisanych na potrzeby wzajemnego uwierzytelniania klienta i menedżera kolejek

Aby zaimplementować wzajemne uwierzytelnianie między klientem a menedżerem kolejek, należy postępować zgodnie z tymi przykładowymi instrukcjami, korzystając z samopodpisanych certyfikatów SSL lub TLS.

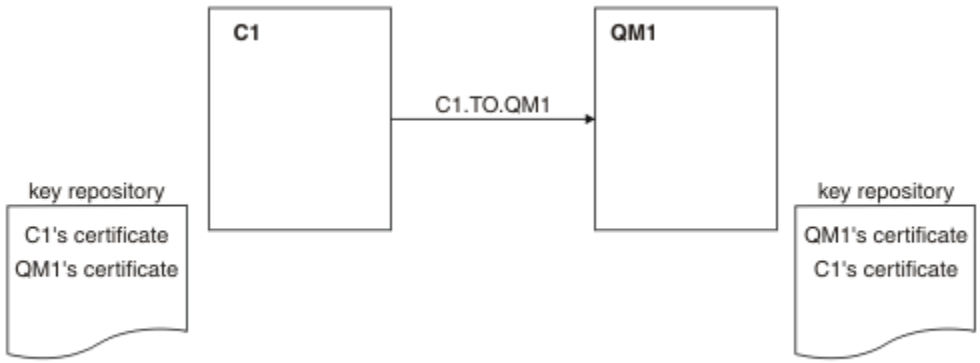
O tym zadaniu

Scenariusz:

- Istnieje klient C1i menedżer kolejek QM1, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między C1 i QM1.
- Zdecydowałeś się przetestować bezpieczną komunikację za pomocą samopodpisanych certyfikatów.

Program DCM w systemie IBM i nie obsługuje certyfikatów samopodpisanych, dlatego to zadanie nie ma zastosowania w systemach IBM i .

Wynikowa konfiguracja wygląda następująco:



Rysunek 23. Konfiguracja wynikający z tego zadania

W programie Rysunek 17 na stronie 221repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat publiczny z C1. Repozytorium kluczy dla C1 zawiera certyfikat dla C1 i certyfikat publiczny z QM1.

Procedura

1. Przygotuj repozytorium kluczy na kliencie i menedżerze kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Utwórz certyfikaty samopodpisane dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
3. Wyodrębnij kopię każdego certyfikatu:
   - W systemach UNIX, Linuxi Windows.
4. Prześlij publiczną część certyfikatu C1 do systemu QM1 i odwrotnie, korzystając z programu narzędziowego, takiego jak FTP.
5. Dodaj certyfikat partnera do repozytorium kluczy dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
6. Wydaj komendę REFRESH SECURITY TYPE (SSL) w menedżerze kolejek.
7. Zdefiniuj kanał połączenia klienckiego w jeden z następujących sposobów:
   - Przy użyciu wywołania MQCONNX ze strukturą MQSCO na C1, zgodnie z opisem w sekcji Tworzenie kanału połączenia klienckiego w kliencie MQI produktu WebSphere MQ.
   - Korzystanie z tabeli definicji kanału klienta zgodnie z opisem w sekcji Tworzenie definicji połączeń z serwerem i połączenia klienckiego na serwerze .
8. Na serwerze QM1zdefiniuj kanał połączenia z serwerem, wydając komendę taką jak w następującym przykładzie:

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Kanał musi mieć taką samą nazwę, jak kanał połączenia klienckiego, który został zdefiniowany w kroku 6, i musi używać tej samej wartości CipherSpec.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 17 na stronie 221 .

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do wyników przedstawionych w poniższym przykładzie.

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                    CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Ustawienie atrybutu filtru SSLPEER dla definicji kanału jest opcjonalne. Jeśli ustawiono definicję kanału SSLPEER, jego wartość musi być zgodna z nazwą wyróżniającą podmiotu w certyfikacie partnera, który został utworzony w kroku 2. Po pomyślnym nawiązaniu połączenia, pole SSLPEER w danych wyjściowych DISPLAY CHSTATUS zawiera nazwę wyróżniającą podmiotu certyfikatu klienta zdalnego.

Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania klienta i menedżera kolejek

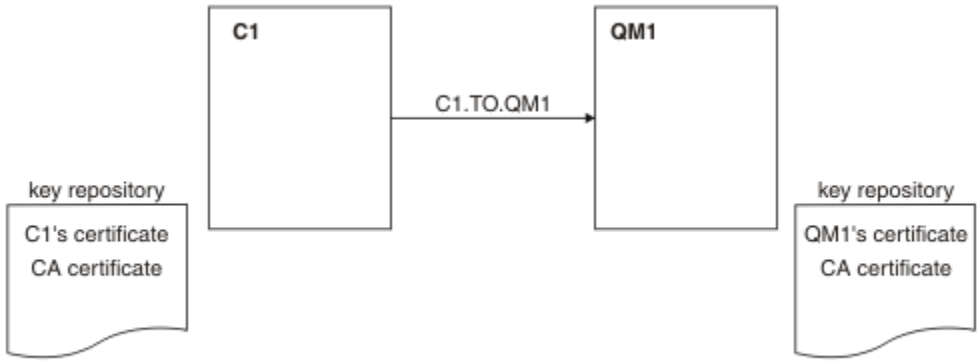
Aby zaimplementować wzajemne uwierzytelnianie między klientem a menedżerem kolejek, należy postępować zgodnie z tymi przykładowymi instrukcjami, korzystając z certyfikatów SSL podpisanych przez ośrodek CA lub TLS.

O tym zadaniu

Scenariusz:

- Istnieje klient C1i menedżer kolejek QM1, które muszą komunikować się bezpiecznie. Wymagane jest wzajemne uwierzytelnianie między C1 i QM1.
- W przyszłości planujesz korzystać z tej sieci w środowisku produkcyjnym, dlatego od początku zdecydowałeś się na korzystanie z podpisanych przez CA certyfikatów.

Wynikowa konfiguracja wygląda następująco:



Rysunek 24. Konfiguracja wynikający z tego zadania

W programie Rysunek 18 na stronie 223repozytorium kluczy dla C1 zawiera certyfikat dla C1 i certyfikat ośrodka CA. Repozytorium kluczy dla QM1 zawiera certyfikat dla QM1 i certyfikat ośrodka CA. W tym przykładzie zarówno certyfikat C1, jak i certyfikat QM1zostały wydane przez ten sam ośrodek CA. Jeśli certyfikat C1i certyfikat QM1zostały wydane przez różne ośrodki CA, repozytoria kluczy dla C1 i QM1 muszą zawierać oba certyfikaty ośrodka CA.

Procedura

1. Przygotuj repozytorium kluczy na kliencie i menedżerze kolejek, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows.
2. Zażądaj certyfikatu podpisanego przez ośrodek CA dla klienta i menedżera kolejek.
   Dla klienta i menedżera kolejek mogą być używane różne usługi CAs.
   - W systemach UNIX, Linuxi Windows.
3. Dodaj certyfikat ośrodka certyfikacji do repozytorium kluczy dla klienta i menedżera kolejek.
   Jeśli klient i menedżer kolejek używają różnych ośrodków certyfikacji, to certyfikat ośrodka certyfikacji dla każdego ośrodka certyfikacji musi być dodany do obu repozytoriów kluczy.
   - W systemach UNIX, Linuxi Windows.
4. Dodaj certyfikat podpisany przez ośrodek CA do repozytorium kluczy dla klienta i menedżera kolejek:
   - W systemach UNIX, Linuxi Windows.
5. Zdefiniuj kanał połączenia klienckiego w jeden z następujących sposobów:

- Przy użyciu wywołania MQCONNX ze strukturą MQSCO na C1, zgodnie z opisem w sekcji Tworzenie kanału połączenia klienckiego w kliencie MQI produktu WebSphere MQ.
- Korzystanie z tabeli definicji kanału klienta zgodnie z opisem w sekcji Tworzenie definicji połączeń z serwerem i połączenia klienckiego na serwerze .

6. Na serwerze QM1zdefiniuj kanał połączenia z serwerem, wydając komendę taką jak w następującym przykładzie:

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
```

   Kanał musi mieć taką samą nazwę, jak kanał połączenia klienckiego, który został zdefiniowany w kroku 6, i musi używać tej samej wartości CipherSpec.

Wyniki

Repozytoria kluczy i kanały są tworzone w sposób ilustrowany w sekcji Rysunek 18 na stronie 223.

Co dalej

Sprawdź, czy zadanie zostało pomyślnie zakończone za pomocą komend DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowe dane wyjściowe są podobne do przedstawionych w poniższym przykładzie.

Z poziomu menedżera kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe są podobne do poniższego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Pole SSLPEER w danych wyjściowych DISPLAY CHSTATUS zawiera nazwę wyróżniającą podmiotu certyfikatu klienta zdalnego, który został utworzony w kroku 2. Nazwa wystawcy jest zgodna z nazwą wyróżniającą podmiotu certyfikatu ośrodka CA, który podpisał certyfikat osobisty dodany w kroku 4.

Anonimowo połączenie klienta z menedżerem kolejek

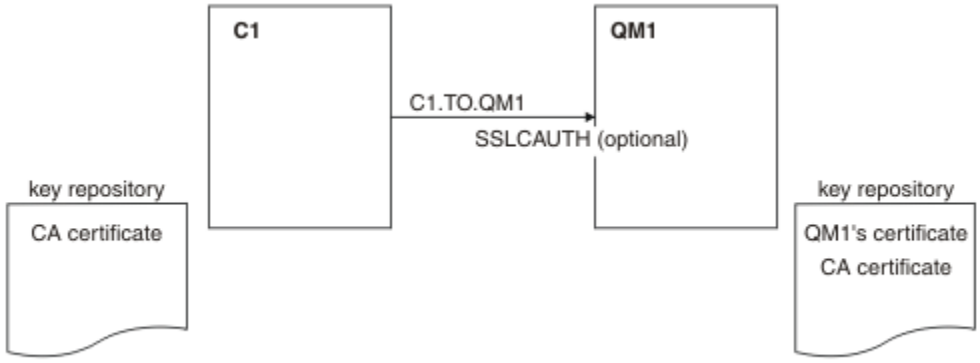
Wykonaj poniższe przykładowe instrukcje, aby zmodyfikować system z wzajemnym uwierzytelnianiem, aby umożliwić menedżerowi kolejek nawiązanie połączenia anonimowo z innym.

O tym zadaniu

Scenariusz:

- Menedżer kolejek i klient (QM1 i C1) zostały skonfigurowane w sposób opisany w sekcji "Korzystanie z certyfikatów podpisanych przez ośrodek CA w celu wzajemnego uwierzytelniania klienta i menedżera kolejek" na stronie 222.
- Użytkownik chce zmienić C1 tak, aby łączył się z nim anonimowo z QM1.

Wynikowa konfiguracja wygląda następująco:



Rysunek 25. Klient i menedżer kolejek zezwalający na anonimowe połączenie

Procedura

1. Usuń certyfikat osobisty z repozytorium kluczy dla C1, zgodnie z systemem operacyjnym:
   - W systemach UNIX, Linuxi Windows. Certyfikat jest oznaczony w następujący sposób:
     - `ibmwebspheremq` , a po nim identyfikator użytkownika logowania złożony z małych liter, na przykład `ibmwebspheremqmyuserid`.
2. Zrestartuj aplikację kliencką lub aplikację kliencką, aby zamknąć i ponownie otworzyć wszystkie połączenia SSL lub TLS.
3. Zezwalaj na anonimowe połączenia z menedżerem kolejek, wydając następującą komendę:

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Wyniki

Repozytoria kluczy i kanały są zmieniane w sposób ilustrowany w programie Rysunek 19 na stronie 224 .

Co dalej

Po zakończeniu działania kanału na serwerze, wartość parametru nazwy węzła na ekranie statusu kanału wskazuje, że wystąpił certyfikat klienta.

Sprawdź, czy zadanie zostało pomyślnie zakończone, wydając niektóre komendy DISPLAY. Jeśli zadanie zakończyło się pomyślnie, wynikowa wartość wyjściowa jest podobna do przedstawionej w poniższym przykładzie:

W menedżerze kolejek QM1wprowadź następującą komendę:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

Wynikowe dane wyjściowe będą podobne do następującego przykładu:

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

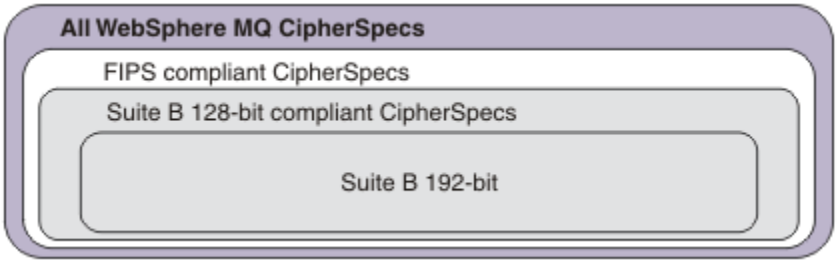
Pola SSLCERTI i SSLPEER są puste, co oznacza, że C1 nie wysłał certyfikatu.

Określanie CipherSpecs

Określ parametr CipherSpec za pomocą parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** MQSC lub **ALTER CHANNEL** MQSC.

Niektóre CipherSpecs , których można użyć z produktem IBM WebSphere MQ , są zgodne ze standardem FIPS. Inne, takie jak NULL_MD5, nie są. Podobnie niektóre CipherSpecs zgodne ze standardem FIPS są również zgodne ze standardem Suite B, chociaż inne nie są zgodne. Wszystkie CipherSpecs zgodne ze standardem Suite B są również zgodne ze standardem FIPS. Wszystkie CipherSpecs zgodne ze standardem Suite B dzielą się na dwie grupy: 128 bitów (na przykład ECDHE_ECDSA_AES_128_GCM_SHA256) i 192 bity (na przykład ECDHE_ECDSA_AES_256_GCM_SHA384).

Na poniższym diagramie przedstawiono relacje między tymi podzbiorami:



W poniższej tabeli przedstawiono specyfikacje szyfrów, których można używać z obsługą protokołów SSL i TLS produktu IBM WebSphere MQ . Jeśli żądasz certyfikatu osobistego, należy podać wielkość klucza dla pary kluczy publicznego i prywatnego. Wielkość klucza używanego podczas uzgadniania SSL jest wielkością zapisaną w certyfikacie, chyba że jest ona określona w specyfikacji szyfrowania CipherSpec(zgodnie z opisem w tabeli).

Nazwa specyfikacji szyfrowania	Używany protokół	Algorytm MAC	Algorytm szyfrowania	Bity szyfrowania	FIPS[1]	Suite B 128-bitowy	Suite B 192-bitowy
NULL_MD5 [a]	SSL 3.0	MD5	Brak	0	Nie	Nie	Nie
NULL_SHA [a]	SSL 3.0	SHA-1	Brak	0	Nie	Nie	Nie
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Nie	Nie	Nie
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Nie	Nie	Nie
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Nie	Nie	Nie
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Nie	Nie	Nie
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Nie	Nie	Nie
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Nie	Nie	Nie
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Nie	Nie	Nie
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Nie [5]	Nie	Nie
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Nie [6]	Nie	Nie

Nazwa specyfikacji szyfrowania	Używany protokół	Algorytm MAC	Algorytm szyfrowania	Bity szyfrowania	FIPS[1]	Suite B 128-bitowy	Suite B 192-bitowy
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Tak	Nie	Nie
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Nie	Nie	Nie
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Nie	Nie	Nie
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Tak	Nie	Nie
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Tak	Nie	Nie
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Tak	Nie	Nie
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Tak	Nie
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Tak
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Tak	Nie	Nie
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Tak	Nie	Nie
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Brak	0	Nie	Nie	Nie
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Brak	0	Nie	Nie	Nie
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Brak	0	Nie	Nie	Nie
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Brak	Brak	0	Nie	Nie	Nie
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Nie	Nie	Nie

Nazwa specyfikacji szyfrowania	Używany protokół	Algorytm MAC	Algorytm szyfrowania	Bity szyfrowania	FIPS[1]	Suite B 128-bitowy	Suite B 192-bitowy

Uwagi:

1. Wskazuje, czy specyfikacja szyfrowania ma certyfikat FIPS na platformie z certyfikatem FIPS. Więcej informacji na temat standardu FIPS zawiera sekcja Standard FIPS (Federal Information Processing Standard).
2. Maksymalna wielkość klucza uzgadniania to 512 bitów. Jeśli którykolwiek z certyfikatów wymienianych podczas uzgadniania SSL ma klucz większy niż 512 bitowy, na potrzeby uzgadniania generowany jest tymczasowy klucz 512-bitowy.
3. Wielkość klucza uzgadniania to 1024 bity.
4. Tej specyfikacji szyfrowania CipherSpec nie można użyć do zabezpieczenia połączenia programu WebSphere MQ Explorer z menedżerem kolejek, chyba że do środowiska JRE używanego przez program Explorer zastosowano odpowiednie nieograniczone pliki strategii.
5. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007.
6. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007. Nazwa `FIPS_WITH_DES_CBC_SHA` jest historyczna i odzwierciedla fakt, że wartość specyfikacji szyfrowania była poprzednio (ale już nie jest) zgodna ze standardem FIPS. Ta specyfikacja szyfrowania jest nieaktualna i jej użycie nie jest zalecane.
7. Ta specyfikacja szyfrowania może zostać użyta do przesłania maksymalnie 32 GB danych. Po przekroczeniu tej wartości połączenie zostanie przerwane i zostanie wyświetlony komunikat o błędzie AMQ9288. Aby uniknąć tego błędu, należy unikać używania algorytmu szyfrowania DES lub włączyć resetowanie klucza tajnego, gdy jest używana ta specyfikacja szyfrowania.

Obsługa platformy:

- a Dostępne na wszystkich obsługiwanych platformach.
- b Dostępne tylko na platformach UNIX, Linux, and Windows .

Pojęcia pokrewne

“Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35

Ten temat zawiera informacje na temat sposobu wyboru odpowiednich specyfikacji CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa, poprzez wykreślenie relacji między CipherSpecs a certyfikatami cyfrowymi w produkcie IBM WebSphere MQ.

Odsyłacze pokrewne

Zdefiniowanie kanału

ZMIEŃ KANAŁ

Uzyskiwanie informacji o specyfikacji CipherSpecs przy użyciu produktu IBM WebSphere MQ Explorer

Za pomocą programu IBM WebSphere MQ Explorer można wyświetlać opisy specyfikacji CipherSpecs.

Aby uzyskać informacje na temat specyfikacji CipherSpecs w produkcie “Określanie CipherSpecs” na stronie 225, należy wykonać następującą procedurę:

1. Otwórz program **IBM WebSphere MQ Explorer** i rozwiń folder **Menedżery kolejek** .
2. Upewnij się, że menedżer kolejek został uruchomiony.
3. Wybierz menedżer kolejek, z którym chcesz pracować, a następnie kliknij opcję **Kanały**.
4. Kliknij prawym przyciskiem myszy kanał, z którym chcesz pracować, i wybierz opcję **Właściwości**.
5. Wybierz stronę właściwości **SSL** .

6. Wybierz z listy opcję CipherSpec , z którą chcesz pracować. Opis jest wyświetlany w oknie znajdującym się poniżej listy.

Alternatywy dla opcji CipherSpecs

W przypadku platform, w których system operacyjny udostępnia obsługę protokołu SSL, system może obsługiwać nowe specyfikacje CipherSpecs. Nową specyfikację CipherSpec można określić za pomocą parametru SSLCIPH, ale wartość, którą należy podać, zależy od używanej platformy.

Uwaga: Ta sekcja nie dotyczy systemów UNIX, Linux i Windows , ponieważ specyfikacje CipherSpecs są dostarczane z produktem WebSphere MQ , dlatego nowe specyfikacje CipherSpecs nie są dostępne po wysyłce.

W przypadku platform, w których system operacyjny udostępnia obsługę protokołu SSL, system może obsługiwać nowe specyfikacje CipherSpecs , które nie są dołączone do produktu “Określanie CipherSpecs” na stronie 225. Nową specyfikację CipherSpec można określić za pomocą parametru SSLCIPH, ale wartość, którą należy podać, zależy od używanej platformy. We wszystkich przypadkach specyfikacja *musi* odpowiadać specyfikacji SSL CipherSpec , która jest poprawna i obsługiwana przez wersję protokołu SSL, w którym działa system.

IBM i

Dwuznakowy łańcuch reprezentujący wartość szesnastkową.

Więcej informacji na temat dozwolonych wartości znajduje się w odpowiedniej dokumentacji produktu (wyszukaj *cipher_spec* w dokumentacji produktu IBM i).

Aby określić wartość, można użyć komendy CHGMQMCHL lub komendy CRTMQMCHL, na przykład:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Aby ustawić parametr SSLCIPH , można również użyć komendy ALTER QMGR MQSC.

z/OS

Dwuznakowy łańcuch reprezentujący wartość szesnastkową. Kody szesnastkowe odpowiadają wartościom zdefiniowanym w protokole SSL.

Więcej informacji na ten temat zawiera opis funkcji gsk_environment_open () w rozdziale referencyjnym API w podręczniku *z/OS Cryptographic Services System SSL Programming*, SC24-5901, gdzie znajduje się lista wszystkich obsługiwanych specyfikacji szyfrów SSL V3.0 i TLS V1.0 w postaci dwucyfrowych kodów szesnastkowych.

Uwagi dotyczące klastrów produktu WebSphere MQ

W przypadku klastrów WebSphere MQ najbezpieczniej jest używać nazw CipherSpec w produkcie “Określanie CipherSpecs” na stronie 225. Jeśli używana jest specyfikacja alternatywna, należy pamiętać, że specyfikacja może nie być poprawna na innych platformach. Więcej informacji zawiera sekcja “SSL i klastry” na stronie 257.

Określanie specyfikacji CipherSpec dla klienta MQI produktu IBM WebSphere MQ

Dostępne są trzy opcje określania wartości CipherSpec dla klienta MQI produktu IBM WebSphere MQ .

Są to następujące opcje:

- Korzystanie z tabeli definicji kanału
- Przy użyciu pola SSLCipherSpec w strukturze MQCD, MQCD_VERSION_7 lub wyższej, w wywołaniu MQCONNX.
- Korzystanie z Active Directory (w systemach Windows z obsługą Active Directory)

Określanie pakietu CipherSuite z klasami produktu IBM WebSphere MQ dla klas Java i IBM WebSphere MQ dla usługi JMS

Klasy IBM WebSphere MQ classes for Java i IBM WebSphere MQ classes for JMS określają CipherSuites w inny sposób niż inne platformy.

Więcej informacji na temat określania pakietu CipherSuite z klasami produktu IBM WebSphere MQ dla języka Java zawiera sekcja Obsługa protokołu SSL (Secure Sockets Layer).

Informacje na temat określania pakietu CipherSuite z klasami IBM WebSphere MQ dla usługi JMS zawiera sekcja Korzystanie z protokołu SSL (Secure Sockets Layer) z klasami produktu WebSphere MQ dla usługi JMS.

Kontrola

Za pomocą komunikatów zdarzeń można sprawdzić, czy w przypadku włamań, włamań lub prób włamań nie ma żadnych uprawnień. Zabezpieczenia systemu można również sprawdzić za pomocą konsoli IBM WebSphere MQ Explorer.

W celu wykrycia prób wykonania nieautoryzowanych działań, takich jak łączenie się z menedżerem kolejek lub umieszczenie komunikatu w kolejce, należy sprawdzić komunikaty o zdarzeniach wygenerowane przez menedżery kolejek, a w szczególności komunikaty o zdarzeniach. Więcej informacji na temat komunikatów zdarzeń menedżera kolejek można znaleźć w sekcji Zdarzenia menedżera kolejek. Więcej informacji na temat monitorowania zdarzeń można znaleźć w sekcji Monitorowanie zdarzeń .

Zabezpieczanie klastrów

Autoryzowanie lub blokowanie menedżerów kolejek łączących się z klastrami lub umieszczania komunikatów w kolejkach klastra. Wymuszenie opuszczenia klastra przez menedżera kolejek. Podczas konfigurowania protokołu SSL dla klastrów należy wziąć pod uwagę kilka dodatkowych uwag.

Zatrzymywanie nieautoryzowanych menedżerów kolejek wysyłających komunikaty

Zapobiegaj nieautoryzowanym menedżerom kolejek wysyłającym komunikaty do menedżera kolejek przy użyciu wyjścia zabezpieczeń kanału.

Zanim rozpoczniesz

Technologia klastrowa nie ma wpływu na sposób działania wyjść zabezpieczeń. Dostęp do menedżera kolejek można ograniczyć w taki sam sposób, jak w rozproszonym środowisku kolejkowania.

O tym zadaniu

Uniemożliwiaj wybranym menedżerom kolejek wysyłanie komunikatów do menedżera kolejek:

Procedura

1. Zdefiniuj program obsługi wyjścia zabezpieczeń kanału w definicji kanału CLUSRCVR .
2. Napisz program, który uwierzytelnia menedżery kolejek w celu wysyłania komunikatów w kanale odbierającym klastry i odmawia im dostępu, jeśli nie są autoryzowane.

Co dalej

Programy obsługi wyjścia zabezpieczeń kanału są wywoływane podczas inicjowania i zakończenia MCA.

Zatrzymywanie nieautoryzowanych menedżerów kolejek umieszczających komunikaty w kolejkach

Użyj atrybutu uprawnienia do umieszczenia kanału w kanale odbiorczym klastra, aby zatrzymać nieautoryzowane menedżery kolejek umieszczające komunikaty w kolejkach. Autoryzuj zdalny menedżer kolejek, sprawdzając ID użytkownika w komunikacie przy użyciu narzędzia RACF w systemie z/OSlub OAM na innych platformach.

O tym zadaniu

W celu kontrolowania dostępu do kolejek należy użyć narzędzi zabezpieczeń platformy oraz mechanizmu kontroli dostępu w produkcie WebSphere MQ .

Procedura

1. Aby uniemożliwić niektórym menedżerom kolejek umieszczanie komunikatów w kolejce, należy skorzystać z narzędzi zabezpieczeń dostępnych na platformie.

   Na przykład:

   - RACF lub inne zewnętrzne menedżery zabezpieczeń w produkcie WebSphere MQ for z/OS
   - Menedżer uprawnień do obiektów (OAM) na innych platformach.
2. Użyj uprawnienia do umieszczania (put authority), PUTAUT, atrybutu w definicji kanału CLUSRCVR .

   Atrybut PUTAUT umożliwia określenie, które identyfikatory użytkowników mają być używane do ustanawiania uprawnień do umieszczania komunikatu w kolejce.

   Opcje w atrybucie PUTAUT są następujące:

   DEF
   Użyj domyślnego ID użytkownika. W systemie z/OSsprawdzenie może dotyczyć zarówno identyfikatora użytkownika otrzymanego z sieci, jak i pochodzącego z parametru MCAUSER.

   CTX
   Użyj identyfikatora użytkownika w informacjach kontekstowych powiązanych z komunikatem. W systemie z/OS sprawdzanie może dotyczyć zarówno identyfikatora użytkownika odebranego z sieci, jak i pochodzącego z MCAUSERlub obu tych elementów. Tej opcji należy użyć, jeśli odsyłacz jest zaufany i uwierzytelniony.

   ONLYMCA (tylkoz/OS)
   Tak jak w przypadku DEF, ale każdy ID użytkownika otrzymany z sieci nie jest używany. Użyj tej opcji, jeśli odsyłacz nie jest zaufany. Użytkownik chce zezwolić na dostęp tylko do określonego zestawu działań, które są zdefiniowane dla użytkownika MCAUSER.

   ALTMCA (tylkoz/OS)
   Tak jak w przypadku CTX, ale każdy ID użytkownika otrzymany z sieci nie jest używany.

Autoryzowanie umieszczania komunikatów w kolejkach klastra zdalnego

Na platformie autoryzuj dostęp do połączenia z menedżerem kolejek i umieść go w kolejce w tym menedżerze kolejek.

O tym zadaniu

Domyślnym zachowaniem jest wykonanie kontroli dostępu w stosunku do SYSTEM.CLUSTER.TRANSMIT.QUEUE. Należy pamiętać, że to zachowanie jest stosowane, nawet jeśli używane jest wiele kolejek transmisji.

Konkretne zachowanie opisane w tym temacie ma zastosowanie tylko wtedy, gdy atrybut **ClusterQueueAccessControl** w pliku qm.ini ma wartość *RQMName*, zgodnie z opisem w sekcji Sekcja zabezpieczeń , a następnie zrestartowany menedżer kolejek.

Procedura

- W przypadku systemów UNIX, Linux i Windows należy wprowadzić następujące komendy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

  Użytkownik może umieszczać komunikaty tylko w określonej kolejce klastra i nie może zawierać żadnych innych kolejek klastra.

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek.

  GroupName
  Nazwa grupy, do której ma zostać przyznany dostęp.

  QueueName
  Nazwa kolejki lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

Co dalej

Jeśli podczas umieszczania komunikatu w kolejce klastra zostanie określona kolejka odpowiedzi, aplikacja konsumująca musi mieć uprawnienia do wysyłania odpowiedzi. Uprawnienia należy ustawić, postępując zgodnie z instrukcjami w sekcji “Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra” na stronie 199.

Informacje pokrewne
Sekcja Security w pliku qm.ini

Zapobieganie łączeniu menedżerów kolejek z klastrem

Jeśli nieuczciwy menedżer kolejek łączy się z klastrem, trudno mu zapobiec otrzymywanie komunikatów, które nie mają być odbierane.

Procedura

Aby upewnić się, że tylko niektóre autoryzowane menedżery kolejek łączą się z klastrem, użytkownik ma do wyboru trzy techniki:

- Za pomocą rekordów uwierzytelniania kanału można zablokować połączenie kanału klastra w oparciu o: zdalny adres IP, nazwę zdalnego menedżera kolejek lub nazwę wyróżniającą SSL/TLS udostępnianej przez system zdalny.
- Napisz program obsługi wyjścia, aby uniemożliwić osobom zarządzającym kolejkami nieuprawnione zapisywanie ich w programie SYSTEM.CLUSTER.COMMAND.QUEUE. Nie należy ograniczać dostępu do produktu SYSTEM.CLUSTER.COMMAND.QUEUE , aby żaden menedżer kolejek nie mógł do niego zapisywać. W przeciwnym razie menedżer kolejek nie może zostać przyłączony do klastra.
- Program obsługi wyjścia zabezpieczeń w definicji kanału produktu CLUSRCVR .

Wyjścia zabezpieczeń w kanałach klastra

Dodatkowe uwagi dotyczące korzystania z wyjść zabezpieczeń w kanałach klastra.

O tym zadaniu

Gdy kanał nadawczy klastra jest uruchamiany po raz pierwszy, używa on atrybutów zdefiniowanych ręcznie przez administratora systemu. Po zatrzymaniu i zrestartowaniu kanału, wybiera on atrybuty z odpowiedniej definicji kanału odbierającego klastry. Pierwotna definicja kanału nadawczego klastra jest zastępowana nowymi atrybutami, w tym atrybutem SecurityExit .

Procedura

1. Należy zdefiniować wyjście zabezpieczeń zarówno na końcu nadajnika klastra, jak i na końcu kanału odbierającego klastry.

   Początkowe połączenie musi zostać nawiązane z uzgadnianiem wyjścia zabezpieczeń, nawet jeśli nazwa wyjścia zabezpieczeń jest wysyłana z definicji dziennika klastra.
2. Sprawdź poprawność obiektu `PartnerName` w strukturze `MQCXP` w wyjściu zabezpieczeń.

   Wyjście musi zezwalać na uruchamianie kanału tylko wtedy, gdy autoryzowany jest menedżer kolejek partnerskich.
3. Zaprojektuj wyjście zabezpieczeń dla definicji odbiornika klastra, który ma być inicjowany odbiornikiem.
4. W przypadku zaprojektowania go jako inicjowanego przez nadawcę, nieautoryzowany menedżer kolejek bez wyjścia zabezpieczeń może dołączyć do klastra, ponieważ nie są wykonywane żadne sprawdzenia zabezpieczeń.

   Dopóki kanał nie zostanie zatrzymany i zrestartowany, można wysłać nazwę `SCYEXIT` z definicji dziennika klastra i wykonane pełne sprawdzenia zabezpieczeń.
5. Aby wyświetlić definicję kanału nadawczego klastra, która jest obecnie używana, należy użyć komendy:

   ```
   DISPLAY CLUSQMGR(queue manager) ALL
   ```

   Komenda wyświetla atrybuty, które zostały wysłane z definicji odbiorcy klastra.
6. Aby wyświetlić pierwotną definicję, użyj komendy:

   ```
   DISPLAY CHANNEL(channel name) ALL
   ```
7. Jeśli menedżery kolejek znajdują się na różnych platformach, konieczne może być zdefiniowanie wyjścia automatycznego definiowania kanału (`CHADEXIT`) w menedżerze kolejek nadawczych klastra.

   Użyj wyjścia automatycznego definiowania kanału, aby ustawić atrybut `SecurityExit` na odpowiedni format dla platformy docelowej.
8. Wdróż i skonfiguruj wyjście zabezpieczeń.

   Systemy Windows, UNIX and Linux

   - Biblioteka dołączania dynamicznego wyjścia zabezpieczeń musi znajdować się w ścieżce określonej w atrybucie `SCYEXIT` definicji kanału.
   - Biblioteka dołączania dynamicznego wyjścia definicji kanału musi znajdować się w ścieżce określonej w atrybucie `CHADEXIT` definicji menedżera kolejek.

Zmuszanie menedżerów kolejek do opuszczenia klastra

Wymuś, aby niepożądany menedżer kolejek opuścił klaster, wydając komendę `RESET CLUSTER` w pełnym menedżerze kolejek repozytorium.

O tym zadaniu

Aby opuścić klaster, można wymusić niepożądany menedżer kolejek. Jeśli na przykład menedżer kolejek jest usuwany, ale jego kanały odbiorcze klastra są nadal zdefiniowane w klastrze. Może zechcesz się schwytać.

Tylko menedżery kolejek pełnego repozytorium są autoryzowane do wysunięcia menedżera kolejek z klastra.

Aby wysuwać menedżera kolejek `OSLO` z klastra `NORWAY`, należy wykonać następującą procedurę:

Procedura

1. W przypadku menedżera kolejek pełnego repozytorium wydaj komendę:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Zamiast wartości QMNAME w komendzie alternatywnej należy użyć wartości QMID :

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

Wyniki

Menedżer kolejek, który jest usuwany, nie zmienia się: jego lokalne definicje klastrów pokazują, że ma on być w klastrze. Definicje we wszystkich innych menedżerach kolejek nie są wyświetlane w klastrze.

Zapobieganie odbierającym komunikaty menedżerom kolejek

Można zapobiec otrzymywanie komunikatów przez menedżera kolejek klastra przez użycie programów obsługi wyjścia, które nie są uprawnione do odbierania.

O tym zadaniu

Trudno jest zatrzymać menedżer kolejek, który jest elementem klastra, definiując kolejkę. Istnieje niebezpieczeństwo, że nieuczciwy menedżer kolejek łączy się z klastrem i definiuje własną instancję jednej z kolejek w klastrze. Teraz może odbierać komunikaty, które nie są autoryzowane do odbioru. Aby zapobiec odbierającym komunikaty menedżera kolejek, należy użyć jednej z następujących opcji podanych w procedurze.

Procedura

- Program obsługi wyjścia kanału w każdym kanale nadawczym klastra. Program obsługi wyjścia używa nazwy połączenia w celu określenia odpowiedniości docelowego menedżera kolejek, który ma zostać wysłany do komunikatów.
- Program obsługi wyjścia obciążenia klastra, który korzysta z rekordów docelowych w celu określenia, czy kolejka docelowa i menedżer kolejek mają być wysyłane do komunikatów.

SSL i klastry

Podczas konfigurowania protokołu SSL dla klastrów należy pamiętać, że definicja kanału CLUSRCVR jest propagowana do innych menedżerów kolejek jako automatycznie zdefiniowany kanał CLUSSDR. Jeśli kanał CLUSRCVR korzysta z protokołu SSL, należy skonfigurować protokół SSL we wszystkich menedżerach kolejek, które komunikują się z użyciem kanału.

Więcej informacji na temat protokołu SSL zawiera sekcja Obsługa protokołu SSL i TLS w produkcie WebSphere MQ. Porady są zwykle stosowane do kanałów klastra, ale warto zwrócić szczególną uwagę na następujące informacje:

W klastrze IBM WebSphere MQ konkretna definicja kanału produktu CLUSRCVR jest często propagowana do wielu innych menedżerów kolejek, w których jest transformowana do automatycznie zdefiniowanego CLUSSDR. Następnie automatycznie zdefiniowany CLUSSDR jest używany do uruchamiania kanału na serwerze CLUSRCVR. Jeśli produkt CLUSRCVR jest skonfigurowany pod kątem połączeń SSL, należy wziąć pod uwagę następujące kwestie:

- Wszystkie menedżery kolejek, które mają komunikować się z tym produktem CLUSRCVR , muszą mieć dostęp do obsługi protokołu SSL. Ten zapis SSL musi obsługiwać specyfikację CipherSpec dla kanału.
- Różne menedżery kolejek, do których propagowane są automatycznie zdefiniowane kanały nadawcze klastra, będą miały inną powiązaną nazwę wyróżniającą. Jeśli na serwerze CLUSRCVR ma być używany sprawdzanie równorzędne nazwy wyróżniającej, należy skonfigurować wszystkie nazwy wyróżniające, które mogą zostać odebrane.

Załóżmy na przykład, że wszystkie menedżery kolejek, które będą udostępniać kanały nadawcze klastra, które połączą się z konkretnym serwerem CLUSRCVR, mają powiązane certyfikaty. Przyjmijmy również, że nazwy wyróżniające we wszystkich tych certyfikatach definiują kraj jako Zjednoczone Królestwo, organizację jako IBM, jednostkę organizacyjną jako IBM WebSphere MQ Development, a wszystkie mają wspólne nazwy w postaci DEVT.QMnnn, gdzie nnn jest numeryczna.

In this case an SSLPEER value of C=UK, O=IBM, OU=WebSphere MQ Development, CN=DEVT.QM* on the CLUSRCVR will allow all the required cluster-sender channels to connect successfully, but will prevent unwanted cluster-sender channels from connecting.

- Jeśli używane są niestandardowe łańcuchy CipherSpec , należy pamiętać o tym, że niestandardowe formaty łańcuchów nie są dozwolone na wszystkich platformach. Przykład: łańcuch CipherSpec RC4_SHA_US ma wartość 05 w systemie IBM i , ale nie jest poprawną specyfikacją w systemach UNIX, Linux lub Windows . Tak więc, jeśli niestandardowe parametry SSLCIPH są używane na serwerze CLUSRCVR, wszystkie wynikowe automatycznie zdefiniowane kanały nadawcze klastra powinny znajdować się na platformach, na których bazową obsługę SSL implementuje ten CipherSpec i na którym można go określić z wartością niestandardową. Jeśli nie można wybrać wartości dla parametru SSLCIPH , który będzie zrozumiały dla całego klastra, konieczne będzie wyjście z definicji automatycznego definiowania kanału, aby zmienić je w sposób, w jaki używane platformy będą zrozumiałe. W miarę możliwości użyj tekstowych łańcuchów CipherSpec (na przykład RC4_MD5_US).

Parametr SSLCRLNL odnosi się do pojedynczego menedżera kolejek i nie jest propagowany do innych menedżerów kolejek w obrębie klastra.

Aktualizowanie klastrowych menedżerów kolejek i kanałów do protokołu SSL

Należy zaktualizować kanały klastra jednocześnie, zmieniając wszystkie kanały CLUSRCVR przed kanałami CLUSSDR .

Zanim rozpoczniesz

Należy wziąć pod uwagę następujące kwestie, ponieważ mogą one mieć wpływ na wybór opcji CipherSpec dla klastra:

- Niektóre obiekty CipherSpecs nie są dostępne na wszystkich platformach. Należy wybrać opcję CipherSpec , która jest obsługiwana przez wszystkie menedżery kolejek w klastrze.
- Niektóre atrybuty CipherSpecs mogą być nowe w bieżącej wersji produktu WebSphere MQ i nie są obsługiwane w starszych wersjach. Klaster zawierający menedżery kolejek działające w różnych wersjach produktu MQ może używać tylko specyfikacji CipherSpecs obsługiwanych przez poszczególne wydania.

  Aby użyć nowej specyfikacji CipherSpec w klastrze, należy najpierw przeprowadzić migrację wszystkich menedżerów kolejek klastra do bieżącej wersji.
- Niektóre atrybuty CipherSpecs wymagają użycia określonego typu certyfikatu cyfrowego, w szczególności tych, które używają szyfrowania krzywej eliptycznej.

Zaktualizuj wszystkie menedżery kolejek w klastrze do produktu WebSphere MQ V6 lub nowszego, jeśli nie znajdują się jeszcze na tych poziomach. Rozdziel certyfikaty i klucze tak, aby protokół SSL był używany z każdym z nich.

O tym zadaniu

Należy zmienić jeden CLUSRCVR jednocześnie i zezwolić na przepływ zmian przez klaster, zanim zostanie on zmieniony. Upewnij się, że nie została zmieniona odwrotna ścieżka, dopóki zmiany dla bieżącego kanału nie zostaną rozdystrybuowane w całym klastrze.

Procedura

1. Przełącz kanały CLUSRCVR na SSL w dowolnej kolejności, w jakiej chcesz.

   Zmiany są wprowadzane w odwrotnym kierunku nad kanałami, które nie są zmieniane na SSL.

2. Przełącz wszystkie ręczne kanały CLUSSDR na SSL.

   Nie ma to żadnego wpływu na działanie klastra, chyba że zostanie użyta komenda REFRESH CLUSTER z opcją REPOS(YES).

   Uwaga: W przypadku dużych klastrów użycie komendy **REFRESH CLUSTER** może zakłócać działanie klastra podczas jej wykonywania oraz później co 27 dni, kiedy obiekty klastra automatycznie wysyłają aktualizacje statusu do wszystkich odpowiednich menedżerów kolejek. Informacje na ten temat zawiera sekcja Odświeżanie dużego klastra może mieć wpływ na jego wydajność i dostępność.

Pojęcia pokrewne

“Określanie CipherSpecs” na stronie 225
Określ parametr CipherSpec za pomocą parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** MQSC lub **ALTER CHANNEL** MQSC.

“Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35
Ten temat zawiera informacje na temat sposobu wyboru odpowiednich specyfikacji CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa, poprzez wykreślenie relacji między CipherSpecs a certyfikatami cyfrowymi w produkcie IBM WebSphere MQ.

Informacje pokrewne

Technologia klastrowa: sprawdzone procedury użycia komendy REFRESH CLUSTER

Wyłączanie protokołu SSL lub TLS w menedżerach kolejek klastrowych i kanałach

Aby wyłączyć protokół SSL lub TLS, należy ustawić parametr SSLCIPH na wartość ' '. Wyłącz obsługę protokołu TLS na kanałach klastra indywidualnie, zmieniając wszystkie kanały odbiornika klastra przed kanałami nadajnika klastra.

O tym zadaniu

Zmień jeden kanał odbiorczy klastra jednocześnie i pozwól, aby zmiany przebiegły przez klaster, a następnie zmieniły się kolejne.

Ważne: Upewnij się, że nie została zmieniona odwrotna ścieżka, dopóki zmiany dla bieżącego kanału nie zostaną rozdystrybuowane w całym klastrze.

Procedura

1. Ustaw wartość parametru SSLCIPH na ' ', pusty łańcuch w pojedynczym cudzysłowie .

   Protokół SSL lub TLS można wyłączyć w kanałach odbiorników klastra w dowolnej kolejności, w jakiej się znajdują.

   Należy pamiętać, że zmiany są wprowadzane w odwrotnym kierunku w kanałach, w których aktywny jest protokół SSL lub TLS.
2. Sprawdź, czy nowa wartość została odzwierciedlona we wszystkich innych menedżerach kolejek, używając komendy **DISPLAY CLUSQMGR(*)** ALL.
3. Wyłącz protokół SSL lub TLS we wszystkich kanałach nadawczych klastra ręcznego.

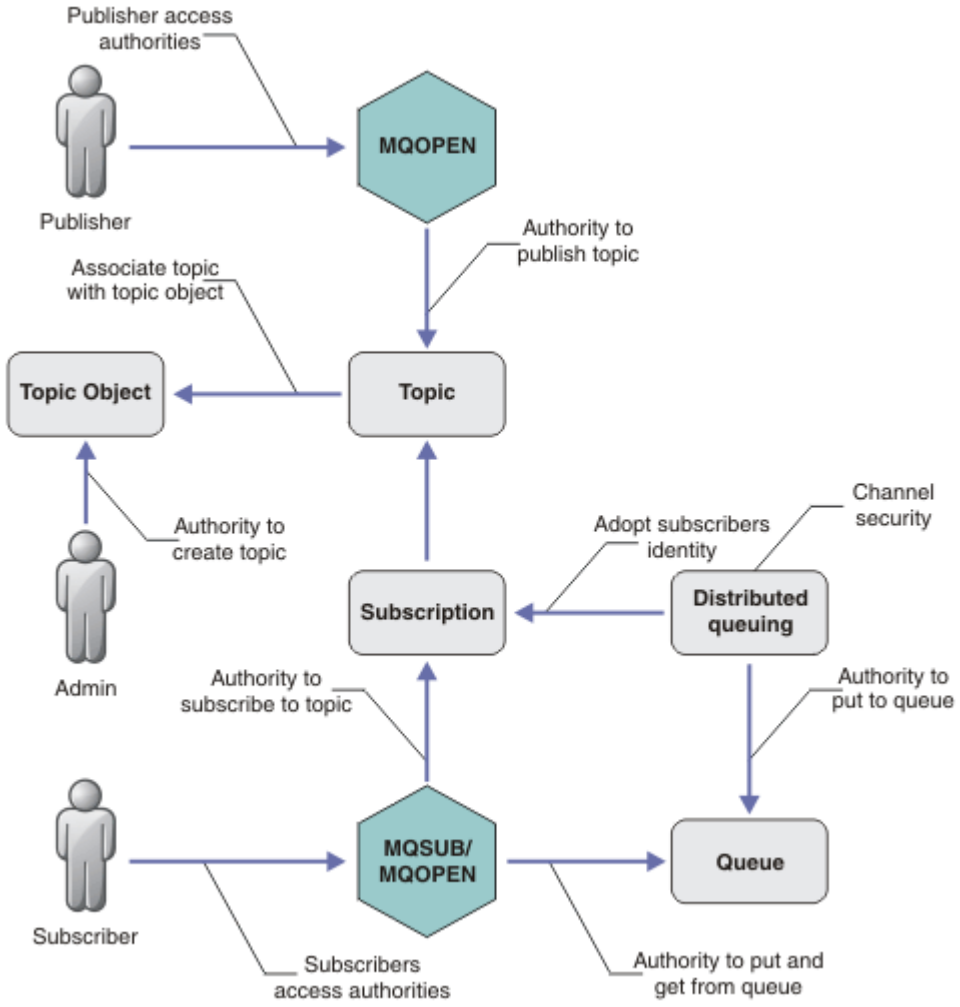
   Nie ma to żadnego wpływu na działanie klastra, o ile nie zostanie użyta komenda **REFRESH CLUSTER** z opcją REPOS (YES).

   W przypadku dużych klastrów użycie komendy **REFRESH CLUSTER** może być zakłócające dla klastra, gdy jest ono w toku, a następnie ponownie w regularnych odstępach czasu, gdy obiekty klastra automatycznie wysyłają aktualizacje statusu do wszystkich zainteresowanych menedżerów kolejek. Więcej informacji na ten temat zawiera sekcja Refreshing w dużym klastrze może mieć wpływ na wydajność i dostępność klastra .
4. Zatrzymaj i zrestartuj kanały nadawcze klastra.

Zabezpieczenia publikowania/subskrypcji

Komponenty i interakcje, które są zaangażowane w publikowanie/subskrybowanie, są opisywane jako wprowadzenie do bardziej szczegółowych wyjaśnień i przykładów, które są następujące.

Istnieje pewna liczba komponentów zaangażowanych w publikowanie i subskrybowanie tematu. Niektóre relacje zabezpieczeń między nimi są zilustrowane w produkcie Rysunek 26 na stronie 260 i opisane w poniższym przykładzie.



Rysunek 26. Relacje zabezpieczeń publikowania/subskrypcji

Tematy

Tematy są identyfikowane za pomocą łańcuchów tematów i zazwyczaj są zorganizowane w drzewa. Patrz sekcja Drzewa tematów. Aby sterować dostępem do tematu, należy powiązać temat z obiektem tematu. “Model zabezpieczeń tematu” na stronie 262 wyjaśnia, jak zabezpieczać tematy przy użyciu obiektów tematów.

Obiekty tematu administracyjnego

You can control who has access to a topic, and for what purpose, by using the command **setmqaut** with a list of administrative topic objects. Zapoznaj się z przykładami “Nadawanie użytkownikowi dostępu do subskrybowania tematu” na stronie 267 i “Przyznaj użytkownikowi prawa dostępu do publikowania w temacie” na stronie 272.

Subskrypcje

Zasubskrybuj jeden lub więcej tematów, tworząc subskrypcję dostarczając łańcuch tematu, który może zawierać znaki wieloznaczne, aby dopasować je do łańcuchów tematów publikacji. Więcej informacji na ten temat zawiera sekcja:

Subskrybuj przy użyciu obiektu tematu
"Subskrybowanie przy użyciu nazwy obiektu tematu" na stronie 263

Subskrybowanie tematu
"Subskrybuj przy użyciu łańcucha tematu, w którym węzeł tematu nie istnieje" na stronie 264

Subskrybuj przy użyciu tematu z użyciem znaków wieloznacznych
"Subskrybuj przy użyciu łańcucha tematu zawierającego znaki wieloznaczne" na stronie 265

Subskrypcja zawiera informacje na temat tożsamości subskrybenta oraz informacje o tożsamości kolejki docelowej, na której mają być umieszczone publikacje. Zawiera również informacje o tym, w jaki sposób publikacja ma być umieszczona w kolejce docelowej.

Podobnie jak w przypadku definiowania subskrybentów, które mają uprawnienia do subskrybowania określonych tematów, można ograniczyć subskrypcje do ich użycia przez pojedynczego subskrybenta. Można również określić, jakie informacje o subskrybencie są używane przez menedżer kolejek, gdy publikacje są umieszczane w kolejce docelowej. Patrz sekcja "Zabezpieczenia subskrypcji" na stronie 277.

Kolejki

Kolejka docelowa jest ważną kolejką zabezpieczoną. Jest on lokalny dla subskrybenta, a publikacje, które są zgodne z subskrypcją, są umieszczane na nim. Należy wziąć pod uwagę dostęp do kolejki docelowej z dwóch perspektyw:

1. Umieszczanie publikacji w kolejce docelowej.
2. Pobieranie publikacji z kolejki docelowej.

Menedżer kolejek umieszcza publikację w kolejce docelowej przy użyciu tożsamości udostępnianej przez subskrybenta. Subskrybent lub program, który został delegowany do wykonywania czynności związanych z uzyskami publikacji, pobiera komunikaty z kolejki. Patrz sekcja "Uprawnienia do kolejek docelowych" na stronie 265.

Brak aliasów obiektów tematów, ale można użyć kolejki aliasowej jako aliasu dla obiektu tematu. W takim przypadku, a także sprawdzanie uprawnień do korzystania z tematu w celu publikowania lub subskrypcji, menedżer kolejek sprawdza uprawnienia do korzystania z kolejki.

Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek

Uprawnienia do publikowania lub subskrybowania tematu są sprawdzane w lokalnym menedżerze kolejek przy użyciu lokalnych tożsamości i autoryzacji. Autoryzacja nie zależy od tego, czy temat jest zdefiniowany, czy też nie, ani w przypadku, gdy jest on zdefiniowany. W związku z tym konieczne jest wykonanie autoryzacji tematu dla każdego menedżera kolejek w klastrze, gdy używane są tematy klastrowe.

Uwaga: Model zabezpieczeń dla tematów różni się od modelu zabezpieczeń dla kolejek. Ten sam wynik dla kolejek można osiągnąć, definiując lokalnie alias kolejki dla każdej kolejki klastrowej.

Menedżery kolejek wymieniają subskrypcje w klastrze. W większości konfiguracji klastra produktu WebSphere MQ kanały są konfigurowane za pomocą komendy PUTAUT=DEF , aby umieszczać komunikaty w kolejkach docelowych za pomocą uprawnień procesu kanału. Konfigurację kanału można zmodyfikować, aby użyć komendy PUTAUT=CTX w celu wymagania, aby użytkownik subskrybujący miał uprawnienia do propagowania subskrypcji do innego menedżera kolejek w klastrze.

Sekcja Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek opisuje sposób zmiany definicji kanałów w celu kontrolowania, kto może propagować subskrypcje na inne serwery w klastrze.

Autoryzacja

Autoryzację można zastosować do obiektów tematu, takich jak kolejki i inne obiekty. Istnieją trzy operacje autoryzacji: pub, subi `resume` , które można stosować tylko w tematach. Szczegółowe informacje są opisane w sekcji Określanie uprawnień dla różnych typów obiektów.

Wywołania funkcji

W programach publikowania i subskrybowania, takich jak w programach w kolejce, sprawdzane są, kiedy obiekty są otwierane, tworzone, zmieniane lub usuwane. Sprawdzanie nie jest wykonywane, gdy wywołania MQI produktu MQPUT lub MQGET są wykonywane w celu umieszczenia i pobrania publikacji.

Aby opublikować temat, należy wykonać MQOPEN w temacie, w którym przeprowadzane są sprawdzenia autoryzacji. Opublikuj komunikaty do uchwytu tematu za pomocą komendy MQPUT , która nie sprawdza autoryzacji.

Aby zasubskrybować dany temat, zwykle należy wykonać komendę MQSUB w celu utworzenia lub wznowienia subskrypcji, a także otworzyć kolejkę docelową w celu otrzymywania publikacji. Alternatywnie można wykonać osobne MQOPEN , aby otworzyć kolejkę docelową, a następnie wykonać MQSUB w celu utworzenia lub wznowienia subskrypcji.

W zależności od tego, które wywołania będą używane, menedżer kolejek sprawdza, czy można zasubskrybować temat i uzyskać wynikowe publikacje z kolejki docelowej. Jeśli kolejka docelowa jest niezarządzana, sprawdzane są również sprawdzanie autoryzacji, czy menedżer kolejek może umieszczać publikacje w kolejce docelowej. Korzysta on z tożsamości, która została adoptowane z zgodnej subskrypcji. Zakłada się, że menedżer kolejek zawsze jest w stanie umieścić publikacje w zarządzanych kolejkach docelowych.

Role

Użytkownicy są zaangażowani w cztery role w działających aplikacjach publikowania/subskrypcji:

1. Publikator
2. Subskrybent
3. Administrator tematu
4. WebSphere MQ Administrator-członek grupy `mqm`

Zdefiniuj grupy z odpowiednimi autoryzacjami, które odpowiadają rolom publikowania, subskrybowania i administrowania tematem. Następnie można przypisać nazwy użytkowników do tych grup, autoryzując je do wykonywania konkretnych zadań publikowania i subskrypcji.

Ponadto konieczne jest rozszerzenie autoryzacji operacji administracyjnych na administratora kolejek i kanałów odpowiedzialnych za przenoszenie publikacji i subskrypcji.

Model zabezpieczeń tematu

Tylko zdefiniowane obiekty tematów mogą mieć powiązane atrybuty zabezpieczeń. Opis obiektów tematów znajduje się w sekcji Obiekty tematu administracyjnego. Atrybuty zabezpieczeń określają, czy określony ID użytkownika, czy grupa uprawnień ma uprawnienia do wykonywania operacji subskrybowania lub publikowania dla każdego obiektu tematu.

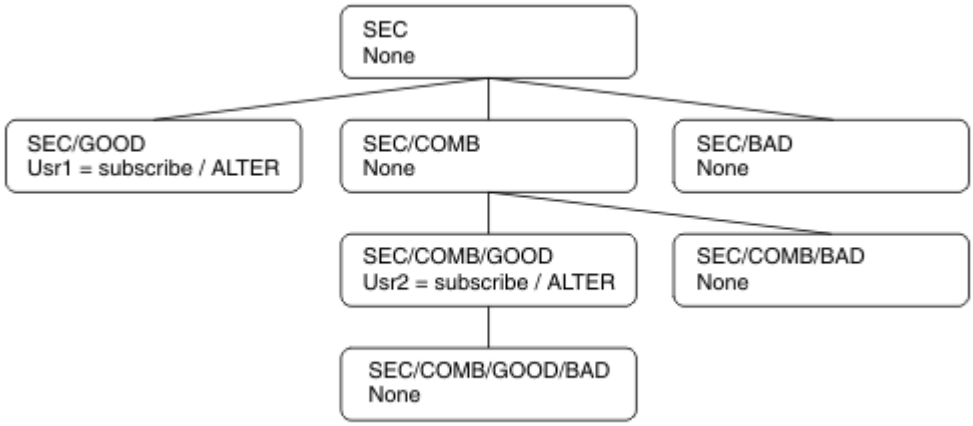
Atrybuty zabezpieczeń są powiązane z odpowiednim węzłem administracyjnym w drzewie tematów. Jeśli podczas operacji subskrypcji lub publikowania wykonywane jest sprawdzenie uprawnień dla konkretnego identyfikatora użytkownika, nadawane uprawnienia są oparte na atrybutach zabezpieczeń powiązanego węzła drzewa tematów.

Atrybuty zabezpieczeń to lista kontroli dostępu, która wskazuje, jakie uprawnienia dany użytkownik systemu operacyjnego lub grupy uprawnień ma do obiektu tematu.

Rozważmy następujący przykład, w którym obiekty tematów zostały zdefiniowane z atrybutami zabezpieczeń lub wyświetlane są uprawnienia:

Tabela 17. Przykładowe uprawnienia do obiektu tematu			
Nazwa tematu	**Łańcuch tematu**	**Uprawnienia-nie z/OS**	**Uprawnienia do systemu z/OS**
SECROOT	SEC	Brak	Brak
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Brak	Brak HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	Brak	Brak HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Brak	Brak HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Brak	Brak HLQ.SUBSCRIBE.SECCOMBN

Drzewo tematów wraz z powiązanymi atrybutami zabezpieczeń w każdym węźle może być reprezentowane w następujący sposób:



Podane przykłady dają następujące autoryzacje:

- W węźle głównym drzewa /SECżaden użytkownik nie ma uprawnień w tym węźle.
- usr1 ma nadane uprawnienie do subskrypcji dla obiektu /SEC/GOOD
- usr2 ma nadane uprawnienie do subskrypcji dla obiektu /SEC/COMB/GOOD

Subskrybowanie przy użyciu nazwy obiektu tematu

Subskrybując obiekt tematu przez określenie nazwy MQCHAR48 , znajduje się odpowiedni węzeł w drzewie tematów. Jeśli atrybuty zabezpieczeń powiązane z węzłem wskazują, że użytkownik ma uprawnienia do subskrybowania, to dostęp jest nadawany.

Jeśli użytkownik nie ma uprawnień dostępu, węzeł nadrzędny w drzewie określa, czy użytkownik ma uprawnienia do subskrybowania na poziomie węzła nadrzędnego. Jeśli tak, to dostęp jest nadawany. Jeśli

nie, to element nadrzędny tego węzła jest uważany za element nadrzędny. Rekurencja jest kontynuowana do momentu, w którym znajduje się węzeł, który nadaje użytkownikowi uprawnienia do subskrybowania. Rekurencja jest zatrzymana, gdy węzeł główny jest traktowany bez uprawnień. W tym ostatnim przypadku odmowa dostępu.

Krótko mówiąc, jeśli dowolny węzeł w ścieżce nadaje uprawnienie do subskrybowania tego użytkownika lub aplikacji, subskrybent może subskrybować ten węzeł lub znajdować się w dowolnym miejscu poniżej tego węzła w drzewie tematów.

Węzeł główny w tym przykładzie to SEC.

Użytkownik ma nadane uprawnienie do subskrypcji, jeśli lista kontroli dostępu wskazuje, że użytkownik ma uprawnienia, lub że grupa uprawnień systemu operacyjnego, której członkiem jest użytkownik, ma uprawnienia.

Tak więc, na przykład:

- Jeśli program `usr1` próbuje zasubskrybować, korzystając z łańcucha tematu produktu `SEC/GOOD`, subskrypcja będzie dozwolona, ponieważ identyfikator użytkownika ma dostęp do węzła powiązanego z tym tematem. Jeśli jednak program `usr1` próbował zasubskrybować łańcuch tematu `SEC/COMB/GOOD` , subskrypcja nie jest dozwolona, ponieważ identyfikator użytkownika nie ma dostępu do węzła powiązanego z tym identyfikatorem.
- Jeśli program `usr2` próbuje zasubskrybować, za pomocą łańcucha tematu produktu `SEC/COMB/GOOD` można zezwolić na to, że identyfikator użytkownika ma dostęp do węzła powiązanego z tym tematem. Jeśli jednak program `usr2` próbował zasubskrybować program `SEC/GOOD` , subskrypcja nie będzie dozwolona, ponieważ identyfikator użytkownika nie ma dostępu do węzła powiązanego z tym identyfikatorem.
- Jeśli program `usr2` próbuje zasubskrybować łańcuch tematu `SEC/COMB/GOOD/BAD` , może to być spowodowane tym, że ID użytkownika ma dostęp do węzła nadrzędnego `SEC/COMB/GOOD`.
- Jeśli program `usr1` lub produkt `usr2` próbuje zasubskrybować łańcuch tematu w produkcie `/SEC/COMB/BAD`, nie jest dozwolone, ponieważ nie mają one dostępu do węzła tematu powiązanego z tym węzłem lub węzłów nadrzędnych tego tematu.

Operacja subskrypcji, która określa nazwę obiektu tematu, który nie istnieje, powoduje błąd MQRC_UNKNOWN_OBJECT_NAME.

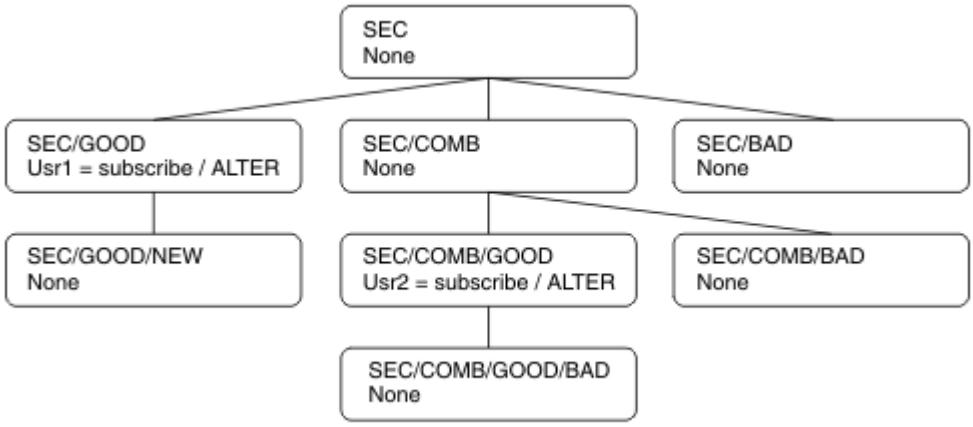
Subskrypcja za pomocą łańcucha tematu, w którym znajduje się węzeł tematu

Zachowanie jest takie samo, jak w przypadku określania tematu przy użyciu nazwy obiektu MQCHAR48 .

Subskrybuj przy użyciu łańcucha tematu, w którym węzeł tematu nie istnieje

Rozważ przypadek aplikacji subskrybującej, określając łańcuch tematu reprezentujący węzeł tematu, który aktualnie nie istnieje w drzewie tematów. Sprawdzanie uprawnień jest wykonywane zgodnie z opisem podanym w poprzedniej sekcji. Sprawdzanie rozpoczyna się od węzła nadrzędnego tego, który jest reprezentowany przez łańcuch tematu. Jeśli uprawnienie jest nadawane, w drzewie tematów zostanie utworzony nowy węzeł reprezentujący łańcuch tematu.

Na przykład program `usr1` próbuje zasubskrybować temat `SEC/GOOD/NEW`. Uprawnienie jest nadawane jako `usr1` ma dostęp do węzła nadrzędnego `SEC/GOOD`. Nowy węzeł tematu zostanie utworzony w drzewie w postaci pokazów na poniższym diagramie. Nowy węzeł tematu nie jest obiektem tematu, w którym nie są powiązane żadne atrybuty zabezpieczeń bezpośrednio; atrybuty są dziedziczone ze swojego elementu nadrzędnego.



Subskrybuj przy użyciu łańcucha tematu zawierającego znaki wieloznaczne

Należy rozważyć przypadek subskrypcji przy użyciu łańcucha tematu, który zawiera znak wieloznaczny. Sprawdzanie uprawnień jest wykonywane względem węzła w drzewie tematów, który jest zgodny z pełną częścią łańcucha tematu.

Jeśli więc aplikacja subskrybuje produkt SEC/COMB/GOOD/*, to sprawdzanie uprawnień jest przeprowadzane zgodnie z opisem w poprzednich dwóch sekcjach w węźle SEC/COMB/GOOD w drzewie tematów.

Analogicznie, jeśli aplikacja wymaga subskrypcji produktu SEC/COMB/*/GOOD, sprawdzenie uprawnień jest wykonywane w węźle SEC/COMB.

Uprawnienia do kolejek docelowych

W przypadku subskrybowania tematu jednym z parametrów jest uchwyt hobj kolejki, która została otwarta dla danych wyjściowych w celu odebrania publikacji.

Jeśli parametr hobj nie został określony, ale jest pusty, zostanie utworzona kolejka zarządzana, jeśli zostaną spełnione następujące warunki:

- Podano opcję MQSO_MANAGED .
- Subskrypcja nie istnieje.
- Tworzenie jest określone.

Jeśli pole hobj jest puste, a istniejąca subskrypcja jest zmieniana lub wznawiana, to poprzednio udostępniona kolejka docelowa może być zarządzana lub niezarządzana.

Aplikacja lub użytkownik tworający żądanie MQSUB musi mieć uprawnienia do umieszczania komunikatów w kolejce docelowej, którą udostępnił. W rezultacie uprawnienia do publikowania komunikatów umieszczanych w tej kolejce. Sprawdzanie uprawnień jest zgodne z istniejącymi regułami sprawdzania zabezpieczeń kolejki.

Sprawdzanie zabezpieczeń obejmuje alternatywny identyfikator użytkownika i sprawdzenie zabezpieczeń kontekstu, jeśli jest to wymagane. Aby można było ustawić dowolne pola kontekstu tożsamości, należy podać opcję MQSO_SET_IDENTITY_CONTEXT oraz opcję MQSO_CREATE lub MQSO_ALTER . Nie można ustawić żadnego z pól kontekstu tożsamości w żądaniu MQSO_RESUME .

Jeśli miejsce docelowe jest kolejką zarządzaną, nie są wykonywane żadne sprawdzenia zabezpieczeń dla zarządzanego miejsca docelowego. Jeśli użytkownik ma prawo zasubskrybować temat, zakłada się, że można używać zarządzanych miejsc docelowych.

Publikowanie przy użyciu nazwy tematu lub łańcucha tematu, w którym znajduje się węzeł tematu

Model zabezpieczeń publikowania jest taki sam jak w przypadku subskrybowania, z wyjątkiem znaków wieloznacznych. Publikacje nie zawierają znaków wieloznacznych, więc nie ma żadnego przypadku łańcucha tematu zawierającego znaki wieloznaczne, które należy rozważyć.

Uprawnienia do publikowania i subskrybowania są różne. Użytkownik lub grupa może mieć uprawnienia do wykonania jednego z nich bez konieczności wykonania innych czynności.

W przypadku publikowania w obiekcie tematu przez określenie nazwy MQCHAR48 lub łańcucha tematu, odpowiedni węzeł w drzewie tematów jest zlokalizowany. Jeśli atrybuty zabezpieczeń powiązane z węzłem tematu wskazują, że użytkownik ma uprawnienia do publikowania, to dostęp jest nadawany.

Jeśli dostęp nie jest nadawany, węzeł nadrzędny w drzewie określa, czy użytkownik ma uprawnienia do publikowania na tym poziomie. Jeśli tak, to dostęp jest nadawany. Jeśli nie, rekurencja będzie kontynuowana aż do momentu, w którym znajduje się węzeł, który nadaje użytkownikowi uprawnienia do publikowania. Rekurencja jest zatrzymana, gdy węzeł główny jest traktowany bez uprawnień. W tym ostatnim przypadku odmowa dostępu.

Krótko mówiąc, jeśli dowolny węzeł w ścieżce nadaje uprawnienia do publikowania w danym użytkowniku lub aplikacji, publikator może publikować w tym węźle lub w dowolnym miejscu poniżej tego węzła w drzewie tematów.

Publikowanie przy użyciu nazwy tematu lub łańcucha tematu, w którym węzeł tematu nie istnieje

Podobnie jak w przypadku operacji subskrybowania, gdy aplikacja publikuje, określając łańcuch tematu reprezentujący węzeł tematu, który aktualnie nie istnieje w drzewie tematów, to sprawdzanie uprawnień jest wykonywane począwszy od elementu nadrzędnego węzła reprezentowanego przez łańcuch tematu. Jeśli uprawnienie jest nadawane, w drzewie tematów zostanie utworzony nowy węzeł reprezentujący łańcuch tematu.

Publikowanie przy użyciu kolejki aliasowej, która jest tłumaczona na obiekt tematu

W przypadku publikowania przy użyciu kolejki aliasowej, która jest tłumaczona na obiekt tematu, sprawdzanie zabezpieczeń odbywa się zarówno w kolejce aliasowej, jak i w temacie bazowym, do którego jest rozstrzygana.

Sprawdzenie zabezpieczeń w kolejce aliasowej sprawdza, czy użytkownik ma uprawnienia do umieszczania komunikatów w tej kolejce aliasowej, a sprawdzanie zabezpieczeń tematu sprawdza, czy użytkownik może publikować w tym temacie. Gdy kolejka aliasowa jest tłumaczona na inną kolejkę, to *nie* są sprawdzane w kolejce bazowej. Sprawdzanie uprawnień jest wykonywane w różny sposób w przypadku tematów i kolejek.

Zamykanie subskrypcji

Jeśli subskrypcja jest zamykana za pomocą opcji MQCO_REMOVE_SUB , jeśli subskrypcja nie została utworzona pod tym uchwytem, należy sprawdzić dodatkowe zabezpieczenia.

Sprawdzenie zabezpieczeń jest wykonywane w celu upewnia się, że użytkownik ma odpowiednie uprawnienia do wykonania tej czynności, ponieważ działanie powoduje usunięcie subskrypcji. Jeśli atrybuty zabezpieczeń powiązane z węzłem tematu wskazują, że użytkownik ma uprawnienia, dostęp jest nadawany. Jeśli nie, to węzeł nadrzędny w drzewie jest uznawany za określenie, czy użytkownik ma uprawnienia do zamknięcia subskrypcji. Rekurencja jest kontynuowana do momentu przyznania uprawnienia albo do węzła głównego.

Definiowanie, modyfikowanie i usuwanie subskrypcji

Jeśli subskrypcja jest tworzona administracyjnie, nie są przeprowadzane sprawdzanie zabezpieczeń, a nie za pomocą żądania API MQSUB . Administrator został już nadany temu uprawnionowi za pomocą komendy.

Przeprowadzane są sprawdzenia zabezpieczeń, aby zapewnić, że publikacje mogą być umieszczane w kolejce docelowej powiązanej z subskrypcją. Sprawdzenia są wykonywane w taki sam sposób, jak w przypadku żądania MQSUB .

Identyfikator użytkownika, który jest używany dla tych sprawdzeń zabezpieczeń, zależy od komendy, która została wydana. Jeśli określono parametr **SUBUSER** , ma ona wpływ na sposób wykonywania operacji sprawdzania, tak jak to pokazano na rysunku Tabela 18 na stronie 267:

Tabela 18. Identyfikatory użytkowników używane do sprawdzania zabezpieczeń komend

Komenda	Określono SUBUSER i puste	Podano i zakończono SUBUSER	Nie określono SUBUSER
	Użyj identyfikatora administratora		Użyj identyfikatora administratora
	Użyj identyfikatora administratora		Użyj ID użytkownika z istniejącej subskrypcji

Jedynym sprawdzonym sprawdzonym zabezpieczeniem podczas usuwania subskrypcji za pomocą komendy DELETE SUB jest sprawdzenie zabezpieczeń komendy.

Przykład konfiguracji zabezpieczeń publikowania/subskrypcji

W tej sekcji opisano scenariusz, który ma konfigurację kontroli dostępu w tematach w sposób umożliwiający stosowanie w razie potrzeby kontroli zabezpieczeń.

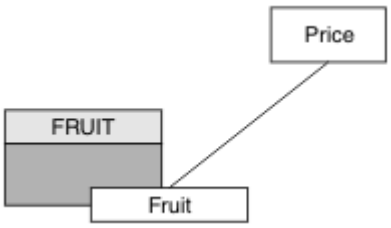
Nadawanie użytkownikowi dostępu do subskrybowania tematu

Ten temat jest pierwszym z nich na liście zadań, które informują użytkownika o tym, jak nadać dostęp do tematów więcej niż jednemu użytkownikowi.

O tym zadaniu

W tym zadaniu przyjęto założenie, że nie istnieją żadne administracyjne obiekty tematu ani nie zdefiniowano żadnych profili dla subskrypcji ani publikacji. Aplikacje tworzą nowe subskrypcje, a nie wznawiają istniejące, i robią to tylko za pomocą łańcucha tematu.

Aplikacja może utworzyć subskrypcję, udostępniając obiekt tematu lub łańcuch tematu albo kombinację obu tych elementów. W zależności od tego, jaki sposób wybierze aplikację, efektem jest dokonanie subskrypcji w określonym punkcie w drzewie tematów. Jeśli ten punkt w drzewie tematów jest reprezentowany przez obiekt tematu administracyjnego, profil zabezpieczeń jest sprawdzany w oparciu o nazwę tego obiektu tematu.



Rysunek 27. Przykład dostępu do obiektu tematu

Tabela 19. Przykładowy dostęp do obiektu tematu		
Temat	**Wymagany dostęp do subskrypcji**	**Obiekt tematu**
Cena	Brak użytkownika	Brak
Cena/Owoce	USER1	fruit

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Uruchom komendę MQSC `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Nadaj dostęp w następujący sposób:
   - Inne platformy:

     Nadaj dostęp do produktu USER1 , aby zasubskrybować temat `"Price/Fruit"` , nadając użytkownikowi dostęp do obiektu FRUIT . W tym celu za pomocą komendy autoryzacji dla platformy:

     Windows UNIX Linux **Systemy Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

Wyniki

Gdy program USER1 próbuje zasubskrybować temat `"Price/Fruit"` , wynik jest pomyślny.

Gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit"` , wynikiem jest niepowodzenie w przypadku komunikatu `MQRC_NOT_AUTHORIZED` , wraz z:

- Windows UNIX Linux Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Należy pamiętać, że jest to ilustracja tego, co widzisz, a nie wszystkie pola.

Nadawanie użytkownikowi dostępu do subskrybowania tematu w obrębie drzewa

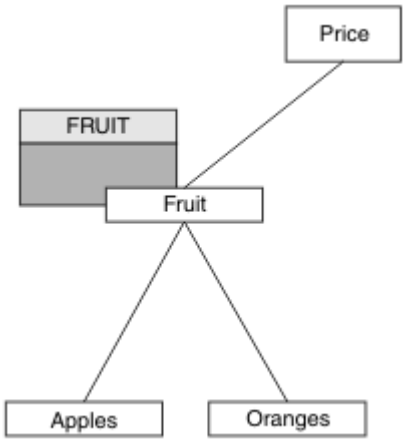
Ten temat jest drugim z listy zadań, które informują o tym, jak nadać dostęp do tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Nadawanie użytkownikowi dostępu do subskrybowania tematu” na stronie 267.

O tym zadaniu

Jeśli punkt w drzewie tematów, w którym aplikacja powoduje, że subskrypcja nie jest reprezentowana przez obiekt tematu administracyjnego, należy przenieść drzewo w górę do momentu, w którym znajduje się najbliższy nadrzędny obiekt tematu administracyjnego. Profil zabezpieczeń jest sprawdzany w oparciu o nazwę tego obiektu tematu.



Rysunek 28. Przykład nadawania dostępu do tematu w drzewie tematów

Tabela 20. Wymagania dotyczące dostępu dla przykładowych tematów i obiektów tematów

Temat	Wymagany dostęp do subskrypcji	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Owoce	USER1	fruit
Cena/Owoce/Jabłka	USER1	
Cena/Owoce/Pomarańcze	USER1	

W poprzednim zadaniu USER1 uzyskano dostęp do subskrypcji tematu `"Price/Fruit"` , nadając mu dostęp do profilu produktu `hlq.SUBSCRIBE.FRUIT` w systemie z/OS i zasubskrybować dostęp do profilu produktu FRUIT na innych platformach. Ten pojedynczy profil nadaje również dostęp do programu USER1 w celu zasubskrybowania produktów `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` i `"Price/Fruit/#"`.

Gdy program USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynik jest pomyślny.

Gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynikiem jest niepowodzenie w przypadku komunikatu `MQRC_NOT_AUTHORIZED` , wraz z:

- W systemie z/OSnastępujące komunikaty widoczne na konsoli, które przedstawiają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Apples"
```

Na co zwrócić uwagę:

- Komunikaty, które są odbierane w systemie z/OS , są identyczne z komunikatami otrzymywanych w poprzednim zadaniu, ponieważ te same obiekty tematów i profile kontrolują dostęp.
- Komunikat o zdarzeniu otrzymany na innych platformach jest podobny do otrzymanego w poprzednim zadaniu, ale rzeczywisty łańcuch tematu jest inny.

Nadaj innemu użytkownikowi dostęp, aby zasubskrybować tylko temat głębiej w obrębie drzewa.

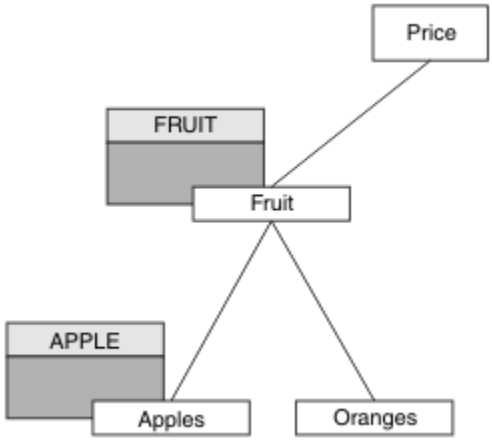
Ten temat jest trzecim na liście zadań, które informują użytkownika o tym, jak przyznać dostęp do subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Nadawanie użytkownikowi dostępu do subskrybowania tematu w obrębie drzewa” na stronie 268.

O tym zadaniu

W poprzednim zadaniu USER2 odmówiono dostępu do tematu `"Price/Fruit/Apples"`. W tym temacie opisano sposób nadawania dostępu do tego tematu, ale nie do żadnych innych tematów.



Rysunek 29. Nadawanie dostępu do konkretnych tematów w drzewie tematów

Tabela 21. Wymagania dotyczące dostępu dla przykładowych tematów i obiektów tematów

Temat	Wymagany dostęp do subskrypcji	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Owoce	USER1	fruit
Cena/Owoce/Jabłka	USER1 i USER2	Apple
Cena/Owoce/Pomarańcze	USER1	

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Uruchom komendę MQSC `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.

2. Nadaj dostęp w następujący sposób:
   - Inne platformy:

     W poprzednim zadaniu USER1 został nadany dostęp do subskrypcji tematu `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do subskrypcji do profilu `FRUIT` .

     Ten pojedynczy profil przyznał również dostęp do produktu USER1 w celu zasubskrybowania produktów `"Price/Fruit/Oranges"` i `"Price/Fruit/#"`, a ten dostęp pozostaje nawet z dodaniem nowego obiektu tematu i powiązanych z nim profili.

     Nadaj dostęp do produktu USER2 , aby zasubskrybować temat `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do subskrypcji w profilu produktu `APPLE` . W tym celu za pomocą komendy autoryzacji dla platformy:

     
     Systemy Windows, UNIX and Linux

     ```
     setmqaut -t topic -n APPLE -p USER2 +sub
     ```

Wyniki

W systemie z/OS, gdy program USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , pierwsze sprawdzenie zabezpieczeń w profilu `hlq.SUBSCRIBE.APPLE` nie powiedzie się, ale podczas przenoszenia drzewa profil `hlq.SUBSCRIBE.FRUIT` umożliwia użytkownikowi USER1 zasubskrybowanie, więc subskrypcja powiedzie się i żaden kod powrotu nie jest wysyłany do wywołania MQSUB. Jednak w przypadku pierwszego sprawdzenia generowany jest komunikat RACF `ICH` :

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynik jest pomyślny, ponieważ sprawdzenie zabezpieczeń jest przekazywane w pierwszym profilu.

Gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit/Oranges"` , wynikiem jest niepowodzenie w przypadku komunikatu `MQRC_NOT_AUTHORIZED` , wraz z:

- 
  Na platformach Windows, UNIX i Linux : następujące zdarzenie autoryzacji:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

Wadą tej konfiguracji jest to, że w systemie z/OSna konsoli są wyświetlane dodatkowe komunikaty produktu `ICH` . Można tego uniknąć, jeśli drzewo tematów zostanie zabezpieczone w inny sposób.

Zmiana kontroli dostępu w celu uniknięcia dodatkowych komunikatów

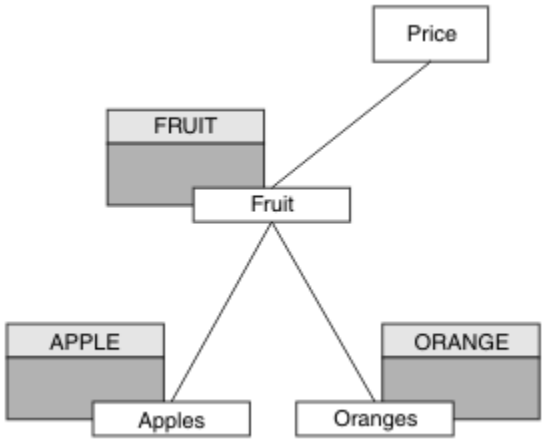
Ten temat jest czwartym z listy zadań, które informują użytkownika o sposobach nadawania dostępu do subskrybowania tematów przez więcej niż jednego użytkownika oraz w celu uniknięcia dodatkowych komunikatów RACF ICH408I w systemie z/OS.

Zanim rozpoczniesz

W tym temacie rozszerzono konfigurację opisaną w sekcji “Nadaj innemu użytkownikowi dostęp, aby zasubskrybować tylko temat głębiej w obrębie drzewa.” na stronie 270 , dzięki czemu można uniknąć dodatkowych komunikatów o błędach.

O tym zadaniu

W tym temacie opisano sposób nadawania dostępu do tematów głębiej w drzewie oraz sposób usuwania dostępu do tematu w dolnej części drzewa, gdy żaden użytkownik nie wymaga tego dostępu.



Rysunek 30. Przykład nadawania kontroli dostępu w celu uniknięcia dodatkowych komunikatów.

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Uruchom komendę MQSC `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Nadaj dostęp w następujący sposób:
   - Inne platformy:

     Skonfiguruj równoważny dostęp za pomocą komend autoryzacji dla platformy:

     Windows UNIX Linux **Systemy Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n ORANGE -p USER1 +sub
     setmqaut -t topic -n APPLE -p USER1 +sub
     ```

Wyniki

W systemie z/OS, gdy program USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , pierwsze sprawdzenie zabezpieczeń w profilu `hlq.SUBSCRIBE.APPLE` powiodło się.

Podobnie, gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynik jest pomyślny, ponieważ sprawdzenie zabezpieczeń jest przekazywane w pierwszym profilu.

Gdy program USER2 próbuje zasubskrybować temat `"Price/Fruit/Oranges"` , wynikiem jest niepowodzenie w przypadku komunikatu `MQRC_NOT_AUTHORIZED` , wraz z:

- Windows UNIX Linux Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

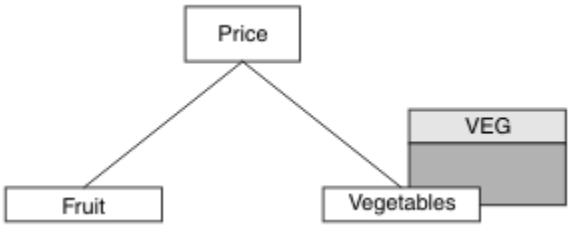
Przyznaj użytkownikowi prawa dostępu do publikowania w temacie

Ten temat jest pierwszym z nich na liście zadań, które podpowiada, w jaki sposób można nadać dostęp do tematów publikowania przez więcej niż jednego użytkownika.

O tym zadaniu

W tym zadaniu przyjęto założenie, że żadne obiekty tematu administracyjnego nie istnieją po prawej stronie drzewa tematów, ani nie zdefiniowano żadnych profili do publikacji. Przyjęto założenie, że publikatory używają tylko łańcucha tematu.

Aplikacja może publikować w temacie, udostępniając obiekt tematu lub łańcuch tematu lub kombinację obu tych elementów. Niezależnie od sposobu wyboru aplikacji, efekt jest publiowany w określonym punkcie w drzewie tematów. Jeśli ten punkt w drzewie tematów jest reprezentowany przez obiekt tematu administracyjnego, profil zabezpieczeń jest sprawdzany w oparciu o nazwę tego obiektu tematu. Na przykład:



Rysunek 31. Nadawanie dostępu publikowania do tematu

Tabela 22. Przykładowe wymagania dotyczące dostępu do publikowania

Temat	Wymagany jest dostęp do publikowania	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Warzywa	USER1	VEG

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Uruchom komendę MQSC `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Nadaj dostęp w następujący sposób:
   - Inne platformy:

     Nadaj dostęp do produktu USER1 , aby opublikować go w temacie `"Price/Vegetables"` , nadając użytkownikowi dostęp do profilu produktu VEG . W tym celu za pomocą komendy autoryzacji dla platformy:

     Windows UNIX Linux **Systemy Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n VEG -p USER1 +pub
     ```

Wyniki

Gdy program USER1 podejmuje próbę opublikowania w temacie `"Price/Vegetables"` , wynikiem jest powodzenie. To znaczy, że wywołanie MQOPEN zakończy się powodzeniem.

Gdy program USER2 podejmie próbę opublikowania tematu `"Price/Vegetables"` , wywołanie MQOPEN nie powiedzie się i zostanie wyświetlony komunikat `MQRC_NOT_AUTHORIZED` wraz z:

- Windows UNIX Linux Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Należy pamiętać, że jest to ilustracja tego, co widzisz, a nie wszystkie pola.

Przyznaj użytkownikowi dostęp do tematu w celu głębszego publikowania tematu w drzewie

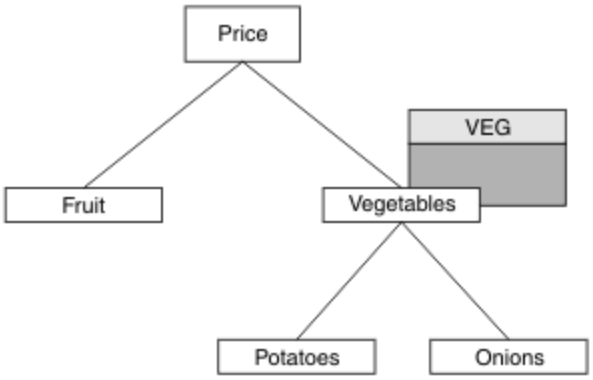
Ten temat jest drugi na liście zadań, które informują o sposobach nadawania dostępu do publikowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Przyznaj użytkownikowi prawa dostępu do publikowania w temacie” na stronie 272.

O tym zadaniu

Jeśli punkt w drzewie tematów, w którym publikowane są aplikacje, nie jest reprezentowany przez administracyjny obiekt tematu, należy przenieść drzewo do momentu, gdy znajduje się najbliższy nadrzędny obiekt tematu administracyjnego. Profil zabezpieczeń jest sprawdzany w oparciu o nazwę tego obiektu tematu.



Rysunek 32. Nadawanie dostępu publikowania do tematu w drzewie tematów

Tabela 23. Przykładowe wymagania dotyczące dostępu do publikowania

Temat	Wymagany dostęp do subskrypcji	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Warzywa	USER1	VEG
Cena/Warzywa/ Ziemniaki	USER1	
Cena/warzywa/ Cebula	USER1	

W poprzednim zadaniu USER1 został nadany dostęp do tematu publikowania `"Price/Vegetables/Potatoes"` , nadając mu dostęp do profilu `hlq.PUBLISH.VEG` w systemie z/OS lub publikując dostęp do profilu produktu VEG na innych platformach. Ten pojedynczy profil nadaje również uprawnienia do publikowania w produkcie USER1 w produkcie `"Price/Vegetables/Onions"`.

Gdy program USER1 podejmuje próbę opublikowania w temacie `"Price/Vegetables/Potatoes"` , wynik jest pomyślny; to wywołanie MQOPEN zakończy się powodzeniem.

Gdy program USER2 próbuje zasubskrybować temat `"Price/Vegetables/Potatoes"` , wynikiem jest niepowodzenie. To oznacza, że wywołanie MQOPEN kończy się niepowodzeniem z komunikatem `MQRC_NOT_AUTHORIZED` , wraz z:

- W systemie z/OSnastępujące komunikaty widoczne na konsoli, które przedstawiają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables/Potatoes"
```

Na co zwrócić uwagę:

- Komunikaty, które są odbierane w systemie z/OS , są identyczne z komunikatami otrzymywanych w poprzednim zadaniu, ponieważ te same obiekty tematów i profile kontrolują dostęp.
- Komunikat o zdarzeniu otrzymany na innych platformach jest podobny do otrzymanego w poprzednim zadaniu, ale rzeczywisty łańcuch tematu jest inny.

Przyznaj dostęp do publikowania i subskrybowania

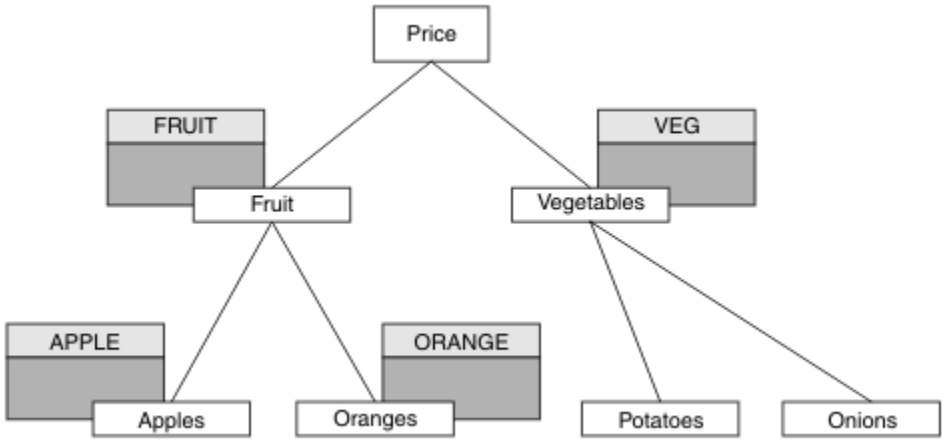
Ten temat jest ostatnim z listy zadań, które informują użytkownika o sposobach nadawania dostępu do publikowania i subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Przyznaj użytkownikowi dostęp do tematu w celu głębszego publikowania tematu w drzewie” na stronie 274.

O tym zadaniu

W poprzednim zadaniu USER1 został nadany dostęp do subskrypcji tematu `"Price/Fruit"`. W tym temacie opisano sposób nadawania dostępu do tego użytkownika w celu publikowania w tym temacie.



Rysunek 33. Nadawanie dostępu do publikowania i subskrybowania

Tabela 24. Przykładowe wymagania dostępu do publikowania i subskrybowania			
Temat	**Wymagany dostęp do subskrypcji**	**Wymagany jest dostęp do publikowania**	**Obiekt tematu**
Cena	Brak użytkownika	Brak użytkownika	Brak
Cena/Owoce	USER1	USER1	fruit
Cena/ Owoce/ Jabłka	USER1 i USER2		Apple
Cena/ Owoce/ Pomarańcze	USER1		Pomarańczowy

Procedura

Nadaj dostęp w następujący sposób:

- Inne platformy:

  Nadaj dostęp do produktu USER1 , aby opublikować go w temacie `"Price/Fruit"` , nadając użytkownikowi publikowanie dostępu do profilu produktu FRUIT . W tym celu za pomocą komendy autoryzacji dla platformy:

  Windows UNIX Linux **Systemy Windows, UNIX and Linux**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

Wyniki

W systemie z/OS, gdy program USER1 próbuje publikować w temacie `"Price/Fruit"` , sprawdzenie zabezpieczeń w wywołaniu MQOPEN.

Gdy program USER2 podejmuje próbę opublikowania w temacie `"Price/Fruit"` , wynikiem jest niepowodzenie w przypadku komunikatu `MQRC_NOT_AUTHORIZED` , wraz z:

- Windows UNIX Linux Na platformach Windows, UNIX i Linux następujące zdarzenie autoryzacji:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

Po wykonaniu kompletnego zestawu tych zadań, USER1 i USER2 następujące uprawnienia dostępu do publikowania i subskrybowania tematów są następujące:

Tabela 25. Pełna lista uprawnień dostępu wynikający z przykładów bezpieczeństwa

Temat	Wymagany dostęp do subskrypcji	Wymagany jest dostęp do publikowania	Obiekt tematu
Cena	Brak użytkownika	Brak użytkownika	Brak
Cena/Owoce	USER1	USER1	fruit
Cena/ Owoce/ Jabłka	USER1 i USER2		Apple
Cena/ Owoce/ Pomarańcze	USER1		Pomarańczowy
Cena/ Warzywa		USER1	VEG
Cena/ Warzywa/ Ziemniaki			
Cena/ warzywa/ Cebula			

Jeśli użytkownik ma inne wymagania dotyczące dostępu do zabezpieczeń na różnych poziomach w drzewie tematów, dokładne planowanie zapewnia, że nie zostaną wyświetlone żadne dodatkowe ostrzeżenia dotyczące zabezpieczeń w dzienniku konsoli z/OS . Konfigurowanie zabezpieczeń na odpowiednim poziomie w drzewie pozwala uniknąć mylących komunikatów zabezpieczeń.

Zabezpieczenia subskrypcji

MQSO_ALTERNATE_USER_AUTHORITY

Pole Identyfikator AlternateUser(Identyfikator użytkownika) zawiera identyfikator użytkownika, który ma być używany do sprawdzania poprawności wywołania MQSUB. Wywołanie może zakończyć się powodzeniem tylko wtedy, gdy ten identyfikator użytkownika AlternateUserjest uprawniony do subskrybowania tematu z określonymi opcjami dostępu, niezależnie od tego, czy identyfikator użytkownika, pod którym aplikacja jest uruchomiona, ma do tego uprawnienia.

MQSO_SET_IDENTITY_CONTEXT

Subskrypcja polega na użyciu znacznika rozliczeniowego i danych tożsamości aplikacji dostarczonych w polach PubAccountingToken (Token) i PubApplIdentityData (Dane tożsamości).

Jeśli ta opcja jest określona, to ta sama kontrola autoryzacji jest przeprowadzana tak, jakby kolejka docelowa była dostępna za pomocą wywołania MQOPEN z opcją MQOO_SET_IDENTITY_CONTEXT, z wyjątkiem sytuacji, w której używana jest również opcja MQSO_MANAGED, w której to przypadku nie ma uprawnień do sprawdzania autoryzacji w kolejce docelowej.

Jeśli ta opcja nie zostanie podana, publikacje wysłane do tego subskrybenta mają domyślnie powiązane z nimi informacje o kontekście:

Tabela 26. Domyślne informacje o kontekście publikowania	
Pole w strukturze MQMD	**Użyta wartość**
UserIdentifier	Identyfikator użytkownika powiązany z subskrypcją (patrz pole SUBUSER na ekranie DISPLAY SBSTATUS) w momencie tworzenia publikacji.
AccountingToken	Określana na podstawie środowiska, jeśli jest to możliwe; w przeciwnym razie należy ustawić wartość MQACT_NONE.
Dane_tożsamości_aplikacji	Ustaw wartość pustą.

Ta opcja jest poprawna tylko z opcją MQSO_CREATE i MQSO_ALTER. W przypadku użycia z opcją MQSO_RESUME, pola PubAccountingToken i PubApplIdentityData są ignorowane, więc ta opcja nie ma żadnego efektu.

Jeśli subskrypcja została zmieniona bez użycia tej opcji, w której wcześniej subskrypcja dostarczyła informacje o kontekście tożsamości, dla zmienionej subskrypcji generowane są domyślne informacje o kontekście.

Jeśli subskrypcja zezwalająca na użycie różnych identyfikatorów użytkowników przy użyciu opcji MQSO_ANY_USERID jest wznawiana przez inny identyfikator użytkownika, domyślny kontekst tożsamości jest generowany dla nowego identyfikatora użytkownika będącego właścicielem subskrypcji, a wszystkie kolejne publikacje są dostarczane z nowym kontekstem tożsamości.

Identyfikator AlternateSecurity

Jest to identyfikator zabezpieczeń, który jest przekazywany z identyfikatorem AlternateUserdo usługi autoryzacji w celu umożliwienia przeprowadzenia odpowiednich sprawdzeń autoryzacji. AlternateSecurityId jest używany tylko wtedy, gdy określono wartość MQSO_ALTERNATE_USER_AUTHORITY, a pole AlternateUserID nie jest całkowicie puste w stosunku do pierwszego znaku o kodzie zero lub do końca pola.

MQSO_ANY_USERID, opcja subskrypcji

Jeśli określono atrybut MQSO_ANY_USERID, tożsamość subskrybenta nie jest ograniczona do pojedynczego identyfikatora użytkownika. Dzięki temu każdy użytkownik może zmienić lub wznowić subskrypcję, gdy mają odpowiednie uprawnienia. Abonament może mieć tylko jeden użytkownik w dowolnym momencie. Próba wznowienia użycia subskrypcji, która jest obecnie używana przez inną aplikację, spowoduje, że wywołanie nie powiedzie się i zostanie wykonana operacja MQRC_SUBSCRIPTION_IN_USE.

Aby dodać tę opcję do istniejącej subskrypcji, wywołanie MQSUB (za pomocą komendy MQSO_ALTER) musi pochodzić z tego samego identyfikatora użytkownika, co oryginalna subskrypcja.

Jeśli wywołanie MQSUB odwołuje się do istniejącej subskrypcji z ustawioną nazwą MQSO_ANY_USERID, a identyfikator użytkownika różni się od oryginalnej subskrypcji, wywołanie powiedzie się tylko wtedy, gdy nowy identyfikator użytkownika ma uprawnienia do subskrybowania tematu. Po pomyślnym zakończeniu, przyszłe publikacje tego subskrybenta są umieszczane w kolejce subskrybenta przy użyciu nowego identyfikatora użytkownika ustawionego w publikacji.

MQSO_FIXED_USERID

Jeśli określono parametr MQSO_FIXED_USERID, subskrypcja może zostać zmieniona lub wznowiona tylko za pomocą jednego identyfikatora użytkownika będącego właścicielem. Ten identyfikator użytkownika jest ostatnim identyfikatorem użytkownika, który zmienił subskrypcję, który ustawił tę opcję, usuwając w ten sposób opcję MQSO_ANY_USERID lub jeśli nie ma żadnych zmian, jest to identyfikator użytkownika, który utworzył subskrypcję.

Jeśli komenda MQSUB odwołuje się do istniejącej subskrypcji z ustawioną opcją MQSO_ANY_USERID i zmienia subskrypcję (za pomocą komendy MQSO_ALTER) w celu użycia opcji MQSO_FIXED_USERID, to identyfikator użytkownika subskrypcji jest teraz stały przy użyciu tego nowego identyfikatora użytkownika. Wywołanie powiedzie się tylko wtedy, gdy nowy identyfikator użytkownika ma uprawnienia do subskrybowania tematu.

Jeśli identyfikator użytkownika inny niż ten, który został zarejestrowany jako posiadający subskrypcje, w celu wznowienia lub zmiany subskrypcji MQSO_FIXED_USERID, wywołanie nie powiedzie się i zostanie on zakończony niepowodzeniem z opcją MQRC_IDENTITY_MISMATCH. Identyfikator użytkownika będącego właścicielem subskrypcji można wyświetlić za pomocą komendy DISPLAY SBSTATUS.

Jeśli nie zostanie podany żaden identyfikator MQSO_ANY_USERID lub MQSO_FIXED_USERID, wartością domyślną jest MQSO_FIXED_USERID.

IBM WebSphere MQ Advanced Message Security

Produkt IBM WebSphere MQ Advanced Message Security (AMS) jest oddzielnie licencjonowanym komponentem produktu IBM WebSphere MQ Advanced Message Security , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM WebSphere MQ Advanced Message Security , a jednocześnie nie ma wpływu na aplikacje końcowe.

IBM WebSphere MQ Advanced Message SecurityPrzegląd

Aplikacje produktu IBM WebSphere MQ mogą używać produktu IBM WebSphere MQ Advanced Message Security do wysyłania poufnych danych, takich jak transakcje finansowe o wysokiej wartości i dane osobowe, z różnymi poziomami ochrony przy użyciu modelu szyfrowania z kluczem publicznym.

Odsyłacze pokrewne

Kody powrotu pakietu GSKit używane w komunikatach IBM WebSphere MQ AMS

Zachowanie, które zostało zmienione między wersją 7.0.1 i wersją 7.5 .

Ponieważ produkt IBM Advanced Message Security stał się komponentem w produkcie WebSphere MQ 7.5, niektóre aspekty funkcji produktu IBM WebSphere MQ AMS uległy zmianie, co może mieć wpływ na istniejące aplikacje, skrypty administracyjne lub procedury zarządzania.

Przed zaktualizowaniem menedżerów kolejek do wersji 7.5należy uważnie zapoznać się z poniższą listą zmian. Przed rozpoczęciem migracji systemów do wersji IBM WebSphere MQ 7.5: należy zdecydować, czy konieczne jest zaplanowanie zmian w istniejących aplikacjach, skryptach i procedurach.

- Instalacja produktu IBM WebSphere MQ AMS jest częścią procesu instalacji produktu WebSphere MQ .
- Funkcje zabezpieczeń produktu IBM WebSphere MQ AMS są włączane wraz z jego instalacją i są kontrolowane za pomocą strategii bezpieczeństwa. Nie ma potrzeby włączania przechwytywaczy w celu umożliwienia przechwycenia danych przez program IBM WebSphere MQ AMS .
- Produkt IBM WebSphere MQ AMS w wersji WebSphere MQ 7.5 nie wymaga użycia komendy **cfgmqs** , jak w autonomicznej wersji produktu IBM WebSphere MQ AMS.

Funkcje i funkcje produktu IBM WebSphere MQ Advanced Message Security

Produkt Advanced Message Security rozszerza usługi zabezpieczeń WebSphere MQ , aby zapewnić podpisywanie i szyfrowanie danych na poziomie komunikatu. Rozszerzone usługi gwarantują, że dane komunikatu nie zostały zmodyfikowane, gdy jest pierwotnie umieszczone w kolejce i po jego pobraniu. Ponadto program IBM WebSphere MQ AMS sprawdza, czy nadawca danych komunikatu ma uprawnienia do umieszczania podpisanych komunikatów w kolejce docelowej.

Poniżej znajduje się pełna lista funkcji programu IBM WebSphere MQ AMS :

- Zabezpieczy transakcje wrażliwe lub o wysokiej wartości przetworzone przez produkt WebSphere MQ.
- Wykrywa i usuwa nieuczciwe lub nieautoryzowane komunikaty, zanim zostaną przetworzone przez aplikację odbierającą.
- Sprawdza, czy komunikaty nie zostały zmodyfikowane podczas przesyłania z kolejki do kolejki.

- Chroni dane nie tylko w czasie, gdy przepływa przez sieć, ale także wtedy, gdy jest umieszczana w kolejce.
- Zabezpieczy istniejące aplikacje napisane przez klienta i aplikacje napisane przez klienta dla produktu WebSphere MQ.

Obsługa błędów

Produkt Advanced Message Security definiuje kolejkę obsługi błędów w celu zarządzania komunikatami, które zawierają błędy lub komunikaty, które nie mogą być niechronione.

Wadliwe komunikaty są traktowane jako wyjątkowe przypadki. Jeśli odebrany komunikat nie spełnia wymagań bezpieczeństwa dla kolejki, na której znajduje się komunikat, na przykład jeśli komunikat jest podpisany w momencie, gdy powinien być zaszyfrowany, deszyfrowanie lub weryfikacja podpisu nie powiedzie się, komunikat jest wysyłany do kolejki obsługi błędów. Komunikat może zostać wysłany do kolejki obsługi błędów z następujących powodów:

- Niezgodność jakości ochrony-istnieje niezgodność jakości ochrony (QOP) między odebranym komunikatem a definicją QOP w strategii bezpieczeństwa.
- Błąd deszyfrowania-komunikat nie może być deszyfrowany.
- Błąd nagłówka PDMQ-nie można uzyskać dostępu do nagłówka komunikatu AMS produktu WebSphere MQ .
- Niezgodność wielkości-długość komunikatu po deszyfrowaniu jest inna niż oczekiwano.
- Niezgodność siły algorytmu szyfrowania-algorytm szyfrowania komunikatów jest słabszy od wymaganego.
- Wystąpił nieznany błąd-wystąpił nieoczekiwany błąd.

Produkt WebSphere MQ AMS korzysta z systemu SYSTEM.PROTECTION.ERROR.QUEUE jako swoją kolejkę obsługi błędów. Wszystkie komunikaty wprowadzone przez produkt IBM WebSphere MQ AMS do systemu SYSTEM.PROTECTION.ERROR.QUEUE są poprzedzone nagłówkiem MQDLH.

Administrator produktu WebSphere MQ może również zdefiniować SYSTEM.PROTECTION.ERROR.QUEUE jako kolejka aliasowa wskazującą inną kolejkę.

Najważniejsze pojęcia

Sekcja zawiera informacje na temat kluczowych pojęć w produkcie Advanced Message Security , które umożliwiają zrozumienie, w jaki sposób narzędzie działa i jak skutecznie je zarządzać.

infrastruktura klucza publicznego

Infrastruktura klucza publicznego (PKI) to system udogodnień, strategii i usług, które wspierają korzystanie z kryptografii klucza publicznego w celu uzyskania bezpiecznej komunikacji.

Nie istnieje żaden standard, który definiuje komponenty infrastruktury klucza publicznego, ale PKI zwykle wiąże się z wykorzystaniem certyfikatów klucza publicznego i składa się z ośrodków certyfikacji (CA) i innych organów rejestracyjnych (RA), które świadczyją następujące usługi:

- Wydawanie certyfikatów cyfrowych
- Sprawdzanie poprawności certyfikatów cyfrowych
- Unieważnianie certyfikatów cyfrowych
- Dystrybucja certyfikatów

Tożsamość użytkowników i aplikacji jest reprezentowana przez pole **nazwa wyróżniająca (DN)** w certyfikacie powiązanym z podpisanymi lub zaszyfrowanymi komunikatami. Produkt Advanced Message Security używa tej tożsamości do reprezentowania użytkownika lub aplikacji. Aby uwierzytelnić tę tożsamość, użytkownik lub aplikacja musi mieć dostęp do magazynu kluczy, w którym zapisany jest certyfikat i powiązany klucz prywatny. Każdy certyfikat jest reprezentowany przez etykietę w magazynie kluczy.

Pojęcia pokrewne

“Korzystanie z magazynów kluczy i certyfikatów” na stronie 305
Aby zapewnić przezroczystą ochronę szyfrującą dla aplikacji WebSphere MQ , program Advanced Message Security używa pliku kluczy, w którym przechowywane są certyfikaty klucza publicznego i klucz prywatny.

certyfikaty cyfrowe

Produkt Advanced Message Security wiąże użytkowników i aplikacje ze standardowymi certyfikatami cyfrowymi X.509 . Certyfikaty X.509 są zwykle podpisywane przez zaufany ośrodek certyfikacji (CA) i obejmują klucze prywatne i publiczne, które są używane do szyfrowania i deszyfrowania.

Certyfikaty cyfrowe zapewniają ochronę przed imitowaniem przez powiązanie klucza publicznego z jego właścicielem, niezależnie od tego, czy właścicielem jest osoba, menedżer kolejek lub inna jednostka. Certyfikaty cyfrowe są również nazywane certyfikatami klucza publicznego, ponieważ dają pewność co do prawa własności klucza publicznego w przypadku korzystania z asymetrycznego schematu klucza. Ten schemat wymaga, aby dla aplikacji został wygenerowany klucz publiczny i klucz prywatny. Dane zaszyfrowane za pomocą klucza publicznego mogą być deszyfrowane tylko za pomocą odpowiedniego klucza prywatnego, podczas gdy dane zaszyfrowane za pomocą klucza prywatnego mogą być deszyfrowane tylko za pomocą odpowiedniego klucza publicznego. Klucz prywatny jest przechowywany w pliku bazy danych kluczy, który jest chroniony hasłem. Tylko jego właściciel ma dostęp do klucza prywatnego używanego do deszyfrowania komunikatów, które są szyfrowane przy użyciu odpowiadającego mu klucza publicznego.

Jeśli klucze publiczne są wysyłane bezpośrednio przez ich właściciela do innego obiektu, istnieje ryzyko, że komunikat może zostać przechwycony, a klucz publiczny podstawiony przez inny. Jest to tzw. atak typu "man-in-the-middle". Rozwiązaniem jest wymiana kluczy publicznych za pośrednictwem zaufanej osoby trzeciej, dające użytkownikowi silne zapewnienie, że klucz publiczny należy do jednostki, z którą się komunikują. Zamiast wysyłać bezpośrednio swój klucz publiczny, należy poprosić zaufaną osobę trzecią o włączenie jej do certyfikatu cyfrowego. Zaufana osoba trzecia, która wydaje certyfikaty cyfrowe, jest nazywana uprawnieniem do certyfikatu (CA).

Więcej informacji na temat certyfikatów cyfrowych zawiera sekcja Co znajduje się w certyfikacie cyfrowym.

Certyfikat cyfrowy zawiera klucz publiczny dla jednostki i określa, że klucz publiczny należy do tego obiektu:

- Jeśli certyfikat jest dla pojedynczego obiektu, jest on nazywany *certyfikatem osobistym* lub *certyfikatem użytkownika*.
- Jeśli certyfikat jest dla ośrodka certyfikacji, certyfikat jest nazywany *certyfikatem ośrodka CA* lub *certyfikatem osoby podpisującej*.

Uwaga: Produkt Advanced Message Security obsługuje samopodpisane certyfikaty zarówno w aplikacjach Java, jak i rodzimych.

Pojęcia pokrewne

“Kryptografia” na stronie 7
Kryptografia to proces przekształcania tekstu w formie czytelnej, o nazwie *plaintext*i postaci nieczytelnej, o nazwie *ciphertext*.

Menedżer uprawnień do obiektów

Menedżer uprawnień do obiektu (Object Authority Manager-OAM) jest komponentem usługi autoryzacji dostarczonym z produktami WebSphere MQ .

Dostęp do obiektów Advanced Message Security jest kontrolowany za pomocą grup użytkowników WebSphere MQ i OAM. Administratorzy mogą używać interfejsu wiersza komend do nadawania lub odbierania autoryzacji zgodnie z wymaganiami. Różne grupy użytkowników mogą mieć różne rodzaje uprawnień dostępu do tych samych obiektów. Na przykład jedna grupa może wykonać operacje PUT i GET dla określonej kolejki, podczas gdy inna grupa może być dozwolona tylko w celu przeglądania kolejki. Podobnie niektóre grupy mogą mieć uprawnienie GET i PUT do kolejki, ale nie mogą zmieniać ani usuwać kolejki.

Za pośrednictwem OAM można sterować:

- Dostęp do obiektów produktu Advanced Message Security za pomocą interfejsu MQI. Gdy program użytkowy próbuje uzyskać dostęp do obiektów, OAM sprawdza, czy profil użytkownika, który zażądał żądania, ma uprawnienia do żądanej operacji. Oznacza to, że kolejki, a także komunikaty w kolejkach, mogą być chronione przed dostępem bez uprawnień.
- Uprawnienie do używania komend PCF i MQSC.

Pojęcia pokrewne
Menedżer uprawnień do obiektów

Obsługiwana technologia

Produkt Advanced Message Security zależy od kilku komponentów technologii w celu udostępnienia infrastruktury zabezpieczeń.

Produkt Advanced Message Security obsługuje następujące aplikacyjne interfejsy programistyczne (API) produktu WebSphere MQ :

- Message Queue Interface (MQI)
- WebSphere MQ Java Message Service (JMS) 1.0.2 i 1.1.
- Klasy podstawowe produktu WebSphere MQ dla języka Java
- Klasy WebSphere MQ dla. Net w trybie niezarządzanym

Uwaga: Produkt Advanced Message Security obsługuje uprawnienia do certyfikatów zgodnych ze standardem X.509 .

Znane ograniczenia

Informacje na temat ograniczeń produktu IBM WebSphere MQ Advanced Message Security.

- Następujące opcje IBM WebSphere MQ nie są obsługiwane:
  - Publikowanie/subskrypcja.
  - Konwersja danych kanału.
  - Listy dystrybucyjne.
  - Segmentacja komunikatów aplikacji
  - Korzystanie z aplikacji niewielowątkowych przy użyciu wyjścia funkcji API na platformach HP-UX .
  - Klasy produktu IBM WebSphere MQ dla środowiska .NET w trybie zarządzanym (połączenia klienta lub powiązań).
  - Aplikacje klienta Message Service Client for .NET (XMS).
  - Klient usługi Message Service dla aplikacji C/C++ (XMS supportPac IA94).
- Wszystkie aplikacje produktu Java są zależne od środowiska wykonawczego IBM Java .

  Produkt IBM WebSphere MQ Advanced Message Security nie obsługuje środowiska JRE udostępnianego przez innych dostawców.
- Aplikacje klienckie JMS i Java przy użyciu produktu IBM WebSphere MQ Advanced Message Security w trybie klienta.

  Dowolna aplikacja JMS lub aplikacja kliencka Java(w tym agenty IBM WebSphere MQ Explorer i IBM WebSphere MQ Managed File Transfer) nie mogą używać produktu IBM WebSphere MQ Advanced Message Security w trybie klienta z menedżerem kolejek produktu WebSphere MQ w wersji wcześniejszej niż Version 7.5.

  Aby można było używać strategii ochrony komunikatów, aplikacje te muszą wchodzić w interakcje z menedżerem kolejek produktu IBM WebSphere MQ Version 7.5 lub łączyć się w trybie powiązań lokalnych z menedżerem kolejek na tym samym komputerze, co aplikacja.

- Należy unikać umieszczania dwóch lub większej liczby certyfikatów z tymi samymi nazwami wyróżniającymi, w jednym pliku kluczy, ponieważ działanie intereceptora produktu IBM WebSphere MQ Advanced Message Security z takimi certyfikatami nie jest zdefiniowane.
- Adapter zasobów IBM WebSphere MQ Version 7.5 nie obsługuje produktu IBM WebSphere MQ Advanced Message Security. Jeśli wymagane jest użycie ochrony komunikatów przy użyciu aplikacji IBM WebSphere MQ classes for JMS lub IBM WebSphere MQ classes for Java działających w środowisku serwera aplikacji, wykonaj następujące czynności:
  - Serwer aplikacji musi być skonfigurowany do korzystania z adaptera zasobów produktu Version 8.0 lub nowszego.
  - Należy użyć przechwytywacza agenta kanału komunikatów (MCA).

Scenariusze użytkownika

Zapoznaj się z możliwami scenariuszami, aby zrozumieć, jakie cele biznesowe można osiągnąć za pomocą programu Advanced Message Security.

Podręcznik Szybki start dla platform Windows

Ten podręcznik służy do szybkiego konfigurowania programu IBM Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów na platformach Windows . Po zakończeniu tego zadania utworzona zostanie kluczowa baza danych w celu weryfikacji tożsamości użytkowników oraz zdefiniowanych strategii podpisywania i szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

W systemie powinny być zainstalowane co najmniej następujące składniki:

- Serwer
- Development Toolkit (dla programów przykładowych)
- Advanced Message Security

Szczegółowe informacje na ten temat można znaleźć w sekcji Składniki produktuIBM WebSphere MQ dla systemów Windows .

Informacje na temat używania komendy **setmqenv** do inicjowania bieżącego środowiska, tak aby odpowiednie komendy WebSphere MQ mogły być zlokalizowane i wykonywane przez system operacyjny, można znaleźć w sekcji setmqenv.

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach używana jest kolejka o nazwie TEST.Q , która służy do przekazywania komunikatów między aplikacjami. Advanced Message Security korzysta z przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym wchodzą one do infrastruktury WebSphere MQ za pośrednictwem standardowego interfejsu WebSphere MQ . Podstawowa konfiguracja jest wykonywana w produkcie WebSphere MQ i jest skonfigurowana w poniższych krokach.

Za pomocą programu WebSphere MQ Explorer można utworzyć menedżer kolejek QM_VERIFY_AMS i jego kolejkę lokalną o nazwie TEST.Q przy użyciu wszystkich domyślnych ustawień kreatora. Można również użyć komend znalezionych w programie \WebSphere MQ\bin. Należy pamiętać, że użytkownik musi być członkiem grupy użytkowników produktu mqm , aby uruchomić następujące komendy administracyjne.

Procedura

1. Tworzenie menedżera kolejek

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Uruchamianie menedżera kolejek

```
strmqm QM_VERIFY_AMS
```

3. Utwórz kolejkę o nazwie TEST.Q , wprowadzając następującą komendę w programie **runmqsc** dla menedżera kolejek QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Wyniki

Jeśli procedura została zakończona, komenda wprowadzona do programu **runmqsc** wyświetli szczegółowe informacje o produkcie TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym przykładzie pojawiają się dwaj użytkownicy: alice, nadawca i bob, odbiorca. Aby móc korzystać z kolejki aplikacji, użytkownicy ci muszą mieć uprawnienia do korzystania z niej. Ponadto, aby pomyślnie korzystać ze strategii ochrony, które zdefiniujemy tych użytkowników, należy nadać im dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** można znaleźć w sekcji **setmqaut** .

Procedura

1. Utwórz dwóch użytkowników i upewnij się, że dla obu tych użytkowników ustawione są wartości HOMEPATH i HOMEDRIVE .
2. Autoryzowanie użytkowników do łączenia się z menedżerem kolejek i do pracy z kolejką

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

3. Należy także zezwolić dwóm użytkownikom na przeglądanie kolejki strategii systemowej i umieszczanie komunikatów w kolejce błędów.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```

Wyniki

Użytkownicy są teraz utworzani i nadane im wymagane uprawnienia.

Co dalej

Aby sprawdzić, czy kroki zostały wykonane poprawnie, należy użyć przykładów amqsput i amqsget zgodnie z opisem w sekcji “7. Testowanie konfiguracji” na stronie 287.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Przechwytywacz wymaga klucza publicznego wysyłającego użytkowników w celu zaszyfrowania komunikatu. W związku z tym należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W systemie rzeczywistym, w którym użytkownicy i aplikacje są rozpraszani na kilku komputerach, każdy użytkownik ma własny prywatny magazyn kluczy. Podobnie w niniejszym podręczniku tworzone są kluczowe bazy danych dla produktów alice i bob , a także certyfikaty użytkowników między nimi.

Uwaga: W tym podręczniku używamy przykładowych aplikacji napisanych w języku C łączących się z powiązaniami lokalnymi. Jeśli planowane jest korzystanie z aplikacji Java za pomocą powiązań klienta,

należy utworzyć magazyn kluczy JKS i certyfikaty za pomocą komendy **keytool** , która jest częścią środowiska JRE (więcej informacji zawiera sekcja “Podręcznik Szybki start dla klientów Java” na stronie 294). W przypadku wszystkich pozostałych języków, a także w przypadku aplikacji Java korzystających z powiązań lokalnych, kroki zawarte w tym podręczniku są poprawne.

Procedura

1. Za pomocą interfejsu GUI programu IBM Key Management (`strmqikm.exe`) utwórz nową bazę danych kluczy dla użytkownika `alice`.

   ```
   Type:       CMS
   Filename:   alicekey.kdb
   Location:   C:/Documents and Settings/alice/AMS
   ```

   Uwaga:

   - Zaleca się użycie silnego hasła, aby zabezpieczyć bazę danych.
   - Upewnij się, że pole wyboru **Stash password to a file** (Stash hasło do pliku) jest zaznaczone.
2. Zmień widok treści bazy danych kluczy na **Personal Certificates**(Certyfikaty osobiste).
3. Wybierz opcję **Nowy samopodpisany**; w tym scenariuszu używane są samopodpisane certyfikaty.
4. Utwórz certyfikat identyfikujący użytkownika `alice` , który będzie używany do szyfrowania, używając następujących pól:

   ```
   Key label: Alice_Cert
   Common Name: alice
   Organisation: IBM
   Country: GB
   ```

   Uwaga:

   - Do celów niniejszego przewodnika korzystamy z samopodpisanego certyfikatu, który można utworzyć bez korzystania z ośrodka certyfikacji. W przypadku systemów produkcyjnych zaleca się, aby nie używać certyfikatów samopodpisanych, ale zamiast tego opierać się na certyfikatach podpisanych przez ośrodek certyfikacji.
   - Parametr **Key label** określa nazwę certyfikatu, który przechwytywacz będzie poszukiwać w celu otrzymania niezbędnych informacji.
   - Parametry **Common Name** i opcjonalne określają szczegóły dotyczące **nazwy wyróżniającej** (DN), która musi być unikalna dla każdego użytkownika.
5. Powtórz krok 1-4 dla użytkownika bob

Wyniki

Dla dwóch użytkowników `alice` i bob każdy z nich ma certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Przechwytywacze produktu Advanced Message Security należy wskazać w katalogu, w którym znajdują się located.This jest to wykonywane za pomocą pliku `keystore.conf` , który przechowuje te informacje w postaci zwykłego tekstu. Każdy użytkownik musi mieć oddzielny plik `keystore.conf` . Ten krok musi być wykonany zarówno dla produktów `alice` , jak i bob.

Treść produktu `keystore.conf` musi mieć postać:

```
cms.keystore = <dir>/keystore_file
cms.certificate = certificate_label
```

Przykład

W tym scenariuszu zawartość pliku `keystore.conf` będzie następująca:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

Uwaga:

- Ścieżka do pliku kluczy musi być podana bez rozszerzenia nazwy pliku.
- Etykieta certyfikatu może zawierać spacje, a więc "Alice_Cert" i "Alice_Cert" na przykład, są rozpoznawane jako etykiety dwóch różnych certyfikatów. Aby jednak uniknąć nieporozumień, lepiej nie używać spacji w nazwie etykiety.
- Dostępne są następujące formaty magazynu kluczy: CMS (Cryptographic Message Syntax), JKS (Java Keystore) i JCEKS (Java Cryptographic Extension Keystore). Więcej informacji zawiera sekcja “Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf)” na stronie 305.
- *%HOMEDRIVE%\%HOMEPATH%*`\.mqs\keystore.conf` (np. C:\Documents and Settings\alice\.mqs\keystore.conf) to domyślne położenie, w którym program Advanced Message Security wyszukuje plik `keystore.conf` . Więcej informacji na temat korzystania z położenia innego niż domyślne dla `keystore.conf`zawiera sekcja “Korzystanie z magazynów kluczy i certyfikatów” na stronie 305.
- Aby utworzyć katalog `.mqs` , należy użyć wiersza komend.

5. Współużytkowanie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwoma kluczowymi bazami danych, aby każdy użytkownik mógł pomyślnie zidentyfikować inne bazy danych. Jest to wykonywane przez wyodrębnienie certyfikatu publicznego każdego użytkownika do pliku, który następnie jest dodawany do bazy danych kluczy innego użytkownika.

Uwaga: Należy uważać, aby użyć opcji *extract* , a nie opcji *export* . Opcja *Wyodrębnij* pobiera klucz publiczny użytkownika, natomiast *eksport* pobiera zarówno klucz publiczny, jak i prywatny. Użycie komendy *export* przez pomyłkę spowodowałoby całkowite skompromitowanie aplikacji, przechodząc do klucza prywatnego.

Procedura

1. Wyodrębnij certyfikat identyfikujący `alice` do pliku zewnętrznego:

   ```
   runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
   -label Alice_Cert -target alice_public.arm
   ```

2. Dodaj certyfikat do magazynu kluczy `bob's` :

   ```
   runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
   Alice_Cert -file alice_public.arm
   ```

3. Powtórz kroki dla bob:

   ```
   runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/bobkey.kdb" -pw passw0rd
   -label Bob_Cert -target bob_public.arm

   runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/alicekey.kdb" -pw passw0rd -label
   Bob_Cert -file bob_public.arm
   ```

Wyniki

Dwaj użytkownicy `alice` i bob są teraz w stanie pomyślnie zidentyfikować siebie nawzajem po utworzeniu i współużytkowanych samopodpisanych certyfikatach.

Co dalej

Upewnij się, że certyfikat znajduje się w magazynie kluczy, przeglądając go za pomocą interfejsu GUI lub uruchamiając następujące komendy, które wypisują jego szczegóły:

```
runmqakm -cert -details -db "C:/Documents and Settings/bob/AMS/bobkey.kdb"
-pw passw0rd -label Alice_Cert
```

```
runmqakm -cert -details -db "C:/Documents and Settings/alice/AMS/alicekey.kdb"
-pw passw0rd -label Bob_Cert
```

6. Definiowanie strategii kolejki

O tym zadaniu

Za pomocą utworzonego menedżera kolejek i przechwytywaczy przygotowanych do przechwytywania komunikatów i uzyskiwania dostępu do kluczy szyfrowania, można rozpocząć definiowanie strategii ochrony w systemie QM_VERIFY_AMS za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy można znaleźć w sekcji setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Jest to przykład strategii zdefiniowanej dla kolejki produktu `TEST.Q` . W tym przykładzie komunikaty są podpisywane z algorytmem SHA1 i szyfrowane za pomocą algorytmu AES256 . `alice` jest jedynym poprawnym nadawcą, a bob jest jedynym odbiorcą komunikatów w tej kolejce:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Uwaga: Nazwy wyróżniające są zgodne z tymi, które zostały określone w certyfikacie odpowiedniego użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wydaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend produktu `setmqspl` , należy użyć opcji `-export` . Umożliwia to przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testowanie konfiguracji

O tym zadaniu

Uruchamiając różne programy pod różnymi użytkownikami, można sprawdzić, czy aplikacja została poprawnie skonfigurowana.

Procedura

1. Przełącz użytkownika do uruchomienia jako użytkownik `alice`

   Kliknij prawym przyciskiem myszy `cmd.exe` i wybierz opcję **Uruchom jako ...**. Po wyświetleniu zapytania zaloguj się jako użytkownik `alice`.
2. Jako że użytkownik `alice` umieł umieścić komunikat przy użyciu przykładowej aplikacji:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. Wpisz tekst komunikatu, a następnie naciśnij klawisz Enter.
4. Przełącz użytkownika do uruchomienia jako użytkownik bob

Otwórz inne okno, klikając prawym przyciskiem myszy `cmd.exe` i wybierając opcję **Uruchom jako ...**. Po wyświetleniu zapytania zaloguj się jako użytkownik bob.

5. Jako użytkownik Bob uzyskaj komunikat przy użyciu przykładowej aplikacji:

```
amqsget TEST.Q QM_VERIFY_AMS
```

Wyniki

Jeśli aplikacja została poprawnie skonfigurowana dla obu użytkowników, komunikat `alice`użytkownika jest wyświetlany, gdy program bob uruchamia aplikację pobierający.

8. Testowanie szyfrowania

O tym zadaniu

Aby sprawdzić, czy szyfrowanie jest wykonywane zgodnie z oczekiwaniami, należy utworzyć kolejkę aliasową, która odwołuje się do oryginalnej kolejki `TEST.Q`. Ta kolejka aliasowa nie będzie miała strategii bezpieczeństwa, więc żaden użytkownik nie będzie miał informacji do zdeszyfrowania wiadomości i dlatego zostaną wyświetlone zaszyfrowane dane.

Procedura

1. Za pomocą komendy **`runmqsc`** w odniesieniu do menedżera kolejek QM_VERIFY_AMS utwórz kolejkę aliasową.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Przyznaj dostęp bob do przeglądania z kolejki aliasowej

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako użytkownik `alice`umieść inny komunikat przy użyciu przykładowej aplikacji, tak jak wcześniej:

```
amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako użytkownik bobprzeglądaj komunikat przy użyciu przykładowej aplikacji za pomocą kolejki aliasowej:

```
amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako użytkownik bob, pobierz komunikat przy użyciu przykładowej aplikacji z kolejki lokalnej:

```
amqsget TEST.Q QM_VERIFY_AMS
```

Wyniki

Dane wyjściowe z aplikacji `amqsbcg` przedstawiają zaszyfrowane dane, które znajdują się w kolejce, udowadniając, że komunikat został zaszyfrowany.

Podręcznik Szybki start dla platform UNIX

Ten podręcznik służy do szybkiego konfigurowania produktu IBM Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów na platformach UNIX . Po zakończeniu tego zadania utworzona zostanie kluczowa baza danych w celu weryfikacji tożsamości użytkowników oraz zdefiniowanych strategii podpisywania i szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

W systemie powinny być zainstalowane co najmniej następujące komponenty:

- Środowisko wykonawcze
- Serwer

- programy przykładowe
- Pakiet IBM Global Security Kit
- MQ Advanced Message Security

Nazwy komponentów na poszczególnych platformach można znaleźć w następujących tematach:

- KomponentyIBM WebSphere MQ dla systemów Linux
- KomponentyIBM WebSphere MQ dla systemów HP-UX
- KomponentyIBM WebSphere MQ dla systemów AIX
- KomponentyIBM WebSphere MQ dla systemów Solaris

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach używana jest kolejka o nazwie TEST.Q , która służy do przekazywania komunikatów między aplikacjami. Advanced Message Security korzysta z przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym wchodzą one do infrastruktury WebSphere MQ za pośrednictwem standardowego interfejsu WebSphere MQ . Podstawowa konfiguracja jest wykonywana w produkcie WebSphere MQ i jest skonfigurowana w poniższych krokach.

Za pomocą programu WebSphere MQ Explorer można utworzyć menedżer kolejek QM_VERIFY_AMS i jego kolejkę lokalną o nazwie TEST.Q przy użyciu wszystkich domyślnych ustawień kreatora. Można również użyć komend znalezionych w programie <MQ_INSTALL_PATH>/bin. Należy pamiętać, że użytkownik musi być członkiem grupy użytkowników produktu mqm , aby uruchomić następujące komendy administracyjne.

Procedura

1. Tworzenie menedżera kolejek

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Uruchamianie menedżera kolejek

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Utwórz kolejkę o nazwie TEST.Q , wprowadzając następującą komendę w programie **runmqsc** dla menedżera kolejek QM_VERIFY_AMS

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Wyniki

Jeśli procedura została zakończona pomyślnie, następująca komenda wprowadzona do programu **runmqsc** wyświetli szczegółowe informacje o produkcie TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym przykładzie pojawiają się dwaj użytkownicy: alice, nadawca i bob, odbiorca. Aby móc korzystać z kolejki aplikacji, użytkownicy ci muszą mieć uprawnienia do korzystania z niej. Ponadto, aby pomyślnie korzystać ze strategii ochrony, które zdefiniujemy tych użytkowników, należy nadać im dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** można znaleźć w sekcji **setmqaut** .

Procedura

1. Utwórz dwóch użytkowników

```
useradd alice
useradd bob
```

2. Autoryzowanie użytkowników do łączenia się z menedżerem kolejek i do pracy z kolejką

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get
```

3. Należy także zezwolić dwóm użytkownikom na przeglądanie kolejki strategii systemowej i umieszczanie komunikatów w kolejce błędów.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```

Wyniki

Grupy użytkowników są teraz tworzone i nadane im wymagane uprawnienia. W ten sposób użytkownicy, którzy są przypisani do tych grup, będą mieli również uprawnienia do łączenia się z menedżerem kolejek oraz do umieszczania i pobierania z kolejki.

Co dalej

Aby sprawdzić, czy kroki zostały wykonane poprawnie, należy użyć przykładów `amqsput` i `amqsget` zgodnie z opisem w sekcji “8. Testowanie szyfrowania” na stronie 294.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Aby zaszyfrować wiadomość, przechwytywacz wymaga klucza prywatnego wysyłającego użytkownika oraz klucza publicznego odbiorcy (-ów). W związku z tym należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W systemie rzeczywistym, w którym użytkownicy i aplikacje są rozpraszani na kilku komputerach, każdy użytkownik ma własny prywatny magazyn kluczy. Podobnie w niniejszym podręczniku tworzone są kluczowe bazy danych dla produktów `alice` i `bob` , a także certyfikaty użytkowników między nimi.

Uwaga: W tym podręczniku używamy przykładowych aplikacji napisanych w języku C łączących się z powiązaniami lokalnymi. Jeśli planowane jest korzystanie z aplikacji Java za pomocą powiązań klienta, należy utworzyć magazyn kluczy JKS i certyfikaty za pomocą komendy **`keytool`** , która jest częścią środowiska JRE (więcej informacji zawiera sekcja “Podręcznik Szybki start dla klientów Java” na stronie 294). W przypadku wszystkich pozostałych języków, a także w przypadku aplikacji Java korzystających z powiązań lokalnych, kroki zawarte w tym podręczniku są poprawne.

Procedura

1. Utwórz nową bazę danych kluczy dla użytkownika `alice`

```
mkdir /home/alice/.mqs -p
runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
```

Uwaga:

- Zaleca się użycie silnego hasła, aby zabezpieczyć bazę danych.
- Parametr `stash` przechowuje hasło do pliku `key.sth` , którego przechwytywacze mogą używać do otwierania bazy danych.

2. Sprawdź, czy baza danych kluczy jest czytelna

```
chmod +r /home/alice/.mqs/alicekey.kdb
```

3. Tworzenie certyfikatu identyfikującego użytkownika `alice` w celu jego użycia w szyfrowaniu

```
runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd
-label Alice_Cert -dn "cn=alice,o=IBM,c=GB" -default_cert yes
```

Uwaga:

- Do celów niniejszego przewodnika korzystamy z samopodpisanego certyfikatu, który można utworzyć bez korzystania z ośrodka certyfikacji. W przypadku systemów produkcyjnych zaleca się, aby nie używać certyfikatów samopodpisanych, ale zamiast tego opierać się na certyfikatach podpisanych przez ośrodek certyfikacji.
- Parametr `label` określa nazwę certyfikatu, który przechwytywacz będzie poszukiwać w celu otrzymania niezbędnych informacji.
- Parametr DN określa szczegóły nazwy wyróżniającej (**Distinguished Name** -DN), która musi być unikalna dla każdego użytkownika.

4. Teraz stworzyliśmy bazę kluczy, powinniśmy ustawić jej własności i zapewnić, że jest ona nieczytelna dla wszystkich innych użytkowników.

```
chown alice /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
chmod 600 /home/alice/.mqs/alicekey.kdb /home/alice/.mqs/alicekey.sth
```

5. Powtórz krok 1-4 dla użytkownika bob

Wyniki

Dla dwóch użytkowników `alice` i bob każdy z nich ma certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Przechwytywacze Advanced Message Security należy wskazywać na katalog, w którym znajdują się kluczowe bazy danych i certyfikaty. Odbywa się to za pomocą pliku `keystore.conf` , który przechowuje te informacje w postaci jawnego tekstu. Każdy użytkownik musi mieć w folderze `.mqs` oddzielny plik `keystore.conf` . Ten krok musi być wykonany zarówno dla produktów `alice` , jak i bob.

Treść produktu `keystore.conf` musi mieć postać:

```
cms.keystore = <dir>/keystore_file
cms.certificate = certificate_label
```

Przykład

W tym scenariuszu zawartość pliku `keystore.conf` będzie następująca:

```
cms.keystore = /home/alice/.mqs/alicekey
cms.certificate = Alice_Cert
```

Uwaga:

- Ścieżka do pliku kluczy musi być podana bez rozszerzenia nazwy pliku.
- Dostępne są następujące formaty magazynu kluczy: CMS (Cryptographic Message Syntax), JKS (Java Keystore) i JCEKS (Java Cryptographic Extension Keystore). Więcej informacji zawiera sekcja “Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf)” na stronie 305.
- `HOME/.mqs/keystore.conf` jest domyślnym położeniem, w którym program Advanced Message Security wyszukuje plik `keystore.conf` . Więcej informacji na temat korzystania z położenia innego niż domyślne dla `keystore.conf`zawiera sekcja “Korzystanie z magazynów kluczy i certyfikatów” na stronie 305.

5. Współużytkowanie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwoma kluczowymi bazami danych, aby każdy użytkownik mógł pomyślnie zidentyfikować inne bazy danych. Jest to wykonywane przez wyodrębnienie certyfikatu publicznego każdego użytkownika do pliku, który następnie jest dodawany do bazy danych kluczy innego użytkownika.

Uwaga: Należy uważać, aby użyć opcji *extract* , a nie opcji *export* . Opcja *Wyodrębnij* pobiera klucz publiczny użytkownika, natomiast *eksport* pobiera zarówno klucz publiczny, jak i prywatny. Użycie komendy *export* przez pomyłkę spowodowałoby całkowite skompromitowanie aplikacji, przechodząc do klucza prywatnego.

Procedura

1. Wyodrębnij certyfikat identyfikujący `alice` do pliku zewnętrznego:

```
runmqakm -cert -extract -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert
-target alice_public.arm
```

2. Dodaj certyfikat do magazynu kluczy `bob's` :

```
runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
alice_public.arm
```

3. Powtórz krok dla `bob`:

```
 runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
bob_public.arm
```

4. Dodaj certyfikat dla pliku kluczy `bob` do `alice's` :

```
runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert -file
bob_public.arm
```

Wyniki

Dwaj użytkownicy `alice` i `bob` są teraz w stanie pomyślnie zidentyfikować siebie nawzajem po utworzeniu i współużytkowanych samopodpisanych certyfikatach.

Co dalej

Sprawdź, czy certyfikat znajduje się w magazynie kluczy, uruchamiając następujące komendy, które drukuje jego szczegóły:

```
runmqakm -cert -details -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert
runmqakm -cert -details -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert
```

6. Definiowanie strategii kolejki

O tym zadaniu

Za pomocą utworzonego menedżera kolejek i przechwytywaczy przygotowanych do przechwytywania komunikatów i uzyskiwania dostępu do kluczy szyfrowania, można rozpocząć definiowanie strategii ochrony w systemie `QM_VERIFY_AMS` za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy można znaleźć w sekcji setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Jest to przykład strategii zdefiniowanej dla kolejki produktu `TEST.Q` . W tym przykładzie komunikaty są podpisywane przez użytkownika `alice` przy użyciu algorytmu `SHA1` i szyfrowane przy użyciu algorytmu

256-bitowego AES .alice jest jedynym poprawnym nadawcą, a bob jest jedynym odbiorcą komunikatów w tej kolejce:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Uwaga: Nazwy wyróżniające są zgodne z tymi, które zostały określone w certyfikacie odpowiedniego użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wydaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend produktu setmqspl , należy użyć opcji -export . Umożliwia to przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testowanie konfiguracji

O tym zadaniu

Uruchamiając różne programy pod różnymi użytkownikami, można sprawdzić, czy aplikacja została poprawnie skonfigurowana.

Procedura

1. Przejdź do katalogu zawierającego przykłady. Jeśli produkt MQ jest zainstalowany w położeniu innym niż domyślne, może to znajdować się w innym miejscu.

   ```
   cd /opt/mqm/samp/bin
   ```

2. Przełącz użytkownika do uruchomienia jako użytkownik alice

   ```
   su alice
   ```

3. Jako użytkownik aliceumieść komunikat przy użyciu przykładowej aplikacji:

   ```
   ./amqsput TEST.Q QM_VERIFY_AMS
   ```

4. Wpisz tekst komunikatu, a następnie naciśnij klawisz Enter.
5. Zatrzymaj działanie jako użytkownik alice

   ```
   exit
   ```

6. Przełącz użytkownika do uruchomienia jako użytkownik bob

   ```
   su bob
   ```

7. Jako użytkownik bobuzyskaj komunikat przy użyciu przykładowej aplikacji:

   ```
   ./amqsget TEST.Q QM_VERIFY_AMS
   ```

Wyniki

Jeśli aplikacja została poprawnie skonfigurowana dla obu użytkowników, komunikat aliceużytkownika jest wyświetlany, gdy program bob uruchamia aplikację pobierający.

8. Testowanie szyfrowania

O tym zadaniu

Aby sprawdzić, czy szyfrowanie jest wykonywane zgodnie z oczekiwaniami, należy utworzyć kolejkę aliasową, która odwołuje się do oryginalnej kolejki TEST.Q. Ta kolejka aliasowa nie będzie miała strategii bezpieczeństwa, więc żaden użytkownik nie będzie miał informacji do zdeszyfrowania wiadomości i dlatego zostaną wyświetlone zaszyfrowane dane.

Procedura

1. Za pomocą komendy **runmqsc** w odniesieniu do menedżera kolejek QM_VERIFY_AMS utwórz kolejkę aliasową.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```

2. Przyznaj dostęp bob do przeglądania z kolejki aliasowej

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```

3. Jako użytkownik `alice`umieść inny komunikat przy użyciu przykładowej aplikacji, tak jak wcześniej:

   ```
   ./amqsput TEST.Q QM_VERIFY_AMS
   ```

4. Jako użytkownik bobprzeglądaj komunikat przy użyciu przykładowej aplikacji za pomocą kolejki aliasowej:

   ```
   ./amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```

5. Jako użytkownik bob, pobierz komunikat przy użyciu przykładowej aplikacji z kolejki lokalnej:

   ```
   ./amqsget TEST.Q QM_VERIFY_AMS
   ```

Wyniki

Dane wyjściowe z aplikacji `amqsbcg` będą zawierać zaszyfrowane dane, które są w kolejce potwierdzające, że komunikat został zaszyfrowany.

Podręcznik Szybki start dla klientów Java

Ten podręcznik służy do szybkiego konfigurowania produktu IBM Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów dla aplikacji Java łączących się przy użyciu powiązań klienta. Po zakończeniu tego procesu utworzony zostanie magazyn kluczy w celu weryfikacji tożsamości użytkowników oraz zdefiniowanych strategii podpisywania i szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

Upewnij się, że zostały zainstalowane odpowiednie komponenty zgodnie z opisem w publikacji **Szybki start** (Windows lub UNIX).

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach używana jest kolejka o nazwie TEST.Q , która służy do przekazywania komunikatów między aplikacjami. Advanced Message Security korzysta z przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym wchodzą one do infrastruktury WebSphere MQ za pośrednictwem standardowego interfejsu WebSphere MQ . Podstawowa konfiguracja jest wykonywana w produkcie WebSphere MQ i jest skonfigurowana w poniższych krokach.

Procedura

1. Tworzenie menedżera kolejek

```
crtmqm QM_VERIFY_AMS
```

2. Uruchamianie menedżera kolejek

```
strmqm QM_VERIFY_AMS
```

3. Utwórz i uruchom program nasłuchujący, wprowadzając następujące komendy w programie **runmqsc** dla menedżera kolejek QM_VERIFY_AMS

```
DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
START LISTENER(AMS.LSTR)
```

4. Utwórz kanał dla naszych aplikacji, za pomocą którego można nawiązać połączenie, wprowadzając następującą komendę w programie **runmqsc** dla menedżera kolejek QM_VERIFY_AMS

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. Utwórz kolejkę o nazwie TEST.Q , wprowadzając następującą komendę w programie **runmqsc** dla menedżera kolejek QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Wyniki

Jeśli procedura została zakończona pomyślnie, następująca komenda wprowadzona do programu **runmqsc** wyświetli szczegółowe informacje o produkcie TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W naszym scenariuszu pojawiają się dwaj użytkownicy: alice, nadawca i bob, odbiornik. Aby móc korzystać z kolejki aplikacji, użytkownicy ci muszą mieć uprawnienia do korzystania z niej. Ponadto, aby pomyślnie korzystać ze strategii ochrony, które zdefiniujemy tych użytkowników, należy nadać im dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** można znaleźć w sekcji **setmqaut** .

Procedura

1. Utwórz dwóch użytkowników zgodnie z opisem w **Podręczniku szybkiego startu** (Windows lub UNIX) dla danej platformy.
2. Autoryzowanie użytkowników do łączenia się z menedżerem kolejek i do pracy z kolejką

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get +inq
```

3. Należy także zezwolić dwóm użytkownikom na przeglądanie kolejki strategii systemowej i umieszczanie komunikatów w kolejce błędów.

```
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p alice -p bob +browse
setmqaut -m QM_VERIFY_AMS -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p alice -p bob +put
```

Wyniki

Użytkownicy są teraz utworzani i nadane im wymagane uprawnienia.

Co dalej

Aby sprawdzić, czy kroki zostały wykonane poprawnie, należy użyć przykładów JmsProducer i JmsConsumer zgodnie z opisem w sekcji “7. Testowanie konfiguracji” na stronie 298.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Aby zaszyfrować komunikat do przechwytywacza, należy użyć klucza publicznego wysyłających użytkowników. W związku z tym należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W systemie rzeczywistym, w którym użytkownicy i aplikacje są rozpraszani na kilku komputerach, każdy użytkownik ma własny prywatny magazyn kluczy. Podobnie w niniejszym podręczniku tworzone są kluczowe bazy danych dla produktów `alice` i bob , a także certyfikaty użytkowników między nimi.

Uwaga: W tym podręczniku używamy przykładowych aplikacji napisanych w języku Java łączących się za pomocą powiązań klienta. Jeśli planowane jest korzystanie z aplikacji Java za pomocą powiązań lokalnych lub aplikacji w języku C, należy utworzyć magazyn kluczy CMS i certyfikaty za pomocą komendy **runmqakm** . Jest to przedstawione w publikacji **Szybki start** (Windows lub UNIX).

Procedura

1. Utwórz katalog, w którym ma zostać utworzony magazyn kluczy, na przykład `/home/alice/.mqs`. Można go utworzyć w tym samym katalogu, w którym jest używany w **Podręczniku szybkiego startu** (Windows lub UNIX) dla danej platformy.

   Uwaga: Ten katalog zostanie określony jako *katalog_magazynowy* w następujących krokach
2. Utwórz nowy magazyn kluczy i certyfikat identyfikujące użytkownika `alice` do użycia w szyfrowaniu

   Uwaga: Komenda **keytool** jest częścią środowiska JRE.

   ```
   keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
   -storepass passw0rd
   -dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
   ```

   Uwaga:

   - Jeśli plik *keystore-dir* zawiera spacje, należy umieścić w cudzysłowie pełną nazwę pliku kluczy.
   - Zaleca się użycie silnego hasła, aby zabezpieczyć magazyn kluczy.
   - Do celów niniejszego przewodnika korzystamy z samopodpisanego certyfikatu, który można utworzyć bez korzystania z ośrodka certyfikacji. W przypadku systemów produkcyjnych zaleca się, aby nie używać samopodpisanych certyfikatów, ale zamiast tego opierać się na certyfikatach podpisanych przez ośrodek certyfikacji.
   - Parametr `alias` określa nazwę certyfikatu, który przechwytywacz będzie poszukiwać w celu otrzymania niezbędnych informacji.
   - Parametr dname określa szczegóły nazwy wyróżniającej (**Distinguished Name** -DN), która musi być unikalna dla każdego użytkownika.
3. W systemie UNIX upewnij się, że magazyn kluczy jest czytelny

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Powtórz procedurę step1-4 dla użytkownika bob

Wyniki

Dla dwóch użytkowników `alice` i bob każdy z nich ma certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Przechwytywacze Advanced Message Security należy wskazywać na katalog, w którym znajdują się kluczowe bazy danych i certyfikaty. Odbywa się to za pomocą pliku `keystore.conf` , który przechowują

te informacje w postaci zwykłego tekstu. Każdy użytkownik musi mieć oddzielny plik `keystore.conf` . Ten krok powinien być wykonany zarówno dla produktów `alice` , jak i bob.

Przykład

W tym scenariuszu zawartość pliku `keystore.conf` dla `alice` będzie następująca:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

W tym scenariuszu zawartość pliku `keystore.conf` dla bob będzie następująca:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Uwaga:

- Ścieżka do pliku kluczy musi być podana bez rozszerzenia nazwy pliku.
- Jeśli użytkownik ma już `keystore.conf` , ponieważ po nim znajduje się **Szybki start** (Windows lub UNIX), można edytować istniejący plik w celu dodania go w powyższych wierszach.
- Więcej informacji na ten temat zawiera sekcja “Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf)” na stronie 305.

5. Współużytkowanie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwoma magazynami kluczy, dzięki czemu każdy użytkownik może pomyślnie zidentyfikować inne. Odbywa się to poprzez wyodrębnienie certyfikatu każdego użytkownika i zaimportowanie go do magazynu kluczy innego użytkownika.

Uwaga: Terminy *extract* i *export* są używane w różny sposób przez różne narzędzia certyfikatu. Na przykład narzędzie IBM GSKit Keyman (ikeyman) wprowadza rozróżnienie, które *wyodrębnia* certyfikaty (klucze publiczne), a także klucze prywatne *eksport* . To rozróżnienie jest niezwykle ważne w przypadku narzędzi, które oferują obie opcje, ponieważ użycie *eksportu* przez pomyłkę całkowicie zagroziłoby aplikacji, przechodząc do jego klucza prywatnego. Ponieważ rozróżnienie jest tak ważne, dokumentacja produktu WebSphere MQ stara się używać tych terminów w spójny sposób. Jednak narzędzie Java keytool udostępnia opcję wiersza komend o nazwie *exportcert* , która wyodrębnia tylko klucz publiczny. Z tych powodów następująca procedura odwołuje się do *wyodrębnienia* certyfikatów przy użyciu opcji *exportcert* .

Procedura

1. Wyodrębnij certyfikat identyfikujący `alice`.

   ```
   keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
   -alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
   ```

2. Zaimportuj certyfikat identyfikujący `alice` do magazynu kluczy, który będzie używany przez produkt bob . Po wyświetleniu monitu należy wskazać, że ten certyfikat będzie zaufany.

   ```
   keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
   -keystore bob-keystore-dir/keystore.jks -storepass passw0rd
   ```

3. Powtórz kroki dla produktu bob .

Wyniki

Dwaj użytkownicy `alice` i bob są teraz w stanie pomyślnie zidentyfikować siebie nawzajem po utworzeniu i współużytkowanych samopodpisanych certyfikatach.

Co dalej

Sprawdź, czy certyfikat znajduje się w magazynie kluczy, uruchamiając następujące komendy, które drukuje jego szczegóły:

```
keytool -list -keystore bob-keystore-dir/keystore.jks -storepass passw0rd -alias Alice_Java_Cert
keytool -list -keystore alice-keystore-dir/keystore.jks -storepass passw0rd -alias Bob_Java_Cert
```

6. Definiowanie strategii kolejki

O tym zadaniu

Za pomocą utworzonego menedżera kolejek i przechwytywaczy przygotowanych do przechwytywania komunikatów i uzyskiwania dostępu do kluczy szyfrowania, można rozpocząć definiowanie strategii ochrony w systemie `QM_VERIFY_AMS` za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy można znaleźć w sekcji setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Jest to przykład strategii zdefiniowanej w kolejce `TEST.Q` , podpisanej przez użytkownika `alice` za pomocą algorytmu SHA1 , i zaszyfrowanej przy użyciu algorytmu 256-bitowego AES dla użytkownika bob:

```
setmqspl -m QM_VERIFY_AMS -p TEST.Q -s SHA1 -a "CN=alice,O=IBM,C=GB" -e AES256 -r
"CN=bob,O=IBM,C=GB"
```

Uwaga: Nazwy wyróżniające są zgodne z tymi, które zostały określone w certyfikacie odpowiedniego użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wydaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend produktu `setmqspl` , należy użyć opcji `-export` . Umożliwia to przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testowanie konfiguracji

Zanim rozpoczniesz

Upewnij się, że używana wersja środowiska Java ma zainstalowane nieograniczone pliki strategii JCE.

Uwaga: Wersja środowiska Java podana w instalacji produktu WebSphere MQ zawiera już te pliki strategii. Można go znaleźć w programie *MQ_INSTALLATION_PATH*`/java/bin`.

O tym zadaniu

Uruchamiając różne programy pod różnymi użytkownikami, można sprawdzić, czy aplikacja została poprawnie skonfigurowana. Aby uzyskać szczegółowe informacje na temat uruchamiania programów w różnych użytkownikach, zapoznaj się z **Podręcznikiem szybkiego startu** (Windows lub UNIX) dla używanej platformy.

Procedura

1. Aby uruchomić te przykładowe aplikacje JMS, należy użyć ustawienia CLASSPATH dla platformy, tak jak pokazano to w sekcji Zmienne środowiskowe używane przez klasy produktu IBM WebSphere MQ dla usługi JMS , aby upewnić się, że katalog przykładów jest dołączony.
2. Jako użytkownik `alice`umieść komunikat przy użyciu przykładowej aplikacji, łącząc się jako klient:

   ```
   java JMSProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
   ```

3. Jako użytkownik bobpobierz komunikat przy użyciu przykładowej aplikacji, łącząc się jako klient:

   ```
   java JMSConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
   ```

Wyniki

Jeśli aplikacja została poprawnie skonfigurowana dla obu użytkowników, komunikat `alice`użytkownika jest wyświetlany, gdy program bob uruchamia aplikację pobierający.

Ochrona kolejek zdalnych

Aby w pełni chronić zdalne połączenia z kolejkami, należy ustawić tę samą strategię w kolejce zdalnej i lokalnej, do której przesyłane są komunikaty.

Gdy komunikat jest umieszczany w kolejce zdalnej, program Advanced Message Security przechwytuje tę operację i przetwarza komunikat zgodnie z zestawem strategii dla kolejki zdalnej. Na przykład dla strategii szyfrowania komunikat jest szyfrowany, zanim zostanie przekazany do WebSphere MQ w celu obsługania go. Po przetworzeniu przez program Advanced Message Security komunikatu umieszczonego w kolejce zdalnej program WebSphere MQ umieszcza go w powiązanej kolejce transmisji i przekazuje go do docelowego menedżera kolejek i kolejki docelowej.

Gdy operacja GET jest wykonywana w kolejce lokalnej, program Advanced Message Security próbuje zdekodować komunikat zgodnie z zestawem strategii w kolejce lokalnej. Aby operacja powiodła się, strategia używana do deszyfrowania komunikatu musi być taka sama, jak ta używana do szyfrowania. Wszelkie rozbieżności spowodują, że komunikat zostanie odrzucony.

Jeśli z jakiegokolwiek powodu obie strategie nie mogą być ustawione w tym samym czasie, udostępniana jest pomostowa obsługa propagacji. Strategię można ustawić w lokalnej kolejce z flagą tolerancji, co oznacza, że strategia powiązana z kolejką może zostać zignorowana, gdy próba pobrania komunikatu z kolejki wiąże się z komunikatem, który nie ma ustawionego zestawu strategii bezpieczeństwa. W takim przypadku program GET podejmie próbę zdeszyfrowania komunikatu, ale umożliwi dostarczenie niezaszyfrowanych komunikatów. W ten sposób strategie w kolejkach zdalnych mogą być ustawione po zabezpieczeniu kolejek lokalnych (i przetestowaniu).

Zapamiętaj: Usuń flagę tolerancji po zakończeniu propagacji Advanced Message Security .

Odsyłacze pokrewne

setmqspl (ustawienie strategii bezpieczeństwa)

Kierowanie komunikatów chronionych przy użyciu produktu WebSphere Message Broker

Produkt IBM Advanced Message Security może chronić komunikaty w infrastrukturze, w której zainstalowany jest produkt WebSphere Message Broker 8.0.0.1 (lub nowszy). Przed zastosowaniem zabezpieczeń w środowisku produktu WebSphere Message Broker należy zapoznać się z naturą obu produktów.

O tym zadaniu

Produkt Advanced Message Security zapewnia kompleksową ochronę ładunku komunikatu. Oznacza to, że tylko strony określone jako poprawne nadawcy i odbiorcy wiadomości są w stanie je produkować lub odbierać. Oznacza to, że w celu zabezpieczenia komunikatów przepływających przez produkt WebSphere Message Broker można zezwolić produktowi WebSphere Message Broker na przetwarzanie komunikatów

bez znajomości ich treści (Scenariusz 1) lub sprawić, że autoryzowany użytkownik będzie mógł odbierać i wysyłać komunikaty (Scenariusz 2).

Scenariusz 1-Broker komunikatów nie może wyświetlić treści komunikatu

Zanim rozpoczniesz

Produkt WebSphere Message Broker powinien być połączony z istniejącym menedżerem kolejek. Zastąp *QMgrName* tą nazwą istniejącego menedżera kolejek w następujących komendach.

O tym zadaniu

W tym scenariuszu Alicja umieszcza zabezpieczony komunikat w kolejce wejściowej `QIN`. W oparciu o właściwość komunikatu `route`Tokomunikat jest kierowany do *bob's* (`QBOB`),[1](`QCECIL`) lub domyślna (`QDEF`) kolejka. Routing jest możliwy, ponieważ produkt Advanced Message Security zabezpiecza tylko ładunek komunikatu, a nie jego nagłówki i właściwości, które pozostają niezabezpieczone i mogą być odczytane przez produkt WebSphere Message Broker. Advanced Message Security jest używany tylko przez *alice*, *bob* i *cecil*. Nie jest konieczne zainstalowanie lub skonfigurowanie go dla produktu WebSphere Message Broker.

WebSphere Broker komunikatów odbiera chroniony komunikat z niezabezpieczonej kolejki aliasowej, aby uniknąć próby deszyfrowania komunikatu. W przypadku bezpośredniego użycia chronionej kolejki komunikat zostanie umieszczony w kolejce DEAD LETTER (DEAD LETTER) jako niemożliwy do odszyfrowania. Komunikat jest kierowany przez produkt WebSphere Message Broker i dociera do kolejki docelowej bez zmian. Oznacza to, że jest on nadal podpisany przez oryginalnego autora (zarówno *bob* , jak i *cecil* akceptują tylko komunikaty wysłane przez *alice*) i chronione jak wcześniej (tylko *bob* i *cecil* mogą go odczytać). WebSphere Message Broker umieszcza kierowany komunikat do niezabezpieczonego aliasu. Odbiorcy pobierają komunikat z chronionej kolejki wyjściowej, w której produkt IBM WebSphere MQ AMS w sposób przezroczysty deszyfruje komunikat.

Procedura

1. Skonfiguruj *alice*, *bob* i *cecil* , aby używać produktu Advanced Message Security zgodnie z opisem w **Podręczniku szybkiego startu** (Windows lub UNIX).

   Upewnij się, że zostały wykonane następujące kroki:

   - Tworzenie i autoryzowanie użytkowników
   - Tworzenie bazy danych kluczy i certyfikatów
   - Tworzenie pliku keystore.conf
2. Podaj certyfikat *alice's* na wartość *jan* i *cecil*, tak więc *alice* może być identyfikowany przez nie podczas sprawdzania podpisów cyfrowych w komunikatach.

   W tym celu należy wyodrębnić certyfikat identyfikujący *alice* do pliku zewnętrznego, a następnie dodać wyodrębniony certyfikat do plików kluczy *bob's* i *cecil's* . Ważne jest, aby użyć metody opisanej w **Czynność 5. Współużytkowanie certyfikatów** w **Podręczniku szybkiego startu** (Windows lub UNIX).
3. Udostępnij certyfikaty *bob* i *cecil* do *alice*, tak więc *alice* może wysyłać wiadomości zaszyfrowane dla *bob* i *cecil*.

   W tym celu należy użyć metody określonej w poprzednim kroku.
4. W menedżerze kolejek zdefiniuj kolejki lokalne o nazwach `QIN`, `QBOB`, `QCECIL` i `QDEF`.

   ```
   DEFINE QLOCAL(QIN)
   ```
5. Skonfiguruj strategię bezpieczeństwa dla kolejki produktu `QIN` do kwalifikującej się konfiguracji. Użyj tej samej konfiguracji dla kolejek `QBOB`, `QCECIL` i `QDEF` .

[1] cecil

```
setmqspl -m QMgrName -p QIN -s SHA1 -a "CN=alice,O=IBM,C=GB"
-e AES256 -r "CN=bob,O=IBM,C=GB" -r "CN=cecil,O=IBM,C=GB"
```

W tym scenariuszu założono, że strategia bezpieczeństwa, w której *alice* jest jedynym autoryzowanym nadawcą, a *bob* i *cecil* , są odbiorcami.

6. Zdefiniuj kolejki aliasowe AIN, ABOB i ACECIL odwołujące się odpowiednio do kolejek lokalnych QIN, QBOB i QCECIL .

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. Sprawdź, czy konfiguracja zabezpieczeń dla aliasów podanych w poprzednim kroku nie jest dostępna. W przeciwnym razie ustaw strategię na wartość NONE.

```
dspmqspl -m QMgrName -p AIN
```

8. W produkcie WebSphere Message Broker utwórz przepływ komunikatów w celu skierowania komunikatów przychodzących do kolejki aliasowej produktu AIN do węzła BOB, CECIL lub DEF, w zależności od właściwości routeTo komunikatu. W tym celu:
   a) Utwórz węzeł MQInput o nazwie IN i przypisz alias AIN jako jego nazwę kolejki.
   b) Utwórz węzły MQOutput o nazwach BOB, CECIL i DEF , a następnie przypisz kolejki aliasowe ABOB, ACECIL i ADEF jako odpowiadające im nazwy kolejek.
   c) Utwórz węzeł trasy i wywołaj go TEST.
   d) Połącz węzeł IN z wejściowym punktem końcowym węzła TEST .
   e) Utwórz terminale wyjściowe bobi cecil dla węzła TEST .
   f) Podłącz terminal wyjściowy bob do węzła BOB .
   g) Podłącz terminal wyjściowy cecil do węzła CECIL .
   h) Połącz węzeł DEF z domyślnym terminalem wyjściowym.
   i) Zastosuj następujące reguły:

```
$Root/MQRFH2/usr/routeTo/text()="bob"
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. Wdróż przepływ komunikatów w komponencie wykonawczym produktu WebSphere Message Broker.
10. Uruchomienie jako użytkownik Alice umieściło komunikat, który zawiera również właściwość komunikatu o nazwie routeTo z wartością bob lub cecil. Uruchomienie przykładowej aplikacji **amqsstm** umożliwi Ci to działanie.

```
Sample AMQSSTMA start
target queue is TEST.Q
Enter property name
routeTo
Enter property value
bob
Enter property name

Enter message text
My Message to Bob
Sample AMQSSTMA end
```

11. Uruchomienie jako użytkownik *jan* wczytanie komunikatu z kolejki QBOB przy użyciu przykładowej aplikacji **amqsget**.

Wyniki

Gdy *alice* umieszcza komunikat w kolejce QIN , komunikat jest chroniony. Jest on pobierany w formie chronionej przez produkt WebSphere Message Broker z kolejki aliasowej produktu AIN . WebSphere Message Broker decyduje, gdzie należy skierować komunikat odczytywanie właściwości routeTo , która jest, jak wszystkie właściwości, niezaszyfrowana. WebSphere Message Broker umieszcza komunikat w odpowiednim niezabezpieczonym aliasie, unikając jego dalszej ochrony. Po odebraniu przez komendę *jan* lub *cecil* z kolejki, komunikat jest deszyfrowany, a podpis cyfrowy jest weryfikowany.

O tym zadaniu

W tym scenariuszu grupa osób może wysyłać komunikaty do produktu WebSphere Message Broker. Inna grupa jest autoryzowana do odbierania komunikatów, które są tworzone przez produkt WebSphere Message Broker. Przesyłanie między stronami i WebSphere Message Broker nie może zostać usunięte.

Należy pamiętać, że produkt WebSphere Message Broker odczytuje strategie ochrony i certyfikaty tylko wtedy, gdy kolejka jest otwierana, dlatego należy ponownie załadować grupę wykonawców po wprowadzeniu aktualizacji strategii ochrony, aby zmiany zostały uwzględnione.

```
mqsireload execution-group-name
```

Jeśli produkt WebSphere Message Broker jest uważany za autoryzowany podmiot uprawniony do odczytu lub podpisywania ładunku komunikatu, należy skonfigurować produkt Advanced Message Security dla użytkownika uruchamianego z usługą WebSphere Message Broker. Należy pamiętać, że nie musi to być ten sam użytkownik, który wstawi/pobiera komunikaty do kolejek, ani użytkownik tworzący i wdrażający aplikacje produktu WebSphere Message Broker.

Procedura

1. Skonfiguruj *alice*, *bob*, *cecil* i *dave* oraz użytkownika usługi produktu WebSphere Message Broker, aby używać produktu Advanced Message Security zgodnie z opisem w publikacji **Szybki start** (Windows lub UNIX).

   Upewnij się, że zostały wykonane następujące kroki:

   - Tworzenie i autoryzowanie użytkowników
   - Tworzenie bazy danych kluczy i certyfikatów
   - Tworzenie pliku keystore.conf
2. Udostępnij certyfikaty *alice*, *bob*, *cecil* i *dave's* dla użytkownika usługi produktu WebSphere Message Broker.

   W tym celu wyodrębnianie do plików zewnętrznych każdego certyfikatu identyfikującego *alice*, *bob*, *cecil* i *dave*, a następnie dodanie wyodrębnionych certyfikatów do magazynu kluczy produktu WebSphere Message Broker. Ważne jest, aby użyć metody opisanej w **Czynność 5. Współużytkowanie certyfikatów** w **Podręczniku szybkiego startu** (Windows lub UNIX).
3. Podaj certyfikat użytkownika usługi produktu WebSphere Message Broker na *alice*, *bob*, *cecil* i *dave*.

   W tym celu należy użyć metody określonej w poprzednim kroku.

   Uwaga: *Alicja* i *jan* potrzebują certyfikatu użytkownika usługi WebSphere Message Broker, aby poprawnie zaszyfrować komunikaty. Użytkownik usługi produktu WebSphere Message Broker wymaga certyfikatów *alice's* i *bob's* w celu zweryfikowania autorów komunikatów. Użytkownik usługi produktu WebSphere Message Broker wymaga certyfikatów *cecil* i *dave* w celu zaszyfrowania komunikatów dla nich. *cecil* i *dave* potrzebują certyfikatu użytkownika usługi WebSphere Message Broker w celu sprawdzenia, czy komunikat pochodzi z produktu WebSphere Message Broker.
4. Zdefiniuj kolejkę lokalną o nazwie IN i zdefiniuj strategię bezpieczeństwa z *alice* i *bob* określonymi jako autorzy i WebSphere Użytkownik usługi produktu Message Broker określonym jako odbiorca:

   ```
   setmqspl -m QMgrName -p IN -s MD5 -a "CN=alice,O=IBM,C=GB" -a "CN=bob,O=IBM,C=GB"
   -e AES256 -r "CN=broker,O=IBM,C=GB"
   ```
5. Zdefiniuj kolejkę lokalną o nazwie OUT i zdefiniuj strategię bezpieczeństwa z użytkownikiem usługi WebSphere Message Broker określonym jako autor oraz *cecil* i *dave* określanymi jako odbiorcy:

   ```
   setmqspl -m QMgrName -p OUT -s MD5 -a "CN=broker,O=IBM,C=GB" -e AES256
   -r "CN=cecil,O=IBM,C=GB" -r "CN=dave,O=IBM,C=GB"
   ```

6. W produkcie WebSphere Message Broker utwórz przepływ komunikatów z węzłem `MQInput` i `MQOutput` . Skonfiguruj węzeł `MQInput` tak, aby używany był węzeł `IN` i węzeł `MQOutput` w celu użycia kolejki `OUT` .
7. Wdróż przepływ komunikatów w komponencie wykonawczym produktu WebSphere Message Broker.
8. Uruchamianie jako użytkownik *alice* lub *jan* umieszczają komunikat w kolejce `IN` przy użyciu przykładowej aplikacji **`amqsput`**.
9. Uruchamianie jako użytkownik *cecil* lub *dave* pobiera komunikat z kolejki `OUT` przy użyciu przykładowej aplikacji **`amqsget`**.

Wyniki

Komunikaty wysłane przez *alice* lub *bob* do kolejki wejściowej `IN` są szyfrowane, zezwalając tylko na to, aby produkt WebSphere Message Broker go odczytany. WebSphere Message Broker będzie akceptować tylko komunikaty od *alice* i *bob* i odrzuci inne. Zaakceptowane komunikaty będą odpowiednio przetwarzane, a następnie podpisane i zaszyfrowane za pomocą kluczy *cecil* i *dave*'s przed umieszczaniem ich w kolejce wyjściowej `OUT`. Tylko *cecil* i *dave* są w stanie go odczytać, komunikaty nie podpisane przez produkt WebSphere Message Broker są odrzucane.

Używanie produktu IBM WebSphere MQ Advanced Message Security z produktem IBM WebSphere MQ Managed File Transfer

W tym scenariuszu wyjaśniono, w jaki sposób skonfigurować produkt Advanced Message Security w taki sposób, aby zapewniał prywatność komunikatów dla danych wysyłanych za pośrednictwem IBM WebSphere MQ Managed File Transfer.

Zanim rozpoczniesz

Upewnij się, że w instalacji produktu WebSphere MQ jest zainstalowany komponent Advanced Message Security , który udostępnia kolejki używane przez produkt IBM WebSphere MQ Managed File Transfer , który ma być zabezpieczany.

Jeśli agenty IBM WebSphere MQ Managed File Transfer łączą się w trybie powiązań, upewnij się, że w lokalnej instalacji jest zainstalowany komponent GSKit.

O tym zadaniu

Gdy przesyłanie danych między dwoma agentami IBM WebSphere MQ Managed File Transfer jest przerwane, prawdopodobnie poufne dane mogą pozostać niezabezpieczone w bazowych kolejkach WebSphere MQ używanych do zarządzania przesyłaniem. W tym scenariuszu wyjaśniono sposób konfigurowania i używania programu Advanced Message Security w celu ochrony danych w kolejkach produktu IBM WebSphere MQ Managed File Transfer .

W tym scenariuszu rozważamy prostą topologię składającą się z jednej maszyny z dwiema kolejkami IBM WebSphere MQ Managed File Transfer i dwoma agentami, `AGENT1` i `AGENT2`, współużytkowaliśmy jeden menedżer kolejek `hubQM`, zgodnie z opisem w scenariuszu Podstawowe przesyłanie plików przy użyciu skryptów. Oba agenty łączą się w ten sam sposób, albo w trybie powiązań, jak i w trybie klienta.

1. Tworzenie certyfikatów

Zanim rozpoczniesz

W tym scenariuszu używany jest prosty model, w którym użytkownik `ftagent` w grupie `FTAGENTS` jest używany do uruchamiania procesów agenta IBM WebSphere MQ Managed File Transfer . Jeśli używane są własne nazwy użytkowników i grup, należy odpowiednio zmienić komendy.

O tym zadaniu

Produkt Advanced Message Security używa kryptografii klucza publicznego do podpisywania i/lub szyfrowania komunikatów w chronionych kolejkach.

Uwaga:

- Jeśli agenty IBM WebSphere MQ Managed File Transfer działają w trybie powiązań, komendy używane do tworzenia magazynu kluczy CMS (Cryptographic Message Syntax) są szczegółowo opisane w **Podręczniku szybkiego startu** (Windows lub UNIX) dla używanej platformy.
- Jeśli agenty IBM WebSphere MQ Managed File Transfer działają w trybie klienta, komendy, które będą potrzebne do utworzenia pliku JKS (Java Keystore), są szczegółowo opisane w podręczniku "Podręcznik Szybki start dla klientów Java" na stronie 294.

Procedura

1. Utwórz samopodpisany certyfikat, aby zidentyfikować użytkownika `ftagent` zgodnie z opisem w odpowiednim podręczniku Szybki start.
   Użyj nazwy wyróżniającej (DN) w następujący sposób:

   ```
   CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB
   ```

2. Utwórz plik `keystore.conf` , aby zidentyfikować położenie magazynu kluczy i certyfikat w nim, zgodnie ze szczegółowymi informacjami w odpowiednim podręczniku Szybki start.

2. Konfigurowanie ochrony komunikatów

O tym zadaniu

Należy zdefiniować strategię bezpieczeństwa dla kolejki danych używanej przez produkt AGENT2za pomocą komendy **setmqspl** . W tym scenariuszu ten sam użytkownik jest używany do uruchamiania obu agentów, dlatego nazwa wyróżniająca osoby podpisującej i odbiorcy są takie same i są zgodne z wygenerowanym przez nas certyfikatem.

Procedura

1. Należy zamknąć agenty IBM WebSphere MQ Managed File Transfer w celu przygotowania do ochrony za pomocą komendy **fteStopAgent** .
2. Utwórz strategię bezpieczeństwa, aby chronić kolejkę produktu SYSTEM.FTE.DATA.AGENT2 .

   ```
   setmqspl -m hubQM -p SYSTEM.FTE.DATA.AGENT2 -s SHA1 -a "CN=ftagent, OU=MFT, O=IBM,
   L=Hursley, ST=Hampshire, C=GB"
   -e AES128 -r "CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB"
   ```

3. Upewnij się, że użytkownik uruchamiający proces agenta IBM WebSphere MQ Managed File Transfer ma dostęp do przeglądania kolejki strategii systemowych i umieszczania komunikatów w kolejce błędów.

   ```
   setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p ftagent +browse
   setmqaut -m hubQM -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p ftagent +put
   ```

4. Zrestartuj agenty IBM WebSphere MQ Managed File Transfer za pomocą komendy **fteStartAgent** .
5. Upewnij się, że agenty zostały pomyślnie zrestartowane za pomocą komendy **fteListAgents** , a następnie sprawdź, czy agenty mają status READY .

Wyniki

Przesyłanie danych z produktu AGENT1 do produktu AGENT2jest teraz możliwe, a treść pliku zostanie bezpiecznie transmitowanych między tymi dwoma agentami.

instalowanieIBM WebSphere MQ Advanced Message Security

Zainstaluj komponent IBM WebSphere MQ Advanced Message Security na różnych platformach.

O tym zadaniu

Pełne procedury instalacyjne znajdują się w sekcji Instalowanie produktu IBM WebSphere MQ Advanced Message Security.

Zadania pokrewne

Deinstalacja produktuIBM WebSphere MQ Advanced Message Security

Korzystanie z magazynów kluczy i certyfikatów

Aby zapewnić przezroczystą ochronę szyfrującą dla aplikacji WebSphere MQ , program Advanced Message Security używa pliku kluczy, w którym przechowywane są certyfikaty klucza publicznego i klucz prywatny.

W produkcie Advanced Message Securityużytkownicy i aplikacje są reprezentowane przez tożsamości infrastruktury klucza publicznego (PKI). Ten typ tożsamości jest używany do podpisywania i szyfrowania komunikatów. Tożsamość PKI jest reprezentowana przez pole **nazwa wyróżniająca (DN)** podmiotu w certyfikacie, który jest powiązany z podpisanymi i zaszyfrowanymi komunikatami. Aby użytkownik lub aplikacja szyfruła swoje komunikaty, wymagają one dostępu do pliku kluczy, w którym przechowywane są certyfikaty i powiązane klucze prywatne i publiczne.

Położenie magazynu kluczy jest udostępniane w pliku konfiguracyjnym magazynu kluczy, który domyślnie jest `keystore.conf` . Każdy użytkownik produktu Advanced Message Security musi mieć plik konfiguracyjny magazynu kluczy wskazujący na plik kluczy. Advanced Message Security Akceptuje następujący format plików kluczy: `.kdb`, `.jceks`, `.jks`.

Domyślnym położeniem pliku `keystore.conf` jest:

- Na platformach UNIX : `$HOME/.mqs/keystore.conf`
- Na platformach Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Jeśli używana jest określona nazwa pliku kluczy i położenie, należy użyć następujących komend:

- W systemie Java: `java -D` *`MQS_KEYSTORE_CONF=path/filename app_name`*
- Dla klienta C i serwera:
  - W systemie UNIX and Linux: `export MQS_KEYSTORE_CONF=`*`path/filename`*
  - W systemie Windows: `set MQS_KEYSTORE_CONF=`*`path\filename`*

    Uwaga: Ścieżka na serwerze Windows może i powinna określać literę napędu, jeśli dostępna jest więcej niż jedna litera napędu.

Pojęcia pokrewne

“Nazwy wyróżniające nadawców” na stronie 319
Nazwy wyróżniające nadawcę (DN) identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce.

“Nazwy wyróżniające odbiorców” na stronie 320
Nazwy wyróżniające odbiorców (DN) identyfikują użytkowników, którzy są uprawnieni do pobierania komunikatów z kolejki.

Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf)

Plik konfiguracyjny magazynu kluczy (`keystore.conf`) wskazuje Advanced Message Security na położenie odpowiedniego magazynu kluczy.

Dostępne są dwa typy konfiguracji CMS i Java (JKS i JCEKS). Wpisy konfiguracji CMS są poprzedzane przedrostkiem `cms.` , a język Java jest poprzedzony przedrostkiem `jks.` lub `jceks.` , w zależności od typu magazynu kluczy.

Plik konfiguracyjny, w zależności od typu pliku konfiguracyjnego, może mieć jedną z następujących struktur:

```
cms.keystore = /<dir>/<keystore_file>
cms.certificate = certificate_label

jceks.keystore = <dir>/Keystore
jceks.certificate = <certificate_label>
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
```

```
jceks.provider = IBMJCE

jks.keystore = <dir>/Keystore
jks.certificate = <certificate_label>
jks.encrypted = no
jks.keystore_pass = <password>
jks.key_pass = <password>
jks.provider = IBMJCE
```

Parametry pliku konfiguracyjnego są zdefiniowane w następujący sposób:

keystore
Ścieżka do pliku kluczy.

Ważne:

- Ścieżka do pliku kluczy nie może zawierać rozszerzenia nazwy pliku.
- W przypadku plików kluczy Java produkt IBM WebSphere MQ AMS obsługuje następujące formaty plików: `.jks`, `.jceks`, `.jck`.

certificate
Etykieta certyfikatu.

encrypted
Status hasła.

keystore_pass
Hasło do pliku kluczy.

Uwaga:

- W przypadku magazynu kluczy CMS produkt IBM WebSphere MQ AMS opiera się na plikach ukrytych haseł (`.sth`), podczas gdy JKS i JCEKS mogą wymagać hasła zarówno dla certyfikatu, jak i klucza prywatnego użytkownika.
- Przechowywanie haseł w zwykłym tekście stanowi zagrożenie dla bezpieczeństwa.

key_pass
Hasło dla klucza prywatnego użytkownika.

Ważne: Przechowywanie haseł w postaci zwykłego tekstu może stanowić zagrożenie dla bezpieczeństwa.

provider
Dostawca zabezpieczeń Java, który implementuje algorytmy szyfrowania wymagane przez certyfikat magazynu kluczy.

Uwaga: Obecnie IBMJCE jest jedynym dostawcą, który jest obsługiwany przez produkt Advanced Message Security.

Ważne: Informacje przechowywane w magazynie kluczy są kluczowe dla bezpiecznego przepływu danych wysyłanych za pomocą programu WebSphere MQ, dlatego administratorzy zabezpieczeń muszą zwracać szczególną uwagę podczas przypisywania uprawnień do tych plików.

Poniżej przedstawiono przykład pliku `keystore.conf` :

```
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE
```

Zadania pokrewne

“Ochrona haseł w języku Java” na stronie 316

Zapisywanie haseł kluczy i kluczy prywatnych jako zwykłego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego produkt Advanced Message Security udostępnia narzędzie, które może scramować te hasła przy użyciu klucza użytkownika, który jest dostępny w pliku kluczy.

Przechwytywanie agenta kanału komunikatów (MCA)

Przechwytywanie MCA umożliwia menedżerowi kolejek działającym w ramach programu IBM WebSphere MQ selektywne włączanie strategii, które mają być stosowane dla kanałów połączenia z serwerem.

Przechwytywanie agenta MCA umożliwia klientom pozostawanie poza programem IBM WebSphere MQ AMS , aby nadal były połączone z menedżerem kolejek, a ich komunikaty są szyfrowane i deszyfrowane.

Przechwytywanie MCA ma na celu udostępnienie możliwości IBM WebSphere MQ AMS , gdy nie można włączyć IBM WebSphere MQ AMS na kliencie. Należy zauważyć, że użycie przechwytywania MCA i klienta z włączoną obsługą IBM WebSphere MQ AMSprowadzi do podwójnej ochrony komunikatów, które mogą być problematyczne w przypadku odbierania aplikacji.

Jeśli błąd 2085 (MQRC_UNKNOWN_OBJECT_NAME) jest zgłaszany wtedy, gdy do łączenia się z menedżerem kolejek z wcześniejszej wersji produktu używany jest klient Version 7.5 lub nowszy, należy wyłączyć produkt IBM WebSphere MQ Advanced Message Security na kliencie. Więcej informacji na ten temat zawiera sekcja “Wyłączanie produktu IBM WebSphere MQ Advanced Message Security na kliencie” na stronie 309.

Plik konfiguracyjny magazynu kluczy

Domyślnie plik konfiguracyjny magazynu kluczy dla przechwytywacza MCA ma wartość `keystore.conf` i znajduje się w katalogu `.mqs` w ścieżce katalogu HOME użytkownika, który uruchomił menedżer kolejek lub program nasłuchujący. Magazyn kluczy można również skonfigurować za pomocą zmiennej środowiskowej MQS_KEYSTORE_CONF. Więcej informacji na temat konfigurowania magazynu kluczy IBM WebSphere MQ AMS zawiera sekcja “Korzystanie z magazynów kluczy i certyfikatów” na stronie 305.

Aby włączyć przechwytywanie agenta MCA, należy podać nazwę kanału, który ma być używany w pliku konfiguracyjnym magazynu kluczy. W przechwytywaniu agenta MCA można użyć tylko typu magazynu kluczy cms.

Przykład konfigurowania przechwytywacza MCA zawiera sekcja “Przykład przechwytywacza IBM WebSphere MQ AMS MCA” na stronie 307.

Ostrzeżenie: Aby zapewnić, że tylko autoryzowani klienci mogą łączyć się i korzystać z tej możliwości, należy wykonać uwierzytelnianie klienta i szyfrowanie na wybranych kanałach, na przykład za pomocą protokołu SSL i SSLPEER lub CHLAUTH TYPE (SSLPEERMAP).

Przykład przechwytywacza IBM WebSphere MQ AMS MCA

Przykładowe zadanie dotyczące konfigurowania przechwytywacza MCA produktu IBM WebSphere MQ AMS .

Zanim rozpoczniesz

Ostrzeżenie: Aby zapewnić, że tylko autoryzowani klienci mogą łączyć się i korzystać z tej możliwości, należy wykonać uwierzytelnianie klienta i szyfrowanie na wybranych kanałach, na przykład za pomocą protokołu SSL i SSLPEER lub CHLAUTH TYPE (SSLPEERMAP).

O tym zadaniu

To zadanie prowadzi użytkownika przez proces konfigurowania systemu do użycia przechwytywacza MCA, a następnie sprawdzania konfiguracji.

Uwaga: W wersjach wcześniejszych niż IBM WebSphere MQ Version 7.5produkt IBM WebSphere MQ AMS był produktem dodatkowym, który musi być oddzielnie zainstalowany, a przechwytywacze skonfigurowane do zabezpieczania aplikacji. Począwszy od wersji Version 7.5 , przechwytywacze są automatycznie włączane i włączane dynamicznie w środowiskach wykonawczych klienta i serwera

MQ . W tym przykładowym przechwytywaniu MCA przechwytywacze są udostępniane na końcu kanału serwera, a starsze środowisko wykonawcze klienta jest używane (w kroku 12) w celu umieszczania niechronionych komunikatów w kanale, tak aby można było zobaczyć je w celu ochrony przez przechwytywacze MCA. Jeśli w tym przykładzie użyto klienta Version 7.5 lub nowszego, to komunikat zostanie dwukrotnie zabezpieczony, ponieważ przechwytywacz środowiska wykonawczego klienta MQ i przechwytywacz agenta MCA będą chronić komunikat w taki sposób, w jaki jest on dostarczany do produktu MQ.

Ostrzeżenie: Zastąp wartość `userID` w kodzie identyfikatorem użytkownika.

Procedura

1. Utwórz bazę danych kluczy i certyfikaty, korzystając z następujących komend, aby utworzyć skrypt powłoki.

   Należy również zmienić **INSTLOC** i **KEYSTORELOC** lub uruchomić wymagane komendy. Należy pamiętać, że utworzenie certyfikatu dla produktu `bob`może nie być konieczne.

```
INSTLOC=/opt/mq75
KEYSTORELOC=/home/testusr/ssl/ams1
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. Współużytkuj certyfikaty między dwoma kluczowymi bazami danych, aby każdy użytkownik mógł pomyślnie zidentyfikować inne bazy danych.

   Ważne jest, aby użyć metody opisanej w **Czynność 5. Współużytkowanie certyfikatów** w **Podręczniku szybkiego startu** (Windows lub UNIX).

3. Utwórz produkt `keystore.conf` z następującą konfiguracją: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. Tworzenie i uruchamianie menedżera kolejek `AMSQMGR1`
5. Zdefiniuj nasłuchiwanie z *portem* `14567` i *elementem sterującym* `QMGR`
6. Wyłącz uprawnienia kanału lub ustaw reguły dla uprawnień kanału.

   Więcej informacji na ten temat zawiera sekcja SET CHLAUTH .

7. Zatrzymaj menedżer kolejek.
8. Ustaw magazyn kluczy:

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

9. Uruchom menedżer kolejek w tej samej powłoce.
10. Ustaw strategię bezpieczeństwa i sprawdź:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

    Więcej informacji na ten temat można znaleźć w sekcji setmqspl i dspmqspl .

11. Ustaw konfigurację kanału:

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Uruchom program **amqsputc** z klienta MQ , który nie włącza automatycznie przechwytywacza MCA, na przykład klienta IBM WebSphere MQ Version 7.1 lub wcześniejszego. Umieść następujące dwa komunikaty:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Usuń strategię bezpieczeństwa i sprawdź wynik:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

14. Przeglądaj kolejkę z poziomu instalacji produktu IBM WebSphere MQ Version 7.5 :

```
/opt/mq75/samp/bin/amqsbcg TESTQ AMSQMGR1
```

Dane wyjściowe przeglądania przedstawiają komunikaty w postaci zaszyfrowanej.

15. Ustaw strategię bezpieczeństwa i sprawdź wynik:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

16. Uruchom program **amqsgetc** z poziomu instalacji produktu IBM WebSphere MQ Version 7.5 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Zadania pokrewne

“Podręcznik Szybki start dla klientów Java” na stronie 294
Ten podręcznik służy do szybkiego konfigurowania produktu IBM Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów dla aplikacji Java łączących się przy użyciu powiązań klienta. Po zakończeniu tego procesu utworzony zostanie magazyn kluczy w celu weryfikacji tożsamości użytkowników oraz zdefiniowanych strategii podpisywania i szyfrowania dla menedżera kolejek.

Odsyłacze pokrewne

“Znane ograniczenia” na stronie 282
Informacje na temat ograniczeń produktu IBM WebSphere MQ Advanced Message Security.

Wyłączanie produktu IBM WebSphere MQ Advanced Message Security na kliencie

Jeśli do nawiązania połączenia z menedżerem kolejek z wcześniejszej wersji produktu jest używany klient Version 7.5 lub nowszy, należy wyłączyć program IBM WebSphere MQ Advanced Message Security (AMS) klienta, a zgłoszony zostanie błąd 2085 (MQRC_UNKNOWN_OBJECT_NAME).

O tym zadaniu

Począwszy od wersji Version 7.5produkt IBM WebSphere MQ Advanced Message Security (AMS) jest automatycznie włączany w kliencie IBM WebSphere MQ , więc domyślnie klient próbuje sprawdzić strategie zabezpieczeń dla obiektów w menedżerze kolejek. Jednak serwery we wcześniejszych wersjach produktu, na przykład Version 7.1, nie mają włączonego produktu AMS , co powoduje zgłoszenie błędu 2085 (MQRC_UNKNOWN_OBJECT_NAME).

Jeśli ten błąd zostanie zgłoszony, podczas próby nawiązania połączenia z menedżerem kolejek z wcześniejszej wersji produktu AMS można wyłączyć na kliencie w następujący sposób:

- W przypadku klientów Java , w dowolny z następujących sposobów:
  - V 7.5.0.4 W tym celu należy ustawić zmienną środowiskową AMQ_DISABLE_CLIENT_AMS.
  - V 7.5.0.4 Ustawiając właściwość systemową Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.

– V 7.5.0.5 Za pomocą właściwości AMS DisableClient, w sekcji **Security** w pliku `mqclient.ini` .

- W przypadku klientów C wykonaj jedną z następujących czynności:
  – V 7.5.0.4 W tym celu należy ustawić zmienną środowiskową AMQ_DISABLE_CLIENT_AMS.
  – V 7.5.0.5 Za pomocą właściwości AMS DisableClient, w sekcji **Security** w pliku `mqclient.ini` .

Procedura

- Aby wyłączyć program AMS na kliencie, należy użyć jednej z następujących opcji:

  V 7.5.0.4 **Zmienna środowiskowa AMQ_DISABLE_CLIENT_AMS**
  Zmienną tę należy ustawić w następujących przypadkach:
  – Jeśli używane jest środowisko wykonawcze Java (JRE) inne niż środowisko IBM Java Runtime Environment (JRE)
  – Jeśli używany jest klient Version 7.5lub nowszy, klient IBM WebSphere MQ classes for Java lub klient IBM WebSphere MQ classes for JMS .

  Można również użyć komendy AMQ_DISABLE_CLIENT_AMS w celu wyłączenia funkcjonalności produktu AMS dla klientów C.

  Utwórz zmienną środowiskową AMQ_DISABLE_CLIENT_AMS i ustaw ją na wartość TRUE w środowisku, w którym aplikacja jest uruchomiona. Na przykład:

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

  V 7.5.0.4 **Właściwość systemowa com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS**
  W przypadku klientów IBM WebSphere MQ classes for JMS i IBM WebSphere MQ classes for Java ustaw właściwość systemową Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS na wartość TRUE dla aplikacji Java .

  Na przykład można ustawić właściwość systemową Java jako opcję `-D` , gdy wywoływana jest komenda Java :

  ```
  java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/
  com.ibm.mqjms.jar  my.java.applicationClass
  ```

  Alternatywnie można określić właściwość systemową Java w pliku konfiguracyjnym JMS , `jms.config`, jeśli aplikacja korzysta z tego pliku.

  V 7.5.0.5 **Właściwość `DisableClientAMS` w pliku `mqclient.ini`**
  W przypadku klientów IBM WebSphere MQ classes for JMS i IBM WebSphere MQ classes for Java oraz dla klientów C dodaj nazwę właściwości `DisableClientAMS` w sekcji **Security** w pliku `mqclient.ini` , jak pokazano w poniższym przykładzie:

  ```
  Security:
  DisableClientAMS=Yes
  ```

  Można również włączyć program AMS , tak jak pokazano to w poniższym przykładzie:

  ```
  Security:
  DisableClientAMS=No
  ```

Co dalej

Więcej informacji na temat problemów z otwieraniem kolejek chronionych produktu AMS zawiera sekcja “Problemy podczas otwierania chronionych kolejek podczas korzystania z produktu JMS” na stronie 334.

Pojęcia pokrewne
“Przechwytywanie agenta kanału komunikatów (MCA)” na stronie 307

Przechwytywanie MCA umożliwia menedżerowi kolejek działającym w ramach programu IBM WebSphere MQ selektywne włączanie strategii, które mają być stosowane dla kanałów połączenia z serwerem.

Zadania pokrewne

Konfigurowanie klienta przy użyciu pliku konfiguracyjnego

Odsyłacze pokrewne

Plik konfiguracyjny IBM WebSphere MQ classes for JMS

Wymagania dotyczące certyfikatów dla AMS

Certyfikaty muszą mieć klucz publiczny RSA, aby można go było używać z produktem Advanced Message Security.

Więcej informacji na temat różnych typów kluczy publicznych i sposobu ich tworzenia zawiera sekcja “Certyfikaty cyfrowe i zgodność ze specyfikacją CipherSpec w produkcie IBM WebSphere MQ” na stronie 35.

Rozszerzenia użycia klucza

Rozszerzenia dotyczące użycia kluczy nakładają dodatkowe ograniczenia na sposób, w jaki można używać certyfikatu.

W produkcie Advanced Message Securityużycie klucza musi być ustawione w następujący sposób: w przypadku certyfikatów w standardzie X.509 V3 lub nowszym, które są używane na potrzeby integralności zabezpieczeń, jeśli ustawione są rozszerzenia klucza, muszą one zawierać co najmniej jedną z dwóch następujących wartości:

- **nonRepudiation**
- **digitalSignature**

W celu zapewnienia jakości ochrony prywatności, jeśli ustawione są rozszerzenia użycia klucza, muszą one również zawierać rozszerzenie **keyEncipherment** .

Pojęcia pokrewne

“Jakość ochrony” na stronie 322

Strategie ochrony danych Advanced Message Security oznaczają jakość ochrony (QOP).

Metody sprawdzania poprawności certyfikatów w produkcie IBM WebSphere MQ Advanced Message Security

Za pomocą programu IBM WebSphere MQ Advanced Message Security można wykrywać i odrzucać odwołane certyfikaty, tak aby komunikaty w kolejkach nie były chronione przy użyciu certyfikatów, które nie spełniają standardów bezpieczeństwa.

Program IBM WebSphere MQ AMS umożliwia sprawdzenie poprawności certyfikatu przy użyciu protokołu OCSP (Online Certificate Status Protocol) lub listy odwołań certyfikatów (CRL).

Produkt IBM WebSphere MQ AMS można skonfigurować zarówno dla sprawdzania OCSP, jak i sprawdzania listy CRL. Jeśli obie metody są włączone, ze względu na wydajność produkt IBM WebSphere MQ AMS najpierw używa protokołu OCSP w celu uzyskania statusu odwołania. Jeśli status odwołania certyfikatu jest nieokreślony po sprawdzeniu OCSP, IBM WebSphere MQ AMS korzysta z sprawdzania listy CRL.

Pojęcia pokrewne

“Protokół OCSP (Online Certificate Status Protocol)” na stronie 312

Protokół OCSP (Online Certificate Status Protocol) określa, czy certyfikat został odwołany, a co za tym jest, pomaga w określeniu, czy certyfikat może być zaufany.

“Listy odwołań certyfikatów (CRL)” na stronie 313

Listy CRL przechowują listę certyfikatów, które zostały oznaczone przez ośrodek certyfikacji (CA), ponieważ nie są już zaufane z różnych powodów, na przykład klucz prywatny został utracony lub skompromikowany.

Protokół OCSP (Online Certificate Status Protocol)

Protokół OCSP (Online Certificate Status Protocol) określa, czy certyfikat został odwołany, a co za tym jest, pomaga w określeniu, czy certyfikat może być zaufany.

Włączanie sprawdzania OCSP w przechwytywaczach rodzimych

Aby włączyć sprawdzanie przez protokół OCSP (Online Certificate Status Protocol) w produkcie Advanced Message Security, należy zmodyfikować plik konfiguracyjny magazynu kluczy.

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego magazynu kluczy:

Uwaga: Wartości poszczególnych opcji podane w tabeli są wartościami domyślnymi.

Należy podać jedną z następujących wartości:

- `ocsp.enable=on`
- `ocsp.url=<reposnder_URL>`
- `ocsp.http.proxy.host=<OCSP_proxy>`

Opcja	Opis
`ocsp.enable=off`	Włączenie sprawdzania OCSP, jeśli sprawdzany certyfikat ma rozszerzenie Authority Info Access z metodą dostępu PKIX_AD_OCSP zawierającą identyfikator URI położenia modułu odpowiadającego OCSP. Możliwe wartości: `on`/`off` (włączone/wyłączone).
`ocsp.url=<reposnder_URL>`	Adres URL modułu odpowiadającego OCSP.
`ocsp.http.proxy.host=<OCSP_proxy>`	Adres URL serwera proxy OCSP.
`ocsp.http.proxy.port=<port_number>`	Numer portu serwera proxy OCSP.
`ocsp.nonce.generation=on/off`	Generowanie wartości jednorazowej podczas wysyłania zapytań do protokołu OCSP. Wartością domyślną jest `off`.
`ocsp.nonce.check=on/off`	Sprawdzanie wartości jednorazowej po odebraniu odpowiedzi z protokołu OCSP. Wartością domyślną jest `off`.
`ocsp.nonce.size=8`	Wielkość wartości jednorazowej w bajtach.
`ocsp.http.get=on/off`	Określenie metody HTTP GET jako metody żądania. Jeśli ta opcja jest ustawiona na wartość `off` (wyłączone), używana jest metoda HTTP POST.
`ocsp.max_response_size=20480`	Wielkość maksymalna odpowiedzi z modułu odpowiadającego OCSP podana w bajtach.
`ocsp.cache_size=100`	Włączenie wewnętrznego buforowania odpowiedzi OCSP i ustawienie limitu dla liczby wpisów w pamięci podręcznej.
`ocsp.timeout=30`	Czas oczekiwania na odpowiedź serwera (w sekundach), po których nastąpi przekroczenie limitu czasu dla produktu Advanced Message Security.

Włączanie sprawdzania protokołu OCSP w środowisku Java
Aby włączyć sprawdzanie protokołu OCSP dla języka Java w produkcie Advanced Message Security, należy zmodyfikować plik `java.security` lub plik konfiguracyjny magazynu kluczy.

O tym zadaniu

Istnieją dwa sposoby włączania sprawdzania protokołu OCSP w produkcie Advanced Message Security:

Korzystanie z java.security
Sprawdź, czy certyfikat ma skonfigurowany dostęp do informacji o uprawnieniach (Authority Information Access-AIA).

Procedura

1. Jeśli program AIA nie został skonfigurowany lub użytkownik chce przesłonić certyfikat, należy zmodyfikować plik `$JAVA_HOME/lib/security/java.security` o następujących właściwościach:

   ```
   ocsp.responderURL=http://url.to.responder:port
   ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
   ```

   i włączyć sprawdzanie protokołu OCSP, edytując plik `$JAVA_HOME/lib/security/java.security` za pomocą następującego wiersza:

   ```
   ocsp.enable=true
   ```

2. Jeśli program AIA jest skonfigurowany, włącz sprawdzanie protokołu OCSP, edytując plik `$JAVA_HOME/lib/security/java.security` w następujący sposób:

   ```
   ocsp.enable=true
   ```

Co dalej

Jeśli używany jest program Java Security Manager, należy wykonać konfigurację, dodać następujące uprawnienie Java do produktu `lib/security/java.policy` .

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

Korzystanie z pliku keystore.conf

Procedura

Dodaj następujący atrybut do pliku konfiguracyjnego:

```
ocsp.enable=true
```

Ważne: Ustawienie tego atrybutu w pliku konfiguracyjnym nadpisuje ustawienia java.security .

Co dalej

Aby zakończyć konfigurowanie, dodaj następujące uprawnienia Java do produktu `lib/security/java.policy`:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Listy odwołań certyfikatów (CRL)

Listy CRL przechowują listę certyfikatów, które zostały oznaczone przez ośrodek certyfikacji (CA), ponieważ nie są już zaufane z różnych powodów, na przykład klucz prywatny został utracony lub skompromikowany.

W celu sprawdzenia poprawności certyfikatów program Advanced Message Security tworzy łańcuch certyfikatów, który składa się z certyfikatu osoby podpisującej oraz łańcucha certyfikatów ośrodka

certyfikacji (CA) aż do bazy zaufania. Baza zaufania jest zaufanym plikiem kluczy, który zawiera zaufany certyfikat lub zaufany certyfikat główny, który jest używany do potwierdzania zaufania certyfikatu.IBM WebSphere MQ AMS weryfikuje ścieżkę certyfikatu przy użyciu algorytmu sprawdzania poprawności PKIX. Po utworzeniu i zweryfikowaniu łańcucha program IBM WebSphere MQ AMS kończy sprawdzanie poprawności certyfikatu, które obejmuje sprawdzenie poprawności daty wydania i daty ważności każdego certyfikatu w łańcuchu na podstawie bieżącej daty, sprawdzenie, czy rozszerzenie użycia klucza znajduje się w certyfikacie jednostki końcowej. Jeśli rozszerzenie jest dopisane do certyfikatu, produkt IBM WebSphere MQ AMS sprawdza, czy ustawione są także wartości **digitalSignature** lub **nonRepudiation** . Jeśli nie są one, `MQRC_SECURITY_ERROR` jest raportowane i rejestrowane. Następnie program IBM WebSphere MQ AMS pobiera listy CRL z plików lub z katalogu LDAP w zależności od wartości określonych w pliku konfiguracyjnym. IBM WebSphere MQ AMSObsługuje tylko listy CRL, które są kodowane w formacie DER. Jeśli w pliku konfiguracyjnym magazynu kluczy nie zostanie znaleziona żadna konfiguracja związana z CRL, program IBM WebSphere MQ AMS nie sprawdza poprawności listy CRL. Dla każdego certyfikatu ośrodka CA produkt IBM WebSphere MQ AMS wysyła zapytania LDAP do list CRL, używając nazw wyróżniających CA, aby znaleźć listę CRL. W zapytaniu LDAP znajdują się następujące atrybuty:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Uwaga: Produkt `deltaRevocationList` jest obsługiwany tylko wtedy, gdy jest określony jako punkty dystrybucji.

Włączanie obsługi sprawdzania poprawności certyfikatu i listy odwołań certyfikatów w przechwytywaczami rodzimych
Konieczne jest zmodyfikowanie pliku konfiguracyjnego magazynu kluczy, aby program Advanced Message Security mógł pobrać CLRs z serwera LDAP (Lightweight Directory Access Protocol).

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego:

Uwaga: Wartości poszczególnych opcji podane w tabeli są wartościami domyślnymi.

Opcja	**Opis**
`crl.ldap.host=<`*`host_name`*`>`	Nazwa hosta serwera LDAP.
`crl.ldap.port=<`*`port_number`*`>`	Numer portu serwera LDAP. Można określić do 11 serwerów. Wiele hostów LDAP jest używanych w celu zapewnienia przezroczystego przełączania awaryjnego w przypadku awarii połączenia LDAP. Oczekuje się, że wszystkie serwery LDAP będą replikami i będą zawierać te same dane. Gdy przechwytywacz języka Java produktu IBM WebSphere MQ AMS pomyślnie nawiąże połączenie z serwerem LDAP, nie podejmuje próby pobrania list CRL z pozostałych udostępnionych serwerów.
`crl.cdp=off`	Ta opcja służy do sprawdzania lub używania rozszerzeń CRLDistributionPoints w certyfikatach.
`crl.ldap.version=3`	Numer wersji protokołu LDAP. Możliwe wartości: 2 lub 3.

Opcja	Opis
`crl.ldap.user=cn=<username>`	Zaloguj się na serwerze LDAP. Jeśli ta wartość nie zostanie podana, atrybuty CRL w katalogu LDAP muszą być odczytywane na poziomie światowym.
`crl.ldap.pass=<password>`	Hasło dla serwera LDAP.
`crl.ldap.cache_lifetime=0`	Czas życia pamięci podręcznej LDAP w sekundach. Możliwe wartości: 0-86400.
`crl.ldap.cache_size=50`	Wielkość pamięci podręcznej LDAP. Tę opcję można określić tylko wtedy, gdy wartość `crl.ldap.cache_lifetime` jest większa niż `0`.
`crl.http.proxy.host=some.host.com`	Port serwera proxy HTTP dla pobierania CRL CDP.
`crl.http.proxy.port=8080`	Numer portu serwera proxy HTTP.
`crl.http.max_response_size=204800`	Maksymalna wielkość CRL (w bajtach), która może zostać pobrana z serwera HTTP zaakceptowanego przez pakiet GSKit.
`crl.http.timeout=30`	Czas oczekiwania na odpowiedź serwera, w sekundach, po upływie którego IBM WebSphere MQ AMS przekroczeń limitu czasu.
`crl.http.cache_size=0`	Wielkość pamięci podręcznej HTTP w bajtach.

Włączanie obsługi listy odwołań certyfikatów w języku Java
Aby włączyć obsługę list CRL w programie Advanced Message Security, należy zmodyfikować plik konfiguracyjny magazynu kluczy, aby umożliwić programowi IBM WebSphere MQ AMS pobieranie list CRL z serwera LDAP (Lightweight Directory Access Protocol) i skonfigurowanie pliku java.security .

Procedura

1. Dodaj następujące opcje do pliku konfiguracyjnego:

Nagłówek	Opis
`crl.ldap.host=<host_name>`	Nazwa hosta LDAP.
`crl.ldap.port=<port_number>`	Numer portu serwera LDAP. Można określić do 11 serwerów. Wiele hostów LDAP jest używanych w celu zapewnienia przezroczystego przełączania awaryjnego w przypadku awarii połączenia LDAP. Oczekuje się, że wszystkie serwery LDAP będą replikami i będą zawierać te same dane. Gdy przechwytywacz języka Java produktu IBM WebSphere MQ AMS pomyślnie nawiąże połączenie z serwerem LDAP, nie podejmuje próby pobrania list CRL z pozostałych udostępnionych serwerów. Język Java nie używa wartości `crl.ldap.user` i crl.ldaworldp.pass . Podczas nawiązywania połączenia z serwerem LDAP nie jest używany użytkownik i hasło. W związku z tym atrybuty CRL w LDAP muszą być odczytywane na poziomie światowym.

Nagłówek	Opis
`crl.cdp=on/off`	Ta opcja służy do sprawdzania lub używania rozszerzeń CRLDistributionPoints w certyfikatach.

2. Zmodyfikuj plik `JRE/lib/security/java.security` przy użyciu następujących właściwości:

Nazwa właściwości	Opis
`com.ibm.security.enableCRLDP`	Ta właściwość przyjmuje następujące wartości: `true`, `false`. Jeśli jest ona ustawiona na wartość `true`, podczas sprawdzania odwołania certyfikatu, listy CRL są umieszczane przy użyciu adresu URL z rozszerzenia listy punktów dystrybucji CRL certyfikatu. Jeśli opcja ta jest ustawiona na wartość `false` lub nie jest ustawiona, sprawdzanie listy CRL za pomocą rozszerzenia punktów dystrybucji CRL jest wyłączone.
`ibm.security.certpath.ldap.cache.lifetime`	Ta właściwość może być używana do ustawiania czasu życia pozycji w pamięci podręcznej LDAP CertStore do wartości w sekundach. Wartość równa 0 wyłącza pamięć podręczną; wartość -1 oznacza nieograniczony czas życia. Jeśli wartość nie zostanie ustawiona, domyślny czas życia wynosi 30 sekund.
`com.ibm.security.enableAIAEXT`	Ta właściwość przyjmuje następujące wartości: `true`, `false`. Jeśli jest ustawiona na wartość `true`, wszystkie rozszerzenia dostępu do informacji o uprawnieniach, które znajdują się w certyfikatach budowanej ścieżki certyfikatu, są sprawdzane w celu określenia, czy zawierają identyfikatory URI LDAP. Dla każdego znalezionego identyfikatora URI LDAP tworzony jest obiekt LDAPCertStore , który jest dodawany do kolekcji CertStores , która jest używana do znajdowania innych certyfikatów wymaganych do zbudowania ścieżki certyfikatu. Jeśli jest ustawiona na wartość `false` lub nie jest ustawiona, dodatkowe obiekty LDAPCertStore nie są tworzone.

Ochrona haseł w języku Java

Zapisywanie haseł kluczy i kluczy prywatnych jako zwykłego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego produkt Advanced Message Security udostępnia narzędzie, które może scramować te hasła przy użyciu klucza użytkownika, który jest dostępny w pliku kluczy.

Zanim rozpoczniesz

Właściciel pliku `keystore.conf` musi mieć pewność, że tylko właściciel pliku będzie uprawniony do odczytu tego pliku. Ochrona haseł opisana w niniejszym rozdziale stanowi jedynie dodatkowy środek ochrony.

Procedura

1. Zmodyfikuj pliki produktu `keystore.conf` , tak aby uwzględniała ścieżkę do magazynu kluczy i etykiety użytkowników.

   ```
   jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
   jceks.certificate = AliceCert
   jceks.provider = IBMJCE
   ```

2. Aby uruchomić narzędzie, wykonaj następujące czynności:

   ```
   java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
   private_key_password
   ```

   Dane wyjściowe z zaszyfrowanymi hasłami są generowane i mogą być kopiowane do pliku `keystore.conf` .

   Aby automatycznie skopiować dane wyjściowe do pliku `keystore.conf` , uruchom komendę:

   ```
   java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
   private_key_password >> ~/<path_to_keystore>/keystore.conf
   ```

   Uwaga:

   Listę domyślnych położeń produktu `keystore.conf` na różnych platformach można znaleźć w sekcji “Korzystanie z magazynów kluczy i certyfikatów” na stronie 305.

Przykład

Poniżej przedstawiono przykład takich danych wyjściowych:

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5ZOr8uRlJmc5qity9MN2CggGBMKCDxdbn1AyPklvdgTsOLG6X3C1YT7oDzwaqZFlOR4t\r\nm
Zsc7JGAx8nqqxLnAucdGn0NWo6xnjZB1n501YGol2k/
PhaQHhFXKMAU9dKg0f8djOtCAOlX4ETe\r\nfYl9LBUt2wk87uM7dSs\=
jceks.keystore_pass=OIdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
\r\nCUvQgu9GuaBMJK2F2OjtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTkDouLaTYTQeulyG0xIl\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

Administrowanie strategiami bezpieczeństwa produktu IBM WebSphere MQ Advanced Message Security

Produkt IBM WebSphere MQ Advanced Message Security używa strategii bezpieczeństwa w celu określenia szyfrowania szyfrowania i algorytmów podpisu do szyfrowania i uwierzytelniania komunikatów przepływających przez kolejki.

Przegląd strategii bezpieczeństwa

Strategie bezpieczeństwa IBM Advanced Message Security są obiektami koncepcyjnymi opisujących sposób szyfrowania i szyfrowania komunikatu.

Szczegółowe informacje na temat atrybutów strategii bezpieczeństwa można znaleźć w następujących podtematach:

Pojęcia pokrewne

“Jakość ochrony” na stronie 322
Strategie ochrony danych Advanced Message Security oznaczają jakość ochrony (QOP).

“Atrybuty strategii bezpieczeństwa” na stronie 321
Za pomocą programu Advanced Message Security można wybrać określony algorytm lub metodę w celu ochrony danych.

Nazwa strategii
Nazwa strategii to unikalna nazwa, która identyfikuje konkretną strategię Advanced Message Security i kolejkę, do której ma ona zastosowanie.

Nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma ona zastosowanie. Istnieje odwzorowanie jeden-do-jednego między strategią Advanced Message Security (IBM WebSphere MQ AMS) a kolejką.

Tworząc strategię o tej samej nazwie, co kolejka, należy aktywować strategię dla tej kolejki. Kolejki bez zgodnych nazw strategii nie są chronione przez produkt IBM WebSphere MQ AMS.

Zasięg strategii jest odpowiedni dla lokalnego menedżera kolejek i jego kolejek. Menedżerowie kolejek zdalnych muszą mieć własne strategie zdefiniowane lokalnie dla kolejek, którymi zarządzają.

Algorytm podpisu
Algorytm podpisu wskazuje algorytm, który powinien być używany przy podpisywaniu komunikatów danych.

Poprawne wartości to:

- MD5
- SHA-1
- SHA-2 Rodzina:
  - SHA256
  - SHA384 (minimalna dopuszczalna długość klucza-768 bitów)
  - SHA512 (minimalna dopuszczalna długość klucza-768 bitów)

Strategia, która nie określa algorytmu podpisywania, lub określa algorytm NONE, oznacza, że komunikaty umieszczone w kolejce powiązanej z tą strategią nie są podpisywane.

Uwaga: Jakość ochrony używana dla funkcji put i get komunikatu musi być zgodna. Jeśli istnieje niezgodność strategii jakości ochrony między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno dla kolejek lokalnych, jak i zdalnych.

Algorytm szyfrowania
Algorytm szyfrowania wskazuje algorytm, który powinien być używany przy szyfrowaniu komunikatów danych umieszczanych w kolejce powiązanej z tą strategią.

Poprawne wartości to:

- RC2
- DES
- 3DES
- AES128
- AES256

Strategia, która nie określa algorytmu szyfrowania lub określa algorytm programu NONE , oznacza, że komunikaty umieszczone w kolejce powiązanej z strategią nie są szyfrowane.

Należy zauważyć, że strategia, która określa algorytm szyfrowania inny niż NONE , musi również określać co najmniej jedną nazwę wyróżniającą (DN) odbiorców i algorytm podpisu, ponieważ zaszyfrowane komunikaty Advanced Message Security również są podpisywane.

Ważne: Jakość ochrony używana dla funkcji put i get komunikatu musi być zgodna. Jeśli istnieje niezgodność strategii jakości ochrony między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno dla kolejek lokalnych, jak i zdalnych.

Tolerancja

Atrybut tolerowania wskazuje, czy IBM Advanced Message Security może akceptować komunikaty bez określonej strategii bezpieczeństwa.

W przypadku pobierania komunikatu z kolejki ze strategią na potrzeby szyfrowania komunikatów, jeśli komunikat nie jest zaszyfrowany, jest on zwracany do aplikacji wywołującej. Poprawne wartości to:

0
Nie (**wartość domyślna**).

1
Tak.

Strategia, która nie określa wartości tolerancji lub określa 0, oznacza, że komunikaty umieszczone w kolejce powiązanej z tą strategią muszą być zgodne z regułami strategii.

Tolerancja jest opcjonalna i istnieje, aby ułatwić wycofanie konfiguracji, w której strategie były stosowane do kolejek, ale te kolejki zawierają już komunikaty, dla których nie określono strategii bezpieczeństwa.

Nazwy wyróżniające nadawców

Nazwy wyróżniające nadawcę (DN) identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce.

Produkt IBM Advanced Message Security (IBM WebSphere MQ AMS) nie sprawdza, czy komunikat został umieszczony w kolejce zabezpieczonej danych przez poprawnego użytkownika, dopóki nie zostanie on pobrany. W tym momencie, jeśli strategia określa co najmniej jednego poprawnego nadawcę, a użytkownik, który umieścił komunikat w kolejce nie znajduje się na liście poprawnych nadawców, produkt IBM WebSphere MQ AMS zwraca błąd do aplikacji pobierającej oraz umieszcza komunikat w swojej kolejce błędów.

Strategia może mieć określonych zero lub więcej nazw wyróżniających nadawców. Jeśli nie określono żadnych nazw wyróżniających nadawców dla strategii, dowolny użytkownik może umieścić w kolejce komunikaty z danymi chronionymi, pod warunkiem, że certyfikat użytkownika jest zaufany.

Nazwy wyróżniające nadawców mają następującą formę:

```
CN=Common Name,O=Organization,C=Country
```

Ważne:

- Wszystkie nazwy wyróżniające muszą być zapisane wielkimi literami. Wszystkie identyfikatory nazw komponentów w nazwie wyróżniającej muszą być określone w kolejności przedstawionej w poniższej tabeli:

Nazwa komponentu	Wartość
CN	Nazwa zwykła obiektu tej nazwy DN, taka jak pełna nazwa lub zamierzony cel urządzenia.
OU	Jednostka w organizacji, z którą jest powiązany obiekt nazwy wyróżniającej, np. dział korporacyjny lub nazwa produktu.
O	Organizacja, z którą powiązany jest obiekt nazwy wyróżniającej, np. korporacja.
L	Miejscowość (miasto lub gmina), w której znajduje się obiekt o nazwie DN.
ST	Nazwa województwa lub prowincji, w której znajduje się obiekt nazwy wyróżniającej.
C	Kraj, w którym znajduje się obiekt o nazwie wyróżniającej (DN).

- Jeśli dla strategii określono jedną lub więcej nazw wyróżniających nadawców, tylko określeni użytkownicy mogą umieszczać komunikaty w kolejce powiązanej ze strategią.
- Nazwy wyróżniające nadawców, jeśli je określono, muszą być zgodne z nazwą wyróżniającą zawartą w certyfikacie cyfrowym powiązanym z użytkownikiem, który umieszcza komunikat.
- Produkt IBM WebSphere MQ AMS obsługuje nazwy wyróżniające z wartościami tylko z zestawu znaków Latin-1 . Aby utworzyć nazwy wyróżniające z użyciem znaków zestawu, należy najpierw utworzyć certyfikat z nazwą wyróżniającą utworzoną w kodowaniu UTF-8 za pomocą platform UNIX z włączonym kodowaniem UTF-8 lub za pomocą programu narzędziowego iKeyman . Następnie należy utworzyć strategię z poziomu platformy UNIX z włączonym kodowaniem UTF-8 lub użyć wtyczki IBM WebSphere MQ AMS do programu WebSphere MQ.

Pojęcia pokrewne

“Nazwy wyróżniające odbiorców” na stronie 320
Nazwy wyróżniające odbiorców (DN) identyfikują użytkowników, którzy są uprawnieni do pobierania komunikatów z kolejki.

Nazwy wyróżniające odbiorców

Nazwy wyróżniające odbiorców (DN) identyfikują użytkowników, którzy są uprawnieni do pobierania komunikatów z kolejki.

Strategia może mieć określonych zero lub więcej nazw wyróżniających odbiorców. Nazwy wyróżniające odbiorców mają następującą postać:

```
CN=Common Name,O=Organization,C=Country
```

Ważne:

- Wszystkie nazwy wyróżniające muszą być zapisane wielkimi literami. Wszystkie identyfikatory nazw komponentów w nazwie wyróżniającej muszą być określone w kolejności przedstawionej w poniższej tabeli:

Nazwa komponentu	Wartość
CN	Nazwa zwykła obiektu tej nazwy DN, taka jak pełna nazwa lub zamierzony cel urządzenia.
OU	Jednostka w organizacji, z którą jest powiązany obiekt nazwy wyróżniającej, np. dział korporacyjny lub nazwa produktu.
O	Organizacja, z którą powiązany jest obiekt nazwy wyróżniającej, np. korporacja.
L	Miejscowość (miasto lub gmina), w której znajduje się obiekt o nazwie DN.
ST	Nazwa województwa lub prowincji, w której znajduje się obiekt nazwy wyróżniającej.
C	Kraj, w którym znajduje się obiekt o nazwie wyróżniającej (DN).

- Jeśli nie określono żadnych nazw wyróżniających odbiorców dla strategii, dowolny użytkownik może pobierać komunikaty z kolejki powiązanej ze strategią.
- Jeśli dla strategii określono jedną lub więcej nazw wyróżniających odbiorców, tylko określeni użytkownicy mogą pobierać komunikaty z kolejki powiązanej ze strategią.
- Nazwy wyróżniające odbiorców, jeśli je określono, muszą być zgodne z nazwą wyróżniającą zawartą w certyfikacie cyfrowym powiązanym z użytkownikiem, który pobiera komunikat.
- Produkt Advanced Message Security obsługuje nazwy wyróżniające z wartościami tylko z zestawu znaków Latin-1 . Aby utworzyć nazwy wyróżniające z użyciem znaków zestawu, należy najpierw utworzyć certyfikat z nazwą wyróżniającą utworzoną w kodowaniu UTF-8 za pomocą platform UNIX

z włączonym kodowaniem UTF-8 lub za pomocą programu narzędziowego iKeyman . Następnie należy utworzyć strategię z poziomu platformy UNIX z włączonym kodowaniem UTF-8 lub użyć wtyczki Advanced Message Security do programu WebSphere MQ.

Pojęcia pokrewne

"Nazwy wyróżniające nadawców" na stronie 319
Nazwy wyróżniające nadawcę (DN) identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce.

Atrybuty strategii bezpieczeństwa

Za pomocą programu Advanced Message Security można wybrać określony algorytm lub metodę w celu ochrony danych.

Strategia bezpieczeństwa jest obiektem pojęciowym opisanym w sposób kryptograficznie zaszyfrowany i podpisany. W poniższej tabeli przedstawiono atrybuty strategii bezpieczeństwa w produkcie Advanced Message Security:

Atrybuty	**Opis**
Nazwa strategii	Unikalna nazwa strategii dla menedżera kolejek.
Algorytm podpisu	Algorytm szyfrowania używany do podpisywania komunikatów przed wysłaniem.
Algorytm szyfrowania	Algorytm szyfrowania używany do szyfrowania komunikatów przed wysłaniem.
Lista adresatów	Lista nazw wyróżniających certyfikatów (DN) potencjalnych odbiorników komunikatu.
Lista kontrolna nazwy wyróżniającej podpisu	Lista nazw wyróżniających sygnatury, które mają zostać sprawdzone podczas pobierania komunikatów.

W programie Advanced Message Securitykomunikaty są szyfrowane za pomocą klucza symetrycznego, a klucz symetryczny jest szyfrowany za pomocą kluczy publicznych odbiorców. Klucze publiczne są szyfrowane za pomocą algorytmu RSA, z kluczami o efektywnej długości do 2048 bitów. Rzeczywiste szyfrowanie klucza asymetrycznego zależy od długości klucza certyfikatu.

Obsługiwane algorytmy klucza symetrycznego są następujące:

- RC2
- DES
- 3DES
- AES128
- AES256

Produkt Advanced Message Security obsługuje również następujące funkcje szyfrowania szyfrującego:

- MD5
- SHA-1
- SHA-2 Rodzina:
  - SHA256
  - SHA384 (minimalna dopuszczalna długość klucza-768 bitów)
  - SHA512 (minimalna dopuszczalna długość klucza-768 bitów)

Uwaga: Jakość ochrony używana dla funkcji put i get komunikatu musi być zgodna. Jeśli istnieje niezgodność strategii jakości ochrony między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno dla kolejek lokalnych, jak i zdalnych.

Jakość ochrony

Strategie ochrony danych Advanced Message Security oznaczają jakość ochrony (QOP).

Trzy poziomy zabezpieczeń w produkcie Advanced Message Security zależą od algorytmów szyfrowania używanych do podpisywania i szyfrowania komunikatu:

- Prywatność-komunikaty umieszczane w kolejce muszą być podpisane i zaszyfrowane.
- Integralność-komunikaty umieszczone w kolejce muszą być podpisane przez nadawcę.
- Brak-nie ma zastosowania żadna ochrona danych.

Strategia, która określa, że komunikaty muszą być podpisane przy umieszczaniu w kolejce, ma QOP INTEGRITY. QOP z INTEGRITY oznacza, że strategia określa algorytm podpisu, ale nie określa algorytmu szyfrowania. Komunikaty zabezpieczone przed integralnością są również nazywane "SIGNED".

Strategia, która określa, że komunikaty muszą być podpisywane i szyfrowane po umieszczaniu go w kolejce, ma QOP PRIVACY. QOP of PRIVACY oznacza, że gdy strategia określa algorytm podpisu i algorytm szyfrowania. Komunikaty chronione przez prywatność są również określane jako "ZAMKNIĘTE".

Strategia, która nie określa algorytmu podpisu lub algorytmu szyfrowania, ma wartość QOP (BRAK). Advanced Message Security Nie zapewnia ochrony danych dla kolejek, dla których istnieje strategia z QOP o wartości NONE.

Zarządzanie strategiami bezpieczeństwa

Strategia bezpieczeństwa jest obiektem pojęciowym opisanym w sposób kryptograficznie zaszyfrowany i podpisany.

Wszystkie zadania administracyjne związane ze strategiami bezpieczeństwa są uruchamiane z następującej lokalizacji:

- Na platformach UNIX : `<MQInstallRoot>/bin`
- Na platformach Windows zadania administracyjne mogą być uruchamiane z dowolnego miejsca, w którym zmienna środowiskowa PATH jest aktualizowana podczas instalacji.

Zadania pokrewne

“Tworzenie strategii bezpieczeństwa” na stronie 322
Strategie bezpieczeństwa definiują sposób, w jaki komunikat jest chroniony podczas umieszczania komunikatu, lub sposób, w jaki komunikat musi być chroniony po odebraniu komunikatu.

“Zmiana strategii bezpieczeństwa” na stronie 323
Za pomocą programu Advanced Message Security można zmieniać szczegóły strategii zabezpieczeń, które zostały już zdefiniowane.

“Wyświetlanie i zrzucanie strategii bezpieczeństwa” na stronie 324
Komenda `dspmqspl` służy do wyświetlania listy wszystkich strategii bezpieczeństwa lub szczegółów nazwanej strategii, w zależności od podanych parametrów wiersza komend.

“Usuwanie strategii bezpieczeństwa” na stronie 325
Aby usunąć strategie bezpieczeństwa w programie Advanced Message Security, należy użyć komendy `setmqspl` .

Tworzenie strategii bezpieczeństwa

Strategie bezpieczeństwa definiują sposób, w jaki komunikat jest chroniony podczas umieszczania komunikatu, lub sposób, w jaki komunikat musi być chroniony po odebraniu komunikatu.

Zanim rozpoczniesz

Istnieją pewne warunki wprowadzania, które muszą być spełnione podczas tworzenia strategii bezpieczeństwa:

- Menedżer kolejek musi być uruchomiony.
- Nazwa strategii bezpieczeństwa musi być zgodna z regułami nazewnictwa obiektów produktu WebSphere MQ.

- Aby utworzyć strategię bezpieczeństwa, użytkownik musi mieć niezbędne uprawnienia `+connect +inq +chg` . Pełną składnię komendy zmiany autoryzacji można znaleźć w sekcji **setmqaut** .
- Upewnij się, że masz niezbędne uprawnienia do działania w kolejkach WebSphere MQ i menedżerach kolejek. Aby uzyskać więcej informacji, zobacz: “Nadawanie uprawnień OAM” na stronie 327

Przykład

Poniżej przedstawiono przykład tworzenia strategii dla menedżera kolejek QMGR. Strategia określa, że komunikaty są podpisywane przy użyciu algorytmu SHA1 i szyfrowane przy użyciu algorytmu AES256 dla certyfikatów o nazwie wyróżniającej: CN=joe, O=IBM, C=US i DN: CN=jane, O=IBM, C = US. Ta strategia jest przyłączona do produktu `MY.QUEUE`:

```
$ setmqspl -m QMGR -p MY.QUEUE -s SHA1 -e AES256 -r CN=joe,O=IBM,C=US -r CN=jane,O=IBM,C=US
```

Poniżej przedstawiono przykład tworzenia strategii w menedżerze kolejek QMGR. Strategia określa, że komunikaty są szyfrowane przy użyciu algorytmu DES dla certyfikatów o nazwach wyróżniających: CN=john, O=IBM, C=US i CN=jeff, O=IBM, C=US i podpisanych przy użyciu algorytmu MD5 dla certyfikatu o nazwie wyróżniającej: CN=phil, O=IBM, C=US

```
$ setmqspl -m QMGR -p MY.OTHER.QUEUE -s MD5 -e DES -r CN=john,O=IBM,C=US -r CN=jeff,O=IBM,C=US
-a CN=phil,O=IBM,C=US
```

Uwaga:

- Jakość ochrony używana dla komunikatu umieszczonego i pobrania musi być zgodna. Jeśli jakość strategii określona dla komunikatu jest słabsza od zdefiniowanej dla kolejki, komunikat jest wysyłany do kolejki obsługi błędów. Ta strategia jest poprawna zarówno dla kolejek lokalnych, jak i zdalnych.

Odsyłacze pokrewne

Pełna lista atrybutów komendy setmqspl

Zmiana strategii bezpieczeństwa

Za pomocą programu Advanced Message Security można zmieniać szczegóły strategii zabezpieczeń, które zostały już zdefiniowane.

Zanim rozpoczniesz

- Musi być uruchomiony menedżer kolejek, w którym ma zostać uruchomione działanie.
- Aby utworzyć strategie bezpieczeństwa, konieczne jest posiadanie uprawnień `+connect +inq +chg` . Pełną składnię komendy zmiany autoryzacji można znaleźć w sekcji **setmqaut** .

O tym zadaniu

Aby zmienić strategie bezpieczeństwa, należy zastosować komendę `setmqspl` do już istniejącej strategii udostępniających nowe atrybuty.

Przykład

Poniżej przedstawiono przykład tworzenia strategii o nazwie MYQUEUE w menedżerze kolejek o nazwie QMGR , która określa, że komunikaty będą szyfrowane przy użyciu algorytmu RC2 dla certyfikatów o nazwach wyróżniających DN:CN=bob, O=IBM, C=US i podpisanych z algorytmem SHA1 dla certyfikatów o nazwach wyróżniających DN:CN=jeff, O=IBM, C = US.

```
setmqspl -m QMGR -p MYQUEUE -e RC2 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Aby zmienić tę strategię, należy wywołać komendę `setmqspl` ze wszystkimi atrybutami z przykładu, zmieniając tylko wartości, które mają zostać zmodyfikowane. W tym przykładzie wcześniej utworzona strategia jest przyłączona do nowej kolejki, a jej algorytm szyfrowania jest zmieniany na AES256:

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Odsyłacze pokrewne

setmqspl

Wyświetlanie i zrzucanie strategii bezpieczeństwa

Komenda `dspmqspl` służy do wyświetlania listy wszystkich strategii bezpieczeństwa lub szczegółów nazwanej strategii, w zależności od podanych parametrów wiersza komend.

Zanim rozpoczniesz

- Aby wyświetlić szczegóły strategii bezpieczeństwa, menedżer kolejek musi istnieć i być uruchomiony.
- Aby menedżer kolejek był wyświetlany i zrzucał strategie bezpieczeństwa, należy mieć wymagane uprawnienia `+connect +inq +dsp` . Pełną składnię komendy zmiany autoryzacji można znaleźć w sekcji **`setmqaut`** .

O tym zadaniu

Poniżej znajduje się lista opcji komendy `dspmqspl` :

Tabela 27. Flagi komend `dspmqspl` .

Opcja komendy	Wyjaśnienie
`-m`	Nazwa menedżera kolejek (**obowiązkowa**).
`-p`	Nazwa strategii.
`-export`	Dodanie tej opcji powoduje wygenerowanie danych wyjściowych, które można łatwo zastosować do innego menedżera kolejek.

Przykład

W tym przykładzie zostaną utworzone dwie strategie bezpieczeństwa dla produktu `venus.queue.manager`:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s MD5 -a "CN=another signer,O=IBM,C=US" -e
NONE
```

W tym przykładzie przedstawiono komendę wyświetlający szczegółowe informacje o wszystkich strategiach zdefiniowanych dla produktu `venus.queue.manager` oraz dane wyjściowe, które wygeneruje:

```
dspmqspl -m  venus.queue.manager

Policy Details:
Policy name: AMS_POL_04_ONE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=signer1,O=IBM,C=US
Recipient DNs: -
Toleration: 0
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

W tym przykładzie przedstawiono komendę wyświetlający szczegóły wybranej strategii bezpieczeństwa zdefiniowanej dla produktu `venus.queue.manager` oraz dane wyjściowe, które wygeneruje:

```
dspmqspl -m venus.queue.manager -p AMS_POL_06_THREE

Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

W następnym przykładzie najpierw tworzymy strategię bezpieczeństwa, a następnie wyeksportujemy strategię za pomocą opcji `-export` :

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Aby zaimportować strategię bezpieczeństwa:

- Na platformach Windows uruchom komendę `policies.bat`
- Na platformach UNIX :
  1. Zaloguj się jako użytkownik należący do grupy administracyjnej produktu `mqm` WebSphere MQ .
  2. Wydaj komendę `. policies.sh`.

Odsyłacze pokrewne

Pełna lista atrybutów komendy dspmqspl

Usuwanie strategii bezpieczeństwa

Aby usunąć strategie bezpieczeństwa w programie Advanced Message Security, należy użyć komendy `setmqspl` .

Zanim rozpoczniesz

Istnieją pewne warunki wprowadzania, które muszą być spełnione podczas zarządzania strategiami bezpieczeństwa:

- Menedżer kolejek musi być uruchomiony.
- Aby utworzyć strategie bezpieczeństwa, konieczne jest posiadanie uprawnień `+connect +inq +chg` . Pełną składnię komendy zmiany autoryzacji można znaleźć w sekcji **`setmqaut`** .

O tym zadaniu

Użyj komendy `setmqspl` z opcją `-remove` .

Przykład

Poniżej przedstawiono przykład usuwania strategii:

```
$ setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

Odsyłacze pokrewne

Pełna lista atrybutów komendy setmqspl

Ochrona kolejki systemowej

Kolejki systemowe umożliwiają komunikację między produktem WebSphere MQ i jego aplikacjami pomocniczymi. Za każdym razem, gdy tworzony jest menedżer kolejek, tworzona jest również kolejka systemowa do przechowywania wewnętrznych komunikatów i danych produktu WebSphere MQ . Można

chronić kolejki systemowe za pomocą programu Advanced Message Security , aby tylko autoryzowani użytkownicy mieli dostęp do nich lub ich odszyfrowywać.

Ochrona kolejki systemowej jest zgodna z tym samym wzorcem, co ochrona kolejek regularnych. Patrz sekcja “Tworzenie strategii bezpieczeństwa” na stronie 322.

Aby korzystać z ochrony kolejki systemowej na platformach Windows , należy skopiować plik `keystore.conf` do następującego katalogu:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

Aby zapewnić ochronę dla systemu `SYSTEM.ADMIN.COMMAND.QUEUE`, serwer komend musi mieć dostęp do serwerów `keystore` i `keystore.conf`, które zawierają klucze i konfigurację, dzięki czemu serwer komend może uzyskać dostęp do kluczy i certyfikatów. Wszystkie zmiany wprowadzone w strategii bezpieczeństwa produktu `SYSTEM.ADMIN.COMMAND.QUEUE` wymagają zrestartowania serwera komend.

Wszystkie komunikaty, które są wysyłane i odbierane z kolejki komend, są podpisywane lub podpisywane i szyfrowane w zależności od ustawień strategii. Jeśli administrator zdefiniuje autoryzowane osoby podpisujące, komunikaty komend, które nie przekazują sprawdzania nazwy wyróżniającej osoby podpisującej, nie są wykonywane przez serwer komend i nie są kierowane do kolejki obsługi błędów produktu Advanced Message Security . Komunikaty wysyłane jako odpowiedzi do tymczasowych kolejek dynamicznych programu WebSphere MQ Explorer nie są chronione przez produkt WebSphere MQ AMS.

Zmiany w strategiach bezpieczeństwa Advanced Message Security wymagają zrestartowania serwera komend WebSphere MQ .

Strategie bezpieczeństwa nie mają wpływu na następujące kolejki SYSTEM:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE

- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

Nadawanie uprawnień OAM

Uprawnienia do plików autoryzują wszystkich użytkowników do wykonywania komend `setmqspl` i `dspmqspl` . Jednak produkt IBM Advanced Message Security korzysta z menedżera uprawnień do obiektu (Object Authority Manager-OAM), a każda próba wykonania tych komend przez użytkownika, który nie należy do grupy mqm, która jest grupą administracyjną WebSphere MQ lub nie ma uprawnień do odczytu ustawień strategii bezpieczeństwa, powoduje błąd.

Procedura

Aby nadać użytkownikowi niezbędne uprawnienia, uruchom komendę:

```
setmqaut -m SOME.QUEUE.MANAGER -t qmgr -p SOME.USER  +connect +inq
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.POLICY.QUEUE -p SOME.USER +browse
+put
setmqaut -m SOME.QUEUE.MANAGER -t queue -n SYSTEM.PROTECTION.ERROR.QUEUE -p SOME.USER +put
```

Zdarzenia dotyczące komend i konfiguracji

Za pomocą programu Advanced Message Securitymożna generować komunikaty zdarzeń dotyczących komend i konfiguracji, które mogą być rejestrowane i służą jako zapis zmian strategii dotyczących kontroli.

Zdarzenia komendy i konfiguracji wygenerowane przez program WebSphere MQ są komunikatami formatu PCF wysłanym do dedykowanych kolejek.

Komunikaty zdarzeń konfiguracji są wysyłane do systemu SYSTEM.ADMIN.CONFIG.EVENT (zdarzenie) w menedżerze kolejek, w którym występuje zdarzenie.

Komunikaty zdarzeń komend są wysyłane do systemu SYSTEM.ADMIN.COMMAND.EVENT (zdarzenie) w menedżerze kolejek, w którym występuje zdarzenie.

Zdarzenia są generowane niezależnie od narzędzi używanych do zarządzania strategiami bezpieczeństwa produktu Advanced Message Security .

W programie Advanced Message Securityistnieją cztery typy zdarzeń wygenerowane przez różne działania w strategiach bezpieczeństwa:

- “Tworzenie strategii bezpieczeństwa” na stronie 322, które generują dwa komunikaty zdarzeń produktu WebSphere MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy
- “Zmiana strategii bezpieczeństwa” na stronie 323, który generuje trzy komunikaty zdarzeń produktu WebSphere MQ :
  - Zdarzenie konfiguracyjne, które zawiera stare wartości strategii bezpieczeństwa
  - Zdarzenie konfiguracyjne, które zawiera nowe wartości strategii bezpieczeństwa.

  - Zdarzenie komendy
- "Wyświetlanie i zrzucanie strategii bezpieczeństwa" na stronie 324, który generuje jeden komunikat zdarzenia WebSphere MQ :
  - Zdarzenie komendy
- "Usuwanie strategii bezpieczeństwa" na stronie 325, który generuje dwa komunikaty zdarzeń produktu WebSphere MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy

Włączanie i wyłączanie rejestrowania zdarzeń

Zdarzenia komendy i konfiguracji są sterujące za pomocą atrybutów menedżera kolejek CONFIGEV i CMDEV. Aby włączyć te zdarzenia, należy ustawić odpowiedni atrybut menedżera kolejek na wartość ENABLED(WŁĄCZONE). Aby wyłączyć te zdarzenia, należy ustawić odpowiedni atrybut menedżera kolejek na wartość DISABLED(WYŁĄCZONE).

Procedura

Zdarzenia konfiguracji

Aby włączyć zdarzenia konfiguracji, należy ustawić opcję CONFIGEV na wartość ENABLED. Aby wyłączyć zdarzenia konfiguracji, należy ustawić parametr CONFIGEV na wartość DISABLED. Na przykład można włączyć zdarzenia konfiguracji przy użyciu następującej komendy MQSC:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Zdarzenia komendy

Aby włączyć zdarzenia komendy, należy ustawić parametr CMDEV na wartość ENABLED(WŁĄCZONE). Aby włączyć zdarzenia komend dla komend z wyjątkiem komend DISPLAY MQSC i Inquire PCF, należy ustawić wartość parametru CMDEV na NODISPLAY. Aby wyłączyć zdarzenia komendy, należy ustawić parametr CMDEV na wartość DISABLED. Na przykład można włączyć zdarzenia komend przy użyciu następującej komendy MQSC:

```
ALTER QMGR CMDEV (ENABLED)
```

Zadania pokrewne

Sterowanie zdarzeniami konfiguracji, komend i programów rejestrujących w produkcie Websphere MQ

Format komunikatu zdarzenia komendy

Komunikat zdarzenia komendy składa się ze struktury MQCFH i parametrów PCF, które są następujące po nim.

Poniżej przedstawiono wybrane wartości MQCFH:

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

Uwaga: Wartość ParameterCount to dwie, ponieważ zawsze istnieją dwa parametry typu MQCFGR (grupa). Każda grupa składa się z odpowiednich parametrów. Dane zdarzenia składają się z dwóch grup: CommandContext i CommandData.

Element CommandContext zawiera następujące elementy:

EventUserID

Opis: Identyfikator użytkownika, który wywołał komendę lub wywołanie, które wygenerował zdarzenie. (Jest to ten sam identyfikator użytkownika, który jest używany do sprawdzania uprawnień do wydania komendy lub wywołania; w przypadku komend otrzymanych z kolejki jest to również identyfikator użytkownika (UserIdentifier) z MD komunikatu komendy).

Identyfikator: MQCACF_EVENT_USER_ID.

Typ danych: MQCFST.

Maksymalna długość: DŁUGOŚĆ_CZASU_MQ.

Zwrócone: Zawsze.

EventOrigin

Opis: Początek działania powodującego zdarzenie.

Identyfikator: MQIACF_EVENT_ORIGIN.

Typ danych: MQCFIN.

Wartości:

KONSOLA MQEVO_CONSOLE
Komenda konsoli-wiersz komend.

MQEVO_MSG
Komunikat komendy z wtyczki programu WebSphere MQ Explorer.

Zwrócone: Zawsze.

EventQMgr

Opis: Menedżer kolejek, w którym wprowadzono komendę lub wywołanie. (Menedżer kolejek, w którym wykonywana jest komenda i która generuje zdarzenie, znajduje się w polu MD komunikatu o zdarzeniu).

Identyfikator: MQCACF_EVENT_Q_MGR.

Typ danych: MQCFST.

Maksymalna długość: Wartość parametru MQ_Q_MGR_NAME_LENGTH.

Zwrócone: Zawsze.

EventAccountingToken

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), token rozliczania (AccountingToken) od MD w komunikacie komendy.

Identyfikator: MQBACF_EVENT_ACCOUNTING_TOKEN.

Typ danych: MQCFBS.

Maksymalna długość: MQ_ACCOUNTING_TOKEN_LENGTH.

Zwrócone: Tylko wtedy, gdy parametr EventOrigin ma wartość MQEVO_MSG.

EventIdentityData

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), dane tożsamości aplikacji (ApplIdentityData) z MD komunikatu komendy.

Identyfikator: MQCACF_EVENT_APPL_IDENTITY.

Typ danych: MQCFST.

Maksymalna długość: MQ_APPL_IDENTITY_DATA_LENGTH.

Zwrócone: Tylko wtedy, gdy parametr EventOrigin ma wartość MQEVO_MSG.

EventApplType

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), typ aplikacji (PutApplType) z MD komunikatu komendy.

Identyfikator: MQIACF_EVENT_APPL_TYPE.

Typ danych: MQCFIN.

Zwrócone: Tylko wtedy, gdy parametr EventOrigin ma wartość MQEVO_MSG.

EventApplName

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), nazwa aplikacji (PutApplName) z MD komunikatu komendy.

Identyfikator: MQCACF_EVENT_APPL_NAME.

Typ danych: MQCFST.

Maksymalna długość: Wartość MQ_APPL_NAME_LENGTH.

Zwrócone: Tylko wtedy, gdy parametr EventOrigin ma wartość MQEVO_MSG.

EventApplOrigin

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), dane o pochodzeniu aplikacji (ApplOriginData) pochodzą z MD komunikatu komendy.

Identyfikator: MQCACF_EVENT_APPL_ORIGIN.

Typ danych: MQCFST.

Maksymalna długość: MQ_APPL_ORIGIN_DATA_LENGTH.

Zwrócone: Tylko wtedy, gdy parametr EventOrigin ma wartość MQEVO_MSG.

Command

Opis: Kod komendy.

Identyfikator: MQIACF_COMMAND.

Typ danych: MQCFIN.

Wartości: **MQCMD_INQUIRE_PROT_POLICY, wartość liczbowa 205**
MQCMD_CREATE_PROT_POLICY, wartość liczbowa 206
MQCMD_DELETE_PROT_POLICY, wartość liczbowa 207
MQCMD_CHANGE_PROT_POLICY wartość liczbowa 208
Są one zdefiniowane w produkcie WebSphere MQ 7.5 `cmqcfc.h`

Zwrócone: Zawsze.

CommandData zawiera elementy PCF składające się na komendę PCF.

Format komunikatu zdarzenia konfiguracji

Zdarzenia konfiguracji to komunikaty PCF w standardowym formacie Advanced Message Security .

Informacje na temat możliwych wartości deskryptora komunikatu MQMD zawiera sekcja Komunikat zdarzenia MQMD (deskryptor komunikatu).

Poniżej przedstawiono wybrane wartości MQMD:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR                      //for both CLI and command server
```

Bufor komunikatów składa się ze struktury MQCFH i struktury parametru, która jest zgodna z tą strukturą. Informacje na temat możliwych wartości MQCFH można znaleźć w sekcji Komunikat zdarzenia MQCFH (nagłówek PCF).

Poniżej przedstawiono wybrane wartości MQCFH:

```
Type = MQCFT_EVENT
Command = MQCMD_CONFIG_EVENT
MsgSeqNumber = 1 or 2          // 2 will be in case of Change Object event
Control = MQCFC_LAST or MQCFC_NOT_LAST     //MQCFC_NOT_LAST will be in case of 1 Change Object
event
ParameterCount = reflects number of PCF parameters following MQCFH
CompCode = MQCC_WARNING
Reason = one of {MQRC_CONFIG_CREATE_OBJECT, MQRC_CONFIG_CHANGE_OBJECT,
MQRC_CONFIG_DELETE_OBJECT}
```

Parametry po MQCFH są następujące:

EventUserID

Opis:	Identyfikator użytkownika, który wywołał komendę lub wywołanie, które wygenerował zdarzenie. (Jest to ten sam identyfikator użytkownika, który jest używany do sprawdzania uprawnień do wydania komendy lub wywołania; w przypadku komend otrzymanych z kolejki jest to również identyfikator użytkownika (UserIdentifier) z MD komunikatu komendy).
Identyfikator:	**MQCACF_EVENT_USER_ID**
Typ danych:	MQCFST.
Długość maksymalna:	DŁUGOŚĆ_CZASU_MQ.
Zwrócone:	Zawsze.

SecurityId

Opis:	Wartość MQMD.AccountingToken w przypadku komunikatów serwera komend lub identyfikatora SID systemu Windows dla komendy lokalnej.
Identyfikator:	**MQBACF_EVENT_SECURITY_ID**
Typ danych:	MQCBS.
Długość maksymalna:	Wartość MQ_SECURITY_ID_LENGTH.
Zwrócone:	Zawsze.

EventOrigin

Opis:	Początek działania powodującego zdarzenie.
Identyfikator:	**MQIACF_EVENT_ORIGIN**
Typ danych:	MQCFIN.

Wartości:

KONSOLA MQEVO_CONSOLE
Komenda konsoli-wiersz komend.

MQEVO_MSG
Komunikat komendy z poziomu wtyczki programu WebSphere MQ Explorer.

Zwrócone: Zawsze.

EventQMgr

Opis: Menedżer kolejek, w którym wprowadzono komendę lub wywołanie. (Menedżer kolejek, w którym wykonywana jest komenda i która generuje zdarzenie, znajduje się w polu MD komunikatu o zdarzeniu).

Identyfikator: **MQCACF_EVENT_Q_MGR**

Typ danych: MQCFST

Długość maksymalna: DŁUGOŚĆ_LUB_DŁUGOŚĆ_MQ_Q_MGR_

Zwrócone: Zawsze.

ObjectType

Opis: Typ obiektu.

Identyfikator: **MQIACF_OBJECT_TYPE**

Typ danych: MQCFIN

Wartość:

Strategia MQOT_PROT_POLICY
Strategia ochrony Advanced Message Security . **1019** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Zwrócone: Zawsze.

PolicyName

Opis: Nazwa strategii Advanced Message Security .

Identyfikator: **MQCA_POLICY_NAME**.

Typ danych: MQCFST.

Wartość: **2112** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Długość maksymalna: MQ_OBJECT_NAME_LENGTH.

Zwrócone: Zawsze.

PolicyVersion

Opis: Wersja strategii Advanced Message Security .

Identyfikator: **MQIA_POLICY_VERSION**

Typ danych: MQCFIN

Wartość **238** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Zwrócone: Zawsze

TolerateFlag

Opis: Flaga tolerowania strategii Advanced Message Security .

Identyfikator: **MQIA_TOLERATE_UNPROTECTED**

Typ danych: MQCFIN

Wartość **235** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Zwrócone: Zawsze.

SignatureAlgorithm

Opis: Algorytm podpisu strategii Advanced Message Security .

Identyfikator: **MQIA_SIGNATURE_ALGORITHM**

Typ danych: MQCFIN

Wartość: **236** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Zwrócone: Za każdym razem, gdy w strategii produktu Advanced Message Security jest zdefiniowany algorytm podpisu

EncryptionAlgorithm

Opis: Algorytm szyfrowania strategii Advanced Message Security .

Identyfikator: **MQIA_ENCRYPTION_ALGORITHM**

Typ danych: MQCFIN

Wartość: **237** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Zwrócone: Za każdym razem, gdy w strategii WebSphere MQ zdefiniowano algorytm szyfrowania

SignerDNs

Opis: Temat DistinguishedName dozwolonych osób podpisujących.

Identyfikator: **MQCA_SIGNER_DN**

Typ danych: MQCFSL

Wartość: **2113** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Długość maksymalna: Najdłuższa nazwa wyróżniająca (DN) osoby podpisującej w strategii, ale nie ma już wartości MQ_DISTINGUISHED_NAME_LENGTH

Zwrócone: Zawsze, gdy jest zdefiniowana w strategii WebSphere MQ .

RecipientDNs

Opis: Temat DistinguishedName dozwolonych osób podpisujących.

Identyfikator: **MQCA_RECIPIENT_DN**

Typ danych: MQCFSL

Wartość: **2114** -wartość liczbowa zdefiniowana w produkcie WebSphere MQ 7.5 lub w pliku `cmqc.h` .

Długość maksymalna:	Najdłuższa nazwa wyróżniająca (DN) odbiorcy w strategii, ale nie jest dłuższa niż wartość MQ_DISTINGUISHED_NAME_LENGTH.
Zwrócone:	Zawsze, gdy jest zdefiniowana w strategii WebSphere MQ .

Problemy i rozwiązania

W tej sekcji opisano sposób rozwiązywania problemów, które mogą wystąpić podczas instalacji IBM . Użyj tych informacji, aby zidentyfikować i rozwiązać problemy związane z produktem Advanced Message Security.

com.ibm.security.pkcsutil.PKCSException: Błąd przy szyfrowaniu treści

Błąd `com.ibm.security.pkcsutil.PKCSException: Error encrypting contents` sugeruje, że IBM Advanced Message Security ma problemy z dostępem do algorytmów szyfrujących.

Jeśli w programie Advanced Message Securityzostanie zwrócony następujący błąd:

```
DRQJP0103E   The IBM WebSphere MQ Advanced Message Security Java interceptor failed to protect
message.
  com.ibm.security.pkcsutil.PKCSException: Error encrypting contents
(java.security.InvalidKeyException: Illegal key size or default parameters)
```

sprawdza, czy strategia bezpieczeństwa JCE w produkcie `JAVA_HOME/lib/security/local_policy.jar/*.policy` nadaje dostęp do algorytmów podpisu używanych w strategii produktu MQ AMS.

Jeśli algorytm podpisywania, który ma być używany, nie jest określony w bieżącej strategii bezpieczeństwa, pobierz poprawny plik strategii Java z następujących miejsc:

- IBM Pliki strategii SDK dla języka Java 1.4.2.
- IBM Pliki strategii SDK dla języka Java 5.0.
- IBM Pliki strategii SDK dla języka Java 6.0.
- IBM Pliki strategii SDK dla języka Java 7.0.

Obsługa środowiska OSGi

Aby używać pakunku OSGi z dodatkowymi parametrami IBM Advanced Message Security , wymagane są dodatkowe parametry.

Uruchom następujący parametr podczas uruchamiania pakunku OSGi:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7
```

W przypadku używania zaszyfrowanego hasła w pliku keystore.confnależy dodać następującą instrukcję, gdy pakunek OSGi jest uruchomiony:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7,com.ibm.misc
```

Ograniczenie: Produkt IBM WebSphere MQ AMS obsługuje komunikację przy użyciu tylko podstawowych klas Java produktu MQ dla kolejek chronionych z poziomu pakunku OSGi.

Problemy podczas otwierania chronionych kolejek podczas korzystania z produktu JMS

Podczas korzystania z produktu IBM WebSphere MQ Advanced Message Securitymogą pojawić się różne problemy podczas otwierania chronionych kolejek.

Używany jest produkt JMS i wyświetlany jest błąd 2085 (MQRC_UNKNOWN_OBJECT_NAME) razem z błędem JMSMQ2008.

Zweryfikowano, że produkt IBM WebSphere MQ Advanced Message Security został skonfigurowany zgodnie z opisem w sekcji “Podręcznik Szybki start dla klientów Java” na stronie 294.

Prawdopodobną przyczyną jest to, że używane jest środowisko wykonawcze inne niżIBM Java . Jest to znane ograniczenie opisane w sekcji “Znane ograniczenia” na stronie 282.

Zmienna środowiskowa AMQ_DISABLE_CLIENT_AMS nie została ustawiona.

Rozwiązanie problemu

Istnieją cztery możliwości pracy wokół tego problemu:

1. Uruchom aplikację JMS w ramach obsługiwanego środowiska wykonawczego IBM Java Runtime Environment (JRE).
2. Przenieś aplikację na tę samą maszynę, na której działa menedżer kolejek, i nawiąże połączenie z użyciem połączenia w trybie powiązań.

   Połączenie w trybie powiązań korzysta z rodzimych bibliotek platformy w celu wykonania wywołań interfejsu API produktu IBM WebSphere MQ . W związku z tym rodzimy przechwytywacz AMS jest używany do wykonywania operacji AMS i nie ma możliwości polegania na możliwościach środowiska JRE.
3. Należy użyć przechwytywacza MCA, ponieważ umożliwia to podpisywanie i szyfrowanie komunikatów zaraz po przyjeździe do menedżera kolejek, bez konieczności wykonywania przez klienta żadnego przetwarzania AMS.

   Ze względu na to, że ochrona jest stosowana w menedżerze kolejek, należy użyć alternatywnego mechanizmu w celu ochrony komunikatów w tranzycie z klienta do menedżera kolejek. Najczęściej jest to osiągane poprzez skonfigurowanie szyfrowania SSL/TLS na kanale połączenia serwera używanego przez aplikację.
4. Ustaw zmienną środowiskową AMQ_DISABLE_CLIENT_AMS, jeśli nie ma być używana IBM WebSphere MQ Advanced Message Security.

Więcej informacji na ten temat zawiera sekcja “Przechwytywanie agenta kanału komunikatów (MCA)” na stronie 307.

Uwaga: Dla każdej kolejki, do której serwer MCA Interceptor będzie dostarczał komunikaty, musi istnieć strategia bezpieczeństwa. Innymi słowy, kolejka docelowa musi mieć strategię zabezpieczeń AMS w miejscu o nazwie wyróżniającej (DN) osoby podpisującej i odbiorcy, które są zgodne z certyfikatem przypisanym do modułu MCA Interceptor. Oznacza to, że nazwa wyróżniająca certyfikatu wyznaczonego przez właściwość `cms.certificate.channel.SYSTEM.DEF.SVRCONN` w `keystore.conf` używanym przez menedżer kolejek.

Uwagi

Niniejsza publikacja została opracowana 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 IBM. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej firmy 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. Używanie tego dokumentu nie daje żadnych praw do tych patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Zapytania w sprawie licencji dotyczących informacji kodowanych przy użyciu dwubajtowych zestawów znaków (DBCS) należy kierować do lokalnych działów IBM Intellectual Property Department lub zgłaszać na piśmie pod adresem:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy typograficzne. 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 podmiotów zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

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

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie

z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
Koordynator współdziałania z oprogramowaniem, Dział 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, zostanie uiszczona stosowna opłata.

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

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary 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 innych niż produkty 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 innych podmiotów 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 programistycznym 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.

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

Informacje dotyczące interfejsu programistycznego

Informacje dotyczące interfejsu programistycznego, o ile są udostępniane, mają być pomocne podczas tworzenia oprogramowania aplikacji do użytku z tym programem.

Podręcznik ten zawiera informacje na temat planowanych interfejsów programistycznych, które umożliwiają klientom pisanie programów w celu uzyskania dostępu do usług IBM WebSphere MQ.

Informacje te mogą również zawierać informacje na temat diagnostyki, modyfikacji i strojenia. Tego typu informacje są udostępniane jako pomoc przy debugowaniu aplikacji.

Ważne: Informacji na temat diagnostyki, modyfikacji i strojenia nie należy używać jako interfejsu programistycznego, ponieważ może on ulec zmianie.

Znaki towarowe

IBM, logo IBM , ibm.com, są znakami towarowymi IBM Corporation, zarejestrowanymi w wielu systemach prawnych na całym świecie. Aktualna lista znaków towarowych IBM jest dostępna w serwisie WWW, w sekcji "Copyright and trademark information"(Informacje o prawach autorskich i znakach towarowych), pod adresemwww.ibm.com/legal/copytrade.shtml. Nazwy innych produktów lub usług mogą być znakami towarowymi IBM lub innych podmiotów.

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

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

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

Ten produkt zawiera oprogramowanie opracowane przez Eclipse Project (http://www.eclipse.org/).

Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Numer pozycji:

(1P) P/N: