9.1

Zabezpieczanie produktu IBM MQ

Uwaga

Przed skorzystaniem z niniejszych informacji oraz produktu, którego one dotyczą, należy zapoznać się z informacjami zamieszczonymi w sekcji “Uwagi” na stronie 677.

To wydanie dotyczy wersji 9 wydania 1 produktu IBM® MQ oraz wszystkich kolejnych wydań i modyfikacji, o ile nie podano inaczej w nowych edycjach.

Spis treści

zabezpieczanieIBM MQ

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

Aktualizacje zabezpieczeń

Upewnij się, że cały sprzęt i oprogramowanie znajdujące się w chronionej strefie oraz na stacjach roboczych operatora znajdują się w ich cyklu życia wsparcia, zostały zaktualizowane z obowiązkowymi aktualizacjami oprogramowania i natychmiast zostały zastosowane aktualizacje zabezpieczeń.

Więcej informacji na temat aktualizacji zabezpieczeń można znaleźć w następujących celach:

- Wszystkie platformy na platformie IBM Security Bulletins
- Raporty APAR dotyczące bezpieczeństwa i integralności systemu w produkcie z/OS są dostępne w portalu IBM Z System Integrity portal.

przegląd zabezpieczeń

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

Pojęcia i mechanizmy bezpieczeństwa

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

Powszechnie akceptowane aspekty bezpieczeństwa są następujące:

- “Identyfikacja i uwierzytelnianie” na stronie 6
- “Autoryzacja” na stronie 6
- “Kontrola” na stronie 7
- “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 10
- “Infrastruktura klucza publicznego (PKI)” na stronie 14

Podczas planowania implementacji produktu IBM MQ należy wziąć pod uwagę, które mechanizmy zabezpieczeń wymagają zaimplementowania tych aspektów bezpieczeństwa, które są dla użytkownika ważne. Informacje o tym, co należy wziąć pod uwagę po zapoznaniu się z tymi tematami, zawiera sekcja “Planowanie wymagań dotyczących bezpieczeństwa” na stronie 81.

Pojęcia pokrewne

“Praca z protokołem SSL/TLS” na stronie 282
W tych tematach znajdują się instrukcje dotyczące wykonywania pojedynczych zadań związanych z używaniem protokołu TLS z produktem IBM MQ.

Zadania pokrewne

Łączenie dwóch menedżerów kolejek za pomocą protokołu TLS

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 MQ , ponieważ IBM 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 MQ z produktem 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 produktu IBM MQ , poprzez napisanie własnych programów obsługi wyjścia.

Pojęcia pokrewne

“Identyfikacja i uwierzytelnianie w produkcie IBM MQ” na stronie 21

W programie IBM 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 MQ” na stronie 22

Za pomocą autoryzacji można ograniczyć poszczególne osoby lub aplikacje, które mogą wykonywać w środowisku produktu IBM 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 85 i powiązane podtematy.

Pojęcia pokrewne

"Kontrola w produkcie IBM MQ" na stronie 22
Program IBM 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 IBM MQ.

Termin *jednostka* jest używany do odwołania się do menedżera kolejek, IBM MQ MQI client, pojedynczego użytkownika lub innego systemu, który może wymieniać komunikaty.

Pojęcia pokrewne

"Kryptografia w produkcie IBM MQ" na stronie 24
Produkt IBM MQ udostępnia kryptografię za pomocą protokołu 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.

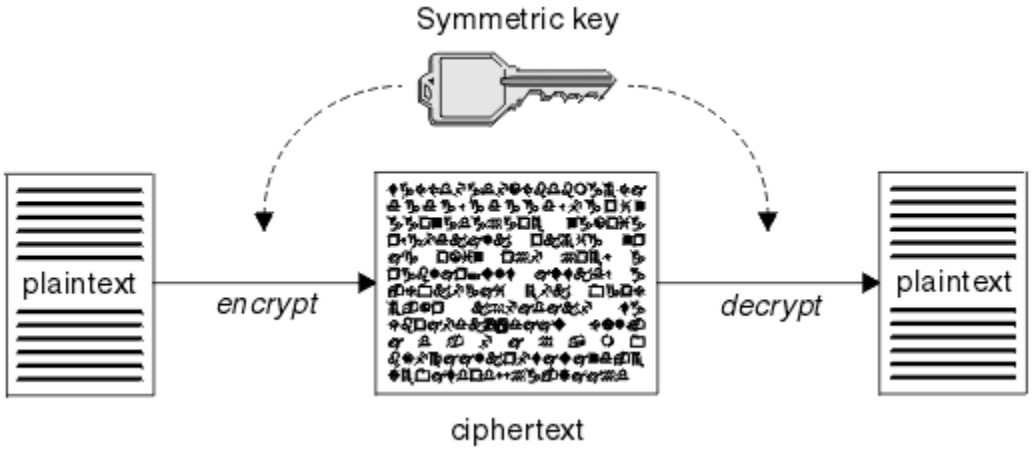
3. Odbiornik konwertuje komunikat zaszyfrować tekst z powrotem do postaci jawnego tekstu. Ta część procesu nosi nazwę *deszyfrowania* (czasem *decyferment*).

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 SSL/TLS” na stronie 19 .

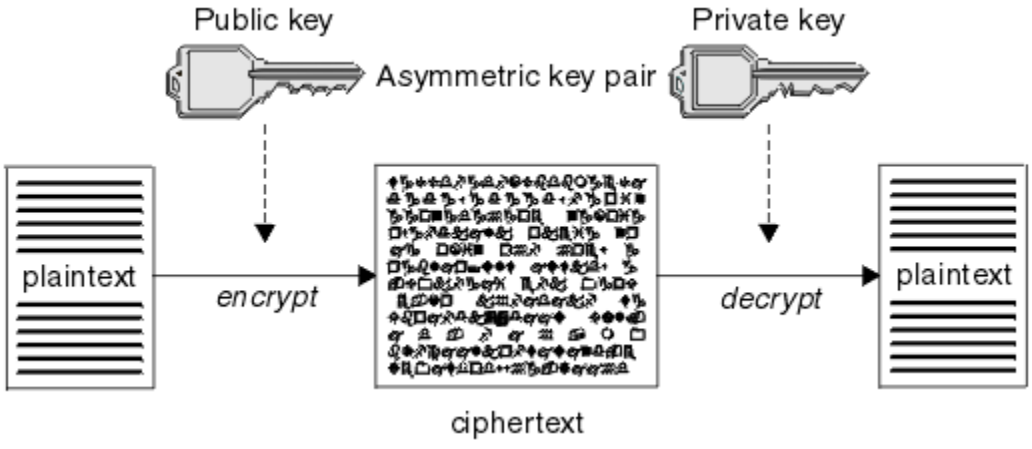
Techniki kryptograficzne wiążą się z ogólnym algorytmem, który jest specyficzny przy użyciu kluczy. Istnieją dwie klasy algorytmu:

- 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 przedstawia 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 przedstawia 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. Streszczenie komunikatu jest obliczane przez funkcję mieszającą i może być szyfrowane, tworząc podpis cyfrowy.

Funkcja mieszająca używana do obliczenia streszczenia komunikatów musi spełniać dwa kryteria:

- To musi być jeden 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 SSL/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 IBM MQ są zgodne ze standardem X.509 , który określa wymagane informacje i format do jego 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 IBM MQ obsługuje certyfikaty cyfrowe zgodne ze standardem X.509 . Wymaga ona opcji uwierzytelniania klienta.

Ponieważ produkt IBM MQ jest systemem równorzędnym, jest on wyświetlany jako uwierzytelnianie klienta w terminologii SSL/TLS. Dlatego każdy certyfikat osobisty używany na potrzeby uwierzytelniania SSL/TLS 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 MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM MQ” na stronie 44.

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). Więcej informacji na ten temat zawiera sekcja “Praca z odwołanymi certyfikatami” na stronie 348.
- 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 .

Ostrzeżenie: W filtrze SSLPEER mogą być używane tylko atrybuty z poniższej tabeli. Nazwy wyróżniające certyfikatów mogą zawierać inne atrybuty, ale filtrowanie nie jest dozwolone dla tych atrybutów.

Tabela 1. Typy atrybutów znajdujące się w nazwie wyróżniającej, które mogą być używane w filtrze SSLPEER

Typ atrybutu	**Opis**
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

Tabela 1. Typy atrybutów znajdujące się w nazwie wyróżniającej, które mogą być używane w filtrze SSLPEER (kontynuacja)	
Typ atrybutu	**Opis**
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 MQ toleruje niektóre zniekształcone nazwy wyróżniające. Więcej informacji na ten temat zawiera sekcja Reguły IBM 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).

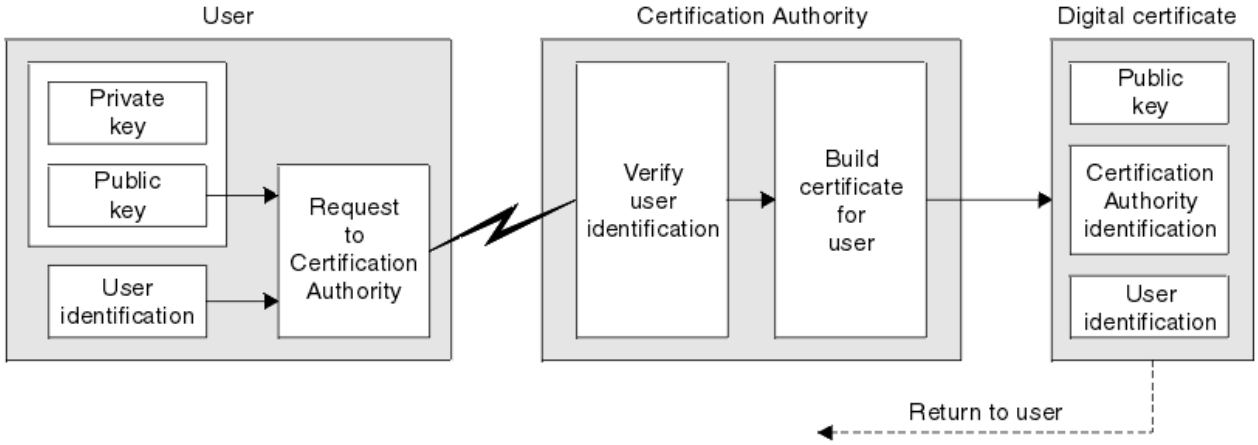
Certyfikat cyfrowy można uzyskać, wysyłając informacje do ośrodka CA, w postaci żądania certyfikatu. Standard X.509 definiuje format dla tych informacji, ale niektóre CAs mają własny format. Żądania certyfikatów są zwykle generowane przez narzędzie do zarządzania certyfikatami używane przez system, na przykład:

- Multi Narzędzie iKeyman w systemie Wiele platform.
- z/OS 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 13 ilustruje proces uzyskiwania certyfikatu cyfrowego z ośrodka CA.



Rysunek 3. Uzyskiwanie certyfikatu cyfrowego

Na diagramie:

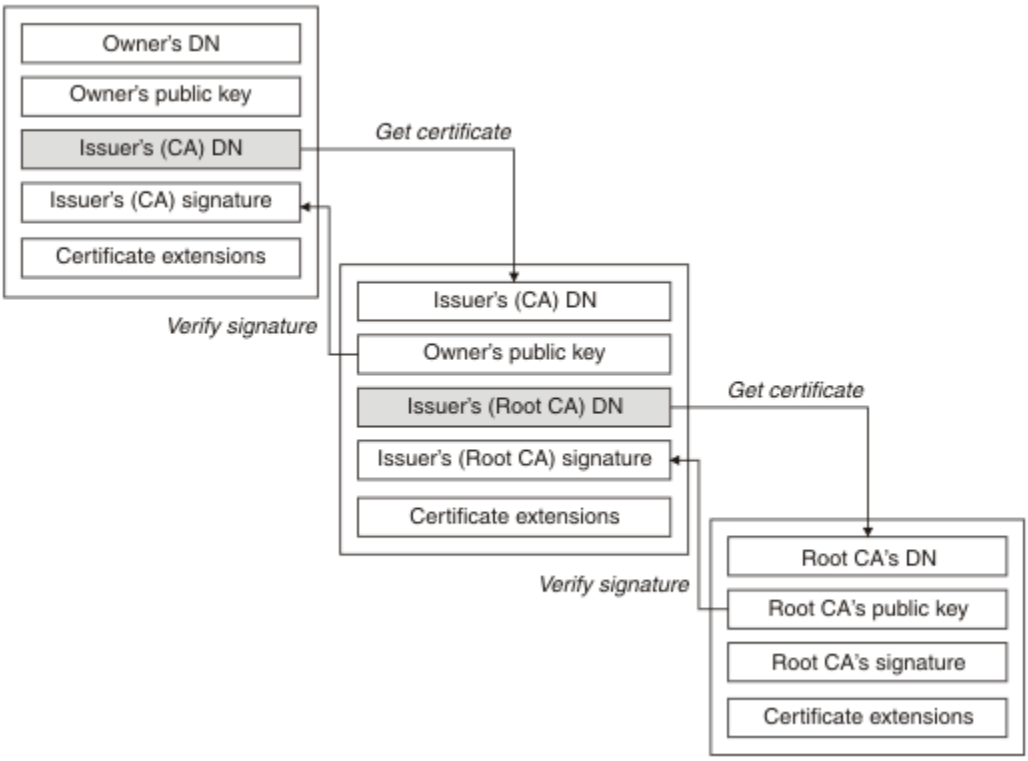
- Identyfikacja użytkownika obejmuje nazwę wyróżniającą podmiotu.
- Identyfikacja ośrodka certyfikacji obejmuje nazwę wyróżniającą ośrodka certyfikacji, który wystawił certyfikat.

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 14 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.

Świadectwa mogą być odwołane z różnych powodów, w tym:

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

Program IBM MQ może sprawdzić, czy certyfikat został unieważniony, wysyłając żądanie do programu odpowiadającego protokołu OCSP (Online Certificate Status Protocol) (tylko w systemie UNIX, Linux®, and Windows). Alternatywnie mogą oni uzyskać dostęp do listy odwołań certyfikatów (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 348.

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 10 . RAs weryfikuje informacje podane w przypadku zażądania certyfikatów cyfrowych. 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: 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 MQ obsługuje protokół 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 TLS w produkcie IBM MQ” na stronie 24
Produkt IBM MQ obsługuje protokół TLS (Transport Layer Security) w celu zapewnienia bezpieczeństwa na poziomie łącza dla kanałów komunikatów i kanałów MQI.

Pojęcia związane z protokołem TLS (Transport Layer Security)

Protokół TLS umożliwia 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.

Protokół TLS zapewnia bezpieczeństwo komunikacji przez internet i umożliwia 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 TLS jest inicjowane przez aplikację, która staje się klientem TLS. Aplikacja, która odbiera połączenie, staje się serwerem TLS. Każda nowa sesja rozpoczyna się uzgadnianiem, zgodnie z definicją w protokołach TLS.

Pełna lista opcji CipherSpecs obsługiwana przez produkt IBM MQ jest dostępna pod adresem “Włączanie opcji CipherSpecs” na stronie 433.

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/TLS

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

Ta sekcja zawiera podsumowanie kroków, które umożliwiają komunikowanie się klienta i serwera TLS ze sobą.

- Uzgodnić wersję protokołu, który ma być używany.
- Wybierz algorytmy szyfrujące.
- Uwierzytelniaj się nawzajem, wymieniając i sprawdzając certyfikaty cyfrowe.

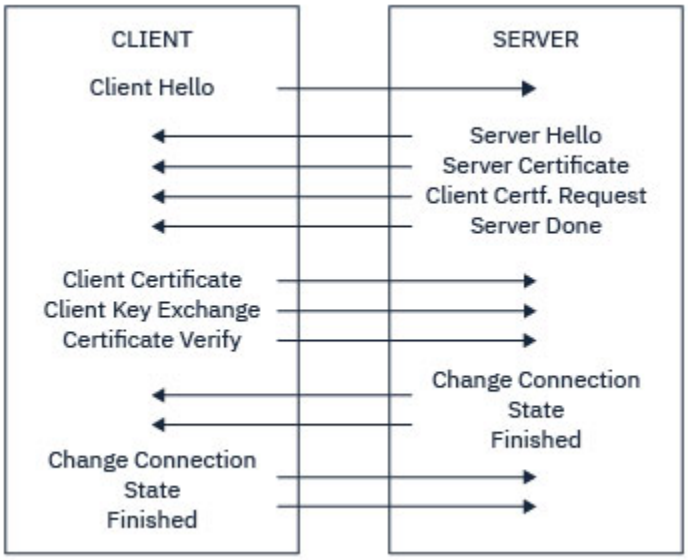
- Użyj technik szyfrowania asymetrycznego, aby wygenerować współużytkowany klucz tajny, który pozwala uniknąć problemu z dystrybucją klucza. Następnie protokół TLS używa klucza współużytkowanego do symetrycznego szyfrowania komunikatów, co jest szybsze niż szyfrowanie asymetryczne.

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

Czynności związane z uzgadnianiem TLS są następujące:

1. Klient TLS wysyła komunikat "klient hello" , który zawiera informacje kryptograficzne, takie jak wersja protokołu 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 TLS odpowiada za pomocą komunikatu "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 TLS weryfikuje certyfikat cyfrowy serwera. Więcej informacji na ten temat zawiera sekcja “Jak TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność” na stronie 17.
4. Klient TLS wysyła przypadkowy łańcuch bajtowy, który umożliwia klientowi i serwerowi obliczenie klucza tajnego używanego do szyfrowania kolejnych danych komunikatu. Sam losowy łańcuch bajtów jest zaszyfrowany kluczem publicznym serwera.
5. Jeśli serwer 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 TLS weryfikuje certyfikat klienta. Więcej informacji na ten temat zawiera sekcja “Jak TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność” na stronie 17.
7. Klient TLS wysyła do serwera komunikat "gotowy" , który jest zaszyfrowany kluczem tajnym, co oznacza, że część klienta została zakończona.
8. Serwer TLS wysyła klientowi komunikat "zakończony" , który jest zaszyfrowany kluczem tajnym, co oznacza, że część serwera została zakończona.
9. Na czas trwania sesji TLS serwer i klient mogą teraz wymieniać komunikaty, które są szyfrowane symetrycznie przy użyciu współużytkowanego klucza tajnego.

Rysunek 5 na stronie 17 przedstawia uzgadnianie TLS.



Rysunek 5. Przegląd uzgadniania TLS

Jak TLS zapewnia 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/TLS” na stronie 15.

Jak protokół TLS zapewnia 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 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 TLS, a ośrodek CA Y wysyła certyfikat do serwera TLS:

Tylko w przypadku uwierzytelniania serwera: serwer TLS musi:

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

i potrzeb klienta TLS:

- Certyfikat CA dla ośrodka CA Y

Jeśli serwer TLS wymaga uwierzytelniania klienta, serwer weryfikuje tożsamość klienta, weryfikując certyfikat cyfrowy klienta za pomocą klucza publicznego dla ośrodka CA, który wystawił certyfikat osobisty klientowi, 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 TLS, jak 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 16 i “6” na stronie 16 przeglądu, klient TLS weryfikuje certyfikat serwera, a serwer TLS weryfikuje certyfikat klienta. Weryfikacja ta ma cztery aspekty:

1. Podpis cyfrowy jest sprawdzany (patrz “Podpisy cyfrowe w SSL/TLS” na stronie 19).
2. Łańcuch certyfikatów jest sprawdzany. Należy mieć pośrednie certyfikaty ośrodka CA (patrz “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 348).

Resetowanie klucza tajnego

Podczas uzgadniania TLS generowane jest *klucz tajny* służący do szyfrowania danych między klientem i serwerem 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 TLS zapewnia poufność

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

Jak protokół TLS zapewnia integralność

Protokół TLS zapewnia integralność danych, obliczając streszczenie komunikatu. Więcej informacji zawiera sekcja “Integralność danych komunikatów” na stronie 472.

Użycie protokołu TLS zapewnia integralność danych, pod warunkiem, że parametr CipherSpec w definicji kanału używa algorytmu mieszającego zgodnie z opisem w tabeli w produkcie “Włączanie opcji CipherSpecs” na stronie 433.

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 połączenia TLS muszą uzgodnić tę samą właściwość CipherSpec , aby móc komunikować się.

Produkt IBM MQ obsługuje protokół TLS 1.2 . Można jednak włączyć nieaktualne atrybuty CipherSpecs, jeśli jest to konieczne.

Więcej informacji na ten temat zawiera sekcja “Włączanie opcji CipherSpecs” na stronie 433 :

- CipherSpecs obsługiwane przez produkt IBM MQ
- Sposób włączania nieaktualnych specyfikacji SSL 3.0 i TLS 1.0 CipherSpecs

Ważne: W przypadku korzystania z kanałów produktu IBM 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 “Włączanie opcji CipherSpecs” na stronie 433.

CipherSuite to zestaw algorytmów szyfrujących używanych przez połączenie 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 zostały określone dla połączenia TLS. Nazwa poprawnego zestawu algorytmów szyfrowania CipherSuite definiuje kombinację algorytmów używanych. Na przykład: CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA określa:

- Algorytm wymiany kluczy RSA i algorytm uwierzytelniania
- Algorytm szyfrowania AES, korzystający z 128-bitowego klucza i trybu łączenia zaszyfrowanych bloków (CBC)
- Kod uwierzytelniania komunikatu SHA-1 (MAC)

Podpisy cyfrowe w SSL/TLS

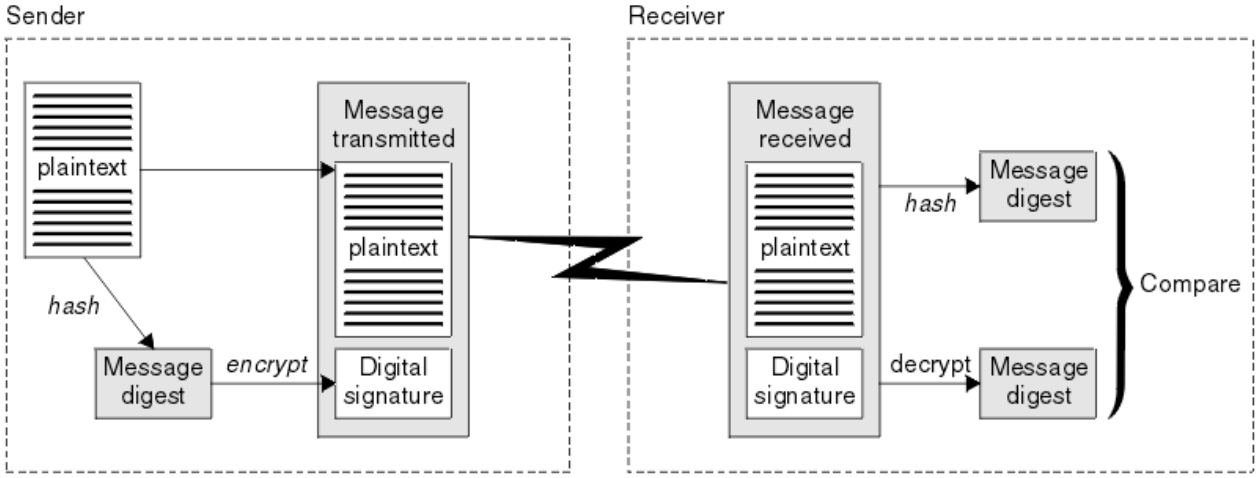
Podpis cyfrowy jest tworzony przez zaszyfrowanie reprezentacji komunikatu. Szyfrowanie korzysta z klucza prywatnego sygnatariusza, a w przypadku efektywności zazwyczaj działa na streszczanie wiadomości, a nie na samym komunikacie.

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 20 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 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.

Pojęcia pokrewne

“National Security Agency (NSA) Suite B Cryptography” na stronie 21
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.

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 ze standardem Suite B, który ma być używany z protokołem TLS 1.2. Po skonfigurowaniu dla operacji zgodnej z pakietem B używane są tylko ograniczone algorytmy szyfrowania wymienione na liście.
2. Profil przejściowy do użycia z protokołem TLS 1.0 lub TLS 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 systemie Windowssystemy UNIX and Linux IBM MQmożna skonfigurować w taki sposób, aby były zgodne z profilem TLS 1.2 zgodnym z pakietem B, ale nie obsługują profilu przejściowego Suite B. Więcej informacji zawiera sekcja “Szyfrowanie NSA Suite B Cryptography w produkcie IBM MQ” na stronie 41.

Odsyłacze 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 MQ mechanizmy zabezpieczeń

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

Produkt IBM 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 MQ

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

Poniżej przedstawiono kilka przykładów identyfikacji i uwierzytelniania w środowisku IBM 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 6
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 MQ

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

Poniżej przedstawiono kilka przykładów autoryzacji w środowisku produktu IBM MQ :

- Zezwalanie tylko autoryzowanym administratorom na wydawanie komend do zarządzania zasobami produktu IBM 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 85 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 MQ

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

Poniżej przedstawiono kilka przykładów kontroli w środowisku produktu IBM 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 7

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 MQ

Poufność można zaimplementować w programie IBM MQ , szyfrując komunikaty.

Poufność może być zapewniona w środowisku IBM MQ w następujący sposób:

- Gdy wysyłający agent MCA pobiera komunikat z kolejki transmisji, produkt IBM MQ używa protokołu 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 MQ mogą być uznane za wystarczające do ochrony ich zawartości przed nieuprawnionym ujawnieniem. Jednak w przypadku większego poziomu zabezpieczeń można użyć programu Advanced Message Security do zaszyfrowania komunikatów zapisanych w kolejkach.
- z/OS V 9.1.4 Komunikaty przechowywane w kolejkach lokalnych mogą być szyfrowane w stanie spoczynku przy użyciu szyfrowania zestawu danych z/OS .

  Patrz sekcja poufność danych w produkcie IBM MQ for z/OS przy użyciu szyfrowania zestawu danych. :NONE.

Pojęcia pokrewne

“Poufność” na stronie 7

Usługa *poufności* zabezpiecza poufne informacje przed nieautoryzowanym ujawnieniem.

Integralność danych w produkcie IBM MQ

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

Integralność danych może być zapewniona w środowisku IBM MQ w następujący sposób:

- Za pomocą protokołu TLS można wykryć, czy treść komunikatu została celowo zmodyfikowana w czasie, gdy była przesyłana przez sieć. W protokole TLS algorytm streszczenia komunikatów umożliwia wykrywanie zmodyfikowanych komunikatów w tranzycie.

  Wszystkie IBM MQ CipherSpecs udostępniają algorytm tworzenia skrótu komunikatu, z wyjątkiem TLS_RSA_WITH_NULL_NULL, który nie zapewnia integralności danych komunikatu.

  Program IBM MQ wykrywa zmodyfikowane komunikaty po ich odebraniu; po odebraniu zmodyfikowanego komunikatu program IBM MQ zgłasza komunikat o błędzie AMQ9661 , a kanał zostanie zatrzymany.
- Podczas zapisywania komunikatów w kolejce lokalnej mechanizmy kontroli dostępu udostępniane przez produkt IBM MQ mogą być uważane za wystarczające, aby zapobiec celowej modyfikacji treści komunikatów.

  Jednak w przypadku większego poziomu zabezpieczeń można użyć programu 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.

  Po wykryciu zmodyfikowanego komunikatu aplikacja próba odebrania komunikatu otrzymuje kod powrotu 2063, a w przypadku użycia wywołania MQGET komunikat zostaje przeniesiony do systemu SYSTEM.PROTECTION.ERROR.QUEUE

Pojęcia pokrewne

“Integralność danych” na stronie 7

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

Kryptografia w produkcie IBM MQ

Produkt IBM MQ udostępnia kryptografię za pomocą protokołu TLS (Transport Security Layer).

Więcej informacji na ten temat zawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24.

Pojęcia pokrewne

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

Protokoły zabezpieczeń TLS w produkcie IBM MQ

Produkt IBM MQ obsługuje protokół TLS (Transport Layer Security) w celu zapewnienia bezpieczeństwa na poziomie łącza dla kanałów komunikatów i kanałów MQI.

Kanały komunikatów i kanały MQI mogą korzystać z protokołu TLS w celu zapewnienia bezpieczeństwa na poziomie łącza. Program wywołujący MCA to klient protokołu TLS, a agent odbierający MCA jest serwerem TLS. Produkt IBM MQ obsługuje protokoły TLS 1.0 i TLS 1.2. Można określić algorytmy szyfrowania, które są używane przez protokół TLS przez podanie wartości CipherSpec jako części definicji kanału.

Uwaga: Z poziomu produktu IBM MQ 8.0.0 Fix Pack 2protokół SSLv3 i korzystanie z niektórych IBM MQ CipherSpecs są nieaktualne. Więcej informacji na ten temat zawiera sekcja Deprecation: SSLv3 protocol.

Za pomocą parametrów SECPROT i SSLCIPH można wyświetlać protokół zabezpieczeń i atrybut CipherSpec w użyciu w kanale.

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

Menedżery kolejek i użytkownicy klienta IBM MQ nie muszą mieć powiązanych z nimi osobistych certyfikatów cyfrowych, gdy działają jako klienci TLS, chyba że po stronie serwera kanału określono wartość SSLCAUTH (REQUIRED).

Certyfikaty cyfrowe są przechowywane w *repozytorium kluczy*. Atrybut **SSLKeyRepository** menedżera kolejek określa położenie repozytorium kluczy, w którym znajduje się certyfikat cyfrowy menedżera kolejek. W systemie klienckim IBM MQ zmienna środowiskowa MQSSLKEYR określa położenie repozytorium kluczy, w którym znajduje się certyfikat cyfrowy użytkownika. Alternatywnie aplikacja kliencka IBM MQ może określić jej położenie w polu **KeyRepository** struktury opcji konfiguracji 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.

Obsługa protokołu TLS

Produkt IBM MQ zapewnia obsługę protokołów TLS 1.0 i TLS 1.2 zgodnie z wykorzystudzonym przez użytkownika platformą. Więcej informacji na temat protokołu TLS można znaleźć w informacjach znajdujących się w podtematach.

IBM i
Obsługa protokołu TLS jest integralna w systemie operacyjnym IBM i .

Klienty Java i JMS
Te klienty używają wirtualnej maszyny języka Java do obsługi protokołu TLS.

Systemy UNIX, Linux, and Windows
Obsługa protokołu TLS jest instalowana wraz z produktem IBM MQ.

z/OS
Obsługa protokołu TLS jest integralna w systemie operacyjnym z/OS . Obsługa protokołu TLS w systemie z/OS jest znana jako *System SSL*(System SSL).

Informacje na temat wymagań wstępnych dotyczących obsługi protokołu IBM MQ TLS znajdują się w sekcji Wymagania systemowe produktu IBM MQ.

Pojęcia pokrewne

“Protokoły zabezpieczeń szyfrujących: TLS” na stronie 15
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 MQ obsługuje protokół TLS.

Repozytorium kluczy SSL/TLS

Wzajemnie uwierzytelnione połączenie TLS wymaga repozytorium kluczy 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. Repozytorium kluczy jest przywołane przez różne nazwy na różnych platformach i środowiskach obsługujących protokół TLS:

- IBM i W systemie IBM i: *baza certyfikatów*
- W systemach Java i JMS: *magazyn kluczy* i *magazyn zaufanych certyfikatów*
- ULW W systemie UNIX, Linux, and Windows: *plik bazy danych kluczy*
- z/OS W systemie z/OS: *keyring*

Więcej informacji na ten temat zawierają sekcje “certyfikaty cyfrowe” na stronie 10 i “Pojęcia związane z protokołem TLS (Transport Layer Security)” na stronie 15.

Wzajemnie uwierzytelnione połączenie TLS wymaga repozytorium kluczy na każdym końcu połączenia. Repozytorium kluczy może zawierać następujące certyfikaty i żądania:

- 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 IBM MQ MQI client. Certyfikaty osobiste są niezbędne dla klienta 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 MQ” na stronie 26.

Położenie repozytorium kluczy zależy od platformy używanej przez użytkownika:

IBM i **IBM i**

Repozytorium kluczy to baza certyfikatów. Domyślna baza certyfikatów systemu znajduje się w `/QIBM/UserData/ICSS/Cert/Server/Default` w zintegrowanym systemie plików (IFS). Produkt IBM MQ przechowuje hasło do bazy certyfikatów w *pliku ukrytych haseł*. Na przykład plikiem ukrytym dla menedżera kolejek `QM1` jest `/QIBM/UserData/mqm/qmgrs/QM1/ssl/Stash.sth`.

Można również określić, że zamiast niego ma być używana baza certyfikatów systemu IBM i . W tym celu należy zmienić wartość atrybutu menedżera kolejek **SSLKEYR** na *SYSTEM. Ta wartość wskazuje, że menedżer kolejek musi korzystać ze składnicy certyfikatów systemu, a menedżer kolejek jest zarejestrowany do użycia jako aplikacja z programem Digital Certificate Manager (DCM).

Baza certyfikatów zawiera również klucz prywatny menedżera kolejek.

ULW **UNIX, Linux, and Windows systemy**

Repozytorium kluczy 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 MQ jest zainstalowany w położeniu domyślnym, równoważną ścieżką w systemie Windows jest C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb.

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: Szyfrujące karty sprzętowe 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, program IBM MQ nadal wymaga dostępu do obu plików bazy danych kluczy i pliku ukrytych haseł.

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

z/OS **z/OS**

Certyfikaty są przechowywane w pliku kluczy w produkcie z/OS.

Inne zewnętrzne menedżery zabezpieczeń (ESM) używają również breloków do przechowywania certyfikatów.

Klucze prywatne są zarządzane przez produkt RACF.

Zabezpieczanie repozytoriów kluczy produktu IBM MQ
Repozytorium kluczy dla produktu IBM 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 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.

Cyfrowe etykiety certyfikatów, zrozumienie wymagań
Podczas konfigurowania protokołu 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.

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 **Subject Distinguished Name** certyfikatu lub **Subject Common Name** . Należy zauważyć, że **Subject Distinguished Name** i **Subject Common Name** są polami w samym certyfikacie. Są one definiowane podczas tworzenia certyfikatu i nie można ich zmieniać. Jeśli jest to konieczne, można zmienić etykietę powiązaną z certyfikatem cyfrowym.

Składnia etykiety certyfikatu

Etykieta certyfikatu może zawierać litery, cyfry i znaki interpunkcyjne, jeśli spełnione są następujące warunki:

- Multi Etykieta certyfikatu może zawierać do 64 znaków.
- z/OS Etykieta certyfikatu może zawierać do 32 znaków.
- Etykieta certyfikatu może zawierać spacje.
- W etykietach rozróżniana jest wielkość liter.
- W systemach, w których używana jest katakana EBCDIC, nie można używać małych liter.

Dodatkowe wymagania dotyczące wartości etykiety certyfikatu są określone w poniższych sekcjach.

W jaki sposób używana jest etykieta certyfikatu?

Produkt IBM MQ korzysta z etykiet certyfikatów w celu znalezienia certyfikatu osobistego, który jest wysyłany podczas uzgadniania TLS. Eliminuje to niejednoznaczność, jeśli w repozytorium kluczy istnieje więcej niż jeden certyfikat osobisty.

Etykietę certyfikatu można ustawić na wartość wybraną przez użytkownika. Jeśli wartość nie zostanie ustawiona, zostanie użyta etykieta domyślna zgodna z konwencją nazewnictwa, w zależności od używanej platformy. Szczegółowe informacje można znaleźć w poniższych sekcjach, dotyczących poszczególnych platform.

Uwagi:

1. Nie można samodzielnie ustawić etykiety certyfikatu w systemach Java lub JMS .
2. Automatycznie zdefiniowane kanały utworzone przez wyjście CHAD (channel automatic definition) nie mogą ustawić etykiety certyfikatu, ponieważ uzgadnianie TLS wystąpiło podczas tworzenia kanału. Ustawienie etykiety certyfikatu w wyjściu CHAD dla kanałów przychodzących nie ma żadnego efektu.

W tym kontekście klient TLS odwołuje się do partnera połączenia inicjującego uzgadnianie, które może być klientem IBM MQ lub innym menedżerem kolejek.

Podczas uzgadniania TLS klient TLS zawsze uzyskuje i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji IBM MQ serwer TLS zawsze żąda certyfikatu od klienta, a klient zawsze udostępnia certyfikat serwerowi, jeśli taki certyfikat zostanie znaleziony. Jeśli klient nie może znaleźć certyfikatu osobistego, klient wysyła odpowiedź no `certificate` na serwer.

Serwer 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 TLS, jest zdefiniowany z parametrem **SSLCAUTH** ustawionym na *REQUIRED* lub zestawem wartości parametru **SSLPEER** .

Należy zauważyć, że kanały przychodzące (w tym odbiornik, requester, odbiornik klastra, serwer niekwalifikowany i kanały połączenia z serwerem) wysyłają skonfigurowany certyfikat tylko wtedy, gdy wersja IBM MQ zdalnego węzła sieci w pełni obsługuje konfigurację etykiety certyfikatu, a kanał używa protokołu TLS CipherSpec.

Niekwalifikowany kanał serwera to taki, który nie ma ustawionego pola CONNAME.

We wszystkich innych przypadkach parametr **CERTLABL** menedżera kolejek określa wysłanie certyfikatu. W szczególności następujące informacje są dostępne tylko w przypadku certyfikatu skonfigurowanego przez parametr **CERTLABL** menedżera kolejek, niezależnie od ustawienia etykiety specyficznej dla kanału:

- W wersjach wcześniejszych niż IBM MQ 9.1.1, wszystkie bieżące klienty Java i JMS .
- V 9.1.1 Klienty IBM MQ 9.1.1, Java i JMS obsługujące obsługę nazw serwera (Server Name Indication-SNI), czyli certyfikaty na kanale za pomocą kanałów.
- Wersje produktu IBM MQ wcześniejszych niż IBM MQ 8.0.
- Zarządzane klienty .NET

Ponadto certyfikat używany przez kanał musi być odpowiedni dla kanału CipherSpec -więcej informacji na ten temat można znaleźć w sekcji “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45 .

Produkt IBM MQ 8.0 i nowszy obsługuje użycie wielu certyfikatów w tym samym menedżerze kolejek przy użyciu etykiety certyfikatu dla każdego kanału, określonego przy użyciu atrybutu **CERTLABL** w definicji kanału. Kanały przychodzące do menedżera kolejek (na przykład połączenia z serwerem lub odbiorcy) polegają na wykrywaniu nazwy kanału za pomocą funkcji SNI (TLS Server Name Indication) w celu przedstawienia poprawnego certyfikatu z menedżera kolejek.

Jeśli kanał łączy się z docelowym menedżerem kolejek za pomocą programu IBM MQ Internet Pass-Thru (MQIPT), a trasa MQIPT zawiera zarówno zestaw **SSLServer** , jak i zestaw **SSLClient** , między punktami końcowymi istnieją dwie oddzielne sesje TLS, a dane SNI nie przepływa przez przerwy w sesji. Uniemożliwia to używanie certyfikatu na podstawie kanału w docelowym menedżerze kolejek w przypadku połączenia TLS między programem MQIPT a menedżerem kolejek. Aby użyć certyfikatu na podstawie kanału w docelowym menedżerze kolejek, w przypadku połączenia TLS, które przechodzi przez MQIPT, trasa MQIPT musi używać trybu proxy TLS, który przekazuje wszystkie przepływy sterowania TLS w stanie nienaruszonym, w tym nazwę SNI. Więcej informacji na temat obsługi protokołu TLS w produkcie MQIPTmożna znaleźć w sekcji Obsługa protokołu SSL/TLS.

Certyfikaty używane dla połączeń TLS, które zostały zakończone lub zainicjowane przez produkt MQIPT , mogą być konfigurowane indywidualnie dla każdej trasy, na przykład przy użyciu właściwości trasy **SSLServerSiteLabel** i **SSLClientSiteLabel** .

Więcej informacji na temat nawiązywania połączenia z menedżerem kolejek przy użyciu uwierzytelniania jednokierunkowego, czyli gdy klient TLS nie wysyła certyfikatu, zawiera sekcja Łączenie dwóch menedżerów kolejek za pomocą uwierzytelniania jednokierunkowego.

Systemy z wieloma platformami

Multi

W systemie Wiele platformserwer TLS wysyła certyfikat do klienta.

W przypadku menedżerów kolejek i klientów poniższe źródła są przeszukiwane w kolejności, w której wartość nie jest pusta. Pierwsza niepusta wartość określa etykietę certyfikatu. Etykieta certyfikatu musi istnieć w repozytorium kluczy. Jeśli nie zostanie znaleziony zgodny certyfikat w poprawnym przypadku i formacie, który jest zgodny z etykietą, wystąpi błąd i uzgadnianie TLS nie powiedzie się.

Menedżery kolejek

1. Atrybut etykiety certyfikatu kanału **CERTLABL**.
2. Atrybut etykiety certyfikatu menedżera kolejek **CERTLABL**.
3. Wartość domyślna, która jest w formacie: `ibmwebspheremq` z dodanym nazwą menedżera kolejek, wszystkie małymi literami. Na przykład dla menedżera kolejek o nazwie `QM1`, domyślną etykietą certyfikatu jest `ibmwebspheremqqm1`.

IBM MQ klienty

1. Atrybut etykiety certyfikatu **CERTLABL** w definicji kanału CLNTCONN.
2. Atrybut struktury MQSCO **CertificateLabel** .
3. Zmienna środowiskowa **MQCERTLABL**.
4. Plik klienta `.ini` (w jego sekcji SSL) **CertificateLabel** , atrybut
5. Wartość domyślna, która ma format: `ibmwebspheremq` z identyfikatorem użytkownika, który jest uruchomiony przez aplikację kliencką, a wszystkie z małymi literami. Na przykład dla ID użytkownika USER1domyślną etykietą certyfikatu jest `ibmwebspheremquser1`.

z/OS systemy

z/OS

Klienty IBM MQ nie są obsługiwane w systemie z/OS. Menedżer kolejek produktu z/OS może jednak działać w roli klienta TLS podczas inicjowania połączenia lub serwera TLS podczas akceptowania żądania połączenia. Wymagania dotyczące etykiet certyfikatów dla menedżerów kolejek produktu z/OS mają zastosowanie zarówno w tych rolach, jak i różnią się od wymagań w produkcie Wiele platform.

W przypadku menedżerów kolejek i klientów poniższe źródła są przeszukiwane w kolejności, w której wartość nie jest pusta. Pierwsza niepusta wartość określa etykietę certyfikatu. Etykieta certyfikatu musi istnieć w repozytorium kluczy. Jeśli nie zostanie znaleziony zgodny certyfikat w poprawnym przypadku i formacie, który jest zgodny z etykietą, wystąpi błąd i uzgadnianie TLS nie powiedzie się.

1. Atrybut etykiety certyfikatu kanału, **CERTLABL**.
2. Jeśli ta opcja jest współużytkowana, atrybut etykiety certyfikatu grupy współużytkowania kolejki **CERTQSGL**.

   Jeśli ta opcja nie jest współużytkowana, atrybut etykiety certyfikatu menedżera kolejek **CERTLABL**.
3. Wartość domyślna, która jest w formacie: `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek lub grupy współużytkowania kolejek. Należy zauważyć, że w tym łańcuchu jest rozróżniana wielkość liter i należy je zapisać w sposób pokazany. Na przykład dla menedżera kolejek o nazwie `QM1`, domyślną etykietą certyfikatu jest `ibmWebSphereMQQM1`.
4. If there is not a certificate found with the format in option “3” na stronie 29, IBM MQ attempts to use the certificate marked as default in the key ring.

Więcej informacji na temat sposobu wyświetlania repozytorium kluczy zawiera sekcja “Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie z/OS” na stronie 329.

IBM MQ Java and IBM MQ JMS clients

Klienty IBM MQ Java i IBM MQ JMS korzystają z infrastruktury dostawcy JSSE (Java Secure Socket Extension) w celu wybrania certyfikatu osobistego podczas uzgadniania TLS i dlatego nie podlegają wymaganiom etykiety certyfikatu.

Domyślnym zachowaniem jest to, że klient JSSE wykonuje iteracje przez certyfikaty w repozytorium kluczy, wybierając pierwszy znaleziony 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 IBM MQ Java w połączeniu z konkretnym dostawcą JSSE, można włączyć debugowanie, ustawiając wartość `javax.net.debug=ssl` w środowisku JVM.

Zmienną można ustawić w aplikacji, konfigurując lub wpisując `-Djavax.net.debug=ssl` w wierszu komend.

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 IBM MQ Explorer. Więcej informacji na ten temat zawiera opis komendy MQCMD_REFRESH_SECURITY i tematu *Ponowne zwalnianie zabezpieczeń TLS* w sekcji IBM MQ Explorer tej dokumentacji produktu.

Pojęcia pokrewne

“Odświeżanie widoku zawartości repozytorium kluczy SSL/TLS przez klienta i ustawień SSl/TLS” na stronie 30
Aby zaktualizować aplikację kliencką przy użyciu odświeżonej treści repozytorium kluczy, należy zatrzymać i zrestartować aplikację kliencką.

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

Nie można odświeżyć zabezpieczeń na kliencie IBM MQ ; dla klientów nie ma odpowiednika komendy REFRESH SECURITY TYPE (SSL) (patrz REFRESH SECURITY). aby uzyskać więcej informacji.

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 29
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).

Ochrona hasłem protokołu MQCSP

W produkcie IBM MQ 8.0można wysyłać hasła, które są zawarte w strukturze MQCSP, chronione, za pomocą funkcji IBM MQ lub zaszyfrowane przy użyciu szyfrowania TLS.

Ważne: Ochrona hasłem protokołu MQCSP jest przydatna w celach testowych i programistycznych, ponieważ korzystanie z zabezpieczenia hasłem protokołu MQCSP jest prostsze niż konfigurowanie szyfrowania TLS, ale nie jako bezpieczne. Do celów produkcyjnych należy używać szyfrowania TLS w preferencjach dotyczących ochrony hasłem produktu IBM MQ , zwłaszcza gdy sieć między klientem a menedżerem kolejek jest niezaufana, ponieważ szyfrowanie TLS jest bezpieczniejsze.

Jeśli chodzi dokładnie o to, jakie szyfrowanie jest używane, a także o jaką ochronę oferuje, należy użyć pełnego szyfrowania TLS. W tej sytuacji algorytmy są powszechnie znane, a użytkownik może wybrać odpowiedni dla przedsiębiorstwa, używając atrybutu kanału **SSLCIPH** .

Więcej informacji na temat struktury MQCSP zawiera sekcja Struktura MQCSP.

Ochrona hasłem jest używana, gdy spełnione są wszystkie następujące warunki:

- Oba końce połączenia korzystają z produktu IBM MQ 8.0lub nowszego.
- Kanał nie używa szyfrowania TLS. Kanał nie używa szyfrowania TLS, jeśli dla kanału jest pusty atrybut **SSLCIPH** lub atrybut **SSLCIPH** jest ustawiony na wartość CipherSpec , która nie udostępnia szyfrowania. Szyfry o wartości NULL, na przykład wartość NULL_SHA, nie zapewniają szyfrowania.
- Ustawiono **MQCSP**.**AuthenticationType** do MQCSP_AUTH_USER_ID_AND_PWD. Ustawienie tej wartości umożliwia wartościowanie większej liczby sprawdzeń w celu podjęcia decyzji o tym, czy ochrona hasłem jest wykonywana. Wartość domyślna **MQCSP**.**AuthenticationType** to MQCSP_AUTH_NONE. Ustawienie domyślne oznacza, że ochrona hasłem nie jest wykonywana. Więcej informacji na ten temat zawiera sekcja **AuthenticationType**.
- Jeśli klient jest programem IBM MQ Explorer, a tryb zgodności z identyfikacją użytkowników nie jest włączony, co nie jest wartością domyślną. Ten warunek ma zastosowanie tylko do programu IBM MQ Explorer.

Jeśli te warunki nie są spełnione, hasło jest wysyłane w postaci jawnej, chyba że jest to zabronione przez ustawienie konfiguracyjne produktu **PasswordProtection** .

Ustawienie konfiguracyjne PasswordProtection

Atrybut **PasswordProtection** w sekcji Kanały w plikach konfiguracyjnych .ini klienta i menedżera kolejek może uniemożliwić wysyłanie haseł w postaci jawnego tekstu. Atrybut może przyjmować jedną z następujących wartości. Wartością domyślną jest `compatible`:

Kompatybilny
Hasło może zostać wysłane w postaci jawnego tekstu, jeśli menedżer kolejek lub klient uruchomił wersję produktu IBM MQ wcześniejszą niż IBM MQ 8.0. Oznacza to, że hasła w postaci zwykłego tekstu są dozwolone w celu zachowania zgodności.

Zatem:

- Hasło jest wysyłane za pomocą protokołu TLS CipherSpec , jeśli używane jest szyfrowanie TLS, a atrybut CipherSpec nie ma wartości NULL.
- Hasło jest wysyłane w postaci jawnego tekstu, jeśli menedżer kolejek lub klient uruchomił wersję produktu IBM MQ wcześniejszą niż IBM MQ 8.0, a szyfrowanie TLS nie jest używane. Hasło jest wysyłane w postaci zwykłego tekstu, ponieważ wersje produktu IBM MQ w wersji wcześniejszej niż IBM MQ 8.0 mogą wysyłać hasła tylko w postaci jawnego tekstu.
- Hasło jest chronione, jeśli zarówno menedżer kolejek, jak i klient uruchamiają wersję produktu IBM MQ w systemie IBM MQ 8.0 lub nowszym, przy użyciu wartości NULL CipherSpec , lub szyfrowanie TLS nie jest używane. **MQCSP**.Parametr **AuthenticationType** musi być ustawiony na wartość MQCSP_AUTH_USER_ID_AND_PWD.
- Połączenie nie powiedzie się, zanim hasło zostanie wysłane, jeśli zarówno menedżer kolejek, jak i klient uruchamiają wersję produktu IBM MQ w wersji IBM MQ 8.0 lub nowszej oraz **MQCSP**.Wartość **AuthenticationType** nie jest ustawiona na wartość MQCSP_AUTH_USER_ID_AND_PWD.

zawsze
Hasło musi być zaszyfrowane za pomocą specyfikacji CipherSpec , która nie jest wartością NULL CipherSpec, ani **MQCSP**.Parametr **AuthenticationType** musi być ustawiony na wartość MQCSP_AUTH_USER_ID_AND_PWD. W przeciwnym razie połączenie nie powiedzie się. Oznacza to, że hasła w postaci jawnej nie są dozwolone.

Zatem:

- Hasło jest wysyłane za pomocą protokołu TLS CipherSpec , jeśli używane jest szyfrowanie TLS, a atrybut CipherSpec nie ma wartości NULL.
- Hasło jest chronione, jeśli zarówno menedżer kolejek, jak i klient uruchamiają wersję produktu IBM MQ w systemie IBM MQ 8.0 lub nowszym, a szyfrowanie TLS nie jest używane albo używana jest wartość NULL CipherSpec . **MQCSP**.Parametr **AuthenticationType** musi być ustawiony na wartość MQCSP_AUTH_USER_ID_AND_PWD.
- Połączenie nie powiedzie się, zanim hasło zostanie wysłane, jeśli menedżer kolejek lub klient uruchomił wersję produktu IBM MQ wcześniejszą niż IBM MQ 8.0, a szyfrowanie TLS nie jest używane. Ponieważ wersje produktu IBM MQ w wersji wcześniejszej niż IBM MQ 8.0 mogą wysyłać hasła tylko w postaci zwykłego tekstu, a program `always` wymaga, aby hasło było szyfrowane lub chronione, nawiązanie połączenia nie powiedzie się.

opcjonalne
Hasło może być opcjonalnie wysłane, ale jest wysyłane w postaci jawnego tekstu, jeśli jest to **MQCSP**.Wartość **AuthenticationType** nie jest ustawiona na wartość MQCSP_AUTH_USER_ID_AND_PWD. Oznacza to, że hasła w postaci zwykłego tekstu mogą być wysyłane przez dowolnego klienta.

Zatem:

- Hasło jest wysyłane za pomocą protokołu TLS CipherSpec , jeśli używane jest szyfrowanie TLS, a atrybut CipherSpec nie ma wartości NULL.
- Hasło jest wysyłane w postaci jawnej, jeśli używana jest wartość NULL CipherSpec i **MQCSP**.Wartość **AuthenticationType** nie jest ustawiona na wartość MQCSP_AUTH_USER_ID_AND_PWD.
- Hasło jest wysyłane w postaci jawnego tekstu, jeśli menedżer kolejek lub klient uruchomił wersję produktu IBM MQ wcześniejszą niż IBM MQ 8.0, a szyfrowanie TLS nie jest używane. Hasło jest

wysyłane w postaci zwykłego tekstu, ponieważ wersje produktu IBM MQ w wersji wcześniejszej niż IBM MQ 8.0 mogą wysyłać hasła tylko w postaci jawnego tekstu.

- Hasło jest chronione, jeśli zarówno menedżer kolejek, jak i klient uruchamiają wersję produktu IBM MQ w wersji IBM MQ 8.0 lub nowszej, szyfrowanie TLS nie jest używane lub używany jest parametr CipherSpec o wartości NULL, a także **MQCSP**.Parametr **AuthenticationType** jest ustawiony na wartość MQCSP_AUTH_USER_ID_AND_PWD.

ostrzeżenie
Hasła w postaci zwykłego tekstu mogą być wysyłane przez dowolnego klienta. Jeśli hasło zwykłego tekstu zostanie odebrane jako komunikat ostrzegawczy (AMQ9297), zostanie zapisany w dziennikach błędów menedżera kolejek.

W przypadku klientów Java i JMS zachowanie atrybutu **PasswordProtection** zmienia się w zależności od wyboru trybu zgodności lub trybu MQCSP:

- Jeśli klienty Java i JMS działają w trybie zgodności, podczas przetwarzania połączenia struktura MQCSP nie jest przetwarzana. Oznacza to, że zachowanie atrybutu **PasswordProtection** jest takie samo, jak w przypadku klientów uruchamiających wersję produktu IBM MQ wcześniejszą niż IBM MQ 8.0.
- Jeśli klienty Java i JMS działają w trybie MQCSP, zachowanie atrybutu **PasswordProtection** jest zachowaniem w sposób opisany poniżej.

Więcej informacji na temat uwierzytelniania połączenia z klientami Java i JMS zawiera sekcja “Uwierzytelnianie połączenia z klientem Java” na stronie 79.

menedżer certyfikatów cyfrowych (Digital Certificate Manager – DCM)

Za pomocą programu DCM można zarządzać certyfikatami cyfrowymi i kluczami prywatnymi w systemie IBM i.

Program Digital Certificate Manager (DCM) umożliwia zarządzanie certyfikatami cyfrowymi i korzystanie z nich w bezpiecznych aplikacjach na serwerze IBM i . Za pomocą programu Digital Certificate Managermożna żądać i przetwarzać certyfikaty cyfrowe pochodzące od ośrodków certyfikacji (CA) lub innych osób trzecich. Użytkownik może również pełnić rolę lokalnego ośrodka certyfikacji w celu tworzenia certyfikatów cyfrowych dla użytkowników i zarządzania nimi.

Program DCM obsługuje także korzystanie z list CRL (Certificate Revocation Lists) w celu zapewnienia mocniejszego procesu sprawdzania poprawności certyfikatu i aplikacji. Za pomocą programu DCM można zdefiniować położenie, w którym określona lista CRL ośrodka certyfikacji znajduje się na serwerze LDAP, dzięki czemu program IBM MQ może sprawdzić, czy konkretny certyfikat nie został odwołany.

Program DCM obsługuje i może automatycznie wykrywać certyfikaty w różnych formatach. Gdy program DCM wykryje certyfikat kodowany PKCS #12 lub certyfikat PKCS #7 , który zawiera zaszyfrowane dane, automatycznie prosi użytkownika o podanie hasła, które zostało użyte do zaszyfrowania certyfikatu. Program DCM nie wyświetla monitów o certyfikaty PKCS #7 , które nie zawierają zaszyfrowanych danych.

Program DCM udostępnia oparty na przeglądarce interfejs użytkownika, który może być używany do zarządzania certyfikatami cyfrowymi aplikacji i użytkowników. Interfejs użytkownika jest podzielony na dwie główne ramki: ramkę nawigacyjną i ramkę zadań.

Ramka nawigacyjna służy do wybierania zadań do zarządzania certyfikatami lub aplikacjami, które ich używają. Niektóre poszczególne zadania są wyświetlane bezpośrednio w głównej ramce nawigacyjnej, ale większość zadań w ramce nawigacyjnej jest zorganizowana w kategorie. Na przykład zarządzanie certyfikatami jest kategorią zadań, która zawiera różne indywidualne zadania z przewodnikiem, takie jak certyfikat widoku, certyfikat odnawiania i certyfikat importu. Jeśli element w ramce nawigacyjnej jest kategorią, która zawiera więcej niż jedno zadanie, w lewo od niej wyświetlana jest strzałka. Strzałka wskazuje, że po wybraniu odsyłacza do kategorii zostanie wyświetlona rozwinięta lista zadań, co umożliwia wybranie zadania do wykonania.

Ważne informacje na temat programu DCM znajdują się w następujących publikacjach IBM Redbooks :

- *IBM i Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements*, SG24-6168. W szczególności zapoznaj się z dodatkami, aby uzyskać podstawowe informacje na temat konfigurowania systemu IBM i jako lokalnego ośrodka CA.

- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659. W szczególności, zob. rozdział 5. *Digital Certificate Manager for AS/400* , który wyjaśnia program AS/400 DCM.

Standardy FIPS (Federal Information Processing Standards)

Niniejszy temat zawiera wprowadzenie do standardu FIPS (Federal Information Processing Standards) Cryptomodule Validation Program of the US National Institute of Standards and Technology oraz funkcji kryptograficznych, które mogą być używane na kanałach TLS.

Te informacje mają zastosowanie do następujących platform:

- ULW UNIX, Linux, and Windows
- z/OS z/OS

ULW Więcej informacji na temat zgodności ze standardem FIPS 140-2 dla połączenia IBM MQ TLS w systemie UNIX, Linux, and Windowszawiera sekcja “Standardy FIPS (Federal Information Processing Standards) dla UNIX, Linux, and Windows” na stronie 33.

z/OS Więcej informacji na temat zgodności ze standardem FIPS 140-2 dla połączenia IBM MQ TLS w systemie z/OSzawiera sekcja “Standardy FIPS (Federal Information Processing Standards) dla produktu z/OS” na stronie 36.

Jeśli sprzęt szyfrujący jest obecny, moduły kryptograficzne używane przez produkt IBM 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 MQ jest również aktualizowany w celu zaimplementowania najnowszego standardu. W rezultacie po zastosowaniu konserwacji mogą być widoczne zmiany w zachowaniu.

Pojęcia pokrewne

“Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.” na stronie 278
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

“Używanie produktów runmqckm, runmqakmi strmqikm do zarządzania certyfikatami cyfrowymi” na stronie 294
W systemach UNIX, Linux, and Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komendy **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

Zadania pokrewne

Włączanie protokołu TLS w produkcie IBM MQ classes for Java

Korzystanie z protokołu TLS (Transport Layer Security) z produktem IBM MQ classes for JMS

Odsyłacze pokrewne

Właściwości TLS obiektów JMS

“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).

ULW *Standardy FIPS (Federal Information Processing Standards) dla UNIX, Linux, and Windows*
Jeśli szyfrowanie jest wymagane w kanale SSL/TLS w systemach Windowsi UNIX and Linux , IBM MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach Windowsi UNIX and Linux oprogramowanie ICC przeszło program FIPS (Federal Information Processing Standards)

Cryptomodule Validation Program) amerykańskiego National Institute of Standards and Technology na poziomie 140-2.

Zgodność z FIPS 140-2 dla połączenia IBM MQ TLS w systemach Windowsi UNIX and Linux jest następująca:

- Dla wszystkich kanałów komunikatów IBM 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 IBM MQ MQI client 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 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 aplikacji IBM MQ classes for Java korzystających z trybu klienta połączenie używa implementacji protokołu 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 aplikacji IBM MQ classes for JMS korzystających z trybu klienta połączenie używa implementacji protokołu 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 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` .
- W przypadku niezarządzanych aplikacji klienckich XMS .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 dokumentacji serwera XMS .NET .
- 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 mają certyfikat FIPS 140-2, z wyjątkiem przypadków opisanych w pliku readme dołączonym do każdego pakietu poprawek lub pakietu aktualizacyjnego.

W przypadku połączeń 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 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 IBM MQ jest skonfigurowany do działania zgodnie ze standardem FIPS 140-2, dodatkowe ograniczenia są wymuszane w odniesieniu do algorytmu Triple DES (3DES) CipherSpecs. 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 program IBM 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 460.

Program IBM 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

"Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS." na stronie 278
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

"Używanie produktów runmqckm, runmqakmi strmqikm do zarządzania certyfikatami cyfrowymi" na stronie 294
W systemach UNIX, Linux, and Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komendy **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

Zadania pokrewne

Włączanie protokołu TLS w produkcie IBM MQ classes for Java

Korzystanie z protokołu TLS (Transport Layer Security) w produkcie IBM MQ classes for JMS

Odsyłacze pokrewne

Właściwości TLS obiektów JMS

"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).

z/OS *Standardy FIPS (Federal Information Processing Standards) dla produktu z/OS*
Jeśli szyfrowanie jest wymagane na kanale SSL/TLS w systemie z/OS , produkt IBM MQ korzysta z usługi o nazwie System SSL. Celem systemowej implementacji protokołu SSL jest zapewnienie możliwości bezpiecznego wykonywania w trybie zaprojektowanym zgodnie z FIPS (Federal Information Processing Standards) Cryptomodule Validation Program of the US National Institute of Standards and Technology (Narodowy Instytut Standaryzacji i Technologii USA) na poziomie 140-2.

Podczas implementowania połączeń zgodnych ze standardem FIPS 140-2 z połączeniami IBM MQ TLS istnieje kilka punktów do rozważenia:

- Aby włączyć kanały komunikatów produktu IBM MQ w celu zapewnienia zgodności z protokołem FIPS, należy spełnić następujące warunki:
  - System SSL Security Level 3 FMID jest zainstalowany i skonfigurowany (patrz sekcja Planowanie instalacji produktu IBM MQ).
  - Poprawność modułów SSL systemu jest sprawdzana.
  - Atrybut SSLFIPS menedżera kolejek został ustawiony na wartość **YES**.

Podczas wykonywania w trybie FIPS, System SSL wykorzystuje funkcję CP Assist for Cryptographic Function (CPACF), gdy jest ona dostępna. Funkcje szyfrujące wykonywane przez sprzęt obsługiwany przez ICSF podczas pracy w trybie innym niż FIPS są nadal wykorzystywane podczas wykonywania w trybie FIPS, z wyjątkiem generowania podpisu RSA, które musi być wykonane w oprogramowaniu.

Tabela 2. Różnice między trybem FIPS i obsługą algorytmu trybu innego niż FIPS.

	Inne niż FIPS		**FIPS**	
Algorytm	**Wielkości kluczy**	**Sprzęt**	**Wielkości kluczy**	**Sprzęt**
RC2	40 i 128			
RC4	40 i 128			

Tabela 2. Różnice między trybem FIPS i obsługą algorytmu trybu innego niż FIPS. (kontynuacja)				
	Inne niż FIPS		**FIPS**	
Algorytm	**Wielkości kluczy**	**Sprzęt**	**Wielkości kluczy**	**Sprzęt**
DES	56	x		
TDES	168	x	168	x
AES	128 i 256	x	128 i 256	x
MD5	48			
SHA-1	160	x	160	x
SHA-2	224, 256, 384 i 512	x	224, 256, 384 i 512	x
RSA	512-4096	x	1024-4096	x
DSA	512-1024		1024	
DH	512-2048		2048	

W trybie FIPS system SSL może używać tylko certyfikatów, które korzystają z algorytmów i wielkości kluczy przedstawionych w tabeli 1. Podczas sprawdzania poprawności certyfikatu X.509 , jeśli zostanie napotkany algorytm niezgodny z trybem FIPS, certyfikat nie może być używany i jest traktowany jako niepoprawny.

W przypadku aplikacji klas IBM MQ korzystających z trybu klienta w produkcie WebSphere Application Server należy zapoznać się z informacjami w sekcji Obsługa standardu Federal Information Processing Standard.

Informacje na temat konfiguracji modułu System SSL zawiera sekcja System SSL Module Verification Setup (Konfiguracja weryfikacji modułu SSL w systemie).

Odsyłacze 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).

Multi *Weryfikowanie konfiguracji protokołu TLS menedżera kolejek za pomocą programu* `mqcertck`

Komenda **MQCERTCK** jest narzędziem służącym do wyszukiwania typowych błędów w konfiguracji TLS menedżera kolejek i udostępnia sugestie dotyczące rozwiązywania problemów.

Wprowadzenie

Komenda **`mqcertck`** sprawdza:

- Istnienie i uprawnienia repozytorium kluczy menedżera kolejek przywoływanego w atrybucie **SSLKEYR** menedżera kolejek.
- Istnienie i ważność certyfikatu dla certyfikatu menedżera kolejek, do którego odwołuje się atrybut **CERTLABL** menedżera kolejek.
- Istnienie i ważność wszystkich certyfikatów przywoływanych w atrybutach **CERTLABL** kanału z włączoną obsługą TLS.
- Repozytorium kluczy i certyfikaty aplikacji klienckich, w tym sprawdzanie, czy certyfikaty są autoryzowane w menedżerze kolejek.

Uwaga: Komenda **`mqcertck`** nie jest dostępna w systemach z/OS i IBM i.

Użycie

Aby użyć komendy **mqcertck** , z poziomu wiersza komend uruchom komendę `mqcertck`wraz z wymaganymi parametrami i wymaganymi parametrami opcjonalnymi.

Opis komendy i jej parametrów zawiera sekcja mqcertck .

Przykład

Właśnie zakończono konfigurowanie menedżera kolejek `QM1` w celu umożliwienia połączeń TLS od klientów łączących się z kanałem SVRCONN menedżera kolejek.

Używanych jest wiele certyfikatów, dlatego zarówno menedżer kolejek, jak i kanał mają etykietę certyfikatu określoną w swoich atrybutach **CERTLABL** . Podczas tworzenia kanału wystąpił błąd w atrybucie **CERTLABL** kanału, więc gdy klient próbuje nawiązać połączenie, menedżer kolejek zwraca kod powrotu 2393 o wartości MQRC_SSL_INITIALIZATION_ERROR.

Przed aktywowaniem menedżera kolejek należy użyć komendy **mqcertck** , aby sprawdzić konfigurację TLS menedżera kolejek.

Należy uruchomić komendę `mqcertck QM1` i otrzymać następujące dane wyjściowe:

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
+-----------------------------------------------------------
| IBM MQ TLS Configuration Test tool
+-----------------------------------------------------------
| Problem identified:
|  No certificate could be found for the channel
|  MQCERTCK.CHANNEL
|  This tool looked in the Queue Manager's key repository
|  located at: 'C:\MQ Data\qmgrs\QM1\ssl\key.kdb'
|  for a certificate with label 'chacert',
|  which is the certificate specified in the channel's
|  CERTLABL attribute, but was unable to find one.
|
| Possible resolution:
|  A valid certificate with the label chacert
|  needs to be added to the key repository.
|
|  Alternatively, alter the channel definition to remove
|  the CERTLABL value. This can be done by executing the
|  following command in runmqsc:
|      ALTER CHANNEL(<Name>) CHLTYPE(<TYPE>) CERTLABL(' ')
+-----------------------------------------------------------
| mqcertck has ended. See above for any problems found.
| If there are problems then resolve these and run this
| tool again.
|
+-----------------------------------------------------------
```

Te dane wyjściowe zawierają zachętę do sprawdzenia definicji kanału dla kanału połączenia z serwerem MQCERTCK.CHANNEL. W tym miejscu zostanie wyświetlony błąd i można go naprawić przed ponownym uruchomieniem komendy `mqcertck` w celu sprawdzenia, czy problem został rozwiązany.

Weryfikowanie połączeń klienckich

Komenda **mqcertck** umożliwia weryfikowanie repozytoriów kluczy klienta, a także konfiguracji TLS menedżera kolejek. W tym celu program **mqcertck** musi mieć możliwość uzyskania dostępu do repozytorium kluczy klienta z komputera, na którym działa menedżer kolejek.

Jeśli podczas uruchamiania komendy **mqcertck** zostanie podany parametr **-clientkeyr** z położeniem repozytorium kluczy klienta (z wyjątkiem rozszerzenia), program **mqcertck** sprawdzi to repozytorium kluczy względem menedżera kolejek.

Jeśli wiadomo, który kanał będzie używany przez klient do nawiązywania połączenia z menedżerem kolejek, można to określić za pomocą opcji **-clientchannel** .

Jeśli klient używa uwierzytelniania wzajemnego w celu nawiązania połączenia z menedżerem kolejek, można użyć parametru **-clientusername** lub **-clientlabel** , aby poinformować komendę **mqcertck** o tym, który certyfikat ma być używany w repozytorium kluczy klienta.

Jeśli używany jest certyfikat domyślny i nie podano etykiety certyfikatu dla aplikacji klienckiej, można użyć parametrów **-clientusername** i **username** , które uruchamiają tę aplikację.

Podczas działania komendy **mqcertck** komenda generuje etykietę certyfikatu `ibmwebspheremqXXXX` , gdzie XXXX jest wartością przekazaną w parametrze **-clientusername** .

Aby w pełni zweryfikować repozytorium kluczy klienta, komenda **mqcertck** tworzy fikcyjne połączenie przy użyciu pakietu GSKit. W tym celu komenda musi mieć dostępny port, z którym może zostać powiązana podczas testów klienta. Port domyślny to 5857, ale jeśli jest już używany, można określić inny port, który będzie używany podczas testów klienta.

Uwaga: Mimo że komenda **mqcertck** jest powiązana z portem, produkt **mqcertck**nie używa komunikacji zewnętrznej, a wszystkie testy są wykonywane lokalnie.

SSL/TLS na serwerze IBM MQ MQI client

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

IBM MQ provides TLS support for IBM MQ MQI clients on Windows, UNIX and Linux systems. Jeśli używany jest produkt IBM MQ classes for Java, należy zapoznać się z Korzystanie z produktu IBM MQ classes for Java , a jeśli używany jest produkt IBM MQ classes for JMS, należy zapoznać się z sekcji Korzystanie z produktu IBM MQ classes for JMS. Pozostała część tej sekcji nie ma zastosowania do środowisk Java ani JMS .

Repozytorium kluczy dla partycji IBM MQ MQI client można określić za pomocą wartości MQSSLKEYR w pliku konfiguracyjnym klienta IBM MQ lub gdy aplikacja użytkownika tworzy wywołanie MQCONNX. Dostępne są trzy opcje określania, że kanał używa protokołu TLS:

- 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 TLS.

Można kontynuować uruchamianie istniejących aplikacji produktu IBM MQ MQI client bez protokołu TLS, dopóki protokół TLS nie zostanie określony na drugim końcu kanału.

Jeśli na komputerze klienta zostaną wprowadzone zmiany do zawartości repozytorium kluczy TLS, położenia repozytorium kluczy TLS, informacji uwierzytelniających lub parametrów sprzętu szyfrującego, należy zakończyć wszystkie połączenia TLS, aby odzwierciedlić te zmiany w kanałach połączenia klienckiego, które aplikacja używa do łączenia się z menedżerem kolejek. Po zakończeniu wszystkich połączeń zrestartuj kanały TLS. Zostaną użyte wszystkie nowe ustawienia TLS. Te ustawienia są analogiczne do tych, które zostały odświeżone przy użyciu komendy REFRESH SECURITY TYPE (SSL) w systemach menedżera kolejek.

Gdy produkt IBM MQ MQI client działa w systemie Windows, w systemie UNIX and Linux ze sprzętem szyfrującym, należy skonfigurować 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 TLS i FIPS są obsługiwane w systemie IBM MQ MQI clients. Więcej informacji na ten temat zawierają sekcje “Resetowanie kluczy tajnych SSL i TLS” na stronie 460 i “Standardy FIPS (Federal Information Processing Standards) dla UNIX, Linux, and Windows” na stronie 33.

Więcej informacji na temat obsługi protokołu TLS dla produktu IBM MQ MQI clientszawiera sekcja “Konfigurowanie zabezpieczeń produktu IBM MQ MQI client” na stronie 277 .

Zadania pokrewne

Konfigurowanie klienta przy użyciu pliku konfiguracyjnego

Określanie, czy kanał MQI używa protokołu SSL/TLS
W przypadku kanału MQI w celu użycia protokołu TLS wartość atrybutu *SSLCipherSpec* kanału połączenia klienckiego musi być nazwą CipherSpec , która jest obsługiwana przez produkt IBM 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 IBM MQ MQI client zgłasza 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 usługi 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 klient IBM MQ może uzyskać dostęp.

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

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 partycji IBM MQ MQI client” na stronie 448
Dostępne są trzy opcje określania wartości CipherSpec dla IBM MQ MQI client.

CipherSpecs i CipherSuites w podręczniku IBM MQ

Produkt IBM MQ obsługuje algorytmy TLS 1.2 CipherSpecsoraz RSA i Diffie-Hellman. Można jednak włączyć nieaktualne atrybuty CipherSpecs, jeśli jest to konieczne.

Więcej informacji na ten temat zawiera sekcja “Włączanie opcji CipherSpecs” na stronie 433 :

- CipherSpecs obsługiwane przez produkt IBM MQ.
- Sposób włączania nieaktualnych specyfikacji SSL 3.0 i TLS 1.0 CipherSpecs.

Produkt IBM MQ obsługuje algorytmy wymiany kluczy RSA i Diffie-Hellmana oraz algorytmy uwierzytelniania. Wielkość klucza używanego podczas uzgadniania TLS 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 19

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 MQ

This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

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 MQ jest również aktualizowany w celu zaimplementowania najnowszego standardu. W rezultacie po zastosowaniu konserwacji mogą być widoczne zmiany w zachowaniu. Plik readme produktu IBM MQ zawiera listę wersji pakietu B wymuszoną przez każdy poziom konserwacyjny produktu. Jeśli produkt IBM MQ został skonfigurowany w taki sposób, aby wymuszał zgodność z pakietem B, należy zawsze zapoznać się z plikiem readme podczas planowania stosowania konserwacji. Więcej informacji na ten temat zawiera sekcja IBM MQ, WebSphere MQi MQSeries -pliki readme.

W systemach Windows, UNIXi Linux produkt IBM MQ można skonfigurować w taki sposób, aby był zgodny z profilem TLS 1.2 zgodnym z pakietem B na poziomach bezpieczeństwa, które przedstawiono w tabeli 1.

Tabela 3. 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

Although the default behavior of IBM MQ is not to comply with the Suite B standard, IBM MQ can be configured to conform to either, or both security levels on Windows, UNIX and Linux systems. Po pomyślnej konfiguracji produktu IBM 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 IBM MQ CipherSpecszawiera sekcja “Włączanie opcji CipherSpecs” na stronie 433

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 IBM MQ musi być skonfigurowany pod kątem używania certyfikatów, których algorytm podpisywania cyfrowego i typ klucza publicznego są dozwolone przez skonfigurowany poziom zabezpieczeń Suite B 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: Komendy **runmqckm** i **strmqikm** nie obsługują tworzenia certyfikatów cyfrowych dla operacji zgodnych ze standardem Suite B.

Tworzenie i wysyłanie żądań certyfikatów cyfrowych

Aby utworzyć samopodpisany certyfikat cyfrowy na potrzeby testowania Suite B, patrz “Tworzenie samopodpisanego certyfikatu osobistego w systemie UNIX, Linux, and Windows” na stronie 302

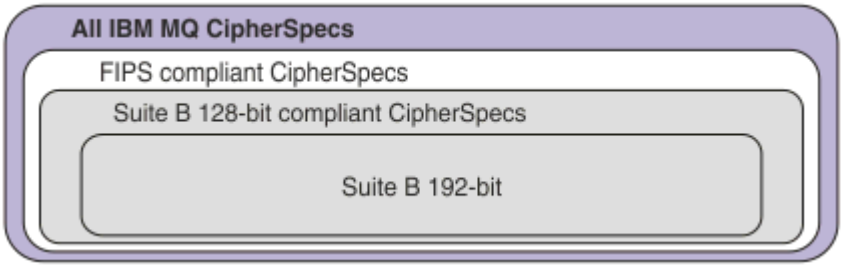
Więcej informacji na temat używania certyfikatu cyfrowego podpisanego przez ośrodek CA na potrzeby produkcji Suite B można znaleźć w sekcji “Żądanie certyfikatu osobistego w systemie UNIX, Linux, and Windows” na stronie 305.

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 MQ jest skonfigurowany do obsługi zgodnej ze standardem FIPS 140-2. W związku z tym możliwe jest skonfigurowanie produktu IBM 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 produktu IBM MQ na potrzeby operacji zgodnej z pakietem B

For information about how to configure IBM MQ on Windows, UNIX and Linux for Suite B compliant operation, see “Konfigurowanie produktu IBM MQ dla pakietu B” na stronie 43.

Produkt IBM MQ nie obsługuje operacji zgodnych ze standardem Suite B na platformach IBM i i z/OS . The IBM MQ Java and JMS clients also do not support Suite B compliant operation.

Pojęcia pokrewne

“Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.” na stronie 278
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

Konfigurowanie produktu IBM MQ dla pakietu B

Produkt IBM MQ można skonfigurować do działania zgodnie ze standardem NSA Suite B na platformach Windowsi UNIX and Linux .

Pakiet B ogranicza zestaw włączonych algorytmów szyfrowania w celu zapewnienia gwarantowanego poziomu bezpieczeństwa. Produkt IBM MQ można skonfigurować do działania zgodnie z pakietem Suite B, aby zapewnić wyższy poziom bezpieczeństwa. Więcej informacji na temat pakietu Suite B zawiera sekcja “National Security Agency (NSA) Suite B Cryptography” na stronie 21. Więcej informacji na temat konfiguracji Suite B i jej wpływu na kanały TLS zawiera sekcja “Szyfrowanie NSA Suite B Cryptography w produkcie IBM MQ” na stronie 41.

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 zgodnych z pakietem B.

Uwaga: W przypadku zmiany ustawień pakietu B menedżera kolejek należy zrestartować usługę MQXR, aby ustawienia te zostały zastosowane.

MQI client

Domyślnie klienty MQI nie wymuszają zgodności z pakietem Suite B. Aby włączyć zgodność klienta MQI z pakietem Suite B, należy wykonać jedną z następujących opcji:

1. Przez ustawienie pola **EncryptionPolicySuiteB** w strukturze MQSCO wywołania MQCONNX na jedną lub więcej z następujących wartości:
   - MQ_SUITE_BNONE
   - 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 co najmniej jedną z następujących wartości:
   - BRAK
   - 128_BIT
   - 192_BIT

   Można podać wiele wartości, używając listy rozdzielanej przecinkami. Użycie wartości NONE z dowolną inną wartością jest niepoprawne.
3. Ustawiając atrybut **EncryptionPolicySuiteB** w sekcji SSL pliku konfiguracyjnego klienta MQI w pliku konfiguracyjnym klienta MQI na jedną lub kilka z następujących wartości:

- BRAK
- 128_BIT
- 192_BIT

Można podać wiele wartości, używając listy rozdzielanej przecinkami. Użycie opcji NONE z dowolną inną wartością jest niepoprawne.

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

Szczegółowe informacje na temat struktury MQSCO zawiera sekcja MQSCO-opcje konfiguracyjne SSL.

Więcej informacji na temat używania pakietu Suite B w pliku konfiguracyjnym klienta zawiera sekcja SSL w pliku konfiguracyjnym klienta.

Więcej informacji na temat używania zmiennej środowiskowej MQSUITEB zawiera sekcja Opisy zmiennych środowiskowych.

.NET

W przypadku niezarządzanych klientów .NET właściwość **MQC.ENCRYPTION_POLICY_SUITE_B** wskazuje typ wymaganych zabezpieczeń Suite B.

Informacje na temat używania pakietu Suite B w produkcie IBM MQ classes for .NETzawiera sekcja Klasa MQEnvironment .NET.

AMQP

Ustawienia atrybutów Suite B dla menedżera kolejek mają zastosowanie do kanałów AMQP w tym menedżerze kolejek. Po zmodyfikowaniu ustawień pakietu B menedżera kolejek należy zrestartować usługę AMQP, aby zmiany odniosły skutek.

Strategie sprawdzania poprawności certyfikatów w produkcie IBM 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 produktu Java . Więcej informacji na temat strategii sprawdzania poprawności certyfikatów znajduje się w dokumentacji środowiska JRE.
- W przypadku systemów IBM i strategia sprawdzania poprawności certyfikatu zależy od biblioteki gniazd chronionych udostępnianej przez system operacyjny. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów znajduje się w dokumentacji systemu operacyjnego.
- W przypadku systemów z/OS strategia sprawdzania poprawności certyfikatu zależy od systemowego komponentu SSL udostępnionego przez system operacyjny. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów znajduje się w dokumentacji systemu operacyjnego.
- 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 systemie UNIX, Linux, and Windowszawiera sekcja “Konfigurowanie strategii sprawdzania poprawności

certyfikatów w programie IBM MQ” na stronie 45. 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 systemie UNIX, Linux, and Windows.

Konfigurowanie strategii sprawdzania poprawności certyfikatów w programie IBM MQ

Można określić, która strategia sprawdzania poprawności certyfikatów TLS jest używana do sprawdzania poprawności certyfikatów cyfrowych odebranych ze zdalnych systemów partnerskich na cztery sposoby.

W menedżerze kolejek strategię sprawdzania poprawności certyfikatu można ustawić w następujący sposób:

- Użycie 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 używa ustawień w następującej kolejności priorytetów:

1. Przy użyciu pola *StrategiaCertificateVal* w strukturze MQSCO klienta. Więcej informacji na temat używania tego pola zawiera sekcja MQSCO-opcje konfiguracyjne SSL.
2. Przy użyciu zmiennej środowiskowej klienta *MQCERTVPOL*. Więcej informacji na temat używania tej zmiennej zawiera sekcja MQCERTVPOL.
3. Przy użyciu ustawienia parametru strojenia sekcji SSL klienta, *StrategiaCertificateVal*. Więcej informacji na temat używania tego ustawienia zawiera sekcja SSL pliku konfiguracyjnego klienta.

Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM MQ” na stronie 44.

Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ

Ten temat zawiera informacje dotyczące wybierania odpowiednich CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa. W tym celu należy zapoznać się z relacją między CipherSpecs i certyfikatami cyfrowymi w produkcie IBM MQ.

Tylko podzbiór obsługiwanych CipherSpecs może być używany ze wszystkimi obsługiwanymi typami certyfikatów cyfrowych. Dlatego konieczne jest wybranie odpowiedniej CipherSpec dla certyfikatu cyfrowego. Podobnie, jeśli strategia bezpieczeństwa organizacji wymaga użycia określonej CipherSpec , należy uzyskać odpowiedni certyfikat cyfrowy dla tej CipherSpec.

Algorytm podpisu cyfrowego MD5 i protokół 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 uważany za słaby przez wielu analityków kryptograficznych, a jego użycie jest na ogół niezalecane. Aby używać nowszych CipherSpecs opartych na protokole TLS 1.2 , należy upewnić się, że certyfikaty cyfrowe nie używają algorytmu MD5 w podpisach cyfrowych. Starsze specyfikacje szyfrowania CipherSpecs , które używają protokołów 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 algorytmu podpisu cyfrowego do wyświetlenia. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Uwaga: Chociaż do wyświetlania wybranych algorytmów podpisu cyfrowego można użyć interfejsu GUI **runmqckm** (iKeycmd) i **strmqikm** (iKeyman), narzędzie **runmqakm** udostępnia szerszy zakres.

Uruchomienie komendy **runmqakm** spowoduje wyświetlenie danych wyjściowych z użyciem podanego algorytmu podpisywania:

```
Label : ibmmqexample
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
```

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

Współdziałanie krzywej eliptycznej i specyfikacji szyfrowania RSA CipherSpecs

V 9.1.4 Nie wszystkie CipherSpecs mogą być używane ze wszystkimi certyfikatami cyfrowymi. CipherSpecs są oznaczone przedrostkiem nazwy CipherSpec . Każdy typ CipherSpec nakłada inne ograniczenia na typ certyfikatu cyfrowego, który może być używany. Te ograniczenia dotyczą wszystkich połączeń TLS systemu IBM MQ , ale są szczególnie istotne dla użytkowników szyfrowania krzywej eliptycznej (Elliptic Curve).

Poniższa tabela zawiera podsumowanie relacji między CipherSpecs i certyfikatami cyfrowymi:

Tabela 4. Relacje między CipherSpecs i certyfikatami cyfrowymi

Typ	Przedrostek nazwy CipherSpec	Opis	Wymagany typ klucza publicznego	Algorytm szyfrowania podpisu cyfrowego	Metoda ustanawiania klucza tajnego
1	ECDHE_ECDSA_	CipherSpecs , które używają kluczy publicznych krzywej eliptycznej, kluczy tajnych krzywej eliptycznej i algorytmów podpisu cyfrowego krzywej eliptycznej.	Krzywa eliptyczna	ECDSA	ECDHE
2	EDHE_RSA_	CipherSpecs , które używają kluczy publicznych RSA, kluczy tajnych krzywej eliptycznej i algorytmów podpisu cyfrowego RSA.	RSA	RSA	ECDHE
V 9.1.4 3	(Wszystkie specyfikacje szyfrowania protokołu TLS 1.3 CipherSpecs)	CipherSpecs , które używają kluczy publicznych Elliptic Curve lub RSA, kluczy tajnych Elliptic Curve i algorytmów podpisu cyfrowego RSA.	Krzywa eliptyczna lub RSA	ECDSA lub RSA	ECDHE lub RSA
4	(wszystkie pozostałe)	CipherSpecs , które używają kluczy publicznych RSA i algorytmów podpisu cyfrowego RSA.	RSA	RSA	RSA

Uwaga: CipherSpecs typu 1 i 2 nie są obsługiwane przez menedżery kolejek i klienty MQI produktu IBM MQ na platformie IBM i .

W wymaganej kolumnie typu klucza publicznego jest wyświetlany typ klucza publicznego, który musi mieć certyfikat osobisty, jeśli używany jest każdy typ CipherSpec. Certyfikat osobisty jest certyfikatem jednostki końcowej, który identyfikuje menedżera kolejek lub klienta dla jego partnera zdalnego.

Kanał można skonfigurować przy użyciu zarówno CipherSpec , która wymaga certyfikatu EC (Elliptic Curve), jak i etykiety certyfikatu RSA, lub w inny sposób. Należy upewnić się, że certyfikat określony w etykiecie certyfikatu jest odpowiedni dla kanału CipherSpec.

Zakładając, że poprawnie skonfigurowano produkt IBM MQ, można wykonać następujące czynności:

- Pojedynczy menedżer kolejek z kombinacją certyfikatów RSA i EC.
- Różne kanały w tym samym menedżerze kolejek używające certyfikatu RSA lub EC.

Algorytm szyfrowania podpisu cyfrowego odnosi się do algorytmu szyfrowania używanego do sprawdzania poprawności węzła sieci. Algorytm szyfrowania jest używany razem z algorytmem mieszającym, takim jak MD5, SHA-1 lub SHA-256 , do obliczenia podpisu cyfrowego. Istnieją różne algorytmy podpisu cyfrowego, których można użyć, na przykład RSA z algorytmem MD5 lub ECDSA z algorytmem SHA-256. W tabeli ECDSA odnosi się do zestawu algorytmów podpisu cyfrowego, które używają ECDSA; RSA odnosi się do zestawu algorytmów podpisu cyfrowego, które używają RSA. Można użyć dowolnego obsługiwanego algorytmu podpisu cyfrowego w zestawie, pod warunkiem że jest on oparty na określonym algorytmie szyfrowania.

Typ 1 CipherSpecs wymagają, aby certyfikat osobisty miał klucz publiczny krzywej eliptycznej. Jeśli używane są te CipherSpecs , do ustanowienia klucza tajnego dla połączenia używana jest umowa klucza Ephemeral Elliptic Curve Diffie Hellman.

Typ 2 CipherSpecs wymagają, aby certyfikat osobisty miał klucz publiczny RSA. Jeśli używane są te CipherSpecs , do ustanowienia klucza tajnego dla połączenia używana jest umowa klucza Ephemeral Elliptic Curve Diffie Hellman.

Typ 3 CipherSpecs wymagają, aby certyfikat osobisty miał klucz publiczny RSA. Jeśli te CipherSpecs są używane, do ustanowienia klucza tajnego dla połączenia używana jest wymiana klucza RSA.

Ta lista ograniczeń nie jest wyczerpująca: w zależności od konfiguracji mogą istnieć dodatkowe ograniczenia, które mogą mieć wpływ na możliwość współdziałania. Na przykład, jeśli produkt IBM MQ jest skonfigurowany pod kątem zgodności ze standardami FIPS 140-2 lub NSA Suite B, ograniczy to również zakres dozwolonych konfiguracji. Więcej informacji na ten temat zawiera poniższa sekcja.

Jeśli konieczne jest użycie różnych typów CipherSpec w tym samym menedżerze kolejek lub aplikacji klienckiej, należy skonfigurować odpowiednią etykietę certyfikatu i kombinację CipherSpec w definicji klienta.

Trzy typy specyfikacji szyfrowania CipherSpec nie współdziałają bezpośrednio: jest to ograniczenie bieżących standardów TLS. Na przykład załóżmy, że wybrano użycie parametru ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec dla kanału odbiorczego o nazwie TO.QM1 w menedżerze kolejek o nazwie QM1, a następnie odbiorca powinien mieć certyfikat osobisty z kluczem Elliptic Curve i podpisem cyfrowym opartym na ECDSA. Jeśli kanał odbiorczy nie spełnia tych wymagań, uruchomienie kanału nie powiedzie się.

Inne kanały łączące się z menedżerem kolejek QM1 mogą używać innych CipherSpecs, pod warunkiem, że każdy kanał używa certyfikatu poprawnego typu dla CipherSpec tego kanału. Załóżmy na przykład, że QM1 korzysta z kanału nadawczego o nazwie TO.QM2 służy do wysyłania komunikatów do innego menedżera kolejek o nazwie QM2. Kanał TO.QM2 może używać specyfikacji szyfrowania typu 3 CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA256 , pod warunkiem, że oba końce kanału używają certyfikatów zawierających klucze publiczne RSA. Atrybut kanału etykiety certyfikatu może być używany do konfigurowania innego certyfikatu dla każdego kanału.

Podczas planowania sieci produktu IBM MQ należy dokładnie rozważyć, które kanały wymagają protokołu TLS, i upewnić się, że typ certyfikatów używanych dla każdego kanału jest odpowiedni do użycia ze specyfikacją szyfrowania (CipherSpec) w tym kanale.

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 ma zostać wyświetlony. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

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

```
Label : ibmmqexample
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
```

W tym przypadku linia typu klucza publicznego wskazuje, że certyfikat ma klucz publiczny krzywej eliptycznej. Wiersz Algorytm podpisu w tym przypadku wskazuje, że używany jest algorytm EC_ecdsa_with_SHA384 : jest on oparty na algorytmie ECDSA. Dlatego ten certyfikat jest odpowiedni tylko dla typu 1 CipherSpecs.

Można również użyć komendy **runmqckm** z tymi samymi parametrami. Po otwarciu repozytorium kluczy i dwukrotnym kliknięciu etykiety certyfikatu można również użyć interfejsu GUI programu **strmqikm** do wyświetlenia algorytmów podpisu cyfrowego. Należy jednak użyć narzędzia **runmqakm** , aby wyświetlić certyfikaty cyfrowe, ponieważ obsługuje ono szerszy zakres algorytmów.

TLS 1.3 CipherSpecs

V 9.1.4

Protokół TLS 1.3 CipherSpecs obsługują zarówno certyfikaty ECDSA, jak i RSA.

Krzywa eliptyczna CipherSpecs i NSA Suite B

Jeśli produkt IBM MQ jest skonfigurowany pod kątem zgodności z profilem TLS 1.2 zgodnym z pakietem Suite B, dozwolone CipherSpecs i algorytmy podpisu cyfrowego są ograniczone zgodnie z opisem w sekcji “Szyfrowanie NSA Suite B Cryptography w produkcie IBM MQ” na stronie 41. Ponadto zakres dopuszczalnych kluczy krzywej eliptycznej jest zmniejszany zgodnie ze skonfigurowanymi poziomami zabezpieczeń.

Na 128-bitowym poziomie bezpieczeństwa 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 . Do żądania certyfikatów cyfrowych dla tego poziomu bezpieczeństwa można użyć komendy **runmqakm** z parametrem -sig_alg o wartości EC_ecdsa_with_SHA256lub EC_ecdsa_with_SHA384.

Na poziomie bezpieczeństwa 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 . Komendy **runmqakm** można użyć do zażądania certyfikatów cyfrowych dla tego poziomu bezpieczeństwa za pomocą parametru -sig_alg o wartości EC_ecdsa_with_SHA384.

Obsługiwane są następujące krzywe eliptyczne NIST:

Tabela 5. Obsługiwane krzywe eliptyczne NIST

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

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

Pojęcia pokrewne

"Włączanie opcji CipherSpecs" na stronie 433
Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

"Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS." na stronie 278
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

"Szyfrowanie NSA Suite B Cryptography w produkcie IBM MQ" na stronie 41
This topic provides information about how to configure IBM MQ on Windows, Linux, and UNIX to conform to the Suite B compliant TLS 1.2 profile.

"National Security Agency (NSA) Suite B Cryptography" na stronie 21
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.

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 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 6. 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

Tabela 6. Zastosowanie reguł CHLAUTH do różnych par kanałów (kontynuacja)	
Typ kanału	**MCA z zastosowaniem reguł CHLAUTH**
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.

Rekordy uwierzytelniania kanału można tworzyć, modyfikować lub usuwać za pomocą komendy MQSC **SET CHLAUTH** lub PCF **Set Channel Authentication Record**.

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 IBM MQ. Należy wówczas zablokować dany adres do czasu zaktualizowania firewalla. Te próby połączenia mogą nie pochodzić z kanałów programu IBM MQ. Mogą pochodzić z innych aplikacji używających gniazd, które są niepoprawnie skonfigurowane w taki sposób, że są skierowane do procesu nasłuchującego programu IBM 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 397.

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 399.

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 klienta” na stronie 402.

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 401.

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 lub TLS” na stronie 402.

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 403.

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 399.

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

Aby wskazać, że jeśli pewien ID użytkownika jest używany przez połączenie z klienta MQI produktu IBM MQ, to ma być używany inny podany 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 klienta na identyfikator użytkownika MCAUSER” na stronie 400.

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 401.

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 399.

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, adresem IP, nazwą hosta, nazwą menedżera kolejek albo nazwą wyróżniającą SSL lub TLS, zostanie użyte najdokładniejsze dopasowanie. Cechy dopasowań:

- Najdokładniejsze dopasowanie to nazwa bez znaków wieloznacznych, na przykład:
  - Nazwa kanału A.B.C
  - Adres IP 192.0.2.6
  - Nazwa hosta `hursley.ibm.com`
  - Nazwa menedżera kolejek 192.0.2.6
- Najogólniejsze dopasowanie to pojedyncza gwiazdka (*) oznaczająca na przykład:
  - Wszystkie nazwy kanałów
  - Wszystkie adresy IP
  - Wszystkie nazwy hostów
  - Wszystkie nazwy menedżerów kolejek
- Wzorzec z gwiazdką na początku łańcucha jest ogólniejszy niż wzorzec, w którym na początku łańcucha zdefiniowano konkretną wartość:
  - W przypadku kanałów wzorzec *.B.C jest ogólniejszy niż wzorzec A.*
  - W przypadku adresów IP wzorzec *.0.2.6 jest ogólniejszy niż wzorzec 192.*
  - W przypadku nazw hostów `*.ibm.com` jest bardziej ogólne niż `hursley.*`
  - W przypadku nazw menedżerów kolejek wzorzec *QUEUEMANAGER jest ogólniejszy niż wzorzec QUEUEMANAGER*
- Wzorzec z gwiazdką w konkretnym miejscu w łańcuchu jest ogólniejszy niż wzorzec, w którym w tym miejscu zdefiniowano konkretną wartość. Ta zasada odnosi się do każdego kolejnego miejsca w łańcuchu:

  - W przypadku kanałów wzorzec A.*.C jest ogólniejszy niż wzorzec A.B.*
  - W przypadku adresów IP wzorzec 192.*.2.6 jest ogólniejszy niż wzorzec 192.0.*.
  - W przypadku nazw hostów `hursley.*.com` jest bardziej ogólne niż `hursley.ibm.*`
  - W przypadku nazw menedżerów kolejek wzorzec Q*MANAGER jest ogólniejszy niż wzorzec QUEUE*
- W przypadku, gdy co najmniej dwa wzorce mają gwiazdkę w tym samym miejscu w łańcuchu, ogólniejszy jest ten wzorzec, który ma mniej węzłów po gwiazdce:
  - W przypadku kanałów A.* jest bardziej ogólne niż A.*.C
  - W przypadku adresów IP 192.* jest bardziej ogólne niż 192.*.2.*.
  - W przypadku nazw hostów `hurlsey.*` jest bardziej ogólne niż `hursley.*.com`
  - W przypadku nazw menedżerów kolejek wzorzec Q* jest ogólniejszy niż wzorzec Q*MGR
- Dodatkowo w przypadku adresu IP:
  - 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 wyróżniającej SSL lub TLS (DN) kolejność podłańcuchów jest następująca:

Tabela 7. 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

Tabela 7. Pierwszeństwo podłańcuchów (kontynuacja)		
Kolejność	**Podłańcuch nazwy wyróżniającej**	**Nazwa**
12	ST=, SP=, S=	Nazwa województwa lub rejonu
13	P=	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 IBM 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 97
W tej sekcji opisano aspekty bezpieczeństwa dotyczące zdalnego przesyłania komunikatów.

Interakcja CHLAUTH i CONNAUTH

Sposób interakcji rekordów uwierzytelniania kanału (CHLAUTH) i uwierzytelniania połączenia (CONNAUTH) w produkcie IBM MQ, w przypadku pojedynczej konwersacji na kanale.

Różne typy powiązań

Produkt IBM MQ obsługuje dwie metody łączenia aplikacji:

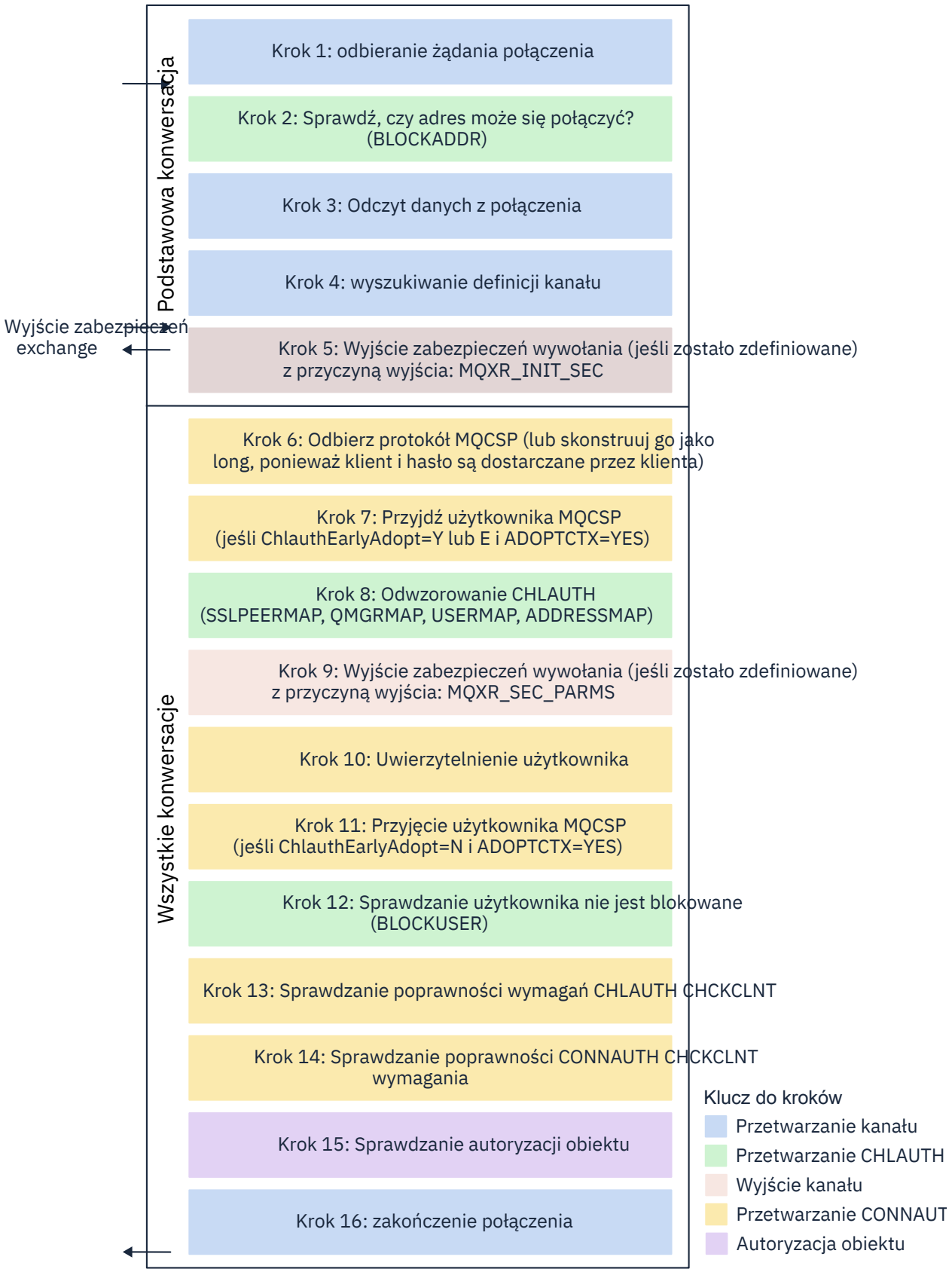
Powiązania lokalne
Ma zastosowanie, gdy aplikacja i menedżer kolejek znajdują się na tym samym obrazie operacyjnym. Wartość CHLAUTH nie jest istotna dla tego typu połączenia aplikacji.

Powiązania klienta
Ma zastosowanie, gdy aplikacja i menedżer kolejek używają sieci do komunikowania się. Aplikacja i menedżer kolejek mogą być uruchomione na tym samym komputerze lub mogą znajdować się na różnych komputerach. W programie IBM MQpołączenie z klientem jest obsługiwane w postaci kanału połączenia z serwerem (SVRCONN) i w takiej sytuacji mają zastosowanie zarówno CONNAUTH, jak i CHLAUTH.

Wiązanie kroków zakończenia kanału odbierającego

Gdy aplikacja łączy się z menedżerem kolejek, wykonywana jest znaczna ilość kontroli, aby zapewnić, że oba końce kanału rozumieją, co jest obsługiwane przez drugi koniec. Odbierający koniec kanału wykonuje dodatkowe sprawdzanie, obejmujące CHLAUTH i CONNAUTH, w celu zapewnienia, że klient może nawiązać połączenie, a proces ten może również obejmować wyjście zabezpieczeń, ponieważ może to mieć wpływ na wynik. Ta faza połączenia kanału jest również nazywana *fazą powiązania*.

Na poniższym diagramie przedstawiono kroki, które przechodzi kanał SVRCONN po uruchomieniu serwera (w menedżerze kolejek):



Krok 1: odbieranie żądania połączenia
Inicjator kanału lub proces nasłuchujący odbiera żądanie połączenia z sieci.

Krok 2: Czy adres jest uprawniony do połączenia?
Przed odczytaniem danych program IBM MQ sprawdza adres IP partnera w stosunku do reguł CHLAUTH, aby sprawdzić, czy adres znajduje się w regule *BLOCKADDR* . Jeśli adres nie zostanie znaleziony, a więc nie zostanie zablokowany, przepływ przechodzi do następnego kroku.

Krok 3: Odczyt danych z kanału
Program IBM MQ odczytuje teraz dane do buforu i rozpoczyna przetwarzanie wysłanych informacji.

Krok 4: wyszukiwanie definicji kanału
W pierwszym przepływie danych program IBM MQ wysyła, między innymi, nazwę kanału, który ma zostać uruchomiony przez wysyłający koniec. Odbierający menedżer kolejek może następnie wyszukać definicję kanału, która zawiera wszystkie ustawienia określone dla kanału.

Krok 5: Wyjście zabezpieczeń wywołania (jeśli jest zdefiniowane)
Jeśli kanał ma zdefiniowany wyjście bezpieczeństwa (SCYEXIT), jest to wywoływane z przyczyną wyjścia (MQCXP.**ExitReason**) ustaw na MQXR_INIT_SEC.

Krok 6: Przyjmij protokół MQCSP
Jeśli jest to konieczne, skonstruuj jeden, o ile identyfikator użytkownika i hasło są dostarczane przez klienta.

Jeśli klient jest aplikacją Java lub JMS działającą w trybie zgodności, klient nie przekaże struktury MQCSP do menedżera kolejek. Zamiast tego, jeśli aplikacja dostarczyła ID użytkownika i hasło, tworzona jest tutaj struktura MQCSP.

Krok 7: adoptuj użytkownika MQCSP (jeśli `ChlauthEarlyAdopt` ma wartość *Y* i ADOPTCTX=YES)
ID użytkownika potwierdzony przez klienta jest uwierzytelniony.

Jeśli parametr CONNAUTH korzysta z protokołu LDAP w celu odwzorowania potwierdzonej nazwy wyróżniającej na krótki identyfikator użytkownika, odwzorowanie jest wykonywane w tym kroku.

Jeśli uwierzytelnianie powiedzie się, identyfikator użytkownika jest przyjmowany przez kanał i jest używany przez krok odwzorowania CHLAUTH.

Uwaga: Od IBM MQ 9.0.4 parametr **ChlauthEarlyAdopt=** *Y* jest automatycznie dodawany do sekcji kanałów w pliku qm.ini dla nowych menedżerów kolejek.

Krok 8: Odwzorowanie CHLAUTH
Pamięć podręczna CHLAUTH jest ponownie sprawdzana w celu wyszukania reguł odwzorowania *SSLPEERMAP*, *USERMAP*, *QMGRMAP*i *ADDRESSMAP*.

Używana jest reguła, która jest zgodna z kanałem przychodzącym w sposób najbardziej konkretny. Jeśli reguła ma wartość **USERSRC***(CHANNEL)* lub *(MAP)*, kanał jest kontynuowany w powiązaniu.

Jeśli reguły CHLAUTH wartościują się do reguły z parametrem **USERSRC***(NOACCESS)*, aplikacja zostanie zablokowana z połączenia z kanałem, chyba że referencje zostaną następnie przesłonięte przy użyciu poprawnego identyfikatora użytkownika i hasła w kroku 9.

Krok 9: Wyjście z zabezpieczenia połączenia (jeśli jest zdefiniowane)
Jeśli kanał ma zdefiniowany wyjście bezpieczeństwa (SCYEXIT), jest to wywoływane z przyczyną wyjścia (MQCXP.**ExitReason**) ustaw na MQXR_SEC_PARMS.

Wskaźnik do MQCSP będzie obecny w polu **SecurityParms** struktury MQCXP.

Struktura MQCSP zawiera wskaźniki do identyfikatora użytkownika (MQCSP.**CSPUserIdPtr**) i hasło (MQCSP.**CSPPasswordPtr**).

Istnieje możliwość zmiany identyfikatora użytkownika i hasła w wyjściu. W poniższym przykładzie przedstawiono sposób, w jaki wyjście zabezpieczeń drukuje wartości identyfikatora użytkownika i hasła w dzienniku kontroli:

```
if (pMQCXP -> ExitReason == MQXR_SEC_PARMS)
{
  /* It is not a good idea for security reasons to print out the user ID */
  /* and password but the following is shown for demonstration reasons */
  printf("User ID: %.*s Password: %.*s\n",
         pMQCXP -> SecurityParms -> CSPUserIdLength,
```

```
        pMQCXP -> SecurityParms -> CSPUserIdPtr,
        pMQCXP -> SecurityParms -> CSPPasswordLength,
        pMQCXP -> SecurityParms -> CSPPasswordPtr);
```

Wyjście może powiedzieć IBM MQ , aby zamknąć kanał, zwracając wartość *MQXCC_CLOSE_CHANNEL* w tabeli MQCXP.**Exitresponse** . W przeciwnym razie przetwarzanie kanału będzie kontynuowane w fazie uwierzytelniania połączenia.

Uwaga: Jeśli asertywny użytkownik zostanie zmieniony przez wyjście zabezpieczeń, reguły odwzorowania CHLAUTH nie zostaną ponownie zastosowane do nowego użytkownika.

Krok 10: Uwierzytelnienie użytkownika

Faza uwierzytelniania jest wykonywana, jeśli parametr CONNAUTH jest włączony w menedżerze kolejek.

Aby to sprawdzić, należy wywołać komendę MQSC DISPLAY QMGR CONNAUTH.

z/OS W poniższym przykładzie przedstawiono dane wyjściowe komendy **DISPLAY QMGR CONNAUTH** z menedżera kolejek działającego w systemie IBM MQ for z/OS.

```
 CSQM201I !MQ25 CSQMDRTC DISPLAY QMGR DETAILS
 QMNAME(MQ25)
 CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
  END QMGR DETAILS
 CSQ9022I !MQ25 CSQMDRTC ' DISPLAY QMGR' NORMAL COMPLETION
```

Multi W poniższym przykładzie przedstawiono dane wyjściowe komendy '**DISPLAY QMGR CONNAUTH**' z menedżera kolejek działającego w systemie IBM MQ for Multiplatforms.

```
     1 : DISPLAY QMGR CONNAUTH
AMQ8408: Display Queue Manager details.
   QMNAME(DEMO)
   CONNAUTH(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
```

Wartość CONNAUTH to nazwa obiektu **AUTHINFO** IBM MQ .

Ponieważ uwierzytelnianie systemu operacyjnego (**AUTHTYPE**(*IDPWOS*)) jest poprawne zarówno na serwerze IBM MQ for Multiplatforms , jak i w produkcie IBM MQ for z/OS, w przykładach używane jest uwierzytelnianie systemu operacyjnego.

z/OS W poniższym przykładzie przedstawiono dostarczony domyślny obiekt dla programu **AUTHTYPE**(*IDPWOS*) z menedżera kolejek działającego w systemie IBM MQ for z/OS.

```
 CSQM293I !MQ25 CSQMDRTC 1 AUTHINFO FOUND MATCHING REQUEST CRITERIA
 CSQM201I !MQ25 CSQMDRTC DISPLAY AUTHINFO DETAILS
 AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
 AUTHTYPE(IDPWOS)
 QSGDISP(QMGR)
 ADOPTCTX(NO)
 CHCKCLNT(NONE)
 CHCKLOCL(OPTIONAL)
 FAILDLAY(1)
 DESCR()
 ALTDATE(2018-06-04)
 ALTTIME(10.43.04)
   END AUTHINFO DETAILS
 CSQ9022I !MQ25 CSQMDRTC ' DISPLAY AUTHINFO' NORMAL COMPLETION
```

Multi W poniższym przykładzie przedstawiono dostarczony domyślny obiekt dla programu **AUTHTYPE**(*IDPWOS*) z menedżera kolejek działającego w systemie IBM MQ for Multiplatforms.

```
 1 : display authinfo(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
AMQ8566: Display authentication information details.
   AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS)
   AUTHTYPE(IDPWOS)                    ADOPTCTX(NO)
   DESCR( )                            CHCKCLNT(REQDADM)
```

```
CHCKLOCL(OPTIONAL)                  FAILDLAY(1)
ALTDATE(2015-06-08)                 ALTTIME(16.35.16)
```

Parametr AUTHINFO TYPE (IDPWOS) ma atrybut o nazwie CHCKCLNT. Jeśli wartość zostanie zmieniona na *REQUIRED* , wszystkie aplikacje klienckie muszą podać poprawny identyfikator użytkownika i hasło.

Jeśli użytkownik został uwierzytelniony w kroku 7, użytkownik nie zostanie uwierzytelniony ponownie, chyba że użytkownik lub hasło w polu SecurityParms struktury MQCXP zostały zmienione przez wyjście zabezpieczeń w kroku 9.

Krok 11: Przyjęcie kontekstu użytkownika MQCSP (jeśli `ChlauthEarlyAdopt=`*N* i ADOPTCTX=YES)
Można ustawić atrybut ADOPTCTX , który określa, czy kanał działa pod kontrolą MCAUSER, czy też identyfikator użytkownika, który został dostarczony przez aplikację.

Jeśli identyfikator użytkownika sprawdzony w polu MQCSP lub **`SecurityParms`** struktury MQXCP został pomyślnie uwierzytelniony, a **ADOPTCTX** ma wartość *YES*, kontekst użytkownika wynikający z kroków 7 i 8 jest przyjmowany jako kontekst używany dla tej aplikacji, chyba że użytkownik lub hasło w polu **`SecurityParms`** struktury MQCXP zostały zmienione przez wyjście zabezpieczeń w kroku 9.

Ten sprawdzony identyfikator użytkownika to identyfikator użytkownika, który jest sprawdzany pod kątem autoryzacji do korzystania z zasobów produktu IBM MQ .

Na przykład użytkownik nie ma ustawionego na kanale SVRCONN zestawu MCAUSER, a klient działa pod kontrolą '`johndoe`' na komputerze z systemem Linux . Aplikacja określa użytkownika '`fred`' w module MQCSP, dzięki czemu kanał zaczyna działać z '`johndoe`' jako aktywny użytkownik MCAUSER. Po sprawdzeniu CONNAUTH użytkownik '`fred`' jest adoptowane, a kanał jest uruchamiany z '`fred`' jako aktywny MCAUSER.

Krok 12: sprawdzenie, czy użytkownik nie jest zablokowany (BLOCKUSER)
Jeśli sprawdzanie **CONNAUTH** powiedzie się, pamięć podręczna CHLAUTH zostanie ponownie sprawdzona w celu sprawdzenia, czy aktywny użytkownik MCAUSER jest zablokowany przez regułę *BLOCKUSER* . Jeśli użytkownik jest zablokowany, kanał zostanie zakończony.

Step13: Sprawdzanie poprawności wymagań CHLAUTH CHCKCLNT
Jeśli reguła CHLAUTH wybrana w kroku 8 dodatkowo określa wartość CHCKCLNT dla REQUIRED lub REQDADM, to sprawdzanie poprawności jest wykonywane w celu zapewnienia, że poprawny identyfikator użytkownika CONNAUTH został dostarczony w celu spełnienia wymagania.

- Jeśli opcja CHCKCLNT (REQUIRED) jest ustawiona, użytkownik musi być uwierzytelniony w kroku 7 lub 10. W przeciwnym razie połączenie zostanie odrzucone.
- Jeśli ustawiony jest parametr CHCKCLNT (REQDADM), użytkownik musi być uwierzytelniony w kroku 7 lub 10 , jeśli to połączenie jest określone jako uprzywilejowane. W przeciwnym razie połączenie zostanie odrzucone.
- Jeśli ustawiona jest wartość CHCKCLNT (ASQMGR), ten krok jest pomijany.

Uwagi:

1. Jeśli ustawiona jest wartość CHCKCLNT (REQUIRED) lub CHCKCLNT (REQDADM), ale parametr CONNAUTH nie jest włączony w menedżerze kolejek, połączenie nie powiedzie się z kodem powrotu MQRC_SECURITY_ERROR (2063) z powodu konfliktu w konfiguracji.
2. Użytkownik nie jest ponownie uwierzytelniony w tym kroku.

Krok 14: Sprawdź poprawność wymagań CONNAUTH CHCKCLNT.
Faza uwierzytelniania jest wykonywana, jeśli parametr CONNAUTH jest włączony w menedżerze kolejek.

Wartość CONNAUTH CHCKCLNT jest sprawdzana w celu określenia, jakie wymagania są ustawione dla połączeń przychodzących:

- Jeśli parametr CHCKCLNT (NONE) jest ustawiony, ten krok jest pomijany.
- Jeśli parametr CHCKCLNT (OPTIONAL) jest ustawiony, ten krok jest pomijany.
- Jeśli ustawiona jest wartość CHCKCLNT (REQUIRED), to użytkownik musi być uwierzytelniony w kroku 7 lub 10. W przeciwnym razie połączenie zostanie odrzucone.

- Jeśli ustawiony jest parametr CHCKCLNT (REQDADM), użytkownik musi być uwierzytelniony w kroku 7 lub 10 , jeśli to połączenie jest określone jako uprzywilejowane. W przeciwnym razie połączenie zostanie odrzucone.

Uwaga: Użytkownik nie jest ponownie uwierzytelniony w tym kroku.

Multi **Krok 15: Sprawdzanie autoryzacji obiektu**
W celu zapewnienia, że aktywny użytkownik MCAUSER ma odpowiednie uprawnienia do nawiązywania połączenia z menedżerem kolejek, zostanie wykonane sprawdzenie.

ULW Więcej informacji na ten temat zawiera sekcja Object Authority Manager.

IBM i Więcej informacji na ten temat zawiera sekcja “Menedżer uprawnień do obiektów w systemie IBM i” na stronie 159.

Krok 16: zakończenie połączenia
Jeśli poprzednie kroki zostały zakończone pomyślnie, połączenie zostanie zakończone.

Pojęcia pokrewne
KONNAUTH
Menedżer kolejek może być skonfigurowany pod kątem używania podanego identyfikatora użytkownika i hasła w celu sprawdzenia, czy użytkownik ma uprawnienia do dostępu do zasobów.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH
ALTER AUTHINFO

Rozwiązywanie problemów z dostępem CHLAUTH
Sugestie dotyczące sposobu rozwiązania niektórych problemów z dostępem podczas korzystania z rekordów uwierzytelniania kanału (CHLAUTH).

Domyślne reguły CHLAUTH

Istnieją trzy domyślne reguły przetwarzania CHLAUTH:

- Brak dostępu do wszystkich kanałów przez użytkowników produktu `MQ-admin*`
- BRAK DOSTĘPU dla wszystkich SYSTEM.* kanały przez wszystkich użytkowników
- ALLOW dostęp do SYSTEM.ADMIN.SVRCONN (użytkownicy spoza programu `MQ-admin`)

Pierwsze dwa reguły blokują dostęp do wszystkich kanałów. Trzecia reguła jest bardziej konkretna, a więc ma pierwszeństwo przed pozostałymi dwoma, jeśli jest to kanał SYSTEM.ADMIN.SVRCONN , umożliwiając w ten sposób dostęp do tego kanału.

Typowe błędy połączenia

Reguły CHLAUTH są używane do określenia, czy kanał może być uruchomiony, a także umożliwiają odwzorowanie przez MCAUSER na inny identyfikator użytkownika. Jeśli kanał nie może zostać uruchomiony, często występują następujące błędy:

- RC 2035 MQRC_NOT_AUTHORIZED
- RC 2059 MQRC_Q_MGR_NOT_AVAILABLE
- AMQ4036 Dostęp nie jest dozwolony
- AMQ9776: Kanał został zablokowany przez użytkownika
- AMQ9777: Kanał został zablokowany
- MQJE001: Wystąpił wyjątek MQException: kod zakończenia 2, przyczyna 2035
- MQJE036: Menedżer kolejek odrzucił próbę połączenia

Powinieneś zablokować dostęp ściśle, a następnie dodać więcej reguł CHLAUTH do kontroli, kto może uzyskać dostęp i uruchomić kanały. Jako środek tymczasowy, a także w celu rozwiązania problemów z wyświetleniem następujących problemów:

- "Wyłącz reguły CHLAUTH" na stronie 63
- "Zmodyfikuj lub usuń reguły CHLAUTH" na stronie 63

Wyłącz reguły CHLAUTH

Jako środek tymczasowy, a także w celu rozwiązania powyższych błędów, można wyłączyć reguły CHLAUTH. Reguły mogą być ponownie włączone w dowolnym momencie, a jeśli wyłączenie reguł CHLAUTH rozwiąże problem z połączeniem, wiadomo, że była to przyczyna.

Aby wyłączyć reguły CHLAUTH, wydaj następującą komendę:

```
runmqsc: ALTER QMGR CHLAUTH (DISABLED)
```

Należy pamiętać, że można również ustawić wartość parametru CHLAUTH na *WARN*, co umożliwia dostęp do nich i protokołuje wynik reguły.

Zmodyfikuj lub usuń reguły CHLAUTH

Można także usunąć lub zmodyfikować regułę CHLAUTH lub reguły, które powodują problem.

Aby zmodyfikować regułę CHLAUTH, należy użyć komendy SET CHLAUTH z parametrem ACTION (REPLACE). Na przykład, aby zmodyfikować regułę domyślną, która nie powoduje żadnego dostępu do wszystkich kanałów przez użytkowników programu `MQ-admin` do wartości WARN, zamiast być zablokowanym, należy wywołać następującą komendę:

```
runmqsc: SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) WARN(YES)
ACTION (REPLACE)
```

Aby usunąć regułę CHLAUTH, należy użyć komendy SET CHLAUTH z parametrem ACTION (REMOVE). Na przykład, aby usunąć regułę domyślną, która nie powoduje żadnego dostępu do wszystkich kanałów przez użytkowników produktu `MQ-admin` , należy wprowadzić następującą komendę:

```
runmqsc: SET CHLAUTH (*) TYPE (BLOCKUSER) USERLIST (*MQADMIN) ACTION (REMOVE)
```

Testowanie dostępu przy użyciu MATCH (RUNCHECK)

Wynik reguł CHLAUTH można przetestować, korzystając z opcji MATCH (*RUNCHECK*) reguły CHLAUTH w runmqsc. Opcja **MATCH** (*RUNCHECK*) zwraca rekord, który jest zgodny z konkretnym kanałem przychodzącym w czasie wykonywania, jeśli kanał ten łączy się z tym menedżerem kolejek. Należy podać:

- Nazwa kanału
- atrybut adresu
- Atrybut SSLPEER, tylko jeśli kanał danych przychodzących używa protokołu SSL lub TLS
- QMNAME, jeśli kanał danych przychodzących jest kanałem menedżera kolejek, lub
- Atrybut CLNTUSER, jeśli kanał danych przychodzących jest kanałem klienta

W poniższym przykładzie sprawdzono, jaka reguła CHLAUTH, z domyślnymi regułami, powoduje, że użytkownik `MQ-admin` `johndoe` uzyskuje dostęp do kanału o nazwie `CHAN1`:

```
runmqsc: DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('johndoe') ADDRESS
('192.168.1.138')

AMQ8878: Display channel authentication record details.
CHLAUTH(*) TYPE(BLOCKUSER)
USERLIST(*MQADMIN)
```

W przypadku użytkownika `johndoe`kanał nie jest uruchamiany, użytkownik zostanie zablokowany z powodu reguły BLOCKUSER dla użytkowników *MQADMIN.

W poniższym przykładzie sprawdzono, jaka reguła CHLAUTH, z domyślnymi regułami, powoduje, że użytkownik `alice` nie jest użytkownikiem programu `MQ-admin` , uzyskując dostęp do kanału o nazwie `CHAN1`:

```
runmqsc: DISPLAY CHLAUTH (CHAN1) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')

AMQ9783: Channel will run using MCAUSER('alice').
```

W przypadku użytkownika `alice`kanał działa, a kanał przekazuje `alice` jako użytkownik MCAUSER. MCAUSER to ID użytkownika używany do sprawdzania uprawnień do obiektów IBM MQ .

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH
WYŚWIETL CHLAUTH

Tworzenie nowych reguł CHLAUTH dla użytkowników
Niektóre wspólne scenariusze dla użytkowników, a także przykładowe reguły CHLAUTH, które mają zostać wykonane.

Ten temat zawiera następujące scenariusze:

- “Kontrolowanie dostępu dla określonych użytkowników administracyjnych MQ” na stronie 64
- “Kontrolowanie dostępu dla konkretnego użytkownika i aplikacji klienckiej IBM MQ” na stronie 65
- “Kontrolowanie dostępu do konkretnego użytkownika za pomocą nazwy wyróżniającej certyfikatu (DN) tego użytkownika” na stronie 65
- “Odwzorowywanie konkretnego użytkownika na użytkownika produktu mqm” na stronie 66

Kontrolowanie dostępu dla określonych użytkowników administracyjnych MQ

W tym scenariuszu należy skonfigurować kanał połączenia z serwerem, który ma być używany wyłącznie w perspektywie administracyjnej, czyli do łączenia się z produktem IBM MQ Explorer. Istnieje konkretny kanał dla tego użycia oraz zdefiniowany adres IP lub adresy, z których mają być akceptowane połączenia, a także dostęp blokowany dla identyfikatora `'mqm'` , jeśli połączenie nie pochodzi z jednego z podanych adresów IP.

Utwórz kanał SVRCONN dla użytkowników IBM MQ Explorer i `MQ-admin` o nazwie `ADMIN.CHAN`:

```
runmqsc: DEFINE CHANNEL (ADMIN.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

W celu przetestowania upewnij się, że zdefiniowano użytkownika, który znajduje się w grupie `MQ-admin` , a nie taki, który jest inny. W tym scenariuszu `mqadm` znajduje się w grupie `MQ-admin` , a `alice` nie.

Zostaną umieszczone domyślne reguły CHLAUTH . Dodaj trzy reguły, aby umożliwić określonym użytkownikowi dostęp do ADMIN.CHAN jako `MQ-admin` z niektórych adresów IP:

- Ustaw NOACCESS z dowolnego adresu
- Ustaw dla tego kanału wartość BLOCKUSER, aby zablokować tylko użytkownika `nobody`, który nadpisuje użytkownika BLOCKUSER *MQADMIN.
- ALLOW dostęp do użytkownika `mqadm` w konkretnej podsieci adresów oraz odwzorowanie na uprawnienia użytkownika programu `mqadm`

```
runmqsc:
SET CHLAUTH (ADMIN.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('ADMIN.CHAN') TYPE(BLOCKUSER) +
DESCR('Rule to override *MQADMIN blockuser on this channel') +
USERLIST('nobody') ACTION(replace)
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER('mqadm') USERSRC(MAP) MCAUSER('mqadm') +
```

```
ADDRESS('192.168.1.*') +
DESCR('Allow mqadm as mqadm on local subnet') ACTION(ADD)
```

W tym momencie użytkownik `mqadm` może uzyskać dostęp i uruchomić ADMIN.CHAN , z podanego zakresu adresów IP.

Istnieje możliwość uruchomienia komendy MATCH (RUNCHECK) w dowolnym momencie, aby wyświetlić wyniki każdej z następujących komend:

```
runmqsc:
DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('mqadm') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE(USERMAP)
ADDRESS(192.168.1.*) CLNTUSER(mqadm)
MCAUSER(mqadm)

DISPLAY CHLAUTH (ADMIN.CHAN) MATCH (RUNCHECK) CLNTUSER ('alice') ADDRESS
('192.168.1.138')
AMQ8878: Display channel authentication record details.
CHLAUTH(ADMIN.CHAN) TYPE(ADDRESSMAP)
ADDRESS(*) USERSRC(NOACCESS)
```

W tym momencie tylko użytkownicy z rekordem CHLAUTH mają dostęp do korzystania z ADMIN.CHAN.

Kontrolowanie dostępu dla konkretnego użytkownika i aplikacji klienckiej IBM MQ

W tym scenariuszu domyślne reguły CHLAUTH są odpowiednie, przy założeniu, że uprawnienia IBM MQ powinny być ustawione dla konkretnego użytkownika, aby udostępnić poprawne uprawnienia IBM MQ (za pomocą komendy setmqaut).

W tym scenariuszu uprawnienia są ustawiane dla użytkownika `mqapp1`, który nie jest użytkownikiem produktu `MQ-admin` . Utwórz kanał SVRCONN, APP1.CHAN, który ma być używany przez określoną aplikację i konkretnego użytkownika.

```
runmqsc: DEFINE CHANNEL (APP1.CHAN) CHLTYPE (SVRCONN) TRPTYPE (TCP)
```

Korzystając z domyślnych reguł CHLAUTH , użytkownik `mqapp1` może uruchomić APP1.CHAN .

Identyfikator użytkownika pochodzący z aplikacji klienckiej IBM MQ jest używany do sprawdzania uprawnień do obiektu IBM MQ . W tym przypadku przy założeniu, że użytkownik 'mqapp1' prowadzi aplikację kliencką IBM MQ , jest ona używana do sprawdzania uprawnień do obiektu IBM MQ . W związku z tym, jeśli program `mqapp1` ma dostęp do obiektów IBM MQ aplikacji, to wszystko jest w porządku; jeśli nie, uzyskasz błędy uprawnień.

Aby zwiększyć bezpieczeństwo, należy utworzyć konkretne reguły CHLAUTH dla identyfikatora użytkownika `mqapp1` , ale w ramach reguł domyślnych żaden członek grupy `MQ-admin` nie może uzyskać dostępu do tego kanału.

```
runmqsc:
SET CHLAUTH (APP1.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('APP1.CHAN') TYPE(USERMAP) +
CLNTUSER('mqapp1') USERSRC(MAP) MCAUSER('mqapp1') +
DESCR('Allow mqapp1 as mqapp1 on local subnet') ACTION(ADD)
```

Kontrolowanie dostępu do konkretnego użytkownika za pomocą nazwy wyróżniającej certyfikatu (DN) tego użytkownika

W tym scenariuszu użytkownik musi mieć certyfikat, który jest przyleciany do menedżera kolejek. Nazwa wyróżniająca jest następnie dopasowywany do ustawienia SSLPEER reguły CHLAUTH, a SSLPEER może używać znaków wieloznacznych.

W przypadku dopasowania, użytkownik może być również odwzorowany na inny użytkownik MCAUSER, aby można było sprawdzić uprawnienia do obiektu IBM MQ . Odwzorowanie użytkownika MCAUSER może

zminimalizować liczbę użytkowników, którzy muszą być zarządzani w menedżerze uprawnień do obiektów produktu IBM MQ (OAM).

Używany jest kanał TLS z certyfikatami, które są używane, a reguły są wymagane do:

- Zablokuj wszystkich użytkowników dla konkretnego kanału
- Zezwól tylko użytkownikom o określonym SSLPEER, którzy korzystają z klienta tego użytkownika na potrzeby dostępu do systemu IBM MQ OAM.

```
.
# block all users on any IP address.
SET CHLAUTH('SSL1.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*')
USERSRC(NOACCESS) DESCR(''block all'') WARN(NO) ACTION(ADD)
.
# override - no MQM admin rule (allow mqm group /mqm admin users to
connect.
SET CHLAUTH('SSL1.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody')
DESCR('override no mqm admin rule') WARN(NO) ACTION(ADD)
.
# allow particular SSLPEER, use client id coming in from channel
SET CHLAUTH('SSL1.SVRCONN') TYPE(SSLPEERMAP)
SSLPEER('CN=JOHNDOE,O=IBM,C=US') USERSRC(CHANNEL) ACTION(ADD)
```

Identyfikator użytkownika klienta, który łączy się z kanałem, jest używany dla uprawnień IBM MQ OAM obiektów IBM MQ , dlatego identyfikator użytkownika musi mieć odpowiednie uprawnienia IBM MQ .

Istnieje możliwość odwzorowania na inny identyfikator użytkownika produktu IBM MQ , jeśli ma być używany:

```
USERSRC(MAP) MCAUSER('mquser1')
```

zamiast USERSRC(CHANNEL).

Odwzorowywanie konkretnego użytkownika na użytkownika produktu mqm

Jest to dodawanie lub modyfikowanie produktu “Kontrolowanie dostępu dla określonych użytkowników administracyjnych MQ” na stronie 64.

Dodaj następującą regułę CHLAUTH, aby odwzorować poszczególnych użytkowników na użytkownika produktu mqm lub identyfikator użytkownika produktu MQ-admin , który ma konfigurację uprawnień do obiektów produktu IBM MQ w produkcie IBM MQ OAM.

```
runmqsc:
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER ('johndoe') USERSRC(MAP) MCAUSER ('mqm') +
ADDRESS('192.168.1-100.*') +
DESCR ('Allow johndoe as MQ-admin on local subnet') ACTION (ADD)
```

Umożliwia to użytkownikowi i odwzorowuje użytkownika produktu johndoe na użytkownika mqm dla konkretnego kanału ADMIN.CHAN.

Pojęcia pokrewne

“Rozwiązywanie problemów z dostępem CHLAUTH” na stronie 62
Sugestie dotyczące sposobu rozwiązania niektórych problemów z dostępem podczas korzystania z rekordów uwierzytelniania kanału (CHLAUTH).

“Tworzenie nowych reguł CHLAUTH dla kanałów” na stronie 67
Aby pomóc w tworzeniu własnych reguł CHLAUTH, tutaj są pewne wspólne scenariusze dla kanałów, a na przykład reguły CHLAUTH, aby je zrealizować.

Odsyłacze pokrewne

USTAW WARTOŚĆ CHLAUTH
WYŚWIETL CHLAUTH

Tworzenie nowych reguł CHLAUTH dla kanałów
Aby pomóc w tworzeniu własnych reguł CHLAUTH, tutaj są pewne wspólne scenariusze dla kanałów, a na przykład reguły CHLAUTH, aby je zrealizować.

Ten temat zawiera następujące scenariusze:

- "Umożliwia dostęp tylko do określonego kanału z określonego zakresu adresów IP." na stronie 67
- "W przypadku konkretnego kanału należy zablokować wszystkich użytkowników, ale zezwolić konkretnym użytkownikom na nawiązanie połączenia." na stronie 67
- "Korzystanie z CHLAUTH dla kanałów odbiorczych i nadawczych" na stronie 68

Umożliwia dostęp tylko do określonego kanału z określonego zakresu adresów IP.

W tym scenariuszu należy wykonać następujące czynności:

- Ustaw brak dostępu do kanału z dowolnego miejsca
- Zezwól na dostęp z określonego adresu IP lub zakresu adresów

```
runmqsc:
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
WARN(NO) ACTION(ADD)
SET CHLAUTH('APP2.CHAN') TYPE(ADDRESSMAP) ADDRESS('9.95.100.1-5')
USERSRC(MAP) MCAUSER('mqapp2') ACTION(ADD)
```

Pozwala to tylko na APP2.CHAN , który ma być uruchomiony, gdy połączenie jest nawiązane z określonego zakresu adresów IP.

Użytkownik łączący się z uprawnieniami MCAUSER jest odwzorowywany na produkt `mqapp2`, a zatem pobiera uprawnienia OAM produktu IBM MQ dla tego użytkownika.

W przypadku konkretnego kanału należy zablokować wszystkich użytkowników, ale zezwolić konkretnym użytkownikom na nawiązanie połączenia.

W tym scenariuszu dostęp do kanału MY.SVRCONN zawiera domyślne reguły CHLAUTH w lokalizacji.

Należy dodać następujące elementy:

```
# block all users
SET CHLAUTH('MY.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR(''block all'') WARN(NO) ACTION(ADD)

# override - no MQM admin rule
SET CHLAUTH('MY.SVRCONN') TYPE(BLOCKUSER) USERLIST('nobody') DESCR('override
no mqm admin rule') WARN(NO) ACTION(ADD)

# allow johndoe userid
SET CHLAUTH('MY.SVRCONN') TYPE(USERMAP) CLNTUSER('johndoe')
USERSRC(CHANNEL) DESCR('allow johndoe userid') ACTION(ADD)
```

Ta pierwsza część kodu blokuje wszystkie osoby z połączenia na serwerze MY.SVRCONN, a następnie kod ten umożliwia uruchomienie tylko kanału MY.SVRCONN , gdy połączenie pochodzi z konkretnego identyfikatora użytkownika `johndoe`.

Użytkownik łączący się z kanałem `johndoe` jest używany dla uprawnień IBM MQ OAM obiektów IBM MQ . Dlatego identyfikator użytkownika musi mieć odpowiednie uprawnienia IBM MQ .

Istnieje możliwość odwzorowania na inny identyfikator użytkownika produktu IBM MQ , jeśli ma być używany:

```
USERSRC(MAP) MCAUSER('mquser1')
```

zamiast `USERSRC(CHANNEL)`.

Korzystanie z CHLAUTH dla kanałów odbiorczych i nadawczych

Można użyć reguł CHLAUTH w celu dodania dodatkowego zabezpieczenia do kanałów odbiorczych i nadawczych, aby ograniczyć dostęp do kanału odbiorczego. Należy pamiętać, że jeśli dodajesz lub dokonujesz zmian w regułach CHLAUTH, zaktualizowane reguły CHLAUTH mają zastosowanie tylko podczas uruchamiania kanału, więc jeśli kanały są już uruchomione, musisz je zatrzymać i uruchomić ponownie, aby aktualizacje CHLAUTH miały zastosowanie.

Reguły CHLAUTH mogą być używane na dowolnym kanale, ale są pewne ograniczenia. Na przykład reguły USERMAP mają zastosowanie tylko do kanałów SVRCONN.

W tym przykładzie możliwe jest połączenie tylko z określonym adresem IP, aby uruchomić TO.MYSVR1 :

```
# First you could lock down the channel by disallowing all
# for channel 'TO.MYSVR1', RCVR channel
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then you could allow this channel to be started
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('192.168.1.134') USERSRC(MAP)
MCAUSER('mqapp') ACTION(ADD)
```

W tym przykładzie możliwe jest połączenie tylko z określonym menedżerem kolejek:

```
# Lock down all access:
SET CHLAUTH('TO.MYSVR1') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
DESCR('Back-stop rule')

# Then allow access from queue manager MYSVR2 and from a particular ipaddress:
SET CHLAUTH('TO.MYSVR1') TYPE(QMGRMAP) QMNAME('MYSVR2') USERSRC(MAP)
MCAUSER('mqapp') ADDRESS('192.168.1.134') ACTION(ADD)
```

Pojęcia pokrewne

“Rozwiązywanie problemów z dostępem CHLAUTH” na stronie 62
Sugestie dotyczące sposobu rozwiązania niektórych problemów z dostępem podczas korzystania z rekordów uwierzytelniania kanału (CHLAUTH).

“Tworzenie nowych reguł CHLAUTH dla użytkowników” na stronie 64
Niektóre wspólne scenariusze dla użytkowników, a także przykładowe reguły CHLAUTH, które mają zostać wykonane.

Odsyłacze pokrewne

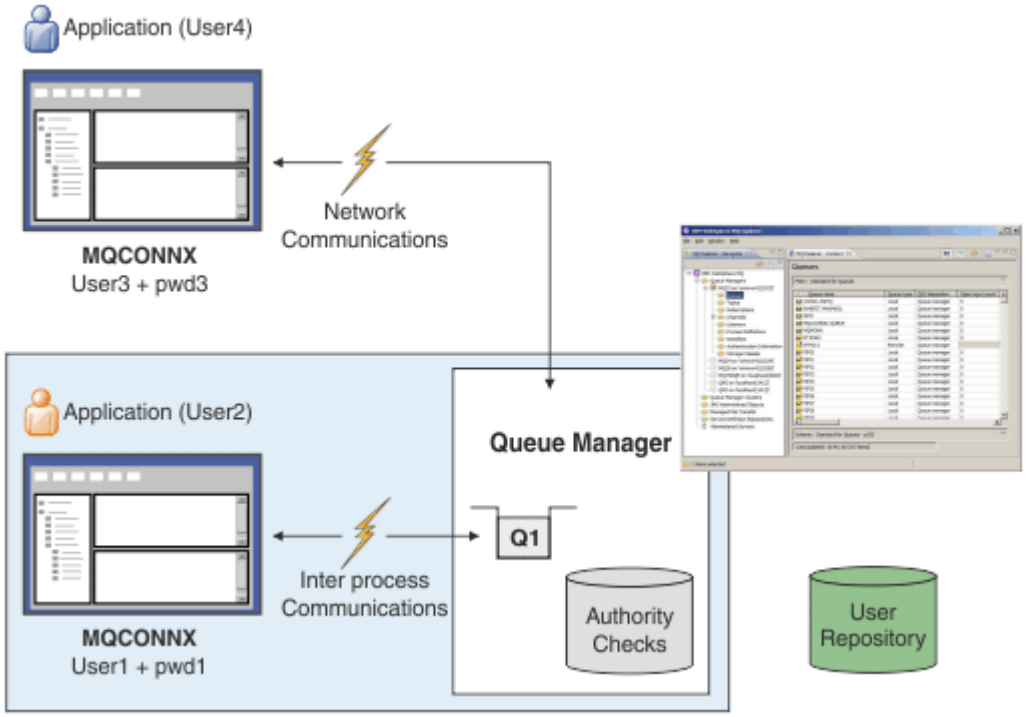
USTAW WARTOŚĆ CHLAUTH

WYŚWIETL CHLAUTH

Uwierzytelnianie połączenia

Uwierzytelnianie połączenia może być realizowane na różne sposoby:

- Aplikacja może podać identyfikator użytkownika i hasło. Aplikacją może być albo klient, albo też może używać powiązań lokalnych.
- Menedżer kolejek może być skonfigurowany do działania na podanym identyfikatorze użytkownika i haśle.
- Repozytorium może być używane do określenia, czy kombinacja ID użytkownika i hasła jest poprawna.



Na diagramie dwie aplikacje nawiązują połączenia z menedżerem kolejek, jedna aplikacja jako klient i jedna przy użyciu powiązań lokalnych. Aplikacje mogą używać różnych interfejsów API do łączenia się z menedżerem kolejek, ale wszystkie mają możliwość podania identyfikatora użytkownika i hasła. Identyfikator użytkownika, na którym działa aplikacja, `User2` i `User4` na diagramie, który jest zwykłym identyfikatorem użytkownika systemu operacyjnego prezentowanym w programie IBM MQ, może być inny niż identyfikator użytkownika udostępniony przez aplikację, `User1` i `User3`.

Menedżer kolejek odbiera komendy konfiguracyjne (na diagramie, IBM MQ Explorer jest używany) i zarządza otwieraniem zasobów i sprawdza uprawnienia dostępu do tych zasobów. W produkcie IBM MQ istnieje wiele różnych zasobów, do których aplikacja może wymagać uprawnień. Diagram ilustruje otwarcie kolejki dla danych wyjściowych, ale te same zasady mają zastosowanie również do innych zasobów.

Szczegółowe informacje na temat repozytorium używanego do sprawdzania identyfikatorów użytkowników i haseł zawiera sekcja Repozytoria użytkowników .

Pojęcia pokrewne

“Uwierzytelnianie połączenia: konfiguracja” na stronie 69
Menedżer kolejek może być skonfigurowany pod kątem używania podanego identyfikatora użytkownika i hasła w celu sprawdzenia, czy użytkownik ma uprawnienia do dostępu do zasobów.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 73

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 74
Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Uwierzytelnianie połączenia: konfiguracja

Menedżer kolejek może być skonfigurowany pod kątem używania podanego identyfikatora użytkownika i hasła w celu sprawdzenia, czy użytkownik ma uprawnienia do dostępu do zasobów.

Włączanie uwierzytelniania połączenia w menedżerze kolejek

W przypadku obiektu menedżera kolejek atrybut **CONNAUTH** może być ustawiony na nazwę obiektu informacji uwierzytelniającej (AUTHINFO). Ten obiekt może być jednym z dwóch typów (atrybut AUTHTYPE):

IDPWOS
Wskazuje, że menedżer kolejek używa lokalnego systemu operacyjnego do uwierzytelniania ID użytkownika i hasła.

IDPWLDAP
Wskazuje, że menedżer kolejek używa serwera LDAP do uwierzytelniania ID użytkownika i hasła.

Uwaga: W polu **CONNAUTH** nie można używać żadnego innego typu obiektu informacji uwierzytelniającej.

IDPWOS i IDPWLDAP są podobne pod względem liczby ich atrybutów, które zostały opisane w tym miejscu. Inne atrybuty są brane pod uwagę później.

Aby sprawdzić połączenia lokalne, należy użyć atrybutu AUTHINFO **CHCKLOCL** (sprawdź połączenia lokalne). Aby sprawdzić połączenia klienta, należy użyć atrybutu AUTHINFO **CHCKCLNT** (sprawdź połączenia klienta). Konfiguracja musi zostać odświeżona przed rozpoznaniem zmian przez menedżer kolejek.

```
ALTER QMGR CONNAUTH(USE.PW)
DEFINE AUTHINFO(USE.PW) +
AUTHTYPE(IDPWOS) +
FAILDLAY(10) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED)
REFRESH SECURITY TYPE(CONNAUTH)
```

Gdzie USE . PW w CONNAUTH jest łańcuchem, który jest zgodny z definicją AUTHINFO.

Zarówno **CHCKLOCL** , jak i **CHCKCLNT** mają ten sam zestaw możliwych wartości, które pozwalają na różnicowanie się w zakresie sprawdzania:

Brak
Wyłącza sprawdzanie.

Opcjonalne
Zapewnia, że jeśli ID użytkownika i hasło są udostępniane przez aplikację, to są one poprawną parą, ale nie są obowiązkowe do ich udostępnienia. Ta opcja może być użyteczna podczas migracji, np.

Ważne: OPCJONALNE to minimalna wartość, którą można ustawić w celu użycia bardziej rygorystycznych reguł CHLAUTH.

Jeśli zostanie wybrana wartość NONE , a połączenie klienta będzie zgodne z rekordem CHLAUTH z wartością CHCKCLNT REQUIRED (lub REQDADM na platformach innych niż z/OS), połączenie nie powiedzie się. Wyświetlany jest komunikat AMQ9793 na platformach innych niż z/OSi komunikat CSQX793E w systemie z/OS.

WYMAGANE
Wymaga, aby wszystkie aplikacje udostępniły poprawny identyfikator użytkownika i hasło. Patrz także następująca uwaga.

REQDADM
Użytkownicy uprzywilejowani muszą podać poprawny identyfikator użytkownika i hasło, ale użytkownicy nieuprzywilejowani są traktowani jak w przypadku ustawienia OPTIONAL . Patrz także następująca uwaga. z/OS (To ustawienie nie jest dozwolone w systemach z/OS).

Uwaga:

Ustawienie opcji **CHCKLOCL** na wartość REQUIRED lub REQDADM oznacza, że nie można administrować menedżerem kolejek lokalnie za pomocą programu **runmqsc** (błąd AMQ8135: Brak autoryzacji), chyba że użytkownik określi parametr -u UserId w wierszu komend produktu **runmqsc** . Po ustawieniu tego zestawu program **runmqsc** wyświetla zachętę dla hasła użytkownika na konsoli.

Podobnie, użytkownik uruchamiający program IBM MQ Explorer w systemie lokalnym będzie widział błąd AMQ4036 podczas próby nawiązania połączenia z menedżerem kolejek. Aby określić nazwę użytkownika i hasło, kliknij prawym przyciskiem myszy lokalny obiekt menedżera kolejek i wybierz opcję **Szczegóły połączenia** > **Właściwości ...** z menu. W sekcji **Userid** wprowadź nazwę użytkownika i hasło, które mają być używane, a następnie kliknij przycisk **OK**.

Podobne uwagi mają zastosowanie do połączeń zdalnych z produktem **CHCKCLNT**.

Wartość **CONNAUTH** jest pusta dla migrowanych menedżerów kolejek, ale ustawionych na wartość *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* dla nowych menedżerów kolejek. Poprzednia definicja **AUTHINFO** domyślnie ma wartość **CHCKCLNT** ustawioną na *REQDADM* .

Dlatego należy podać poprawne hasło systemu operacyjnego dla wszystkich istniejących klientów, korzystając z identyfikatora użytkownika uprzywilejowanego w celu nawiązania połączenia.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP dla aplikacji klienckiej zostanie wysłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienta są odpowiednio chronione, należy zapoznać się z “Ochrona hasłem protokołu MQCSP” na stronie 30.

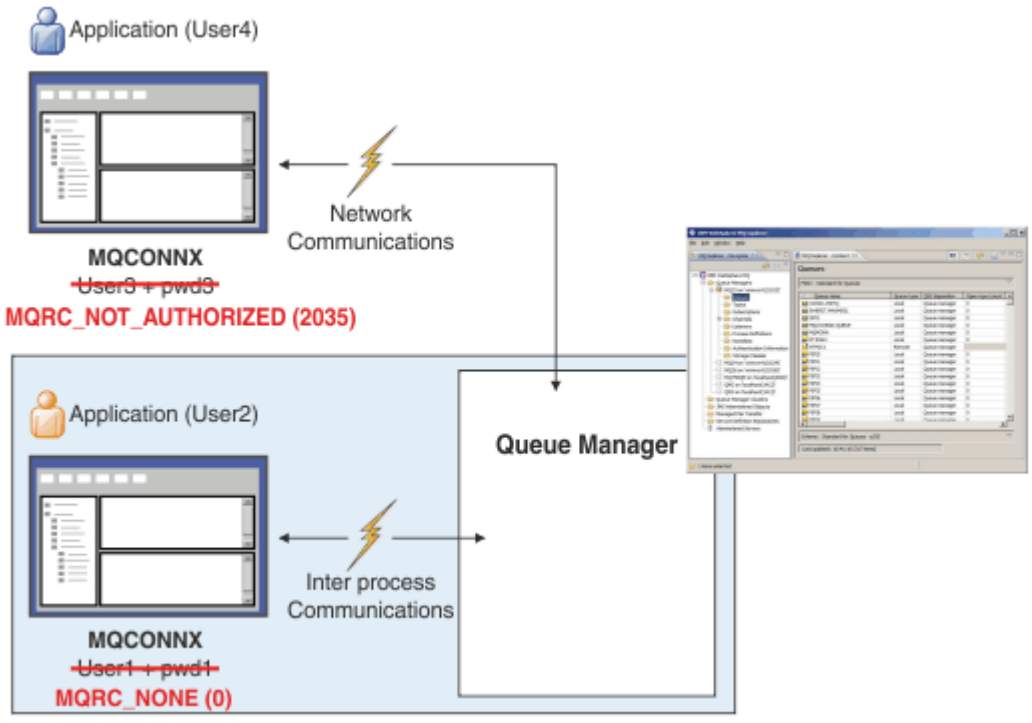
Granulacja konfiguracji

Oprócz produktów **CHCKLOCL** i **CHCKCLNT** , które są używane do włączania sprawdzania identyfikatora użytkownika i hasła, wprowadzono udoskonalenia reguł produktu CHLAUTH , dzięki czemu możliwe jest korzystanie z bardziej konkretnej konfiguracji przy użyciu produktu **CHCKCLNT**.

Ogólną wartość parametru **CHCKCLNT** można ustawić na wartość OPTIONAL, a następnie zaktualizować ją, aby była bardziej rygorystyczną dla niektórych kanałów, ustawiając parametr **CHCKCLNT** na wartość REQUIRED lub REQDADM w regule CHLAUTH . Domyślnie reguły produktu CHLAUTH będą uruchamiane z produktem CHCKCLNT(ASQMGR) , dlatego ta granulacja nie musi być używana. Na przykład:

```
DEFINE AUTHINFO(USE.PW) AUTHTYPE(xxxxxx) +
CHCKCLNT(OPTIONAL)
SET CHLAUTH('*') TYPE(ADDRESSMAP) +
ADDRESS('*') USERSRC(CHANNEL) +
CHCKCLNT(REQUIRED)
SET CHLAUTH('*') TYPE(SSLPEERMAP) +
SSLPEER('CN=*') USERSRC(CHANNEL)
```

Powiadomienie o błędzie



Błąd jest rejestrowany, jeśli aplikacja nie dostarcza identyfikatora użytkownika i hasła, jeśli jest to wymagane, lub dostarcza niepoprawną kombinację, nawet jeśli jest ona opcjonalna.

Uwaga: Gdy sprawdzanie hasła jest wyłączone za pomocą opcji NONE na serwerze **CHCKLOCL** lub **CHCKCLNT**, niepoprawne hasła nie są wykrywane.

Uwierzytelnienie zakończone niepowodzeniem jest wstrzymane przez liczbę sekund określoną przez atrybut **FAILDLAY** , zanim błąd zostanie zwrócony do aplikacji. Zapewnia to ochronę przed wielokrotnym nawiązaniem połączenia przez aplikację.

Błąd jest rejestrowany na wiele sposobów:

Aplikacja
Aplikacja zwraca standardowy błąd zabezpieczeń serwera IBM MQ , RC2035 -MQRC_NOT_AUTHORIZED.

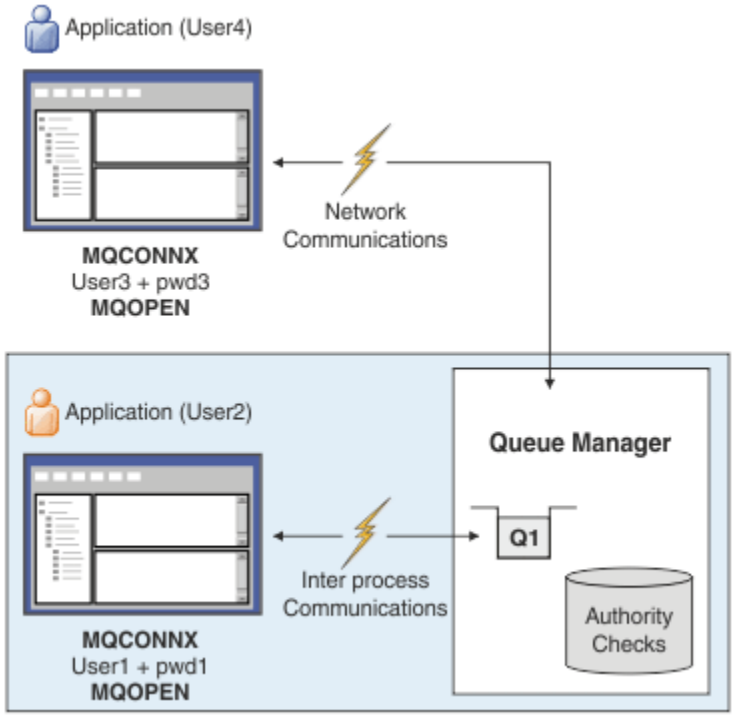
Administrator
Administrator produktu IBM MQ widzi zdarzenie zgłoszone w dzienniku błędów, dlatego może się upewnić, że aplikacja została odrzucona, ponieważ identyfikator użytkownika i hasło nie powiodły się, a nie dlatego, że na przykład nie ma uprawnień do połączenia .

Narzędzie do monitorowania
Narzędzie do monitorowania może być również powiadamiane o niepowodzeniu, jeśli użytkownik włączy zdarzenia uprawnień, wysyłając komunikat zdarzenia do systemu SYSTEM.ADMIN.QMGR.EVENT :

```
ALTER QMGR AUTHOREV(ENABLED)
```

To zdarzenie "Nieautoryzowane" jest zdarzeniem połączenia typu 1 i udostępnia te same pola co inne zdarzenia typu 1, z dodatkowym polem, udostępnionym identyfikatorem użytkownika MQCSP. Hasło nie jest podane w komunikacie o zdarzeniu. Oznacza to, że w komunikacie o zdarzeniu są dwa identyfikatory użytkowników: identyfikator, pod którym aplikacja jest uruchomiona, oraz identyfikator, który jest prezentowany przez aplikację w celu sprawdzenia identyfikatora użytkownika i hasła.

Relacja z autoryzacją



Menedżer kolejek można skonfigurować w taki sposób, aby identyfikatory użytkowników i hasła były udostępniane przez niektóre aplikacje, ponieważ identyfikator użytkownika, pod którym aplikacja jest uruchomiona, może nie być tym samym identyfikatorem użytkownika, który został przedstawiony przez aplikację wraz z hasłem, gdy aplikacja otwiera kolejkę dla danych wyjściowych, na przykład:

```
ALTER QMGR CONNAUTH(USE.PWD)
DEFINE AUTHINFO(USE.PWD) +
AUTHTYPE(xxxxxx) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED) +
ADOPTCTX(YES)
```

Sposób obsługi identyfikatorów użytkowników i haseł jest kontrolowany przez atrybut **ADOPTCTX** w obiekcie informacji uwierzytelniającej.

ADOPTCTX (TAK)
Wszystkie sprawdzenia autoryzacji dla aplikacji są wykonywane przy użyciu tego samego identyfikatora użytkownika, który został uwierzytelniony przez hasło, poprzez wybranie opcji adopcji kontekstu jako kontekstu aplikacji dla pozostałej części życia połączenia.

Ostrzeżenie: W przypadku używania opcji ADOPTCTX (YES) i identyfikatorów użytkowników systemu operacyjnego należy upewnić się, że identyfikator użytkownika, który jest adoptowane, nie przekracza maksymalnej długości identyfikatorów użytkowników. Więcej informacji zawiera sekcja “Identyfikatory użytkownika” na stronie 84.

ADOPTCTX (NIE)
Aplikacja udostępnia ID użytkownika i hasło dla celów uwierzytelniania ich w czasie połączenia, ale następnie kontynuuje używanie ID użytkownika, który jest uruchomiony w ramach przyszłych sprawdzeń autoryzacji. Ta opcja może być przydatna podczas migracji lub jeśli planowane jest użycie innych mechanizmów, takich jak rekordy uwierzytelniania kanału, w celu przypisania identyfikatora użytkownika agenta kanału komunikatów (message channel user identifier-MCAUSER).

Ostrzeżenie:

Jeśli parametr **ADOPTCTX(YES)** jest używany w obiekcie informacji uwierzytelniającej, nie można adopować innego kontekstu zabezpieczeń, chyba że w sekcji kanałów w pliku `qm.ini` zostanie ustawiony parametr **ChlauthEarlyAdopt** .

Na przykład domyślny obiekt informacji uwierzytelniających jest ustawiony na wartość **ADOPTCTX(YES)**, a użytkownik `fred` jest zalogowany. Skonfigurowane są następujące dwa reguły CHLAUTH:

```
SET CHLAUTH('MY.CHLAUTH') TYPE(ADDRESSMAP) DESCR('Block all access by
default') ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
SET CHLAUTH('MY.CHLAUTH') TYPE(USERMAP) DESCR('Allow user bob and force
CONNAUTH') CLNTUSER('bob') CHCKCLNT(REQUIRED) USERSRC(CHANNEL)
```

Następująca komenda jest wydawana z zamiarem uwierzytelnienia komendy jako adoptowane kontekst zabezpieczeń użytkownika bob:

```
runmqsc -c -u bob QMGR
```

W rzeczywistości menedżer kolejek używa kontekstu zabezpieczeń produktu `fred`, a nie produktu bob, a połączenie nie powiedzie się.

Więcej informacji na temat produktu **ChlauthEarlyAdopt**zawiera sekcja Atrybuty sekcji kanałów.

Pojęcia pokrewne

“Uwierzytelnianie połączenia” na stronie 68

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 73

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 74

Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Uwierzytelnianie połączenia: zmiany aplikacji

Aplikacja może podać identyfikator użytkownika i hasło w strukturze parametrów zabezpieczeń połączenia (MQCSP), gdy wywoływany jest program MQCONNX. Identyfikator użytkownika i hasło są przekazywane do sprawdzania, czy do menedżera uprawnień do obiektu (OAM) dostarczanego z menedżerem kolejek lub komponentu usługi autoryzacji dostarczanego z menedżerem kolejek w systemach z/OS . Nie ma potrzeby pisania własnego interfejsu niestandardowego.

Jeśli aplikacja jest uruchomiona jako klient, identyfikator użytkownika i hasło są również przekazywane do wyjść zabezpieczeń po stronie klienta i po stronie serwera w celu ich przetworzenia. Mogą być również używane do ustawiania atrybutu ID użytkownika agenta kanału komunikatów (MCAUSER) instancji kanału. Wyjście zabezpieczeń jest wywoływane z przyczyną wyjścia MQXR_SEC_PARMS dla tego przetwarzania. Wyjścia zabezpieczeń po stronie klienta i wyjście przed nawiązaniem połączenia mogą wprowadzać zmiany w tabeli MQCONN, zanim zostanie ona wysłana do menedżera kolejek.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP dla aplikacji klienckiej zostanie wysłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienta są odpowiednio chronione, należy zapoznać się z “Ochrona hasłem protokołu MQCSP” na stronie 30.

Korzystając z łańcucha XAOPEN w celu podania identyfikatora użytkownika i hasła, można uniknąć konieczności wprowadzania zmian w kodzie aplikacji.

Uwaga:

Z programu IBM WebSphere MQ 6.0wyjście zabezpieczeń umożliwiło ustawienie protokołu MQCSP. Dlatego też klienty na tym poziomie lub później nie muszą być aktualizowane.

Jednak w wersjach produktu IBM MQ wcześniejszych niż IBM MQ 8.0protokół MQCSP nie umieł żadnych ograniczeń na podstawie identyfikatora użytkownika i hasła, które zostały udostępnione przez aplikację. Jeśli te wartości są używane z opcjami udostępnitymi przez produkt IBM MQ , istnieją ograniczenia, które dotyczą korzystania z tych funkcji, ale jeśli tylko przekazujesz je do własnych wyjść, limity te nie mają zastosowania.

Pojęcia pokrewne

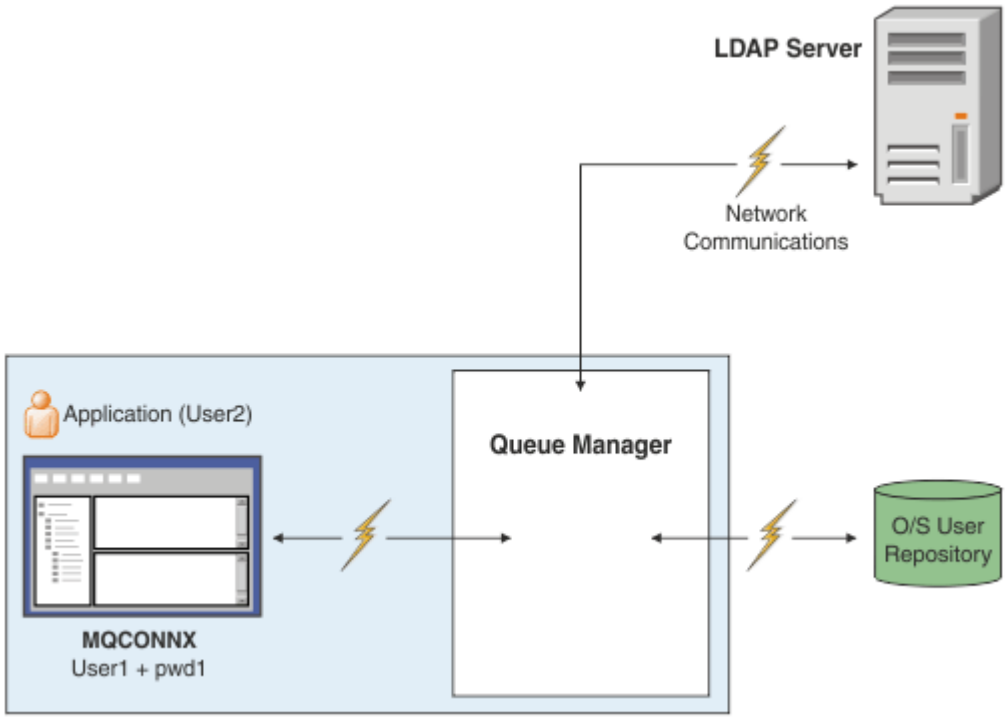
“Uwierzytelnianie połączenia” na stronie 68

“Uwierzytelnianie połączenia: konfiguracja” na stronie 69
Menedżer kolejek może być skonfigurowany pod kątem używania podanego identyfikatora użytkownika i hasła w celu sprawdzenia, czy użytkownik ma uprawnienia do dostępu do zasobów.

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 74
Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Uwierzytelnianie połączenia: repozytoria użytkowników

Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.



Rysunek 7. Typy obiektów informacji uwierzytelniającej

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)
DEFINE AUTHINFO(USE.LDAP) +
AUTHTYPE(IDPWLDAP) +
CONNAME('ldap1(389),ldap2(389)') +
LDAPUSER('CN=QMGR1') +
LDAPPWD('passw0rd') SECCOMM(YES)
```

Istnieją dwa typy obiektów informacji uwierzytelniającej, które są przedstawione na diagramie:

- Wartość IDPWOS jest używana do wskazania, że menedżer kolejek używa lokalnego systemu operacyjnego do uwierzytelniania identyfikatora użytkownika i hasła. W przypadku korzystania z lokalnego systemu operacyjnego należy ustawić wspólne atrybuty zgodnie z opisem w poprzednich tematach.
- Wartość IDPWLDAP jest używana do wskazania, że menedżer kolejek używa serwera LDAP do uwierzytelniania ID użytkownika i hasła. Więcej informacji na ten temat zawiera sekcja dotycząca korzystania z serwera LDAP.

Dla każdego menedżera kolejek można wybrać tylko jeden typ obiektu informacji uwierzytelniającej, nadając mu nazwę odpowiedniego obiektu w atrybucie **CONNAUTH** menedżera kolejek.

Używanie serwera LDAP do uwierzytelniania.

W polu **CONNAME** wpisz adres serwera LDAP dla menedżera kolejek. Można podać więcej adresów dla serwera LDAP w postaci listy rozdzielanej przecinkami, co może pomóc w nadmiarowości, jeśli serwer LDAP sam nie udostępnia tej funkcji.

Ustaw wymagany identyfikator i hasło serwera LDAP w polach **LDAPUSER** i **LDAPPWD** , aby menedżer kolejek mógł uzyskać dostęp do serwera LDAP i wyszukać informacje o rekordach użytkowników.

Bezpieczne połączenie z serwerem LDAP

W przeciwieństwie do kanałów, nie ma parametru **SSLCIPH** włączającego używanie protokołu TLS do komunikacji z serwerem LDAP. W tym przypadku IBM MQ działa jako klient serwera LDAP, więc większość

konfiguracji jest wykonywana na serwerze LDAP. Niektóre istniejące parametry w pliku IBM MQ są używane do konfigurowania sposobu działania połączenia.

Ustaw pole **SECCOMM** , aby określić, czy połączenie z serwerem LDAP ma korzystać z protokołu TLS.

Oprócz tego atrybutu atrybuty menedżera kolejek **SSLFIPS** i **SUITEB** ograniczają zestaw wybranych specyfikacji szyfrowania. Certyfikat używany do identyfikowania menedżera kolejek na serwerze LDAP jest certyfikatem menedżera kolejek `ibmwebspheremq` *`qmgr-name`* lub wartością atrybutu **CERTLABL** . Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

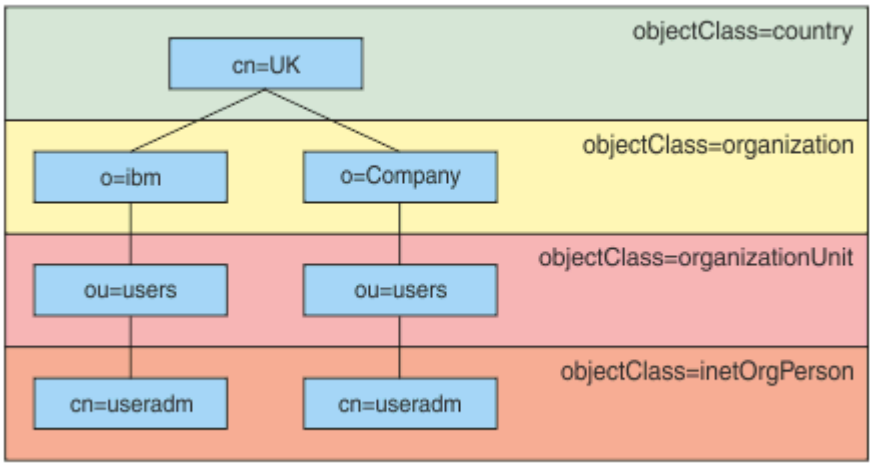
Repozytorium użytkowników LDAP

Jeśli używane jest repozytorium użytkowników LDAP, w menedżerze kolejek należy wykonać więcej czynności konfiguracyjnych niż tylko w celu poinformowania menedżera kolejek, gdzie znajduje się serwer LDAP.

Identyfikatory użytkowników zdefiniowane na serwerze LDAP mają strukturę hierarchiczną, która jednoznacznie je identyfikuje. Dlatego aplikacja może połączyć się z menedżerem kolejek i przedstawić swój identyfikator użytkownika jako pełny hierarchiczny identyfikator użytkownika.

Aby jednak uprościć informacje, które aplikacja musi udostępnić, można skonfigurować menedżer kolejek w taki sposób, aby zakładał, że pierwsza część hierarchii jest wspólna dla wszystkich identyfikatorów, i automatycznie dodać ją przed skróconym identyfikatorem udostępnianym przez aplikację. Menedżer kolejek może następnie przedstawić pełny identyfikator serwerowi LDAP.

Ustaw wartość BASEDNU na początkowy punkt, w którym wyszukiwanie LDAP będzie szukać identyfikatora w hierarchii LDAP. Po ustawieniu BASEDNU należy upewnić się, że podczas wyszukiwania identyfikatora w hierarchii LDAP zwracany jest tylko jeden wynik.



Rysunek 8. Przykładowa hierarchia LDAP

Na przykład w systemie Rysunek 8 na stronie 76 BASEDNU można ustawić wartość "ou=users, o=ibm, c = UK" lub ", o=ibm, c = UK". Ponieważ jednak nazwa wyróżniająca zawierająca "cn = useradm" istnieje zarówno w gałęzi "o = ibm", jak i w gałęzi "o=Company", wartość BASEDNU nie może być ustawiona na "c = UK". Ze względu na wydajność i bezpieczeństwo należy użyć najwyższego punktu w hierarchii LDAP, z którego można odwołać się do wszystkich potrzebnych identyfikatorów użytkowników. W tym przykładzie jest to "ou=users, o=ibm, c = UK".

Aplikacja może wprowadzić do menedżera kolejek identyfikator użytkownika bez podawania nazwy atrybutu LDAP, na przykład `CN=` . Jeśli właściwość USRFIELD zostanie ustawiona na nazwę atrybutu LDAP, ta wartość zostanie dodana jako przedrostek do identyfikatora użytkownika, który pochodzi z aplikacji. Może to być przydatne podczas migracji z identyfikatorów użytkowników systemu operacyjnego do identyfikatorów użytkowników LDAP, ponieważ aplikacja może w obu przypadkach prezentować ten sam łańcuch i można uniknąć zmiany aplikacji.

Dlatego pełny identyfikator użytkownika przedstawiony serwerowi LDAP wygląda następująco:

```
USRFIELD = ID_from_application BASEDNU
```

Pojęcia pokrewne

“Uwierzytelnianie połączenia” na stronie 68

“Uwierzytelnianie połączenia: konfiguracja” na stronie 69
Menedżer kolejek może być skonfigurowany pod kątem używania podanego identyfikatora użytkownika i hasła w celu sprawdzenia, czy użytkownik ma uprawnienia do dostępu do zasobów.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 73

Wyjście zabezpieczeń po stronie klienta w celu wstawienia ID użytkownika i hasła (`mqccred`)

Jeśli istnieją aplikacje klienckie, które są wymagane do wysłania identyfikatora użytkownika lub hasła, ale nie można zmienić jeszcze źródła, to istnieje wyjście zabezpieczeń dostarczane z programem IBM MQ 8.0 o nazwie **`mqccred`** , którego można użyć. Produkt **`mqccred`** udostępnia identyfikator użytkownika i hasło w imieniu aplikacji klienckiej z pliku `.ini` . Ten identyfikator użytkownika i hasło są wysyłane do menedżera kolejek, który, jeśli jest tak skonfigurowany, uwierzytelni je.

Przegląd

`mqccred` to wyjście zabezpieczeń, które działa na tym samym komputerze, co aplikacja kliencka. Umożliwia on podanie informacji o identyfikatorze użytkownika i haśle w imieniu aplikacji klienckiej, gdzie informacje te nie są dostarczane przez samą aplikację. Informacje o ID użytkownika i haśle są dostarczane w strukturze znanej jako Parametry zabezpieczeń połączenia (MQCSP) i zostaną uwierzytelnione przez menedżer kolejek, jeśli skonfigurowano uwierzytelnianie połączenia .

Informacje o ID użytkownika i haśle są pobierane z pliku `.ini` na komputerze klienckim. Hasła w pliku są chronione przez zaciemnianie za pomocą komendy **`runmqccred`** , a także przez zapewnienie, że uprawnienia do plików w pliku `.ini` są ustawione tak, że tylko ID użytkownika uruchamiający aplikację kliencką (a więc wyjście) są w stanie go odczytać.

Położenie

Produkt **`mqccred`** jest zainstalowany:

Windows platformy
W katalogu *`installation_directory`*`\Tools\c\Samples\mqccred\`

UNIX platformy
W katalogu *`installation_directory`*`/samp/mqccred`

Uwagi: Wyjście:

1. Działa wyłącznie jako wyjście kanału bezpieczeństwa i musi być jedynym takim wyjściem zdefiniowanym na kanale.
2. Zwykle jest nazwana przez tabelę definicji kanału klienta (CCDT), ale klient Java może mieć bezpośrednie wyjście z obiektów JNDI lub wyjście może zostać skonfigurowane dla aplikacji, które ręcznie konstruują strukturę MQCD .
3. Należy skopiować programy **`mqccred`** i **`mqccred_r`** do katalogu `var/mqm/exits` .

   Na przykład na 64-bitowym komputerze platformy UNIX wywołaj komendę:

   ```
   cp installation_directory/samp/mqccred/lib64/* /var/mqm/exits
   ```

   Więcej informacji na ten temat zawiera sekcja Krok po kroku przykład testowania komendy mqccred .
4. Może działać w poprzednich wersjach produktu IBM MQ(z powrotem jako IBM WebSphere MQ 7.0.1).

Konfigurowanie identyfikatorów i haseł użytkowników

Plik `.ini` zawiera sekcje dla każdego menedżera kolejek, z ustawieniem globalnym dla nieokreślonych menedżerów kolejek. Każda sekcja zawiera nazwę menedżera kolejek, ID użytkownika oraz zwykły tekst lub obfusowane hasło.

Plik `.ini` należy zmodyfikować ręcznie, korzystając z dowolnego edytora i dodać atrybut hasła zwykłego tekstu do sekcji. Uruchom udostępniony program **runmqccred** , który pobiera plik `.ini` i zastępuje atrybut **Password** atrybutem **OPW** , zaciemnionym formularzem hasła.

Opis komendy i jej parametrów można znaleźć w sekcji runmqccred .

Plik `mqccred.ini` zawiera informacje o identyfikatorze użytkownika i haśle.

Plik szablonu `.ini` znajduje się w tym samym katalogu, w którym znajduje się wyjście, w celu udostępnienia punktu początkowego dla przedsiębiorstwa.

Domyślnie plik ten będzie wyszukiany w programie $HOME/`.mqs/mqccred.ini`. Jeśli chcesz go znaleźć w innym miejscu, możesz użyć zmiennej środowiskowej *MQCCRED* , aby wskazać na nią:

```
MQCCRED=C:\mydir\mqccred.ini
```

Jeśli używana jest wartość *MQCCRED*, zmienna musi zawierać pełną nazwę pliku konfiguracyjnego, w tym dowolny typ pliku `.ini` . Ponieważ ten plik zawiera hasła (nawet jeśli są one zaciemnione), użytkownik powinien chronić plik przy użyciu uprawnień systemu operacyjnego w celu zapewnienia nieuprawnionym osobom ich odczytania. Jeśli użytkownik nie ma odpowiednich uprawnień do pliku, wyjście nie zostanie uruchomione pomyślnie.

Jeśli aplikacja dostarczyła już strukturę MQCSP , wyjście jest normalnie zgodne z tą strukturą i nie będzie wstawiać żadnych informacji z pliku `.ini` . Można jednak to zmienić, korzystając z atrybutu **Force** w sekcji.

Ustawienie parametru **Force** na wartość *TRUE* powoduje usunięcie identyfikatora użytkownika i hasła dostarczonego przez aplikację, a także zastąpienie tych, które mają być używane w wersji pliku ini.

Można także ustawić atrybut **Force** w sekcji globalnej pliku, aby ustawić domyślną wartość tego pliku.

Wartością domyślną dla **Force** jest *FALSE*.

Istnieje możliwość podania ID użytkownika i hasła dla wszystkich menedżerów kolejek lub dla każdego pojedynczego menedżera kolejek. Poniżej przedstawiono przykład pliku `mqccred.ini` :

```
# comments are permitted
AllQueueManagers:
User=abc
OPW=%^&aervrgtsr

QueueManager:
Name=QMA
User=user1
OPW=H&^dbgfh

Force=TRUE

QueueManager:
Name=QMB
User=user2
password=passw0rd
```

Uwagi:

1. Poszczególne definicje menedżera kolejek mają pierwszeństwo przed ustawieniem globalnym.
2. W atrybutach nie jest rozróżniana wielkość liter.

Ograniczenia

Gdy to wyjście jest używane, lokalny ID użytkownika osoby, na której działa aplikacja, nie przepływa z klienta do serwera. Jedyne dostępne informacje o tożsamości pochodzą z zawartości pliku ini.

Dlatego należy skonfigurować menedżer kolejek tak, aby był używany produkt **ADOPTCTX(YES)**, lub odwzorować żądanie połączenia przychodzącego na odpowiedni identyfikator użytkownika za pomocą jednego z dostępnych mechanizmów, na przykład “Rekordy uwierzytelniania kanału” na stronie 50.

Ważne: W przypadku dodania nowych haseł lub aktualizacji starych haseł komenda **runmqccred** przetwarza tylko hasła w postaci jawnej, pozostawiając nietknięte zaciemnione hasła.

Debugowanie

Wyjście zapisuje do standardowego śledzenia produktu IBM MQ , gdy jest ono włączone.

Aby pomóc w debugowaniu problemów z konfiguracją, wyjście może być również zapisywane bezpośrednio w stdout.

Brak danych wyjścia zabezpieczeń kanału (**SCYDATA**) Konfiguracja jest zwykle wymagana dla kanału. Można jednak określić:

BŁĄD
Nie można znaleźć pliku konfiguracyjnego tylko w przypadku warunków błędu drukowania informacji o wydruku.

DEBUG
Wyświetla te warunki błędów i dodatkowe instrukcje śledzenia.

NOCHECKS
Pomija ograniczenia dotyczące uprawnień do plików, a ponadto ograniczenie, że plik `.ini` nie powinien zawierać żadnych niechronionych haseł.

Do pola **SCYDATA** można umieścić jeden lub więcej tych elementów, rozdzielając je przecinkami, w dowolnej kolejności. Na przykład: `SCYDATA=(NOCHECKS,DEBUG)`.

Należy zauważyć, że w elementach rozróżniana jest wielkość liter i muszą one być zapisane wielkimi literami.

Użycie `mqccred`

Po ustawieniu zestawu plików można wywołać wyjście kanału, aktualizując definicję kanału połączenia klienckiego w celu uwzględnienia atrybutu `SCYEXIT('mqccred(ChlExit)')`:

```
DEFINE CHANNEL(channelname) CHLTYPE(clntconn) +
CONNAME(remote machine) +
QMNAME(remote qmgr) +
SCYEXIT('mqccred(ChlExit)') +
REPLACE
```

Odsyłacze pokrewne
SCYDATA
SCYEXIT
runmqccred

Uwierzytelnianie połączenia z klientem Java

Uwierzytelnianie połączenia to funkcja w produkcie IBM MQ , która umożliwia skonfigurowanie menedżera kolejek w celu uwierzytelniania aplikacji przy użyciu podanego identyfikatora użytkownika i hasła. Gdy aplikacja jest aplikacją Java korzystaniową z powiązań klienta, uwierzytelnianie połączenia może być uruchamiane w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Tryb zgodności

Przed IBM MQ 8.0klient Java mógł wysłać ID użytkownika i hasło w kanale połączenia klienckiego do kanału połączenia z serwerem, a następnie przekazać je do wyjścia zabezpieczeń w polach **RemoteUserIdentifier** i **RemotePassword** struktury MQCD. W trybie zgodności zachowanie to jest zachowywane.

Ten tryb może być używany w połączeniu z uwierzytelnianiem połączenia i migrować z dala od wszystkich wyjść zabezpieczeń, które wcześniej były używane do wykonywania tego samego zadania.

Należy użyć parametru ADOPTCTX (YES) lub innej metody, na przykład reguły CHLAUTH opartej na certyfikacie TLS, w celu ustawienia działającego MCAUSER, gdy tryb zgodności jest używany, podobnie jak w tym trybie, identyfikator użytkownika po stronie klienta nie jest wysyłany do menedżera kolejek.

Tryb zgodności operacji może być włączony na zasadzie połączenia między połączeniem lub globalnie:

- W produkcie IBM MQ classes for Javaustaw właściwość *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* na wartość `false` we właściwościach hashtable, które są przekazywane do konstruktora **com.ibm.mq.MQQueueManager** .
- W produkcie IBM MQ classes for JMSustaw właściwość *JmsConstants.Parametr USER_AUTHENTICATION_MQCSP* ma wartość `false`w przypadku odpowiedniej fabryki połączeń przed utworzeniem połączenia.
- Globalnie należy określić właściwość systemową Java *-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication= N* w wierszu komend podczas uruchamiania aplikacji, tak jak pokazano to w poniższym przykładzie:

```
java -Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=N application_name
```

Tryb zgodności jest domyślnym ustawieniem.

Tryb uwierzytelniania MQCSP

W tym trybie wysyłany jest identyfikator użytkownika po stronie klienta, a także identyfikator użytkownika i hasło, które mają być uwierzytelniane, dzięki czemu możliwe jest użycie opcji ADOPTCTX (NO). Identyfikator użytkownika i hasło są dostępne dla wyjścia zabezpieczeń połączenia z serwerem w strukturze MQCSP , która jest udostępniana w strukturze MQCXP.

Ten tryb działania może być włączony w zależności od połączenia lub globalnie:

- W produkcie IBM MQ classes for Javaustaw właściwość *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* na wartość `true` w tabeli mieszającej właściwości, która jest przekazywana do konstruktora **com.ibm.mq.MQQueueManager** .
- W produkcie IBM MQ classes for JMSustaw właściwość *JmsConstants.Parametr USER_AUTHENTICATION_MQCSP* ma wartość `true`, a następnie w odpowiedniej fabryce połączeń przed utworzeniem połączenia.
- Globalnie ustaw właściwość systemową *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* na wartość wskazującą na wartość true (prawda), na przykład przez dodanie `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=Y` do wiersza komend.

Wybieranie trybu uwierzytelniania w programie IBM MQ Explorer

IBM MQ Explorer jest aplikacją Java , dlatego te dwa tryby, tryb zgodności i tryb uwierzytelniania MQCSP mają zastosowanie również do niego.

V 9.1.0 W produkcie IBM MQ 9.1.0domyślnym trybem uwierzytelniania MQCSP jest tryb uwierzytelniania. Przed IBM MQ 9.1domyślnym trybem zgodności jest tryb zgodności.

W przypadku paneli, w których podany jest identyfikator użytkownika, istnieje pole wyboru umożliwiające włączenie lub wyłączenie trybu zgodności:

- V 9.1.0 Domyślnie w produkcie IBM MQ 9.1.0to pole wyboru nie jest zaznaczone. Aby użyć trybu zgodności, zaznacz to pole wyboru.
- Przed IBM MQ 9.1.0domyślnie to pole wyboru jest włączone. Aby użyć uwierzytelniania MQCSP, usuń zaznaczenie tego pola wyboru.

Pojęcia pokrewne

"Uwierzytelnianie połączenia" na stronie 68

"Uwierzytelnianie połączenia: zmiany aplikacji" na stronie 73

"Uwierzytelnianie połączenia: repozytoria użytkowników" na stronie 74

Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Bezpieczeństwo komunikatów w produkcie IBM MQ

Zabezpieczenia komunikatów w infrastrukturze IBM MQ są udostępniane przez produkt Advanced Message Security.

Advanced Message Security (AMS) Rozszerza usługi zabezpieczeń produktu IBM 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

"Advanced Message Security" na stronie 580

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

Planowanie wymagań dotyczących bezpieczeństwa

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

Produktu IBM 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 IBM MQ udostępnia szereg usług zabezpieczeń na poziomie łącza, w tym obsługę protokołu TLS (Transport Layer Security).

Podczas planowania instalacji produktu IBM MQnależy wziąć pod uwagę pewne aspekty zabezpieczeń:

- Multi W systemie Wiele platform, jeśli te aspekty zostaną zignorowane i nic nie zostanie użyte, nie będzie można używać produktu IBM MQ.
- z/OS W systemie z/OSefekt ignorowania tych aspektów polega na tym, że zasoby produktu IBM MQ są niechronione. Oznacza to, że wszyscy użytkownicy mają dostęp do wszystkich zasobów produktu IBM MQ i mogą je zmieniać.

Uprawnienie do administrowania produktem IBM MQ

Administratorzy produktu IBM MQ muszą mieć uprawnienia do:

- Wydawanie komend do administrowania programem IBM MQ
- UżyjIBM MQ Explorer
- IBM i Użyj paneli administracyjnych i komend produktu IBM i .
- z/OS Użyj operacji i paneli sterujących w systemie z/OS

- z/OS Użyj programu narzędziowego IBM MQ CSQUTIL w systemie z/OS
- z/OS Dostęp do zestawów danych menedżera kolejek w systemie z/OS

Aby uzyskać więcej informacji, patrz:

- ULW “Uprawnienie do administrowania produktem IBM MQ w systemie UNIX, Linux, and Windows” na stronie 415
- IBM i “Uprawnienie do administrowania produktem IBM MQ w systemie IBM i” na stronie 86
- z/OS “Uprawnienie do administrowania produktem IBM MQ w systemie z/OS” na stronie 87

Uprawnienia do pracy z obiektami IBM MQ

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

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

Aplikacje mogą również używać komend PCF (Programmable Command Format) w celu uzyskania dostępu do tych obiektów produktu IBM MQ oraz do uzyskiwania dostępu do kanałów i obiektów informacji uwierzytelniających. Obiekty te mogą być chronione przez program IBM 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 MQ” na stronie 89.

Bezpieczeństwo kanału

Identyfikatory użytkowników powiązane z agentami kanału komunikatów (MCAs) muszą mieć uprawnienia dostępu do różnych zasobów produktu IBM 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 112.

Dodatkowe uwarunkowania

Jeśli używane są określone funkcje produktu IBM MQ lub rozszerzenia produktu podstawowego, należy wziąć pod uwagę następujące aspekty bezpieczeństwa:

- “Zabezpieczenia klastrów menedżerów kolejek” na stronie 125
- “Zabezpieczenia dla publikowania/subskrypcji produktu IBM MQ” na stronie 126
- “zabezpieczenia dlaIBM MQ Internet Pass-Thru” na stronie 127

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.

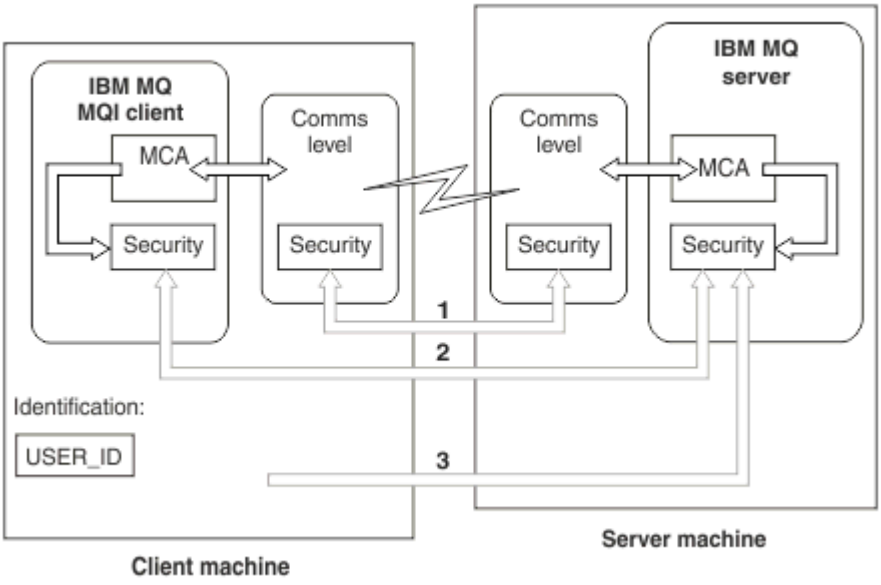
Użytkownik musi zdecydować, w jaki sposób będzie identyfikować użytkowników aplikacji IBM MQ , pamiętając o tym, że różne systemy operacyjne obsługują identyfikatory użytkowników o różnych długościach. Za pomocą rekordów uwierzytelniania kanału można odwzorować jeden identyfikator użytkownika na inny lub określić ID użytkownika na podstawie pewnego atrybutu połączenia. Kanały IBM MQ korzystające z protokołu 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 MQ. Więcej informacji na ten temat zawierają następujące sekcje:

- “Odwzorowywanie zdalnego menedżera kolejek na identyfikator użytkownika MCAUSER” na stronie 399
- “Odwzorowywanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER” na stronie 400
- “Odwzorowywanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER” na stronie 401
- “Odwzorowywanie adresu IP na identyfikator użytkownika MCAUSER” na stronie 403

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. Na diagramie przedstawiono IBM MQ MQI client , który jest połączony z serwerem. Zabezpieczenia są stosowane na czterech poziomach, zgodnie z opisem w poniższym tekście. Agent MCA jest agentem kanału komunikatów.



Rysunek 9. Zabezpieczenia w połączeniu klient/serwer

1. Poziom komunikacji

   Patrz strzałka 1. Aby zaimplementować zabezpieczenia na poziomie komunikacji, należy użyć protokołu TLS. Więcej informacji na ten temat zawiera sekcja “Protokoły zabezpieczeń szyfrujących: TLS” na stronie 15.
2. Rekordy uwierzytelniania kanału

   Patrz strzałki 2 i 3. Uwierzytelnianie może być kontrolowane za pomocą adresu IP lub nazw wyróżniających 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 50.

3. Uwierzytelnianie połączenia

   Patrz strzałka 3. Klient wysyła identyfikator i hasło. Więcej informacji na ten temat zawiera sekcja “Uwierzytelnianie połączenia: konfiguracja” na stronie 69.

4. 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.

5. 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 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.

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

W produkcie IBM MQ 8.0można wysyłać hasła, które są zawarte w strukturze MQCSP.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP dla aplikacji klienckiej zostanie wysłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienta są odpowiednio chronione, należy zapoznać się z “Ochrona hasłem protokołu MQCSP” na stronie 30.

Identyfikatory użytkownika

Podczas tworzenia identyfikatorów użytkowników dla aplikacji klienckich identyfikatory użytkowników nie mogą być dłuższe niż maksymalna dozwolona długość. Nie należy używać zastrzeżonych ID użytkowników NIEZNANE i NOBODY. Jeśli serwer, z którym łączy się klient, jest serwerem IBM MQ for Windows , należy uniknąć użycia znaku at (@). Dozwolona długość identyfikatorów użytkowników zależy od platformy, która jest używana dla serwera:

- z/OS Linux UNIX W systemach z/OS i UNIX and Linuxmaksymalna długość identyfikatora użytkownika wynosi 12 znaków.
- IBM i W systemie IBM imaksymalna długość identyfikatora użytkownika wynosi 10 znaków.
- Windows W systemie Windows, jeśli zarówno serwer IBM MQ MQI client, jak i serwer IBM MQ znajdują się w systemie Windows, a serwer ma dostęp do domeny, w której zdefiniowany jest identyfikator użytkownika klienta, maksymalna długość identyfikatora użytkownika wynosi 20 znaków. Jeśli jednak serwer IBM MQ nie jest serwerem Windows , identyfikator użytkownika jest obcinany do 12 znaków.
- Jeśli do przekazywania referencji jest używana struktura MQCSP, maksymalna długość identyfikatora użytkownika wynosi 1024 znaki. Identyfikator użytkownika struktury MQCSP nie może być używany do obejścia maksymalnej długości identyfikatora użytkownika używanej przez produkt IBM MQ w celu autoryzacji. Więcej informacji na temat struktury MQCSP zawiera sekcja “Identyfikowanie i uwierzytelnianie użytkowników przy użyciu struktury MQCSP” na stronie 344.

W systemach UNIX and Linux wartością domyślną jest to, że identyfikatory użytkowników są używane do uwierzytelniania, a grupy są używane do autoryzacji. Można jednak skonfigurować te systemy w taki sposób, aby autoryzowane były dla identyfikatorów użytkowników. Więcej informacji na ten temat zawiera sekcja “Uprawnienia oparte na użytkownikach OAM w systemie UNIX and Linux” na stronie 363. Systemy Windows mogą używać obu ID użytkowników zarówno do uwierzytelniania, jak i do autoryzacji i grup do autoryzacji.

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.

Ograniczone identyfikatory użytkowników

Identyfikatory użytkowników UNKNOWN i grupy NOBODY mają specjalne znaczenie dla IBM MQ. Utworzenie ID użytkownika w systemie operacyjnym o nazwie UNKNOWN lub grupie o nazwie NOBODY może mieć niezamierzone wyniki.

Identyfikatory użytkowników podczas nawiązywania połączenia z serwerem IBM MQ for Windows

Windows

Serwer IBM MQ for Windows nie obsługuje połączenia klienta Windows , jeśli klient jest uruchomiony pod ID 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.

Planowanie autoryzacji

Zaplanuj użytkowników, którzy będą mieli uprawnienia administracyjne i zaplanuj sposób autoryzowania użytkowników aplikacji do odpowiedniego używania obiektów IBM MQ , w tym tych, które łączą się z IBM MQ MQI client.

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

- Autoryzacja do wykonywania operacji administracyjnych
- Autoryzacja aplikacji do używania produktu IBM 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 MQ

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

Administratorzy produktu IBM MQ muszą mieć uprawnienia do:

- Wydaj komendy, aby administrować programem IBM MQ.
- Windows Linux Należy używać komponentu IBM MQ Explorer.
- z/OS Użyj operacji i paneli sterujących w systemie z/OS.
- z/OS Użyj programu narzędziowego IBM MQ , CSQUTIL, w systemie z/OS.
- z/OS Uzyskaj dostęp do zestawów danych menedżera kolejek w systemie z/OS.

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

Windows UNIX *Authority to administer IBM MQ on UNIX and Windows systems*

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

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

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

Dodatkowo w systemach Windows konta SYSTEM i Administrator mają pełny dostęp do zasobów IBM MQ .

Wszyscy członkowie grupy mqm mają dostęp do wszystkich zasobów systemu IBM 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 IBM MQ .

Administratorzy mogą używać komendy sterującej **runmqsc** do wydawania komend IBM 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.

IBM MQ Explorer wydaje komendy PCF służące do wykonywania zadań administracyjnych. Administratorzy nie muszą mieć dodatkowych uprawnień do używania produktu IBM MQ Explorer do administrowania menedżerem kolejek w systemie lokalnym. Gdy produkt IBM 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 MQ” na stronie 89.
- Informacje na temat komend, które działają na kanałach, inicjatorach kanałów, nasłuchiwaniach i klastrach, zawiera sekcja Zabezpieczenia kanału.
- z/OS Informacje na temat komend MQSC, które są przetwarzane przez serwer komend w systemie IBM MQ for z/OS, zawiera sekcja “Zabezpieczenia komend i zabezpieczenia zasobów komend w systemie z/OS” na stronie 88.

For more information about the authority you need to administer IBM MQ on UNIX and Windows systems, see the related information.

IBM i *Uprawnienie do administrowania produktem IBM MQ w systemie IBM i*

Aby być administratorem produktu IBM MQ w systemie IBM i, użytkownik musi być członkiem grupy *QMQMADM*. Ta grupa ma właściwości podobne do tych należących do grupy mqm w systemach UNIX i Windows . W szczególności, grupa QMQMADM jest tworzona podczas instalowania produktu IBM MQ for IBM i, a członkowie grupy QMQMADM mają dostęp do wszystkich zasobów systemu IBM MQ w systemie. Użytkownik ma również dostęp do wszystkich zasobów produktu IBM MQ , jeśli użytkownik ma uprawnienia *ALLOBJ.

Administratorzy mogą używać komend CL do administrowania produktem IBM MQ.Jedną z tych komend jest GRTMQMAUT, która jest używana do nadawania uprawnień innym użytkownikom. Inna komenda, STRMQMMQSC, umożliwia administratorowi wydawanie komend MQSC do lokalnego menedżera kolejek.

Istnieją dwie grupy komend CL udostępniane przez produkt IBM MQ for IBM i:

Grupa 1
Aby wydać komendę w tej kategorii, użytkownik musi być członkiem grupy QMQMADM lub mieć uprawnienia *ALLOBJ. GRTMQMAUT i STRMQMMQSC należą do tej kategorii, na przykład.

Grupa 2
Aby wydać komendę w tej kategorii, użytkownik nie musi należeć do grupy QMQMADM lub mieć uprawnienia *ALLOBJ. Zamiast tego wymagane są dwa poziomy uprawnień:

- Użytkownik wymaga uprawnienia IBM i do korzystania z komendy. Uprawnienie to jest nadawane za pomocą komendy GRTOBJAUT.
- Użytkownik wymaga uprawnienia IBM MQ do uzyskania dostępu do dowolnego obiektu IBM MQ powiązanego z komendą. Uprawnienie to jest nadawane za pomocą komendy GRTMQMAUT.

Poniższe przykłady przedstawiają komendy w tej grupie:

- CRTMQMQ, Tworzenie kolejki MQM
- CHGMQMPRC, Zmiana procesu MQM
- DLTMQMNL, Usunięcie listy nazw MQM
- DSPMQMAUTI, Wyświetlenie informacji uwierzytelniających MQM
- CRTMQMCHL, Tworzenie kanału MQM

Więcej informacji na temat tej grupy komend zawiera sekcja “Autoryzacja aplikacji do używania produktu IBM MQ” na stronie 89.

Pełną listę komend grupy 1 i 2 można znaleźć w sekcji “Uprawnienia dostępu do obiektów IBM MQ w systemie IBM i” na stronie 160 .

Więcej informacji na temat uprawnień wymaganych do administrowania produktem IBM MQ w systemie IBM izawiera sekcja Administrowanie produktem IBM i .

z/OS *Uprawnienie do administrowania produktem IBM MQ w systemie z/OS*

Ta kolekcja tematów opisuje różne aspekty uprawnień, które należy administrować programem IBM MQ for z/OS.

z/OS *Sprawdzanie uprawnień w systemie z/OS*

Produkt IBM MQ for z/OS korzysta z narzędzia SAF (System Authorization Facility) w celu kierowania żądań do kontroli uprawnień do zewnętrznego menedżera zabezpieczeń (ESM), takiego jak z/OS Security Server Resource Access Control Facility (RACF). Produkt IBM MQ nie sprawdza własnych uprawnień.

Zakłada się, że jako ESM używany jest produkt RACF . Jeśli używany jest inny program ESM, może być konieczne zinterpretowanie informacji udostępnionych dla produktu RACF w sposób, który jest odpowiedni dla ESM.

Można określić, czy dla każdego menedżera kolejek lub dla każdego menedżera kolejek w grupie współużytkowania kolejek ma być włączone lub wyłączone sprawdzanie uprawnień.Ten poziom sterowania jest nazywany *bezpieczeństwem podsystemu*. Jeśli wyłączono zabezpieczenia podsystemu dla konkretnego menedżera kolejek, nie są wykonywane żadne sprawdzenia uprawnień dla tego menedżera kolejek.

Jeśli zabezpieczenia podsystemu zostaną włączone dla określonego menedżera kolejek, sprawdzenia uprawnień mogą być wykonywane na dwóch poziomach:

Zabezpieczenia na poziomie grupy współużytkowania kolejki
Uprawnienia do sprawdzania uprawnień korzystają z profili produktu RACF , które są współużytkowane przez wszystkie menedżery kolejek w grupie współużytkowania kolejek. Oznacza to, że istnieje mniej profili definiujących i konserwujących, co ułatwia administrowanie bezpieczeństwem.

zabezpieczenia na poziomie menedżera kolejek
Uprawnienia do sprawdzania uprawnień korzystają z profili produktu RACF specyficznych dla menedżera kolejek.

Istnieje możliwość użycia kombinacji grupy współużytkowania kolejek i zabezpieczeń na poziomie menedżera kolejek. Można na przykład ustawić profile specyficzne dla menedżera kolejek, aby przesłonić te należące do grupy współużytkowania kolejki, do której należy.

Zabezpieczenia na poziomie podsystemu, zabezpieczenia na poziomie grupy współużytkowania kolejki oraz zabezpieczenia na poziomie menedżera kolejek są włączone lub wyłączone przez zdefiniowanie *profili przełącznika*. Profil przełącznika to normalny profil produktu RACF , który ma specjalne znaczenie dla produktu IBM MQ.

z/OS *Zabezpieczenia komend i zabezpieczenia zasobów komend w systemie z/OS*

Zabezpieczenia komend odnoszą się do uprawnień do wydania komendy; uprawnienie do zasobu komendy odnosi się do uprawnień do wykonania operacji na zasobie. Oba są implementowane y przy użyciu klas RACF .

Sprawdzanie uprawnień jest przeprowadzane, gdy administrator produktu IBM MQ wydaje komendę MQSC. Jest to nazywane *bezpieczeństwem komend*.

Aby zaimplementować zabezpieczenia komend, należy zdefiniować pewne profile produktu RACF i nadać niezbędne grupy i identyfikatory użytkowników do tych profili na wymaganych poziomach. Nazwa profilu zabezpieczeń komend zawiera nazwę komendy MQSC.

Niektóre komendy MQSC wykonują operacje na zasobie IBM MQ , takie jak komenda DEFINE QLOCAL w celu utworzenia kolejki lokalnej. Gdy administrator wysyła komendę MQSC, przeprowadzane są kontrole uprawnień w celu określenia, czy żądana operacja może zostać wykonana na zasobie określonym w komendzie. Jest to nazywane *bezpieczeństwem zasobów komend*.

Aby zaimplementować zabezpieczenia zasobów komend, należy zdefiniować pewne profile produktu RACF i nadać niezbędne grupy i identyfikatory użytkowników do tych profili na wymaganych poziomach. Nazwa profilu dla zabezpieczeń zasobów komendy zawiera nazwę zasobu IBM MQ i jego typ (QUEUE, PROCESS, NAMELIST, TOPIC, AUTHINFO lub CHANNEL).

Zabezpieczenia komend i zabezpieczenia zasobów komend są niezależne. Na przykład w przypadku wydania komendy przez administratora:

```
DEFINE QLOCAL(MOON.EUROPA)
```

wykonywane są następujące kontrole uprawnień:

- Zabezpieczenia komend sprawdzają, czy administrator ma uprawnienia do wydawania komendy DEFINE QLOCAL.
- Zabezpieczenia zasobów komend sprawdzają, czy administrator ma uprawnienia do wykonywania operacji w kolejce lokalnej o nazwie MOON.EUROPA.

Zabezpieczenia komend i zabezpieczenia zasobów komend można włączyć lub wyłączyć, definiując profile przełączników.

z/OS *Komendy MQSC i systemowa kolejka wejściowa komend w systemie z/OS*

W tym temacie opisano sposób, w jaki serwer komend przetwarza komendy MQSC kierowane do kolejki wejściowej komend systemowych w systemie z/OS.

Zabezpieczenia komend i zabezpieczenia zasobów komend są również używane, gdy serwer komend pobiera komunikat zawierający komendę MQSC z kolejki wejściowej komend systemu.Identyfikator użytkownika, który jest używany do sprawdzania uprawnień, znajduje się w polu *UserIdentifier* w deskryptorze komunikatu komunikatu zawierającego komendę MQSC. Ten identyfikator użytkownika musi mieć wymagane uprawnienia w menedżerze kolejek, w którym komenda jest przetwarzana. Więcej informacji na temat pola *UserIdentifier* i sposobu jego ustawiania zawiera sekcja Kontekst komunikatu.

Komunikaty zawierające komendy MQSC są wysyłane do kolejki wejściowej komend systemowych w następujących okolicznościach:

- Panele kontrolne i operacje wysyłają komendy MQSC do kolejki wejściowej komend systemu docelowego menedżera kolejek. Komendy MQSC odpowiadają działaniom, które użytkownik wybiera

na panelach. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator użytkownika TSO administratora.

- Funkcja COMMAND programu narzędziowego IBM MQ CSQUTIL wysyła komendy MQSC w wejściowym zestawie danych do kolejki wejściowej komend systemu docelowego menedżera kolejek. Funkcje COPY i EMPTY wysyłają komendy DISPLAY QUEUE i DISPLAY STGCLASS. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator użytkownika zadania.
- Komendy MQSC w zestawach danych CSQINPX są wysyłane do kolejki wejściowej komend systemowych menedżera kolejek, z którym połączony jest inicjator kanału. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

  Sprawdzanie uprawnień nie jest wykonywane, gdy komendy MQSC są wysyłane z zestawów danych CSQINP1 i CSQINP2 . Istnieje możliwość kontrolowania użytkowników, którzy mogą aktualizować te zestawy danych za pomocą zabezpieczenia zestawu danych RACF .
- W ramach grupy współużytkowania kolejki inicjator kanału może wysyłać komendy START CHANNEL do kolejki wejściowej komend systemu menedżera kolejek, z którym jest połączony. Komenda jest wysyłana, gdy kanał wychodzący korzystający ze współużytkowanej kolejki transmisji jest uruchamiany przez wyzwalanie. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator użytkownika przestrzeni adresowej inicjatora kanału.
- Aplikacja może wysyłać komendy MQSC do kolejki wejściowej komend systemowych. Domyślnie pole *UserIdentifier* w każdym komunikacie jest ustawiane na identyfikator użytkownika powiązany z aplikacją.
- W systemach UNIX, Linux, and Windows komenda sterująca **runmqsc** może być używana w trybie pośrednim do wysyłania komend MQSC do kolejki wejściowej komend systemowych menedżera kolejek w systemie z/OS. Pole *UserIdentifier* w każdym komunikacie jest ustawiane na identyfikator użytkownika administratora, który wydał komendę **runmqsc** .

z/OS *Dostęp do zestawów danych menedżera kolejek w systemie z/OS*

Administratorzy produktu IBM MQ for z/OS muszą mieć uprawnienia do uzyskiwania dostępu do zestawów danych menedżera kolejek. W tej sekcji opisano sposób, w jaki zestawy danych wymagają ochrony RACF .

Te zestawy danych obejmują:

- V 9.1.0 Zestawy danych, do których odwołuje się CSQINP1, CSQINP2i CSQINPT, w uruchomionej procedurze zadania menedżera kolejek.
- Zestawy stron menedżera kolejek, aktywne zestawy danych dziennika, zestawy danych dziennika archiwalnego i zestawy danych programu startowego (BSDSs)
- Zestawy danych, do których odwołuje się CSQXLIB i CSQINPX, w procedurze uruchomionej zadania inicjatora kanału

Należy chronić zestawy danych, aby żaden nieautoryzowany użytkownik nie mógł uruchomić menedżera kolejek ani uzyskać dostępu do żadnych danych menedżera kolejek. Aby to zrobić, należy użyć zabezpieczenia zestawu danych RACF .

Autoryzacja aplikacji do używania produktu IBM 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 MQ , wywołując wywołania MQI:

- Menedżery kolejek
- Kolejki
- Procesy
- Listy nazw

- Tematy

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

Aplikacje, w tym kontekście, zawierają elementy napisane przez użytkowników i dostawców, a także te, które są dostarczane z produktem IBM MQ for z/OS. Do aplikacji dostarczanych z produktem IBM MQ for z/OS należą:

- Panele kontrolne i operacje
- Program narzędziowy IBM MQ CSQUTIL
- Program narzędziowy do obsługi kolejki niedostarczanych komunikatów, CSQUDLQH

Aplikacje, które korzystają z produktów IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NETlub klientów usług komunikatów dla środowisk C/C++ i .NET , używają pośrednio interfejsu MQI.

MCA także wywołuje wywołania MQI i identyfikatory użytkowników powiązane z MCAs, które potrzebują uprawnień dostępu do tych obiektów IBM MQ . Więcej informacji na temat tych identyfikatorów użytkowników i wymaganych przez nie uprawnień zawiera sekcja “Autoryzacja kanału” na stronie 112.

W systemie z/OSaplikacje mogą również używać komend MQSC w celu uzyskania dostępu do tych obiektów produktu IBM MQ , ale zabezpieczenia komend i zabezpieczenia zasobów komend zapewniają uprawnienia do sprawdzania uprawnień w tych okolicznościach. z/OS Więcej informacji na ten temat zawiera sekcja “Zabezpieczenia komend i zabezpieczenia zasobów komend w systemie z/OS” na stronie 88 i “Komendy MQSC i systemowa kolejka wejściowa komend w systemie z/OS” na stronie 88.

W systemie IBM iużytkownik, który wydaje komendę CL z grupy 2, może wymagać uprawnień do uzyskania dostępu do obiektu IBM MQ powiązanego z komendą. Więcej informacji na ten temat zawiera sekcja “Gdy przeprowadzane są kontrole uprawnień” na stronie 90.

Gdy przeprowadzane są kontrole uprawnień

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

W systemie IBM isprawdzenia uprawnień mogą być również wykonywane, gdy użytkownik wysyła komendę CL do grupy 2, która uzyskuje dostęp do dowolnego z tych obiektów IBM MQ . 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 MQ. Program IBM MQ zakłada, że użytkownicy są wpisani do bazowego systemu operacyjnego i są przez niego uwierzytelniani.

Gdy aplikacja otwiera obiekt IBM 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 z/OSjest wykonywane sprawdzenie profilu kolejki produktu RACF , który jest zgodny z nazwą zdalnego menedżera kolejek. W systemie Wiele platformjest 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 IBM 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 92.

IBM i W systemie IBM i, gdy użytkownik wydaje komendę CL w grupie 2, która działa na obiekcie IBM MQ

Ta reguła obejmuje przypadek, w którym komenda CL w grupie 2 działa na obiekcie informacji uwierzytelniającej.

W celu określenia, czy użytkownik ma uprawnienia do wykonywania operacji na obiekcie IBM MQ powiązanym z komendą, wykonywane są kontrole. Sprawdzenia są wykonywane, chyba że użytkownik jest członkiem grupy QMQMADM lub ma uprawnienia *ALLOBJ . Wymagane uprawnienia zależą od typu operacji, jaką wykonuje komenda na obiekcie. Na przykład komenda **CHGMQMQ**, Zmiana kolejki MQM, wymaga uprawnień do zmiany atrybutów kolejki określonej przez komendę. Natomiast komenda **DSPMQMQ**, Wyświetlenie kolejki MQM, wymaga uprawnienia do wyświetlania atrybutów kolejki określonej przez komendę.

Wiele komend działa na więcej niż jednym obiekcie. Na przykład, aby wydać komendę **DLTMQMQ**, należy usunąć kolejkę MQM, wymagane są następujące uprawnienia:

- Uprawnienie do nawiązywania połączenia z menedżerem kolejek określonym przez komendę
- Uprawnienie do usuwania kolejki określonej przez komendę

Niektóre komendy nie działają na żadnym obiekcie. W takim przypadku użytkownik wymaga tylko uprawnienia IBM i do wydawania jednej z tych komend. **STRMQMLSR**, Przykładem takiej komendy jest uruchamianie programu nasłuchującego MQM.

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 umiesła komunikat; na przykład transakcję 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.

ULW IBM i *Uprawnienia do pracy z obiektami IBM MQ w systemach IBM i , UNIX, Linux, and Windows*

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

AUTHENTICATION.

Sprawdzanie uwierzytelniania wykonywane przez usługę OAM udostępniane z produktem IBM 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 i spełnione są następujące warunki:

- Jeśli struktura MQCSP została dostarczona przez aplikację łączącą, oraz
- Atrybut *AuthenticationType* w strukturze MQCSP ma wartość MQCSP_AUTH_USER_ID_AND_PWD, oraz
- Wartość CHCKLOCL lub CHKCCLNT w skonfigurowanym obiekcie AUTHINFO nie jest równa 'NONE'

Kroki uwierzytelniania w systemie OAM sprawdzają poprawność hasła za pomocą usług systemu operacyjnego, które mogły zostać skonfigurowane w celu przeprowadzenia dodatkowych operacji sprawdzania, takich jak sprawdzenie, czy nazwa użytkownika nie zawiera zbyt wielu niepoprawnych prób wprowadzenia hasła.

Istnieje możliwość użycia alternatywnych mechanizmów uwierzytelniania w przypadku pisania nowego komponentu usługi autoryzacji lub uzyskania od dostawcy jednego z nich.

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 IBM i IBM i , UNIX, Linux, and Windows , *usługa autoryzacji* udostępnia kontrolę dostępu, gdy aplikacja wysyła wywołanie MQI w celu uzyskania dostępu do obiektu IBM 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.

Windows W systemie Windows OAM daje członkom grupy Administratorzy uprawnienia do uzyskiwania dostępu do wszystkich obiektów IBM MQ , nawet jeśli włączona jest opcja UAC. Dodatkowo w systemach Windows konto SYSTEM ma pełny dostęp do zasobów IBM MQ .

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

IBM i W systemie IBM i , o ile użytkownik nie jest członkiem grupy QMQMADM lub ma uprawnienie *ALLOBJ, usługa autoryzacji zapewnia również sprawdzanie uprawnień, gdy użytkownik wysyła komendę CL do grupy 2, która działa na dowolnym z tych obiektów IBM MQ lub obiekcie informacji uwierzytelniających.

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 MQ .

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

OAM przechowuje listę kontroli dostępu (ACL) dla każdego obiektu IBM 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 IBM i IBM i i 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. Produkty AIX i Linux podniosły ten limit, ale produkt IBM MQ nadal obserwuje 12 znaków ograniczenia na wszystkich platformach UNIX . Jeśli używany jest identyfikator użytkownika o długości większej niż 12 znaków, program IBM 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 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.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP dla aplikacji klienckiej zostanie wysłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienta są odpowiednio chronione, należy zapoznać się z IBM MQochroną hasła CSP.

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.

IBM i W systemie IBM iadministrator używa komendy CL GRTMQMAUT do nadawania uprawnień i komendy CL RVKMQMAUT do odbierania uprawnień. Można również używać profili ogólnych.Na przykład komenda CL:

```
GRTMQMAUT MQMNAME(JUPITER) OBJTYPE(*Q) OBJ('MOON.*') USER(VOYAGER) AUT(*PUT)
```

Udostępnia tę samą funkcję co poprzedni przykład komendy **setmqaut** . Umożliwia ona członkom grupy VOYAGER umieszczanie komunikatów w dowolnej kolejce o nazwie, która rozpoczyna się od znaków `MOON.` .

IBM i Komenda CL DSPMQMAUT wyświetla bieżące uprawnienia, które użytkownik lub grupa ma dla określonego obiektu. Komendy CL WRKMQMAUT i WRKMQMAUTD są również dostępne do pracy z bieżącymi uprawnieniami powiązanymi z obiektami i profilami ogólnymi.

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

Multi *Korzystanie z PCF w celu uzyskania dostępu do komend OAM*
W systemach IBM i, UNIX, Linux, and Windows można używać komend PCF w celu uzyskania dostępu do komend administracyjnych OAM.

Komendy PCF i ich równoważne komendy OAM są następujące:

Tabela 8. 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.

z/OS *Uprawnienia do pracy z obiektami IBM MQ w systemie z/OS*

W systemie z/OSistnieje siedem kategorii kontroli uprawnień powiązanych z wywołaniami do interfejsu MQI. Należy zdefiniować niektóre profile produktu RACF i nadać odpowiednie uprawnienia dostępu do tych profili. Za pomocą profilu *RESLEVEL* można określić liczbę użytkowników, którzy mają być sprawdzani.

Siedem kategorii sprawdzania uprawnień powiązanych z wywołaniami interfejsu MQI:

Bezpieczeństwo połączenia
Sprawdzanie uprawnień, które są wykonywane, gdy aplikacja łączy się z menedżerem kolejek

Bezpieczeństwo kolejki
Sprawdzanie uprawnień, które są wykonywane, gdy aplikacja otwiera kolejkę lub usuwa stałą kolejkę dynamiczną.

Zabezpieczenia procesu
Uprawnienia sprawdzające, które są wykonywane, gdy aplikacja otwiera obiekt procesu

Zabezpieczenia listy nazw
Uprawnienia sprawdzające, które są wykonywane, gdy aplikacja otwiera obiekt listy nazw

alternatywne zabezpieczenie użytkownika
Uprawnienia sprawdzające, które są wykonywane, gdy aplikacja żąda alternatywnego uprawnienia użytkownika podczas otwierania obiektu

zabezpieczenie kontekstu
Uprawnienia sprawdzające, które są wykonywane, gdy aplikacja otwiera kolejkę i określa, że ma zamiar ustawić lub przekazać informacje kontekstu w komunikatach umieszczanych w kolejce.

Zabezpieczenia tematów
Uprawnienia sprawdzające, które są wykonywane po otwarciu tematu przez aplikację

Każda kategoria kontroli uprawnień jest implementowana w taki sam sposób, w jaki implementowane są zabezpieczenia komend i zabezpieczenia zasobów komend. Należy zdefiniować niektóre profile produktu RACF i nadać wymagane grupy i identyfikatory użytkowników dostęp do tych profili na wymaganych poziomach. W przypadku zabezpieczeń kolejki poziom dostępu określa typy operacji, które aplikacja może wykonywać w kolejce. W przypadku zabezpieczeń kontekstowych poziom dostępu określa, czy aplikacja może:

- Przekaz wszystkie pola kontekstu
- Przekaz wszystkie pola kontekstu i ustaw pola kontekstu tożsamości
- Przekaz i ustaw wszystkie pola kontekstu

Poszczególne kategorie sprawdzania uprawnień można włączyć lub wyłączyć, definiując profile przełączników.

Wszystkie kategorie, z wyjątkiem zabezpieczeń połączenia, nazywane są łącznie *zabezpieczeniem zasobów API*.

Domyślnie, gdy funkcja API-resource security check jest wykonywana w wyniku wywołania MQI z aplikacji przy użyciu połączenia wsadowego, sprawdzane jest tylko jeden identyfikator użytkownika. Gdy sprawdzenie jest wykonywane w wyniku wywołania MQI z aplikacji CICS lub IMS lub z inicjatora kanału, sprawdzane są dwa identyfikatory użytkowników.

Definiując *profil RESLEVEL*, można jednak określić, czy sprawdzane są wartości zerowe, jedno lub dwa identyfikatory użytkowników. Liczba sprawdzanych identyfikatorów użytkowników jest określana na podstawie identyfikatora użytkownika powiązanego z typem połączenia, gdy aplikacja łączy się z menedżerem kolejek, a poziom dostępu, który ma identyfikator użytkownika, ma profil RESLEVEL. Identyfikator użytkownika powiązany z każdym typem połączenia jest następujący:

- Identyfikator użytkownika zadania łączącego dla połączeń wsadowych.
- Identyfikator użytkownika przestrzeni adresowej CICS dla połączeń CICS
- Identyfikator użytkownika przestrzeni adresowej regionu produktu IMS dla połączeń produktu IMS
- Identyfikator użytkownika przestrzeni adresowej inicjatora kanału dla połączeń inicjatora kanału

Więcej informacji na temat uprawnień do pracy z obiektami IBM MQ w systemie z/OSzawiera sekcja “Uprawnienie do administrowania produktem IBM MQ w systemie z/OS” na stronie 87.

Zabezpieczenia dla zdalnego przesyłania komunikatów

W tej sekcji opisano aspekty bezpieczeństwa dotyczące zdalnego przesyłania komunikatów.

Użytkownik musi udostępnić użytkownikom uprawnienia do korzystania z narzędzi IBM 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 podmiotu 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.

IBM i *Zabezpieczenia obiektów produktu IBM MQ for IBM i*

W tej sekcji opisano aspekty bezpieczeństwa dotyczące zdalnego przesyłania komunikatów.

Użytkownik musi udostępnić użytkownikom uprawnienia do korzystania z narzędzi IBM MQ for IBM i . Ten ośrodek jest organizowany zgodnie z działaniami, które mają być podjęte 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 mają uprawnienia do korzystania z kolejek.
- Kanały komunikatów muszą być tworzone i kontrolowane przez autoryzowanych użytkowników.

Agent kanału komunikatów w ośrodku zdalnym musi sprawdzić, czy dostarczona wiadomość pochodzi od użytkownika z uprawnieniami do wypaczania wiadomości 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:

- Dekret w definicji kanału, w którym komunikaty muszą zawierać dopuszczalne uprawnienia *kontekstu* , w przeciwnym razie są usuwane.
- Zaimplementuj rekordy uwierzytelniania kanału w celu odrzucenia niepożądanych prób połączenia lub aby ustawić wartość MCAUSER na podstawie jednej z następujących wartości: zdalny adres IP, ID użytkownika zdalnego, podana nazwa wyróżniająca TLS lub nazwa zdalnego menedżera kolejek.
- Zaimplementuj sprawdzanie zabezpieczeń wyjścia 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.
- Zaimplementuj przetwarzanie komunikatów wyjścia użytkownika, aby upewnić się, że pojedyncze komunikaty są sprawdzane w celu autoryzacji.

Poniżej przedstawiono kilka faktów na temat sposobu działania zabezpieczeń przez produkt IBM MQ for IBM i :

- Użytkownicy są identyfikowani i uwierzytelniani przez produkt IBM i.
- Usługi menedżera kolejek wywoływane przez aplikacje są uruchamiane z uprawnieniami profilu użytkownika menedżera kolejek, ale w procesie użytkownika.
- Usługi menedżera kolejek wywoływane przez komendy użytkownika są uruchamiane z uprawnieniami profilu użytkownika menedżera kolejek.

Linux UNIX *Zabezpieczenia obiektów w systemie 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 MQ .

Zawsze należy uruchamiać amqcrsta jako identyfikator użytkownika "mqm".

Identyfikatory użytkowników w systemie 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.

Windows *Zabezpieczenia obiektów w systemach Windows*

Jeśli ten identyfikator będzie używać komend administracyjnych produktu IBM MQ , użytkownicy administracyjni muszą należeć zarówno do grupy mqm, jak 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, systemy UNIX and Linux używają wielkich liter dla identyfikatorów użytkowników w komunikatach. Aby umożliwić Windows, w systemach UNIX and Linux używanie małych identyfikatorów użytkowników w komunikatach, agent kanału komunikatów (MCA) musi wykonywać odpowiednie konwersje znaków alfabetycznych.

Aby umożliwić Windows, w systemach UNIX and Linux korzystanie z 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 produkcie UNIX, Linux, and Windows z innych przyczyn.

Korzystanie z niestandardowej usługi autoryzacji

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

Komponent usługi autoryzacji dostarczany z produktem IBM 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 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 9. 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 101 .
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	Używana, gdy żaden inny identyfikator użytkownika 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 101 .

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 produktu IBM MQ MQI clientsproces, który wydaje wywołania MQI, jest agentem MCA połączonym 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.

Klient IBM 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:

- z/OS 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 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 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.

ULW W przypadku serwerów w systemie UNIX, Linux, and Windowstreść pola `MCAUserIdentifier` otrzymanego od klienta jest zmieniana na małe litery.

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

Linux UNIX 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 IBM MQ JMS , jest identyfikatorem użytkownika maszyny JVM, 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 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 102
Ten temat zawiera informacje na temat różnych aspektów zabezpieczeń na poziomie łącza oraz zabezpieczeń na poziomie aplikacji, a także porównuje dwa poziomy zabezpieczeń.

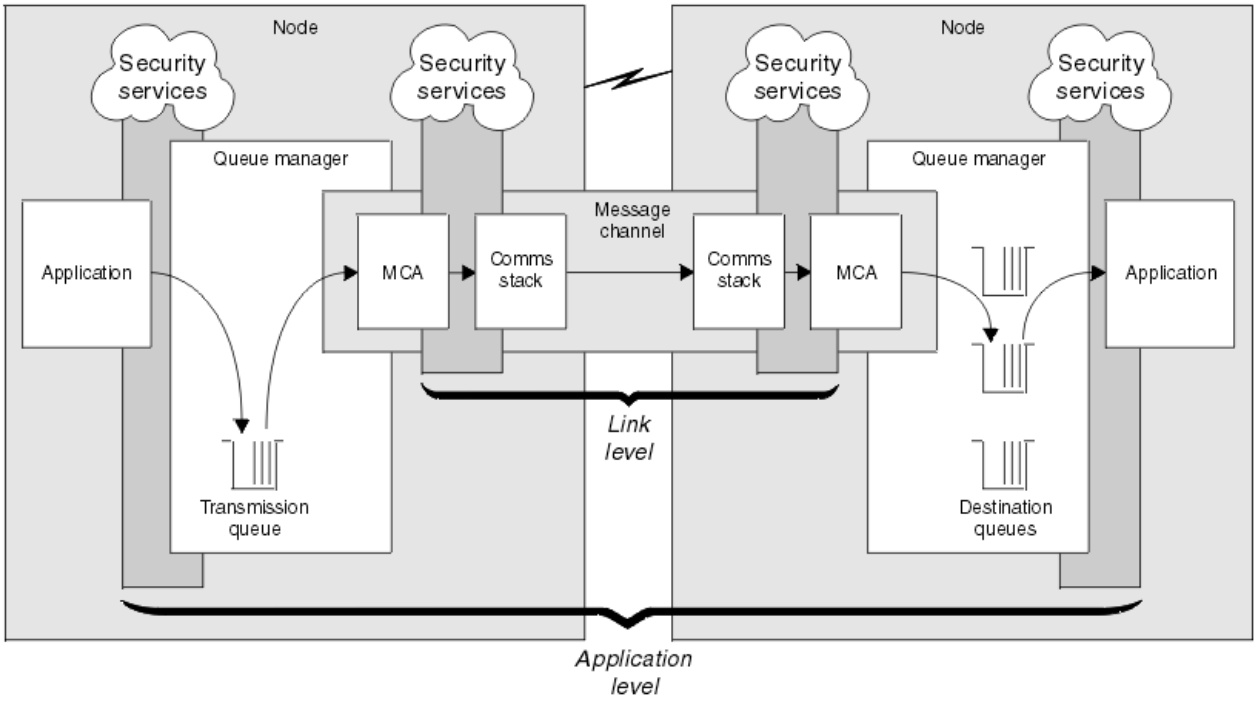
“Programy obsługi wyjścia kanału” na stronie 108
Programy obsługi wyjścia kanału to programy, które są wywoływane w zdefiniowanych miejscach w sekwencji przetwarzania MCA. Użytkownicy i dostawcy mogą zapisywać własne programy obsługi wyjścia kanału. Niektóre z nich są dostarczane przez produkt IBM.

“Ochrona kanałów za pomocą protokołu SSL/TLS” na stronie 114
Obsługa protokołu TLS w produkcie IBM 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 10 na stronie 103.



Rysunek 10. 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.

z/OS V 9.1.4 Szyfrowanie zestawu danych z/OS może zapewnić pewną ochronę komunikatów przechowywanych w kolejkach, ale tylko w przypadku danych pozostających w stanie spoczynku w lokalnym menedżerze kolejek. Patrz sekcja poufność danych w produkcie IBM MQ for z/OS przy użyciu szyfrowania zestawu danych. :NONE.

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 i jest ilustrowana w produkcie Rysunek 10 na stronie 103.

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 IBM MQ mogą być 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 IBM 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 produkcie Rysunek 10 na stronie 103.

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 MQ

Podstawowym sposobem zapewnienia poufności i integralności danych w produkcie IBM MQ jest użycie protokołu TLS. Więcej informacji na temat korzystania z protokołu TLS w produkcie IBM MQzawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24. W przypadku uwierzytelniania produkt IBM 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 50.

Zapewnianie bezpieczeństwa na poziomie łącza

Istnieje możliwość udostępnienia własnych usług 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 108. W tym samym temacie opisano także program obsługi wyjścia kanału dostarczany z programem IBM MQ for 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 IBM MQlub kombinację dowolnego z tych współpracujących ze sobą. Zabezpieczenia na poziomie aplikacji są ilustrowane w produkcie Rysunek 10 na stronie 103.

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 Advanced Message Security (AMS) jest komponentem produktu IBM MQ , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM MQ , a jednocześnie nie wpływa 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 MQ. Takie rozwiązania wymagają jednak specjalistycznych umiejętności i mogą być skomplikowane i kosztowne w utrzymaniu. Advanced Message Security pomaga w sprostaniu tym wyzwaniom podczas przenoszenia informacji wokół przedsiębiorstwa pomiędzy praktycznie każdym rodzajem komercyjnego systemu informatycznego.

Produkt Advanced Message Security rozszerza funkcje zabezpieczeń produktu IBM 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 MQ , jak i klienty.
- Integruje się z produktem Managed File Transfer w celu udostępnienia kompleksowego bezpiecznego rozwiązania do przesyłania komunikatów.

Więcej informacji na ten temat zawiera sekcja “Advanced Message Security” na stronie 580.

Zapewnianie bezpieczeństwa na poziomie aplikacji
Istnieje możliwość udostępnienia własnych usług zabezpieczeń na poziomie aplikacji. W celu ułatwienia zaimplementowania zabezpieczeń na poziomie aplikacji produkt IBM MQ udostępnia dwa wyjścia, wyjście funkcji API oraz wyjście funkcji API.

Wyjście funkcji API i wyjście funkcji API-przejście może zapewnić identyfikowanie 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 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 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.

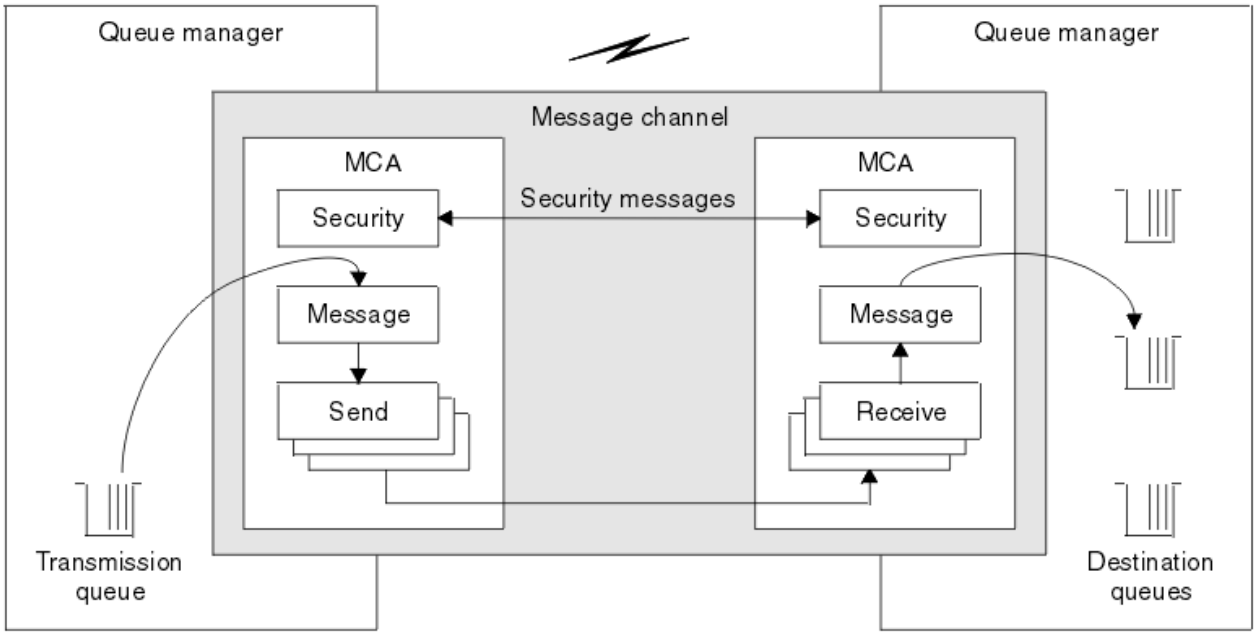
Programy obsługi wyjścia kanału

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 produkt 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 11 na stronie 108 i są opisane w poniższych tematach.



Rysunek 11. 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.

Więcej informacji na temat wyjść zabezpieczeń zawiera sekcja "Zabezpieczenia na poziomie łącza przy użyciu wyjścia zabezpieczeń" na stronie 105.

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 IBM MQ MQI client 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 105.

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 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 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.

Więcej informacji na temat wyjścia wysyłania i odbierania zawiera sekcja “Zabezpieczenia na poziomie łącza za pomocą wyjść wysyłania i odbierania” na stronie 106.

Planowanie integralności danych

Zaplanuj sposób zachowania integralności danych.

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

Na poziomie aplikacji można korzystać z programów obsługi wyjścia funkcji API, jeśli standardowe urządzenia nie spełniają wymagań. Do cyfrowego podpisywania komunikatów można użyć programu Advanced Message Security (AMS) w celu ochrony przed nieautoryzowanymi modyfikacjami.

Na poziomie łącza można wybrać użycie protokołu 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/TLS” na stronie 114
Obsługa protokołu TLS w produkcie IBM MQ korzysta z obiektu informacji uwierzytelniających menedżera kolejek i różnych komend MQSC. Należy również rozważyć użycie certyfikatów cyfrowych.

“Integralność danych w produkcie IBM MQ” na stronie 23
Istnieje możliwość użycia usługi integralności danych w celu wykrycia, czy komunikat został zmodyfikowany.

“Planowanie dla produktu Advanced Message Security” na stronie 107
Produkt Advanced Message Security (AMS) jest komponentem produktu IBM MQ , który zapewnia wysoki poziom ochrony poufnych danych przepływających przez sieć produktu IBM MQ , a jednocześnie nie wpływa na aplikacje końcowe.

Wywołania wyjścia kanału i struktury danych

Odsyłacze pokrewne

Odwołanie do wyjścia funkcji API

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 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 MQ przy użyciu interfejsów produktu IBM MQ
Skonfiguruj produkt IBM MQ w taki sposób, aby wystawiał zdarzenia instrumentacji, a w szczególności zdarzenia komend i zdarzenia konfiguracji.

Zmiany wprowadzone w produkcie IBM MQ poza jego kontrolą
Niektóre zmiany mogą mieć wpływ na zachowanie produktu IBM MQ , ale nie mogą być bezpośrednio monitorowane przez produkt IBM 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 MQ
Do kontrolowania działań, takich jak uruchamianie i zatrzymywanie menedżerów kolejek, może być konieczne użycie narzędzi systemu operacyjnego. W niektórych przypadkach produkt IBM MQ może być skonfigurowany do wydawania zdarzeń instrumentacji.

Działanie aplikacji w produkcie IBM MQ
W celu kontrolowania działań aplikacji, na przykład otwierania kolejek, umieszczania i pobierania komunikatów, należy skonfigurować produkt IBM 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 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 produktem IBM 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 należy zapewnić dostęp do różnych zasobów produktu IBM MQ . Agenty kanału komunikatów (Message Channel Agents-MCAs) to zasadniczo aplikacje produktu IBM MQ , które przenoszą komunikaty między menedżerami kolejek i jako takie wymagają dostępu do różnych zasobów produktu IBM MQ w celu poprawnego działania.

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 programie IBM MQkanały mogą być chronione przez obsługę protokołu 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 .
- Przy użyciu identyfikatora użytkownika powiązanego z kanałem odbierającym można otworzyć kolejki docelowe w celu umieszczenia komunikatów w kolejkach. Obejmuje to interfejs MQI (Message queuing Interface), więc może być konieczne dodatkowe sprawdzenie kontroli dostępu, jeśli nie jest używany menedżer uprawnień do obiektu (OAM) produktu IBM MQ . 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 ma pełne prawa administracyjne i nie wymaga 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.
- Nie jest konieczne nadawanie uprawnień *dsp* i *ctrlx* dla ID użytkownika MCAUSER kanału odbiorczego.
- Przed IBM MQ 8.0.0 Fix Pack 4, jeśli używany jest identyfikator użytkownika, który nie ma uprawnień administracyjnych IBM MQ , należy nadać uprawnienia **dsp** i **ctrlx** dla kanału do tego identyfikatora użytkownika, aby kanał działał.

  W produkcie IBM MQ 8.0.0 Fix Pack 4nie ma uprawnień do sprawdzania, kiedy kanał resynchronizuje się i koryguje numery kolejne.

  Jednak ręczne wydanie komendy RESET CHANNEL nadal wymaga **+dsp** i **+ctrlx** we wszystkich wersjach.

  Ostrzeżenie: Gdy resetowanie kanału jest wymagane dla potwierdzenia zadania wsadowego komunikatu, program IBM MQ próbuje wysłać zapytanie do kanału, które wymaga uprawnienia **+dsp** .
- 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. Poniższe komendy są przykładami typu komendy, które można wydać, aby nadać uprawnienia do identyfikatora użytkownika z systemu zdalnego:

```
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 50
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 MQ nie są obiektami IBM MQ , dostęp do nich nie jest kontrolowany przez OAM. Produkt IBM 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.

Identyfikator użytkownika musi również należeć do grupy mqm na komputerze docelowym, aby wydać równoważne komendy MQSC za pomocą komendy Escape PCF lub za pomocą komendy `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 Tabela 12 na stronie 133.

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 108 .

Ochrona kanałów za pomocą protokołu SSL/TLS

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

Certyfikaty cyfrowe i repozytoria kluczy

Zaleca się ustawienie atrybutu etykiety certyfikatu menedżera kolejek (**CERTLABL**) do nazwy certyfikatu osobistego, który ma być używany dla większości kanałów, i przesłonić go pod kątem wyjątków, ustawiając etykietę certyfikatu na tych kanałach, które wymagają różnych certyfikatów.

Jeśli potrzebne jest wiele kanałów z certyfikatami, które różnią się od domyślnego zestawu certyfikatów w menedżerze kolejek, należy rozważyć podzielenie kanałów między kilkoma menedżerami kolejek lub użyć proxy MQIPT przed menedżerem kolejek w celu przedstawienia innego certyfikatu.

Dla każdego kanału można użyć innego certyfikatu, ale jeśli w repozytorium kluczy jest zbyt wiele certyfikatów, może to mieć wpływ na wydajność podczas uruchamiania kanałów TLS. Spróbuj zachować liczbę certyfikatów w repozytorium kluczy na mniej niż 50 i rozważyć, aby wartość 100 była wartością maksymalną, ponieważ wydajność pakietu GSKit gwałtownie zmniejsza się z większymi repozytoriami kluczy.

Zezwolenie na wiele certyfikatów w tym samym menedżerze kolejek zwiększa prawdopodobieństwo, że w tym samym menedżerze kolejek zostanie użyte wiele certyfikatów ośrodka CA. Zwiększa to prawdopodobieństwo startów przestrzeni nazw nazwy wyróżniającej certyfikatu dla certyfikatów wydawanych przez oddzielne uprawnienia do certyfikatów.

Podczas gdy profesjonalne ośrodki certyfikacji mogą być bardziej ostrożne, w domu certyfikacji często brakuje jasnych konwencji nazewnictwa i można skończyć z niezamierzonych meczów między jednym ca CA i inny.

Oprócz nazwy wyróżniającej podmiotu należy zapoznać się z nazwą wyróżniającą wystawcy certyfikatu. W tym celu należy użyć rekordu SSLPEERMAP uwierzytelniania kanału i ustawić zarówno pola **SSLPEER** , jak i **SSLCERTI** odpowiednio do nazwy wyróżniającej podmiotu i nazwy wyróżniającej wystawcy.

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:

ULW W systemach Windows, UNIXi Linux można używać certyfikatów samopodpisanych. Instrukcje na ten temat zawiera sekcja “Tworzenie samopodpisanego certyfikatu osobistego w systemie UNIX, Linux, and Windows” na stronie 302.

IBM i W systemach IBM i można używać certyfikatów podpisanych przez lokalny ośrodek CA. Instrukcje na ten temat zawiera sekcja “Żądanie certyfikatu serwera w systemie IBM i” na stronie 286 .

z/OS W systemie z/OSmożna korzystać z samopodpisanych lub lokalnych certyfikatów podpisanych przez ośrodek CA. Instrukcje znajdują się w sekcji “Tworzenie samopodpisanego certyfikatu osobistego w systemie z/OS” na stronie 331 lub “Żądanie certyfikatu osobistego w systemie z/OS” na stronie 331 .

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 certyfikatów cyfrowych. Podobnie, jeśli strategia bezpieczeństwa organizacji wymaga użycia określonej specyfikacji CipherSpec , konieczne jest uzyskanie odpowiednich certyfikatów cyfrowych.

Więcej informacji na temat relacji między obiektami CipherSpecs i certyfikatami cyfrowymi można znaleźć w sekcji “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45 .

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 IBM MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w produkcie IBM MQ” na stronie 44.

Planowanie sprawdzania odwołań certyfikatów

Zezwolenie na wiele certyfikatów z różnych ośrodków certyfikacji może potencjalnie powodować niepotrzebne dodatkowe sprawdzanie odwołań certyfikatów.

W szczególności, jeśli jawnie skonfigurowano użycie serwera odwołań z określonego ośrodka CA, na przykład przy użyciu obiektu AUTHINFO lub struktury rekordu informacji uwierzytelniającej (MQAIR), sprawdzenie wycofania nie powiedzie się, jeśli zostanie przedstawiony certyfikat z innego ośrodka CA.

Należy unikać jawnej konfiguracji serwera odwołań certyfikatów. Zamiast tego należy włączyć sprawdzanie niejawne, w którym każdy certyfikat zawiera swoje własne położenie serwera odwołań w rozszerzeniu certyfikatu, na przykład Punkt dystrybucji CRL lub Dostęp OCSP AuthorityInfo.

Więcej informacji na ten temat zawierają opcje OCSPCheckExtensions i CDPCheckExtensions.

Komendy i atrybuty dla obsługi TLS

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

- Następujące komendy MQSC obsługują protokół TLS:

  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 TLS:

CERTLABL
Definiuje etykietę certyfikatu osobistego, która ma być używana.

SSLCRLNL
Atrybut SSLCRLNL określa listę nazw obiektów informacji uwierzytelniających, które są używane do udostępniania położeń odwołań certyfikatów w celu umożliwienia sprawdzania rozszerzonego certyfikatu TLS.

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

SSLEV
Określa, czy komunikat o zdarzeniu TLS jest zgłaszany, jeśli kanał korzystający z protokołu TLS nie nawiąże połączenia TLS.

SSLFIPS
Określa, czy tylko algorytmy certyfikowane przez FIPS mają być używane, jeśli kryptografia jest przeprowadzana w produkcie IBM 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 UNIX, Linux, and Windows 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 TLS w systemach Windows i UNIX and Linux .

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

- Następujące parametry kanału obsługują protokół TLS:

CERTLABL
Definiuje etykietę certyfikatu osobistego, która ma być używana.

SSLCAUTH
Określa, czy produkt IBM MQ wymaga i sprawdza poprawność certyfikatu od klienta TLS.

SSLCIPH
Określa siłę szyfrowania i funkcję (CipherSpec), na przykład TLS_RSA_WITH_AES_128_CBC_SHA. Specyfikacja CipherSpec musi być zgodna z obu końcami kanału.

SSLPEER
Określa nazwę wyróżniającą (unikalny identyfikator) dozwolonych partnerów.

W tej sekcji opisano komendy **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**i **dspmqfls** w celu obsługi obiektu informacji uwierzytelniających. Opisano również komendę **runmqckm** (iKeycmd) w celu zarządzania certyfikatami w systemach UNIX and Linux oraz narzędzia **runmqakm** do zarządzania certyfikatami w systemie UNIX, Linux, and Windows. Patrz następujące sekcje:

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

Przegląd zabezpieczeń kanałów za pomocą protokołu TLS, patrz

- “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24

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

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

z/OS *IBM MQ for z/OS Kanał połączenia z serwerem*

Kanał SVRCONN programu IBM MQ for z/OS nie jest bezpieczny bez implementowania uwierzytelniania kanału lub dodawania wyjścia zabezpieczeń przy użyciu protokołu TLS. Kanały SVRCONN nie mają zdefiniowanego domyślnego wyjścia zabezpieczeń.

Kwestie dotyczące bezpieczeństwa

Kanały SVRCONN nie są bezpieczne, jak początkowo zdefiniowane, SYSTEM.DEF.SVRCONN , np. Aby zabezpieczyć kanał SVRCONN, należy skonfigurować uwierzytelnianie kanału za pomocą komendy SET CHLAUTH lub zainstalować wyjście zabezpieczeń i zaimplementować protokół TLS.

Należy użyć publicznie dostępnego przykładowego wyjścia zabezpieczeń, samodzielnie napisz wyjście zabezpieczeń lub zakupić wyjście zabezpieczeń.

Dostępnych jest kilka przykładów, które można wykorzystać jako dobry punkt wyjścia do pisania własnego wyjścia bezpieczeństwa kanału SVRCONN.

W programie IBM MQ for z/OSelement CSQ4BCX3 w bibliotece hlq.SCSQC37S jest próbką wyjścia zabezpieczeń napisanej w języku C. Przykładowy plik CSQ4BCX3 jest również dostarczany wstępnie skompilowany w bibliotece hlq.SCSQAUTH .

Przykładowy program zewnętrzny CSQ4BCX3 można zaimplementować, kopiując skompilowany element hlq.SCSQAUTH(CSQ4BCX3) do biblioteki ładowania, która jest przydzielona do DD CSQXLIB w tabeli CHIN proc. Należy pamiętać, że CHIN wymaga, aby biblioteka ładująca została ustawiona jako "Program Controlled".

Zmień kanał SVRCONN, aby ustawić CSQ4BCX3 jako wyjście zabezpieczeń.

V 9.1.4 Gdy klient łączy się za pomocą tego kanału SVRCONN, CSQ4BCX3 uwierzytelni się za pomocą pary **RemoteUserIdentifier** i **RemotePassword** z tabeli MQCD lub z IBM MQ 9.1.4, pary **CSPUserIdPtr** i **CSPPasswordPtr** z protokołu MQCSP. Jeśli uwierzytelnianie powiedzie się, skopiuje on **RemoteUserIdentifier** do programu **MCAUserIdentifier**, zmieniając kontekst tożsamości wątku.

W przypadku systemów Long Term Support i Continuous Delivery przed IBM MQ 9.1.4, gdy klient łączy się za pomocą tego kanału SVRCONN, CSQ4BCX3 uwierzytelni się za pomocą pary **RemoteUserIdentifier** i **RemotePassword** z MQCD. Jeśli uwierzytelnianie powiedzie się, skopiuje on **RemoteUserIdentifier** do programu **MCAUserIdentifier**, zmieniając kontekst tożsamości wątku.

W przypadku pisania klienta IBM MQ Java można użyć elementów wywoływanych, aby wysłać zapytanie do użytkownika, a następnie ustawić wartości MQEnvironment.userID i MQEnvironment.password. Te wartości zostaną przekazane po nawiązaniu połączenia.

Po zakończeniu działania wyjścia zabezpieczeń istnieje dodatkowa obawa, że identyfikator użytkownika i hasło są przesyłane w postaci jawnego tekstu przez sieć po nawiązaniu połączenia, podobnie jak treść wszystkich kolejnych komunikatów produktu IBM MQ . Za pomocą protokołu TLS można zaszyfrować początkowe informacje o połączeniu, a także treść wszystkich komunikatów produktu IBM MQ .

Przykład

Aby zabezpieczyć system IBM MQ Explorer SVRCONN SYSTEM.ADMIN.SVRCONN wykonaj następujące kroki:

1. Skopiuj plik hlq.SCSQAUTH(CSQ4BCX3) do biblioteki ładowania, która jest przydzielona do DD CSQXLIB w aplikacji CHINIT Proc.
2. Sprawdź, czy biblioteka ładowania jest kontrolowana przez program.
3. Zmień SYSTEM ADMIN.SVRCONN , aby użyć wyjścia zabezpieczeń CSQ4BCX3.
4. W programie IBM MQ Explorerkliknij prawym przyciskiem myszy nazwę menedżera kolejek produktu z/OS , wybierz opcję **Szczegóły połączenia** > **Właściwości** > **ID użytkownika** i wprowadź identyfikator użytkownika produktu z/OS .
5. Połącz się z menedżerem kolejek produktu z/OS , wprowadzając hasło.

Dodatkowe informacje

Aby program CSQ4BCX3 został uruchomiony w środowisku kontrolowanym przez program, wszystkie załadowane do przestrzeni adresowej CHIN muszą być załadowane z biblioteki kontrolowanej przez program, na przykład wszystkie biblioteki w bibliotece STEPLIB i wszystkie biblioteki nazwane w definicji CSQXLIB DD. To set a load library as Program Controlled issue RACF commands. W poniższym przykładzie nazwa biblioteki ładowania jest następująca: MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

Aby zmienić kanał SVRCONN w celu zaimplementowania CSQ4BCX3, należy wprowadzić następującą komendę IBM MQ :

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

W powyższym przykładzie używana nazwa kanału SVRCONN to SYSTEM ADMIN.SVRCONN.

Więcej informacji na temat wyjść kanału znajduje się w sekcji “Programy obsługi wyjścia kanału” na stronie 108 .

Zadania pokrewne

Pisanie programów obsługi wyjścia kanału w systemie z/OS

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 IBM 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.

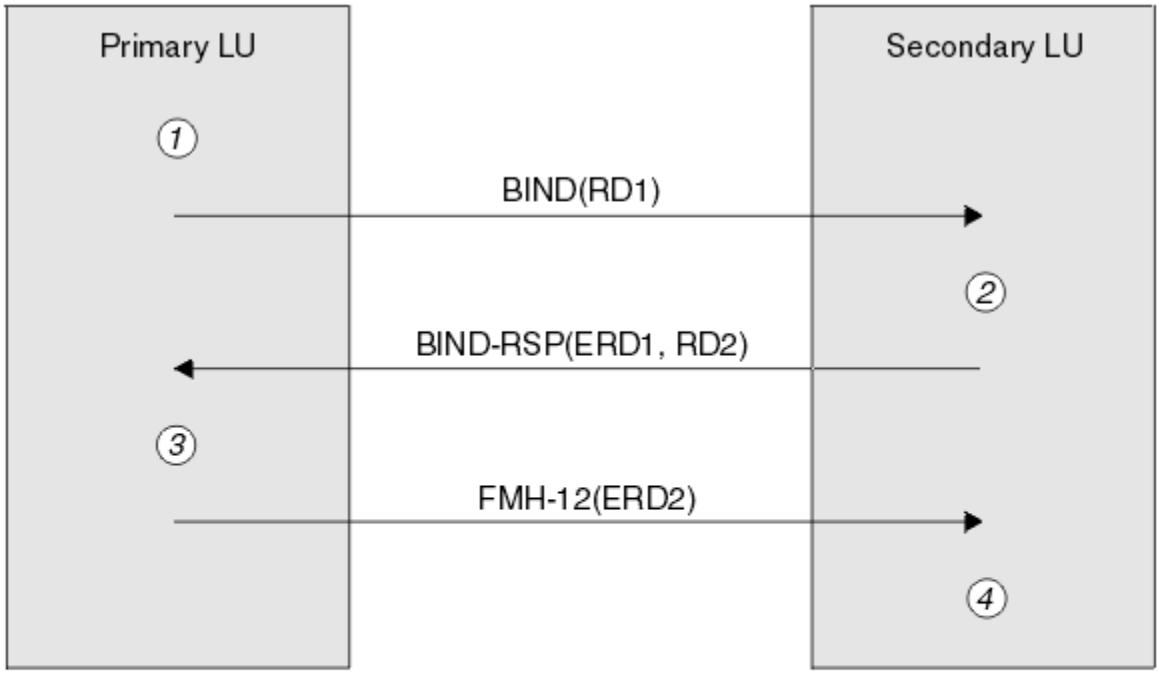
Więcej ogólnych informacji o kryptografii na poziomie sesji zawiera sekcja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*(Skorowidz protokołów równorzędnych), SC31-6808(jednostka logiczna architektury sieci).

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 12 na stronie 121 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 12. Przepływy dla uwierzytelniania na poziomie sesji

Protokół dla uwierzytelniania na poziomie sesji jest następujący. Liczby w procedurze odpowiadają numerom w programie Rysunek 12 na stronie 121.

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*.

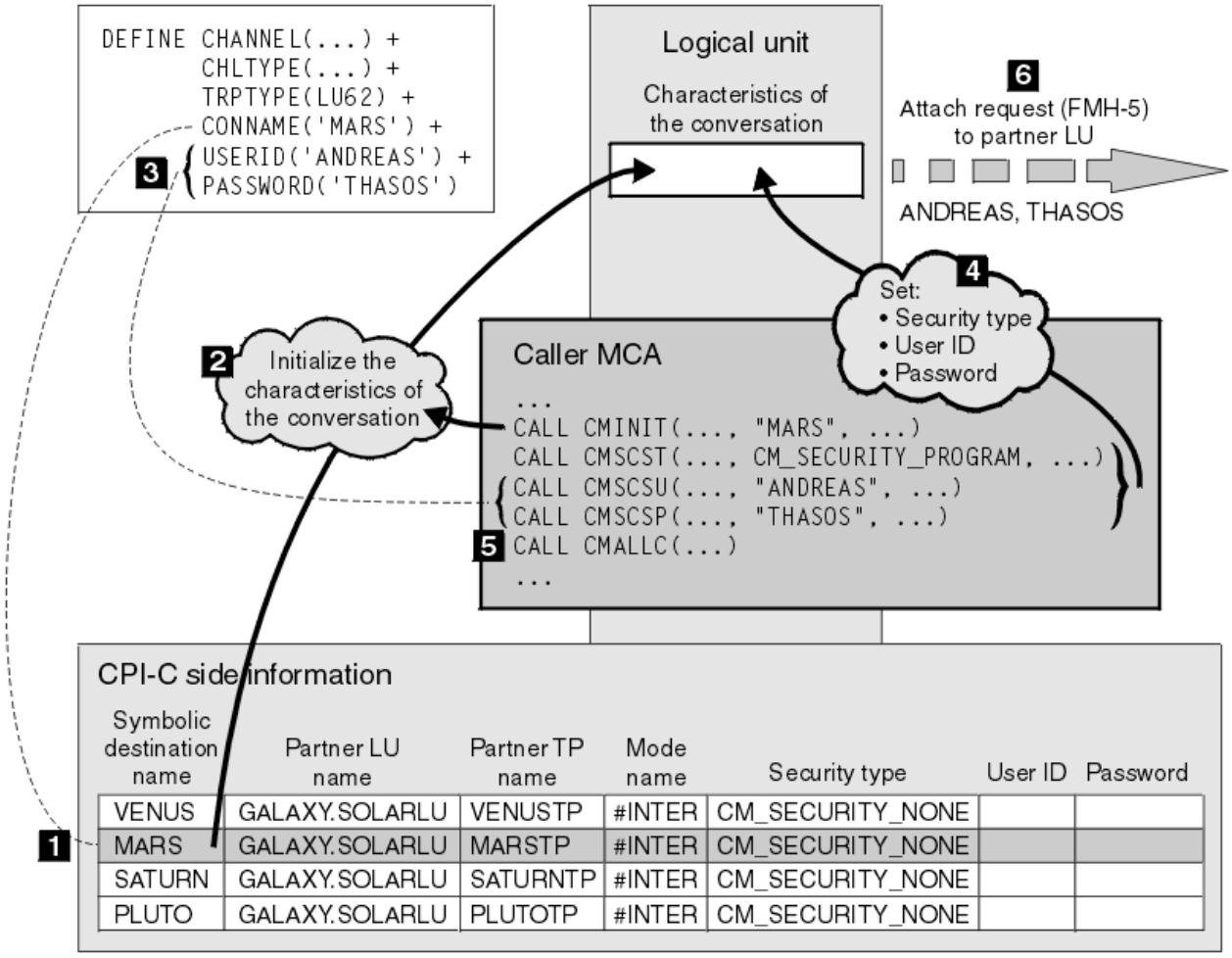
W poniższych tematach opisano, w jaki sposób produkt IBM MQ udostępnia obsługę uwierzytelniania na poziomie konwersacji.

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. Informacje specyficzne dla produktu z/OSznajdują się w publikacji *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 usług wywoływalnych konwersacji APPC/MVS TP można znaleźć w publikacji *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Windows IBM i UNIX *Obsługa uwierzytelniania na poziomie konwersacji w systemach IBM i, UNIXi Windows*
W tym temacie opisano sposób uzyskiwania informacji o tym, jak działa uwierzytelnianie na poziomie konwersacji w systemach IBM i, UNIXi Windows.

Obsługa uwierzytelniania na poziomie konwersacji w systemach IBM i, UNIXi Windows została zilustrowana w programie Rysunek 13 na stronie 123. 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 13. Obsługa uwierzytelniania na poziomie konwersacji w produkcie IBM MQ

W systemach IBM i, UNIXi Windowsagent MCA korzysta z wywołań CPI-C (Common Programming Interface Communications) w celu 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.

Uwierzytelnianie na poziomie konwersacji i IBM MQ for z/OS
W tym temacie opisano sposób uzyskiwania informacji o sposobie działania uwierzytelniania na poziomie konwersacji w systemie z/OS.

W systemie IBM MQ for z/OS, MCAs nie korzysta z funkcji CPI-C. Zamiast tego korzystają z usług wywoływalnych przetwarzania transakcyjnego APPC/MVS TP, implementacji zaawansowanej komunikacji program-program (Advanced Program-to-Program Communication-APPC), która ma pewne funkcje CPI-C. Gdy program wywołujący MCA przydziela konwersację, w wywołaniu jest określony typ zabezpieczeń SAME. Dlatego też, ponieważ jednostka logiczna APPC/MVS obsługuje trwałą weryfikację tylko dla konwersacji przychodzących, a nie dla konwersacji wychodzących, istnieją dwie możliwości:

- Jeśli partnerska jednostka logiczna ufa jednostce logicznej APPC/MVS i zaakcepta już zweryfikowany identyfikator użytkownika, jednostka logiczna APPC/MVS wysyła żądanie przyłączenia zawierające:
  - Identyfikator użytkownika przestrzeni adresowej inicjatora kanału

  - Nazwa profilu zabezpieczeń, który, jeśli używany jest produkt RACF , jest nazwą bieżącej grupy połączeń dla identyfikatora użytkownika przestrzeni adresowej inicjatora kanału.
  - Indykator już zweryfikowany
- Jeśli partnerska jednostka logiczna nie ma zaufania do jednostki logicznej APPC/MVS i nie zaakceptują już zweryfikowanego identyfikatora użytkownika, jednostka logiczna APPC/MVS wysyła żądanie przyłączenia, które nie zawiera informacji o zabezpieczeniach.

W systemie IBM MQ for z/OSparametry USERID i PASSWORD w komendzie DEFINE CHANNEL nie mogą być używane dla kanału komunikatów i są poprawne tylko na końcu połączenia klienta w kanale MQI. Z tego powodu żądanie przyłączenia z jednostki logicznej APPC/MVS nigdy nie zawiera wartości określonych przez te parametry.

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 MQ decyduje o tym, który menedżer kolejek ma wysłać ten komunikat. Gdy wiele aplikacji wysyła komunikaty do kolejki klastra, program IBM MQ równoważy obciążenie dla każdego z menedżerów kolejek, które mają instancję kolejki. Jeśli jeden z systemów udostępniających sklonowany menedżer kolejek nie powiedzie się, program IBM MQ będzie kontynuował równoważenie obciążenia przez pozostałe menedżery kolejek 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). z/OS W celu uzyskania uwag dotyczących produktu IBM MQ for z/OSnależy zapoznać się z “Zabezpieczenia w klastrach menedżerów kolejek w systemie z/OS” na stronie 271.

Zadania pokrewne

“Zapobieganie odbierającym komunikaty menedżerom kolejek” na stronie 477
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 MQ

Jeśli używany jest produkt IBM 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 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 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 MQ Multicast.

IBM 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 MQ (na przykład aplikacje LLM. Więcej informacji na ten temat zawiera sekcja Multicast interoperability with IBM MQ Low Latency Messaging), dlatego może być konieczne zaimplementowanie własnych procedur bezpieczeństwa, ponieważ odbieranie aplikacji nie może być pewne z okresu ważności pól kontekstu.

Istnieją trzy procesy zabezpieczeń, które należy rozważyć:

Kontrola dostępu

Kontrola dostępu w produkcie IBM MQ jest oparta na identyfikatorach użytkowników. Więcej informacji na ten temat zawiera sekcja “Kontrola dostępu dla klientów” na stronie 99.

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 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 na ten temat zawiera sekcja "Blokowanie konkretnych adresów IP" na stronie 397.

zabezpieczenia dlaIBM MQ Internet Pass-Thru

Produkt IBM MQ Internet Pass-Thru może uprościć komunikację za pośrednictwem firewalla, ale ma to wpływ na bezpieczeństwo.

Produkt IBM MQ Internet Pass-Thru (MQIPT) jest opcjonalnym komponentem produktu IBM MQ , który może być używany do implementowania rozwiązań przesyłania komunikatów między zdalnymi serwisami w sieci Internet.

Produkt MQIPT umożliwia dwóm menedżerom kolejek wymianę komunikatów lub aplikację kliencką IBM MQ do łączenia się z menedżerem kolejek w sieci Internet bez konieczności bezpośredniego połączenia TCP/IP. Jest to przydatne w przypadku, gdy firewall zabrania bezpośredniego połączenia TCP/IP między dwoma systemami. Sprawia, że przejście protokołu kanału IBM MQ jest prostsze i łatwiejsze do opanowania przez tunelowanie przepływów wewnątrz protokołu HTTP lub przez działanie jako proxy. Korzystając z protokołu TLS (Transport Layer Security), można go również używać do szyfrowania i deszyfrowania komunikatów wysyłanych przez Internet.

Jeśli system IBM MQ komunikuje się z produktem MQIPT, o ile nie jest używany tryb proxy SSL w produkcie MQIPT, należy się upewnić, że specyfikacja CipherSpec używana przez produkt IBM MQ jest zgodna z zestawem CipherSuite używanym przez produkt MQIPT:

- Gdy serwer MQIPT działa jako serwer TLS, a produkt IBM MQ łączy się jako klient TLS, specyfikacja CipherSpec używana przez produkt IBM MQ musi odpowiadać CipherSuite , który jest włączony w odpowiednim pliku kluczy MQIPT .
- Gdy serwer MQIPT działa jako klient TLS i łączy się z serwerem IBM MQ TLS, pakiet MQIPT CipherSuite musi być zgodny z atrybutem CipherSpec zdefiniowanym w odbierającym kanale IBM MQ .

W przypadku przeprowadzania migracji z produktu MQIPT do zintegrowanej obsługi protokołu IBM MQ TLS, należy przesłać certyfikaty cyfrowe z pliku kluczy MQIPT przy użyciu produktu **mqiptKeyman** lub **mqiptKeycmd**.

Więcej informacji na ten temat zawiera sekcja IBM MQ Internet Pass-Thru.

z/OS Lista kontrolna implementacji zabezpieczeń produktu IBM MQ for z/OS

W tym temacie opisano procedurę krok po kroku, której można użyć do wypracować i zdefiniować implementację zabezpieczeń dla każdego z menedżerów kolejek produktu IBM MQ .

Produkt RACF udostępnia definicje dla klas zabezpieczeń produktu IBM MQ w dostarczonej statycznej tabeli deskryptora klasy (CDT). Podczas pracy z listą kontrolną można określić, które z tych klas są wymagane przez konfigurację. Należy upewnić się, że zostały one aktywowane zgodnie z opisem w sekcji "Klasy zabezpieczeń produktu RACF" na stronie 188.

Szczegółowe informacje, w szczególności "Profile używane do sterowania dostępem do zasobów produktu IBM MQ" na stronie 199, znajdują się w innych sekcjach.

Jeśli wymagane jest sprawdzenie zabezpieczeń, należy wykonać następującą listę kontrolną, aby ją zaimplementować:

1. Aktywuj klasę RACF MQADMIN (wielkie profile) lub MXADMIN (mieszane profile przypadków).
   - Czy zabezpieczenia mają być na poziomie grupy współużytkowania kolejek, na poziomie menedżera kolejek lub w połączeniu obu tych elementów?

     Patrz "Profile do sterowania grupą współużytkowania kolejek lub zabezpieczeniami na poziomie menedżera kolejek" na stronie 193.
2. Czy potrzebujesz zabezpieczenia połączenia?
   - **Tak**: Aktywacja klasy MQCONN. Zdefiniuj odpowiednie profile połączeń na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQCONN. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.

     Uwaga: Dostęp do odpowiedniego profilu połączenia muszą mieć tylko użytkownicy żądania API `MQCONN` lub identyfikatory użytkowników przestrzeni adresowej CICS lub IMS .
   - **Nie**: należy zdefiniować wartość hlq.NO.CONNECT.CHECKS profil na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
3. Czy potrzebne są sprawdzanie uprawnień w komendach?
   - **Tak**: Aktywuj klasę MQCMDS. Zdefiniuj odpowiednie profile komend na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQCMDS. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.

     Jeśli używana jest grupa współużytkowania kolejek, może być konieczne dołączenie identyfikatorów użytkowników używanych przez sam menedżer kolejek i inicjatora kanału. Patrz sekcja "Konfigurowanie zabezpieczeń zasobów produktu IBM MQ for z/OS" na stronie 262.
   - **Nie**: należy zdefiniować wartość hlq.NO.CMD.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
4. Czy potrzebne są zabezpieczenia zasobów używanych w komendach?
   - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj odpowiednie profile, aby chronić zasoby na komendach na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili. Ustaw parametr CMDUSER w parametrze CSQ6SYSP na domyślny identyfikator użytkownika, który ma być używany do sprawdzania zabezpieczeń komend.

     Jeśli używana jest grupa współużytkowania kolejek, może być konieczne dołączenie identyfikatorów użytkowników używanych przez sam menedżer kolejek i inicjatora kanału. Patrz sekcja "Konfigurowanie zabezpieczeń zasobów produktu IBM MQ for z/OS" na stronie 262.
   - **Nie**: należy zdefiniować wartość hlq.NO.CMD.RESC.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
5. Czy potrzebne są zabezpieczenia kolejki?

- **Tak**: Aktywuj klasę MQQUEUE lub MXQUEUE. Zdefiniuj odpowiednie profile kolejek dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQQUEUE lub MXQUEUEclass. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
- **Nie**: należy zdefiniować wartość hlq.NO.QUEUE.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.

6. Czy potrzebne są zabezpieczenia procesu?
   - **Tak**: Aktywuj klasę MQPROC lub MXPROC. Zdefiniuj odpowiednie profile procesów na poziomie menedżera kolejek lub grupy współużytkowania kolejek i zezwalaj na dostęp odpowiednich użytkowników lub grup do tych profili.
   - **Nie**: należy zdefiniować wartość hlq.NO.PROCESS.CHECKS dla odpowiedniego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
7. Czy potrzebujesz zabezpieczenia listy nazw?
   - **Tak**: Aktywuj komendę MQNLIST lub MXNLISTclass. Zdefiniuj odpowiednie profile listy nazw na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQNLIST lub MXNLIST. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: należy zdefiniować wartość hlq.NO.NLIST.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
8. Czy potrzebne są zabezpieczenia tematów?
   - **Tak**: Aktywuj klasę MXTOPIC. Zdefiniuj odpowiednie profile tematów na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MXTOPIC. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: należy zdefiniować wartość hlq.NO.TOPIC.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
9. Czy wszyscy użytkownicy muszą chronić korzystanie z opcji `MQOPEN` lub `MQPUT1` związanych z korzystaniem z kontekstu?
   - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj profile hlq.CONTEXT.queuename w kolejce, menedżerze kolejek lub na poziomie grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: należy zdefiniować wartość hlq.NO.CONTEXT.CHECKS profil dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
10. Czy należy chronić korzystanie z alternatywnych identyfikatorów użytkowników?
    - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj odpowiednią wartość parametru hlq.ALTERNATE.USER. Profile produktu *alternateuserid* dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek i zezwalają na dostęp wymaganych użytkowników lub grup do tych profili.
    - **Nie**: należy zdefiniować profil hlq.NO.ALTERNATE.USER.CHECKS w przypadku wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
11. Czy chcesz dostosować, które identyfikatory użytkowników mają być używane do sprawdzania bezpieczeństwa zasobów poprzez RESLEVEL?
    - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Należy zdefiniować profil hlq.RESLEVEL na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN. Następnie należy zezwolić na dostęp wymaganych użytkowników lub grup do profilu.
    - **Nie**: upewnij się, że w klasie MQADMIN lub MXADMIN nie ma profili ogólnych, które mogą mieć zastosowanie do pliku hlq.RESLEVEL. Zdefiniuj profil hlq.RESLEVEL dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek i upewnij się, że żaden użytkownik lub grupy nie mają do niego dostępu.

12. Czy konieczne jest określenie limitu czasu nieużywanych identyfikatorów użytkowników z produktu IBM MQ ?
    - **Tak**: określ wartości limitu czasu, które mają być używane, a następnie wydaj komendę MQSC ALTER SECURITY, aby zmienić parametry TIMEOUT i INTERVAL.
    - **Nie**: wydaj komendę MQSC ALTER SECURITY, aby ustawić wartość INTERVAL na zero.

    Uwaga: Zaktualizuj zestaw danych wejściowych inicjowania CSQINP1 używany przez podsystem w taki sposób, aby komenda MQSC ALTER SECURITY była uruchamiana automatycznie podczas uruchamiania menedżera kolejek.
13. Czy korzystasz z rozproszonego kolejkowania?
    - **Tak**: użyj rekordów uwierzytelniania kanału. Więcej informacji na ten temat zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 50.
    - Można również określić odpowiednią wartość atrybutu MCAUSER dla każdego kanału lub zapewnić odpowiednie wyjścia zabezpieczeń kanału.
14. Czy chcesz użyć protokołu TLS (Transport Layer Security)?
    - **Tak**: aby określić, że każdy użytkownik prezentujący certyfikat osobisty TLS zawierający określoną nazwę wyróżniającą ma używać konkretnego użytkownika MCAUSER, należy ustawić rekord uwierzytelniania kanału typu SSLPEERMAP. Określić można pojedynczą nazwę wyróżniającą lub wzorzec zawierający znaki wieloznaczne.
    - Zaplanuj infrastrukturę TLS. Zainstaluj opcję System SSL produktu z/OS. W produkcie RACFnależy skonfigurować filtry nazw certyfikatów (CNF), jeśli są używane, a także certyfikaty cyfrowe. Skonfiguruj pierścień kluczy SSL. Upewnij się, że atrybut SSLKEYR menedżera kolejek jest niepusty i wskazuje na pierścień kluczy SSL. Upewnij się również, że wartość atrybutu SSLTASKS wynosi co najmniej 2.
    - **Nie**: Upewnij się, że parametr SSLKEYR jest pusty, a SSLTASKS ma wartość zero.

    Więcej informacji na temat protokołu TLS można znaleźć w sekcji “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24.
15. Czy korzystasz z klientów?
    - **Tak**: użyj rekordów uwierzytelniania kanału.
    - Można również określić odpowiednią wartość atrybutu MCAUSER dla każdego kanału połączenia z serwerem lub zapewnić odpowiednie wyjścia bezpieczeństwa kanału, jeśli jest to wymagane.
16. Sprawdź ustawienia przełącznika.

    IBM MQ wysyła komunikaty, gdy uruchamiany jest menedżer kolejek, który wyświetla ustawienia zabezpieczeń. Te komunikaty służą do określania, czy przełączniki są ustawione poprawnie.
17. Czy wysyłać hasła z aplikacji klienckich?
    - **Tak**: upewnij się, że opcja z/OS jest zainstalowana i że program Integrated Cryptographic Service Facility (ICSF) jest uruchomiony dla najlepszej ochrony.
    - **Nie**: można zignorować komunikat o błędzie informując, że narzędzie ICSF nie zostało uruchomione.

    Więcej informacji na temat ICSF zawiera sekcja “Korzystanie z narzędzia Integrated Cryptographic Service Facility (ICSF)” na stronie 271

Konfigurowanie zabezpieczeń

Ta kolekcja tematów zawiera informacje specyficzne dla różnych systemów operacyjnych, a także dla klientów.

ULW Konfigurowanie zabezpieczeń w systemie UNIX, Linux, and Windows

Zagadnienia dotyczące bezpieczeństwa specyficzne dla systemów UNIX, Linux, and Windows .

Menedżery kolejek produktu IBM 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 MQ
Istnieje możliwość zdefiniowania zestawu użytkowników, którzy mogą wydawać komendy do administrowania produktem IBM MQ.

Kto może używać obiektów IBM 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 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 MQ; nie należy używać standardowych komend systemu operacyjnego do nadawania lub odbierania uprawnień do zasobów MQI.

ULW Jak autoryzacje działają w systemie UNIX, Linux, and Windows

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 słów kluczowych z listy autoryzacji dla komendy `setmqaut` dla konkretnej 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.

ULW *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 produktów **MQOPEN** i **MQPUT1**sprawdzanie 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 10 na stronie 132, Tabela 11 na stronie 132, Tabela 12 na stronie 133i Tabela 13 na stronie 134 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 10. Autoryzacja zabezpieczeń wymagana dla wywołań MQCONN

Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 134)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCONN	Nie dotyczy	Nie dotyczy	MQZAO_CONNECT

Tabela 11. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN

Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 134)**	**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 134)**	MQZAO_INPUT	Nie dotyczy	Nie dotyczy
MQOO_OUTPUT (normalna kolejka) **(“3” na stronie 134)**	MQZAO_OUTPUT	Nie dotyczy	Nie dotyczy

Tabela 11. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN (kontynuacja)

Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 134)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_PASS_ IDENTITY_CONTEXT **("4" na stronie 134)**	MQZAO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	Nie dotyczy	Brak sprawdzenia
MQOO_PASS_ALL_ CONTEXT **("4" na stronie 134, "5" na stronie 134)**	MQZAO_PASS _ALL_CONTEXT	Nie dotyczy	Brak sprawdzenia
MQOO_SET_ IDENTITY_CONTEXT **("4" na stronie 134, "5" na stronie 134)**	MQZAO_SET_ KONTEKST_IDENTYFIKATORA	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stronie 134)**
MQOO_SET_ ALL_CONTEXT **("4" na stronie 134, "7" na stronie 134)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 134)**
MQOO_OUTPUT (kolejka transmisji) **("8" na stronie 134)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 134)**
MQOO_SET	MQZAO_SET	Nie dotyczy	Brak sprawdzenia
MQOO_ALTERNATE_ USER_AUTHORITY	**("9" na stronie 134)**	**("9" na stronie 134)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("9" na stronie 134, "10" na stronie 134)**

Tabela 12. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1

Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 134)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	MQZAO_PASS_ IDENTITY_CONTEXT **("11" na stronie 134)**	Nie dotyczy	Brak sprawdzenia
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **("11" na stronie 134)**	Nie dotyczy	Brak sprawdzenia
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("11" na stronie 134)**	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stronie 134)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("11" na stronie 134)**	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 134)**
(Kolejka transmisji) **("8" na stronie 134)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 134)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**("12" na stronie 134)**	Nie dotyczy	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" na stronie 134)**

Tabela 13. Autoryzacja zabezpieczeń wymagana dla wywołań MQCLOSE			
Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 134)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCO_DELETE	MQZAO_DELETE **("13" na stronie 134)**	Nie dotyczy	Nie dotyczy
MQCO_DELETE _PURGE	MQZAO_DELETE **("13" na stronie 134)**	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 134).
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 wtedy, gdy spełnione są oba poniższe stwierdzenia:
    - Trwała kolejka dynamiczna jest zamykana i usuwana.
    - Kolejka nie została utworzona za pomocą wywołania MQOPEN , które zwróciło uchwyt obiektu, który jest używany.

    W przeciwnym razie nie będzie sprawdzania.

ULW *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 139)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(“2” na stronie 139)**
Temat	MQZAO_CREATE **(“2” na stronie 139)**
Proces	MQZAO_CREATE **(“2” na stronie 139)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(“2” na stronie 139)**
Informacje uwierzytelniające	MQZAO_CREATE **(“2” na stronie 139)**
Kanał	MQZAO_CREATE **(“2” na stronie 139)**
Kanał połączenia klienta	MQZAO_CREATE **(“2” na stronie 139)**
Program nasłuchujący	MQZAO_CREATE **(“2” na stronie 139)**
Usługa	MQZAO_CREATE **(“2” na stronie 139)**
Informacje o komunikacji	MQZAO_CREATE **(“2” na stronie 139)**

DEFINE *obiekt* REPLACE (“1” na stronie 139, “3” na stronie 139)

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

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

Obiekt	Wymagane uprawnienia
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
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

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

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
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, jak w przypadku opcji DEFINE *obiekt* NOREPLACE.

Informacje pokrewne

Technologia klastrowa: sprawdzone procedury użycia komendy REFRESH CLUSTER

ULW *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	**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

Kopiuj *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 146)**

Kopiuj *obiekt* (z zastąpami) (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
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)**

Obiekt	Wymagane uprawnienia
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 zastąpami) (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	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

Zapytaj *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DISPLAY
Temat	MQZAO_DISPLAY

Obiekt	Wymagane uprawnienia
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

Sprawdź nazwy *obiektu*

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
Informacje o komunikacji	Brak sprawdzenia

Uruchomienie *obiektu*

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

Obiekt	Wymagane uprawnienia
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

Komenda	Obiekt	Wymagane uprawnienia
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'	Wymagane jest członkostwo w grupie 'mqm'
Resetowanie klastra	Wymagane jest członkostwo w grupie 'mqm'	Wymagane jest członkostwo w grupie 'mqm'
Zawieś klaster menedżera kolejek	Wymagane jest członkostwo w grupie 'mqm'	Wymagane jest członkostwo w grupie 'mqm'
Wznów klaster menedżera kolejek	Wymagane jest członkostwo w grupie 'mqm'	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.

AIX 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.

O tym zadaniu

W systemie AIXmożna użyć narzędzia SMITTY w celu utworzenia grupy, dodania użytkownika do grupy, wyświetlenia listy użytkowników należących do grupy oraz usunięcia użytkownika z grupy.

Procedura

1. Z poziomu SMITTY wybierz opcję **Security and Users** (Bezpieczeństwo i użytkownicy) i naciśnij klawisz Enter.
2. Wybierz opcję **Grupy** i naciśnij klawisz Enter.
3. Aby utworzyć grupę, wykonaj następujące kroki:
   a) Wybierz opcję **Dodaj grupę** i naciśnij klawisz Enter.
   b) Wprowadź nazwę grupy i nazwy wszystkich użytkowników, którzy mają zostać dodani do grupy, rozdzielając je przecinkami.
   c) Naciśnij klawisz Enter, aby utworzyć grupę.
4. Aby dodać użytkownika do grupy, wykonaj następujące kroki:
   a) Wybierz opcję **Zmień/pokaż charakterystykę grup** i naciśnij klawisz Enter.
   b) Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.
   c) Dodaj nazwy użytkowników, którzy mają być dodawani do grupy, oddzielając je przecinkami.
   d) Naciśnij klawisz Enter, aby dodać nazwy do grupy.
5. Aby wyświetlić kto jest w grupie, wykonaj następujące kroki:
   a) Wybierz opcję **Zmień/pokaż charakterystykę grup** i naciśnij klawisz Enter.
   b) Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.
6. Aby usunąć użytkownika z grupy, wykonaj następujące kroki:
   a) Wybierz opcję **Zmień/pokaż charakterystykę grup** i naciśnij klawisz Enter.
   b) Wprowadź nazwę grupy, aby wyświetlić listę członków grupy.
   c) Usuń z grupy nazwę użytkownika, który ma zostać usunięty.
   d) Naciśnij klawisz Enter, aby usunąć nazwę z grupy.

Linux 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.

O tym zadaniu

W systemie Linuxinformacje o grupach są przechowywane w pliku `/etc/group` . Za pomocą komend można utworzyć grupę, dodać użytkownika do grupy, wyświetlić listę użytkowników należących do grupy, a następnie usunąć użytkownika z grupy.

Procedura

1. Aby utworzyć nową grupę, należy użyć komendy **groupadd** .
   Wywołaj następującą komendę:

   ```
   groupadd -g group-ID group-name
   ```

   gdzie *identyfikator-grupy* to liczbowy identyfikator grupy, a *nazwa_grupy* jest nazwą grupy.
2. Aby dodać członka do grupy uzupełniającej, należy użyć komendy **usermod** w celu wyświetlenia listy grup dodatkowych, do których użytkownik jest aktualnie członkiem, oraz grup dodatkowych, do których użytkownik ma zostać członkiem.
   Na przykład, jeśli użytkownik jest już członkiem grupy `groupa`i ma stać się członkiem `groupb`, należy użyć następującej komendy:

   ```
   usermod -G groupa,groupb user-name
   ```

   gdzie *nazwa-użytkownika* jest nazwą użytkownika.
3. Aby wyświetlić osobę, która jest członkiem grupy, należy użyć komendy **getent** .
   Wywołaj następującą komendę:

   ```
   getent group group-name
   ```

   gdzie *nazwa_grupy* jest nazwą grupy.
4. Aby usunąć członka z grupy uzupełniającej, należy użyć komendy **usermod** w celu wyświetlenia grup dodatkowych, do których użytkownik ma pozostać członkiem.
   Na przykład, jeśli podstawową grupą użytkownika jest `users` , a użytkownik jest także członkiem grup `mqm`, `groupa` i `groupb`, aby usunąć użytkownika z grupy `mqm` , należy użyć następującej komendy:

   ```
   usermod -G groupa,groupb user-name
   ```

   gdzie *nazwa-użytkownika* jest nazwą użytkownika.

Solaris 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.

O tym zadaniu

W systemie Solarisinformacje o grupach są przechowywane w pliku `/etc/group` . Za pomocą komend można utworzyć grupę, dodać użytkownika do grupy, wyświetlić listę użytkowników należących do grupy, a następnie usunąć użytkownika z grupy.

Procedura

1. Aby utworzyć nową grupę, należy użyć komendy **groupadd** .
   Wywołaj następującą komendę:

   ```
   groupadd -g group-ID group-name
   ```

   gdzie *identyfikator-grupy* to liczbowy identyfikator grupy, a *nazwa_grupy* jest nazwą grupy.

2. Aby dodać członka do grupy uzupełniającej, należy użyć komendy **usermod** w celu wyświetlenia listy grup dodatkowych, do których użytkownik jest aktualnie członkiem, oraz grup dodatkowych, do których użytkownik ma zostać członkiem.
   Na przykład, jeśli użytkownik jest już członkiem grupy `groupa` i ma stać się członkiem `groupb`, należy użyć następującej komendy:

   ```
   usermod -G groupa,groupb user-name
   ```

   gdzie *nazwa-użytkownika* jest nazwą użytkownika.
3. Aby dowiedzieć się, kto jest członkiem grupy, należy sprawdzić pozycję dla tej grupy w pliku `/etc/group` .
4. Aby usunąć członka z grupy uzupełniającej, należy użyć komendy **usermod** w celu wyświetlenia grup dodatkowych, do których użytkownik ma pozostać członkiem.
   Na przykład, jeśli podstawową grupą użytkownika jest `users` , a użytkownik jest także członkiem grup `mqm`, `groupa` i `groupb`, aby usunąć użytkownika z grupy `mqm` , należy użyć następującej komendy:

   ```
   usermod -G groupa,groupb user-name
   ```

   gdzie *nazwa-użytkownika* jest nazwą użytkownika.

Windows Tworzenie grup i zarządzanie nimi w systemie Windows

W systemie Windowsza pomocą funkcji Zarządzanie komputerem można administrować grupami na stacji roboczej lub na serwerze składowym.

O tym zadaniu

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 przypisach do grupy użytkownika nie są rozpoznawane do czasu zrestartowania menedżera kolejek lub do wydania komendy MQSC **REFRESH SECURITY** (lub równoważnika PCF).

Panel Zarządzanie komputerem produktu Windows służy do pracy z użytkownikami i grupami. Wszelkie zmiany wprowadzone do bieżącego zalogowanego użytkownika mogą nie być skuteczne, dopóki użytkownik nie zaloguje się ponownie.

Windows *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**.

Windows *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.

Windows *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.

Windows *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.

Windows Specjalne uwagi dotyczące zabezpieczeń w systemie Windows

Niektóre funkcje zabezpieczeń zachowują się inaczej w różnych wersjach produktu Windows.

Zabezpieczenia systemu IBM MQ są oparte na wywołaniach interfejsu API systemu operacyjnego w celu uzyskania informacji na temat autoryzacji użytkowników i przynależności do grup. Niektóre funkcje nie działają identycznie w systemach Windows . Ta kolekcja tematów zawiera opisy sytuacji, w których różnice te mogą mieć wpływ na bezpieczeństwo systemu IBM MQ podczas uruchamiania produktu IBM MQ w środowisku Windows .

Windows *Lokalne i domenowe konta użytkowników dla usługi IBM MQ Windows*

Działający produkt IBM MQ musi sprawdzać, czy dostęp do menedżerów kolejek i do kolejek mogą uzyskiwać tylko autoryzowani użytkownicy. Wymaga to specjalnego konta użytkownika, którego program IBM MQ może używać do wysyłania zapytań o informacje o użytkownikach próbujący uzyskać dostęp.

- “Konfigurowanie kont użytkowników specjalnych za pomocą Prepare IBM MQ Wizard” na stronie 150
- “Korzystanie z produktu IBM MQ z Active Directory” na stronie 151
- “Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows” na stronie 151

Konfigurowanie kont użytkowników specjalnych za pomocą Prepare IBM MQ Wizard

Prepare IBM MQ Wizard tworzy specjalne konto użytkownika, dzięki czemu usługa Windows może być współużytkowana przez procesy, które muszą jej używać (patrz sekcja Konfigurowanie produktu IBM MQ przy użyciu kreatora przygotowania produktu IBM MQ).

Usługa Windows jest współużytkowana przez procesy klienta dla instalacji produktu IBM MQ . Dla każdej instalacji tworzona jest jedna usługa. Każda usługa ma nazwę `MQ_`*`InstallationName`* i ma nazwę wyświetlaną `IBM MQ(`*`InstallationName`*`)`.

Ze względu na to, że każda usługa musi być współużytkowana przez sesje logowania nieinteraktywne i interaktywne, należy uruchomić każdą z nich na specjalnym koncie użytkownika. Można użyć jednego specjalnego konta użytkownika dla wszystkich usług lub utworzyć inne specjalne konta użytkowników. Każde specjalne konto użytkownika musi mieć uprawnienia użytkownika do `logowania się jako usługa`, aby uzyskać więcej informacji na temat Tabela 14 na stronie 152. Jeśli ID użytkownika nie ma uprawnień do uruchomienia usługi, usługa nie zostanie uruchomiona i w dzienniku zdarzeń systemowych Windows zostanie zwrócony błąd. Zwykle użytkownik uruchomił produkt Prepare IBM MQ Wizardi poprawnie ustawił ID użytkownika. Jeśli jednak ID użytkownika został skonfigurowany ręcznie, możliwe jest rozwiązanie problemu, który będzie musiał zostać rozwiązany.

Podczas instalowania produktu IBM MQ i uruchamiania produktu Prepare IBM MQ Wizard po raz pierwszy tworzone jest lokalne konto użytkownika dla usługi o nazwie MUSR_MQADMIN z wymaganymi ustawieniami i uprawnieniami, w tym `Logowanie w postaci usługi`.

W kolejnych instalacjach produkt Prepare IBM MQ Wizard tworzy konto użytkownika o nazwie MUSR_MQADMIN*x*, gdzie *x* jest kolejnym dostępnym numerem reprezentującym identyfikator użytkownika, który nie istnieje. Hasło użytkownika MUSR_MQADMIN*x* jest generowane losowo podczas tworzenia konta i jest używane do konfigurowania środowiska logowania dla usługi. Wygenerowane hasło nie traci ważności.

To konto IBM MQ nie ma wpływu na strategie kont, które są skonfigurowane w systemie w celu wymagania, aby hasła kont zostały zmienione po pewnym czasie.

Hasło nie jest znane poza tym jednorazowym przetwarzaniem i jest przechowywane przez system operacyjny Windows w zabezpieczonej części rejestru.

Korzystanie z produktu IBM MQ z Active Directory

W niektórych konfiguracjach sieciowych, w których konta użytkowników są definiowane w kontrolerach domeny korzystających z usługi katalogowej Active Directory , lokalne konto użytkownika, na którym działa produkt IBM MQ , może nie mieć uprawnień wymaganych do wysyłania zapytań o członkostwo w grupie innych kont użytkowników domeny. Podczas instalowania produktu IBM MQprodukt Prepare IBM MQ Wizard określa, czy jest to przypadek, przeprowadzając testy i zadając pytania dotyczące konfiguracji sieci.

Jeśli lokalne konto użytkownika, na którym działa produkt IBM MQ , nie ma wymaganych uprawnień, Prepare IBM MQ Wizard wyświetli zapytanie o szczegóły konta użytkownika należącego do domeny z określonymi prawami użytkownika. Informacje na temat tworzenia i konfigurowania konta domeny produktu Windows zawiera sekcja Tworzenie i konfigurowanie kont domeny Windows dla produktu IBM MQ. Informacje o prawach użytkownika, które są wymagane przez konto użytkownika domeny, zawiera sekcja Tabela 14 na stronie 152.

Po wprowadzeniu poprawnych szczegółów konta dla konta użytkownika domeny w Prepare IBM MQ Wizardkreator skonfiguruje usługę IBM MQ Windows w taki sposób, aby była uruchamiana w ramach nowego konta. Szczegóły konta są przechowywane w zabezpieczonej części rejestru i nie mogą być odczytane przez użytkowników.

Gdy usługa jest uruchomiona, usługa IBM MQ Windows jest uruchamiana i pozostaje uruchomiona tak długo, jak długo usługa jest uruchomiona. Administrator produktu IBM MQ , który loguje się na serwerze po uruchomieniu usługi Windows , może za pomocą konsoli IBM MQ Explorer administrować menedżerami kolejek na serwerze. Łączy to IBM MQ Explorer z istniejącym procesem usługi Windows . Te dwa działania wymagają różnych poziomów uprawnień, zanim będą mogły pracować:

- Proces uruchamiania wymaga uprawnień uruchamiania.
- Administrator produktu IBM MQ wymaga uprawnień dostępu.

Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows

W poniższej tabeli znajduje się lista praw użytkownika wymaganych dla kont użytkowników lokalnych i domen, w których działa usługa Windows dla instalacji produktu IBM MQ .

Tabela 14. Uprawnienia użytkownika wymagane przez usługę IBM MQ dla systemu Windows	
Uprawnienie	**Opis**
Zaloguj się jako zadanie wsadowe	Umożliwia uruchomienie usługi IBM MQ Windows w ramach tego konta użytkownika.
Zaloguj się jako usługa	Umożliwia użytkownikom ustawienie usługi IBM MQ Windows w celu zalogowania się przy użyciu skonfigurowanego konta.
Zamknij system	Umożliwia usłudze IBM MQ Windows zrestartowanie serwera, jeśli jest on skonfigurowany w taki sposób, gdy odtwarzanie usługi nie powiedzie się.
zwiększanie limitu miejsca na dysku	Wymagany dla wywołania systemu operacyjnego `CreateProcessAsUser` .
działanie jako część systemu operacyjnego	Wymagany dla wywołania systemu operacyjnego `LogonUser` .
Pomijanie sprawdzania przeglądania	Wymagany dla wywołania systemu operacyjnego `LogonUser` .
zamiana znacznika poziomu procesu	Wymagany dla wywołania systemu operacyjnego `LogonUser` .

Uwaga: W środowiskach działających na ASP i w aplikacjach IIS mogą być wymagane prawa do programów debugowania.

Konto użytkownika domeny musi mieć ustawione uprawnienia użytkownika Windows jako efektywne prawa użytkownika wymienione w aplikacji Zasady zabezpieczeń lokalnych. Jeśli nie, ustaw je za pomocą aplikacji Zasady zabezpieczeń lokalnych lokalnie na serwerze lub za pomocą domeny aplikacji Zabezpieczenia domeny.

Windows *Uprawnienia zabezpieczeń serwera Windows*

Instalacja produktu IBM MQ zachowuje się inaczej na serwerze Windows , w zależności od tego, czy użytkownik lokalny lub użytkownik domeny wykonuje instalację.

Jeśli *lokalny* użytkownik zainstaluje program IBM MQ, program Prepare IBM MQ Wizard wykryje, że lokalny użytkownik utworzony dla usługi IBM MQ Windows może pobrać informacje o przynależności do grupy dotyczące użytkownika instalujący. Program Prepare IBM MQ Wizard zadaje użytkownikowi pytania dotyczące konfiguracji sieci, aby określić, czy istnieją inne konta użytkowników zdefiniowane w kontrolerach domeny działających w systemie Windows 2000 lub nowszym. Jeśli tak, usługa IBM MQ Windows musi działać pod kontem użytkownika domeny z określonymi ustawieniami i uprawnieniami. Program Prepare IBM MQ Wizard prosi użytkownika o podanie szczegółów konta użytkownika zgodnie z opisem w sekcji Konfigurowanie produktu IBM MQ za pomocą kreatora przygotowania produktu IBM MQ.

Jeśli użytkownik *domena* zainstaluje produkt IBM MQ, program Prepare IBM MQ Wizard wykryje, że lokalny użytkownik utworzony dla usługi IBM MQ Windows nie może pobrać informacji o przypisach grupy do użytkownika instalujący. W takim przypadku program Prepare IBM MQ Wizard zawsze pyta użytkownika o szczegóły konta użytkownika domeny dla usługi IBM MQ Windows , która ma być używana.

Gdy usługa IBM MQ Windows musi korzystać z konta użytkownika domeny, produkt IBM MQ nie może działać poprawnie, dopóki nie zostanie to skonfigurowane za pomocą Prepare IBM MQ Wizard. Prepare IBM MQ Wizard nie zezwala użytkownikowi na kontynuowanie wykonywania innych zadań, dopóki usługa Windows nie zostanie skonfigurowana z odpowiednim kontem.

Więcej informacji na ten temat zawiera sekcja Tworzenie i konfigurowanie kont domeny dla produktu IBM MQ.

Windows *Zmiana nazwy użytkownika powiązanej z usługą IBM MQ*

Użytkownik może zmienić nazwę użytkownika powiązaną z usługą IBM MQ , tworząc nowe konto i wprowadzając jego szczegóły przy użyciu Prepare IBM MQ Wizard.

O tym zadaniu

Podczas instalowania produktu IBM MQ i uruchamiania produktu Prepare IBM MQ Wizard po raz pierwszy tworzony jest lokalny konto użytkownika dla usługi o nazwie MUSR_MQADMIN. W kolejnych instalacjach produkt Prepare IBM MQ Wizard tworzy konto użytkownika o nazwie MUSR_MQADMIN*x*, gdzie *x* jest kolejnym dostępnym numerem reprezentującym identyfikator użytkownika, który nie istnieje.

Może być konieczna zmiana nazwy użytkownika powiązanej z usługą IBM MQ z wartości MUSR_MQADMIN lub MUSR_MQADMIN*x* na inną. Może to być na przykład konieczne, jeśli menedżer kolejek jest powiązany z programem Db2, który nie akceptuje nazw użytkowników o długości większej niż 8 znaków.

Procedura

1. Utwórz nowe konto użytkownika (na przykład **NEW_NAME**)
2. Użyj Prepare IBM MQ Wizard , aby wprowadzić szczegóły nowego konta użytkownika.

Zadania pokrewne

Konfigurowanie produktu IBM MQ za pomocą kreatora przygotowania produktu IBM MQ

Windows *Zmiana hasła do lokalnego konta użytkownika usługi IBM MQ Windows*

Hasło lokalnego konta użytkownika usługi IBM MQ Windows można zmienić, korzystając z panelu Zarządzanie komputerem.

O tym zadaniu

Aby zmienić hasło dla lokalnego konta użytkownika usługi IBM MQ Windows , wykonaj następujące kroki:

Procedura

1. Zidentyfikuj użytkownika, w którym usługa jest uruchomiona.
2. Zatrzymaj usługę IBM MQ z poziomu panelu Zarządzanie komputerem.
3. Zmień wymagane hasło w taki sam sposób, w jaki zmienisz hasło danej osoby.
4. Przejdź do właściwości usługi IBM MQ z panelu Zarządzanie komputerem.
5. Wybierz stronę **Logowanie** .
6. Upewnij się, że podana nazwa konta jest zgodna z nazwą użytkownika, dla którego hasło zostało zmodyfikowane.
7. Wpisz hasło w polach **Hasło** i **Potwierdź hasło** , a następnie kliknij przycisk **OK**.

Windows *Zmiana hasła dla usługi IBM MQ Windows dla instalacji działającej pod kontem użytkownika domeny*

Alternatywą dla użycia Prepare IBM MQ Wizard w celu wprowadzenia szczegółów konta użytkownika domeny można użyć panelu Zarządzanie komputerem w celu zmiany szczegółów **logowania** dla konkretnej usługi IBM MQ .

O tym zadaniu

Jeśli usługa IBM MQ Windows dla instalacji działa pod kontem użytkownika domeny, można zmienić hasło dla konta w następujący sposób:

Procedura

1. Zmień hasło dla konta domenowego na kontrolerze domeny. Może być konieczne poproś administratora domeny o to, aby zrobił to dla Ciebie.
2. Wykonaj następujące kroki, aby zmodyfikować stronę **Logowanie** dla usługi IBM MQ .
   a) Zidentyfikuj użytkownika, pod którym usługa jest uruchomiona.
   b) Zatrzymaj usługę IBM MQ z poziomu panelu Zarządzanie komputerem.
   c) Zmień wymagane hasło w taki sam sposób, w jaki zmienisz hasło danej osoby.
   d) Przejdź do właściwości usługi IBM MQ z panelu Zarządzanie komputerem.
   e) Wybierz stronę **Logowanie** .
   f) Upewnij się, że podana nazwa konta jest zgodna z nazwą użytkownika, dla którego hasło zostało zmodyfikowane.
   g) Wpisz hasło w polach **Hasło** i **Potwierdź hasło** , a następnie kliknij przycisk **OK**.

   Konto użytkownika, na którym działa usługa IBM MQ Windows , wykonuje dowolne komendy MQSC, które są wykonywane przez aplikacje interfejsu użytkownika lub są wykonywane automatycznie podczas uruchamiania systemu, zamykania systemu lub odtwarzania usługi. W związku z tym konto użytkownika musi mieć uprawnienia administracyjne w produkcie IBM MQ . Domyślnie jest ona dodawana do lokalnej grupy mqm na serwerze. Jeśli przypisanie to zostanie usunięte, usługa IBM MQ Windows nie będzie działać. Więcej informacji na temat praw użytkownika zawiera sekcja “Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows” na stronie 151.

   Jeśli wystąpi problem z zabezpieczeniem konta użytkownika, na którym działa usługa IBM MQ Windows , komunikaty o błędach i opisy pojawią się w systemowym dzienniku zdarzeń.

Zadania pokrewne

Konfigurowanie produktu IBM MQ za pomocą kreatora przygotowania produktu IBM MQ

Windows *Uwagi dotyczące awansowania serwerów Windows do kontrolerów domeny*

Podczas awansowania serwera Windows do kontrolera domeny należy rozważyć, czy ustawienie zabezpieczeń odnoszące się do uprawnień użytkownika i grupy jest odpowiednie. Podczas zmiany stanu maszyny Windows między serwerem a kontrolerem domeny należy wziąć pod uwagę, że może to mieć wpływ na działanie produktu IBM MQ , ponieważ produkt IBM MQ korzysta z lokalnie zdefiniowanej grupy mqm.

Ustawienia zabezpieczeń odnoszące się do użytkowników domeny i uprawnień grupowych

Produkt IBM MQ wykorzystuje informacje o przynależności do grup w celu zaimplementowania strategii bezpieczeństwa, co oznacza, że ważne jest, aby ID użytkownika wykonujący operacje IBM MQ mógł określić przypisania do grup innych użytkowników.

W przypadku awansowania serwera Windows do kontrolera domeny użytkownik jest prezentowany z opcją ustawienia zabezpieczeń odnosząca się do uprawnień użytkownika i grupy. Ta opcja określa, czy dowolne użytkownicy mogą pobierać przypisania do grup z aktywnego katalogu. Jeśli kontroler domeny jest skonfigurowany w taki sposób, że konta lokalne mają uprawnienia do wysyłania zapytań o członkostwo w grupie kont użytkowników domeny, domyślny identyfikator użytkownika utworzony przez produkt IBM MQ podczas procesu instalacji może uzyskać członkostwo w grupie dla innych użytkowników, jeśli jest to wymagane. Jeśli jednak kontroler domeny jest skonfigurowany w taki sposób, że konta lokalne nie mają uprawnień do wysyłania zapytań o przypisanie do grupy kont użytkowników domeny, to program IBM MQ nie zakończy sprawdzania, czy użytkownicy zdefiniowani w domenie są uprawnieni do dostępu do menedżerów kolejek lub do kolejek, a dostęp nie powiedzie się. Jeśli produkt Windows jest używany na kontrolerze domeny, który został skonfigurowany w ten sposób, należy użyć specjalnego konta użytkownika należącego do domeny z wymaganymi uprawnieniami.

W tym przypadku należy wiedzieć:

- Sposób zachowania uprawnień zabezpieczeń dla używanej wersji produktu Windows .

- Sposób zezwalania członkom grupy domeny mqm na odczytywanie członkostwa w grupie.
- Sposób konfigurowania usługi IBM MQ Windows do uruchamiania w ramach użytkownika domeny.

Więcej informacji na ten temat zawiera sekcja Konfigurowanie kont użytkowników dla produktu IBM MQ.

IBM MQ dostęp do lokalnej grupy mqm

Gdy serwery Windows są awansowane do kontrolerów domeny lub z nich demotowane, produkt IBM MQ traci dostęp do lokalnej 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. Objaw jest błędem wskazującego na brak lokalnej grupy mqm, na przykład:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

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 uprzywilejowanych użytkowników produktu IBM 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 domeny uprzywilejowanej IBM MQ identyfikatory wymagane przez wymagany poziom uprawnień.

Windows *Ograniczenia dotyczące grup zagnieżdżonych w systemie Windows*

Istnieją ograniczenia dotyczące korzystania z grup zagnieżdżonych. Wynikają one częściowo z poziomu funkcjonalnego domeny, a częściowo z ograniczeń produktu IBM MQ .

Active Directory może obsługiwać różne typy grup w kontekście domeny w zależności od poziomu funkcjonalnego domeny. Domyślnie domeny produktu Windows 2003 znajdują się w " Windows 2000 mieszany " poziom funkcjonalny. (Windows Server 2008 i Windows Server 2012 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 Active Directory , obowiązują dalsze ograniczenia dotyczące identyfikatorów używanych przez produkt IBM MQ. Sieciowe interfejsy API używane przez produkt IBM MQ nie obsługują wszystkich konfiguracji obsługiwanych przez poziom funkcjonalny domeny. W rezultacie program IBM MQ nie może wysłać zapytania o przypisania do grup 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.

Windows *Autoryzowanie użytkowników do zdalnego używania produktu IBM MQ*

Jeśli konieczne jest utworzenie i uruchomienie menedżerów kolejek po nawiązaniu połączenia z produktem IBM MQ zdalnie, należy mieć dostęp do użytkownika `Utwórz obiekty globalne` .

O tym zadaniu

Uwaga: Administratorzy mają domyślnie dostęp do użytkowników `Tworzenie obiektów globalnych` , dlatego jeśli jesteś administratorem, możesz tworzyć i uruchamiać menedżery kolejek po nawiązaniu połączenia zdalnie bez zmiany praw użytkownika.

Jeśli nawiążesz połączenie z komputerem z systemem Windows przy użyciu usług terminalowych lub połączenia ze zdalnym pulpitem, a wystąpiły problemy podczas tworzenia, uruchamiania lub usuwania menedżera kolejek, może to być spowodowane tym, że użytkownik nie ma dostępu do opcji `Utwórz obiekty globalne`.

Dostęp użytkownika `Utwórz obiekty globalne` jest ograniczany przez użytkowników uprawnionych 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 niej zastosowanie dostęp użytkownika `Utwórz obiekty globalne` .

Gdy połączenie jest nawiązane zdalnie z komputerem z produktem Windows przy użyciu usług terminalowych lub połączenia zdalnego pulpitu, aplikacje działają we własnej lokalnej przestrzeni nazw. W przypadku próby utworzenia lub usunięcia menedżera kolejek za pomocą komendy IBM MQ Explorer lub komendy **crtmqm** lub **dltmqm** albo uruchomienia menedżera kolejek za pomocą komendy **strmqm** , spowoduje to niepowodzenie autoryzacji. Spowoduje to utworzenie FDC IBM MQ z identyfikatorem sondy XY132002.

Uruchamianie menedżera kolejek przy użyciu programu IBM MQ Explorerlub użycie komendy **amqmdain qmgr start** działa poprawnie, ponieważ komendy te nie uruchamiają bezpośrednio menedżera kolejek. Zamiast tego komendy wysyłają żądanie uruchomienia menedżera kolejek do osobnego procesu działającego w globalnej przestrzeni nazw.

Jeśli różne metody administrowania programem IBM MQ nie działają w przypadku korzystania z usług terminalowych, należy spróbować ustawić prawo użytkownika `Utwórz obiekty globalne` .

Procedura

1. Otwórz panel Narzędzia administracyjne:

   Windows Server 2008 i Windows Server 2012
   Dostęp do tego panelu można uzyskać za pomocą opcji **Panel sterowania** > **System i konserwacja** > **Narzędzia administracyjne**.

   Windows 8.1
   Dostęp do tego panelu można uzyskać przy użyciu opcji **Narzędzia administracyjne** > **Zarządzanie komputerem** .
2. Kliknij dwukrotnie opcję **Zasady zabezpieczeń lokalnych**.
3. Rozwiń pozycję **Zasady lokalne**.
4. Kliknij opcję **Przypisanie praw użytkownika**.
5. Dodaj nowego użytkownika lub grupę do strategii `Utwórz obiekty globalne` .

Windows *Program obsługi wyjścia kanału SSPI w systemie Windows*

Produkt IBM 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 platformy Windows .

Wyjście zabezpieczeń udostępnia następujące usługi identyfikacji i uwierzytelniania:

uwierzytelnianie jednokierunkowe
W ten sposób obsługiwana jest obsługa uwierzytelniania menedżera LAN Windows NT (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 IBM WebSphere MQ 7.0.

Ta usługa jest zwykle używana w kanale MQI w celu włączenia menedżera kolejek serwera w celu uwierzytelnienia aplikacji IBM MQ MQI client . 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 IBM WebSphere MQ 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 umożliwia on menedżerowi kolejek serwera i aplikacji IBM MQ MQI client uwierzytelnianie siebie nawzajem. 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.

Windows *Stosowanie plików szablonów zabezpieczeń w systemie Windows*

Zastosowanie szablonu może mieć wpływ na ustawienia zabezpieczeń stosowane do plików i katalogów produktu IBM MQ . Jeśli używany jest szablon wysoce bezpieczny, należy go zastosować przed zainstalowaniem produktu IBM MQ.

Produkt 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 produkt 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 do plików i katalogów produktu IBM MQ . Jeśli chcesz użyć szablonu Highly Secure, skonfiguruj komputer przed zainstalowaniem produktu IBM MQ.

Jeśli szablon wysoce bezpieczny zostanie zastosowany do komputera, na którym jest już zainstalowany produkt IBM MQ , wszystkie uprawnienia ustawione w plikach i katalogach IBM 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.

Windows *Konfigurowanie dodatkowych uprawnień dla aplikacji Windows łączących się z produktem IBM MQ*

Konto, w ramach którego uruchomione procesy produktu IBM MQ może wymagać dodatkowej autoryzacji przed przyznaniem dostępu SYNCHRONIZE do procesów aplikacji, może być wymagane.

O tym zadaniu

Problemy mogą wystąpić, jeśli aplikacje produktu Windows , na przykład strony ASP, nawiązują połączenie z produktem IBM MQ , które są skonfigurowane do uruchamiania na poziomie bezpieczeństwa wyższym niż zwykle.

Program IBM MQ wymaga ZSYNCHRONIZOWANIA dostępu do procesów aplikacji w celu skoordynowania określonych działań. Gdy aplikacja serwera po raz pierwszy próbuje połączyć się z menedżerem kolejek IBM MQ , modyfikuje proces w celu nadania uprawnień SYNCHRONIZE administratorom produktu IBM MQ . Jednak konto, w ramach którego uruchamiane jest procesy IBM MQ , może wymagać dodatkowej autoryzacji, zanim będzie można uzyskać dostęp do żądanego dostępu.

Aby skonfigurować dodatkowe uprawnienia do identyfikatora użytkownika, w ramach którego działają procesy produktu IBM MQ , wykonaj następujące kroki:

Procedura

1. Uruchom narzędzie Zasady zabezpieczeń lokalnych, a następnie kliknij opcję **Ustawienia zabezpieczeń**->**Zasady lokalne**->**Przypisania do prawej strony użytkownika**, a następnie kliknij opcję **Debuguj programy**.
2. Kliknij dwukrotnie opcję **Debuguj programy**, a następnie dodaj identyfikator użytkownika produktu IBM MQ do listy.

   Jeśli system znajduje się w domenie 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.

IBM i Konfigurowanie zabezpieczeń w systemie IBM i

Zabezpieczenia w systemie IBM i są implementowane przy użyciu zabezpieczeń na poziomie obiektu IBM MQ Object Authority Manager (OAM) i IBM i .

Uwagi dotyczące zabezpieczeń, które należy uwzględnić podczas określania uprawnień dostępu do obiektów produktu IBM MQ .

Podczas konfigurowania uprawnień dla użytkowników w przedsiębiorstwie należy wziąć pod uwagę następujące kwestie:

1. Uprawnienia do nadawania i odbierania uprawnień do komend IBM MQ for IBM i za pomocą komend IBM i GRTOBJAUT i RVKOBJAUT .

   W bibliotece QMQM niektóre obiekty niezwiązane z komendą (* cmd) są ustawione tak, aby miały uprawnienie ***PUBLIC** do ***USE**. Nie należy zmieniać uprawnień do tych obiektów ani używać listy autoryzacji do udostępniania uprawnień. Wszelkie niepoprawne uprawnienia mogą spowodować naruszenie funkcjonalności produktu IBM MQ .
2. Podczas instalacji produktu IBM MQ for IBM itworzone są następujące specjalne profile użytkowników:

   QMQM
   Jest używany przede wszystkim dla wewnętrznych funkcji produktu. Można go jednak używać do uruchamiania zaufanych aplikacji przy użyciu opcji MQCNO_FASTPATH_BINDINGS. Więcej informacji na ten temat zawiera sekcja Nawiązywanie połączenia z menedżerem kolejek przy użyciu wywołania MQCONNX.

   QMQMADM
   Jest używany jako profil grupowy dla administratorów produktu IBM MQ. Profil grupowy umożliwia dostęp do komend CL i zasobów IBM MQ .

   W przypadku używania komendy SBMJOB do wprowadzania programów, które wywołują komendy IBM MQ , użytkownik nie może jawnie ustawić parametru QMQMADM. Zamiast tego należy ustawić wartość USER na QMQM lub inny profil użytkownika, dla którego określono QMQMADM jako grupę.

3. Jeśli komendy kanału są wysyłane do menedżerów kolejek zdalnych, należy upewnić się, że profil użytkownika jest członkiem grupy QMQMADM w systemie docelowym. Listę komend PCF i MQSC można znaleźć w sekcji Komendy CL programuIBM MQ for IBM i.
4. Zestaw grup powiązany z użytkownikiem jest buforowany, gdy autoryzacje grupowe są obliczane przez OAM.

   Wszystkie zmiany wprowadzone w elementach grupy użytkownika po umieszczaniu w pamięci podręcznej zestawu grup nie są rozpoznawane do czasu zrestartowania menedżera kolejek lub wykonania komendy RFRMQMAUT w celu odświeżenia zabezpieczeń.
5. Ogranicz liczbę użytkowników, którzy mają uprawnienia do pracy z komendami, które są szczególnie wrażliwe. Są to następujące komendy:
   - Tworzenie menedżera kolejek komunikatów (Create Message Queue Manager- CRTMQM)
   - Usunięcie menedżera kolejek komunikatów (Delete Message Queue Manager- DLTMQM)
   - Uruchomienie menedżera kolejek komunikatów (Start Message Queue Manager- STRMQM)
   - Zakończenie menedżera kolejek komunikatów (End Message Queue Manager- ENDMQM)
   - Uruchomienie serwera komend (Start Command Server- STRMQMCSVR)
   - Zakończenie serwera komend (End Command Server- ENDMQMCSVR)
6. Definicje kanałów zawierają specyfikację programu obsługi wyjścia zabezpieczeń. Tworzenie i modyfikowanie kanału wymaga szczególnej uwagi. Szczegółowe informacje na temat wyjść zabezpieczeń można znaleźć w sekcji “Wyjście zabezpieczeń-przegląd” na stronie 108.
7. Można zastąpić programy obsługi wyjścia kanału i monitora wyzwalacza. Zabezpieczeniem takich zastępów jest odpowiedzialność programisty.

IBM i Menedżer uprawnień do obiektów w systemie IBM i

Menedżer uprawnień do obiektów (Object Authority Manager-OAM) zarządza autoryzacjami użytkowników w celu manipulowania obiektami IBM MQ , w tym kolejkami i definicjami procesów. Udostępnia on także interfejs komend, za pomocą którego można nadawać lub odbierać uprawnienia dostępu do obiektu dla określonej grupy użytkowników. Decyzja zezwalania na dostęp do zasobu jest podejmowana przez OAM, a menedżer kolejek jest zgodny z tą decyzją. Jeśli OAM nie może podjąć decyzji, menedżer kolejek uniemożliwi dostęp do tego zasobu.

Za pośrednictwem OAM można sterować:

- Dostęp do obiektów produktu IBM MQ za pomocą interfejsu MQI. Gdy program użytkowy podejmuje próbę uzyskania dostępu do obiektu, OAM sprawdza, czy profil użytkownika, który zażądał żądania, ma autoryzację dla żądanej operacji.

  W szczególności oznacza to, że kolejki, a także komunikaty w kolejkach, mogą być chronione przed dostępem bez uprawnień.
- Uprawnienie do używania komend PCF i MQSC.

Różne grupy użytkowników mogą mieć różne uprawnienia dostępu do tego samego obiektu. Na przykład w przypadku konkretnej kolejki jedna grupa może wykonać operacje put i get; inna grupa może być dozwolona tylko w celu przeglądania kolejki (MQGET z opcją przeglądania). Podobnie niektóre grupy mogą mieć uprawnienia do pobierania i umieszczania uprawnień do kolejki, ale nie mogą zmieniać ani usuwać kolejki.

Komendy IBM MQ for IBM i i wykonywanie operacji na obiektach IBM MQ for IBM i

IBM i Uprawnienia IBM MQ w systemie IBM i

Aby uzyskać dostęp do obiektów IBM MQ , należy użyć uprawnień do wydania komendy i uzyskania dostępu do obiektu, do którego się odwołuje. Administratorzy mają dostęp do wszystkich zasobów produktu IBM MQ .

Dostęp do obiektów produktu IBM MQ jest kontrolowany przez uprawnienia do:

1. Wydaj komendę IBM MQ
2. Dostęp do obiektów IBM MQ , do których odwołuje się komenda

Wszystkie komendy CL produktu IBM MQ for IBM i są dostarczane z właścicielem QMQM, a profil administracyjny (QMQMADM) ma uprawnienia *USE z uprawnieniami *PUBLIC ustawionym na *EXCLUDE.

Uwaga: Program QSRDUPER jest używany przez instalator programu licencjonowanego IBM MQ for IBM i do duplikowania obiektów Command (*CMD) w bibliotece QSYS. W wersji IBM i V5R4 i nowszych program QSRDUPER został zmieniony w taki sposób, że domyślnym zachowaniem jest utworzenie komendy proxy, a nie duplikatu oryginalnej komendy. Komenda proxy przekieruje wykonanie komendy do innej komendy i ma atrybut PRX. Jeśli komenda proxy o tej samej nazwie, co kopiowana komenda, istnieje w bibliotece QSYS, uprawnienia prywatne do komendy proxy nie są nadawane komendzie w bibliotece produktu. Próby wyświetlenia lub uruchomienia komendy proxy w bibliotece QSYS sprawdzają uprawnienia komendy docelowej w bibliotece produktu. Wszelkie zmiany w uprawnieniach do obiektów *CMD należy więc wykonać w bibliotece produktu (QMQM), a te w bibliotece QSYS nie muszą być modyfikowane. Na przykład:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

Zmiany w strukturze uprawnień niektórych komend CL produktu pozwalają na publiczne korzystanie z tych komend, jeśli użytkownik posiada wymagane uprawnienia OAM do obiektów IBM MQ w celu wprowadzenia tych zmian.

Aby być administratorem produktu IBM MQ w systemie IBM i, użytkownik musi być członkiem grupy *QMQMADM*. Ta grupa ma właściwości podobne do właściwości grupy mqm w systemach UNIX, Linux i Windows . W szczególności, grupa QMQMADM jest tworzona podczas instalowania produktu IBM MQ for IBM i, a członkowie grupy QMQMADM mają dostęp do wszystkich zasobów systemu IBM MQ w systemie. Użytkownik ma również dostęp do wszystkich zasobów produktu IBM MQ , jeśli użytkownik ma uprawnienia *ALLOBJ.

Administratorzy mogą używać komend CL do administrowania produktem IBM MQ. Jedną z tych komend jest GRTMQMAUT, która jest używana do nadawania uprawnień innym użytkownikom. Inna komenda, STRMQMMQSC, umożliwia administratorowi wydawanie komend MQSC do lokalnego menedżera kolejek.

Pojęcia pokrewne

“Uprawnienie do administrowania produktem IBM MQ w systemie IBM i” na stronie 86

IBM i *Uprawnienia dostępu do obiektów IBM MQ w systemie IBM i*

Uprawnienia dostępu wymagane do uruchamiania komend CL programu IBM MQ .

IBM MQ for IBM i kategoryzuje komendy CL produktu na dwie grupy:

Grupa 1

Aby przetworzyć te komendy, użytkownicy muszą należeć do grupy użytkowników QMQMADM lub mieć uprawnienia *ALLOBJ. Użytkownicy posiadający jeden z tych uprawnień mogą przetwarzać wszystkie komendy we wszystkich kategoriach bez konieczności posiadania dodatkowych uprawnień.

Uwaga: Uprawnienia te zastępują dowolne uprawnienie OAM.

Komendy te mogą być pogrupowane w następujący sposób:

- Komendy serwera komend
  - ENDMQMCSVR, Serwer komend End IBM MQ
  - STRMQMCSVR, Uruchom Serwer komend IBM MQ
- Komenda procedury obsługi kolejki niedostarczanych komunikatów
  - STRMQMDLQ, Uruchom program IBM MQ Dead-Letter Queue Handler
- Komenda nasłuchiwania
  - ENDMQMLSR, Zakończenie programu nasłuchującego IBM MQ
  - STRMQMLSR, Uruchomienie obiektu nasłuchiwania bez obiektu

- Komendy odtwarzania
  - RCDMQMIMG, Rekord Obiekt IBM MQ -Obraz
  - RCRMQMOBJ, Re-tworzenie obiektu IBM MQ
  - WRKMQMTRN, Praca z transakcjami kolejkowymi IBM MQ
- Komendy menedżera kolejek
  - CRTMQM, Tworzenie menedżera kolejek komunikatów
  - DLTMQM, Usunięcie menedżera kolejek komunikatów
  - ENDMQM, Zakończenie menedżera kolejek komunikatów
  - STRMQM, Uruchomienie menedżera kolejek komunikatów
- Komendy ochrony
  - GRTMQMAUT, Nadanie uprawnień do obiektu IBM MQ
  - RVKMQMAUT, Revoke IBM MQ -Uprawnienia do obiektu
- Komenda śledzenia
  - TRCMQM, Śledzenie zadania IBM MQ
- Komendy transakcji
  - RSVMQMTRN, Rozstrzygnij transakcję IBM MQ
- Komendy monitora wyzwalacza
  - STRMQMTRM, Uruchom monitor wyzwalacza
- IBM MQKomendy SC
  - RUNMQSC, Uruchamianie Komendy SC IBM MQ
  - STRMQMMQSC, Uruchomienie Komendy SC IBM MQ

Grupa 2

Pozostałe komendy, dla których wymagane są dwa poziomy uprawnień:

1. IBM i , aby uruchomić komendę. Administrator IBM MQ ustawia to za pomocą komendy **GRTOBJAUT** , aby przesłonić ograniczenie *PUBLIC (*EXCLUDE) dla użytkownika lub grupy użytkowników.

   Na przykład:

   ```
   GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
   ```

2. Uprawnienie IBM MQ do manipulowania obiektami IBM MQ powiązanymi z komendą lub komendami, z uwagi na poprawne uprawnienia IBM i w kroku 1.

   Uprawnienie to jest kontrolowane przez użytkownika posiadającego odpowiednie uprawnienia OAM dla wymaganego działania, ustawionego przez administratora IBM MQ za pomocą komendy **GRTMQMAUT** .

   Na przykład:

   ```
   GRTMQMAUT *connect authority to the queue manager + *admchg authority to
           the queue
   ```

Komendy można pogrupować w następujący sposób:

- Komendy kanałów
  - CHGMQMCHL, Zmiana kanału IBM MQ

    Wymaga to * uprawnienia do połączenia z menedżerem kolejek oraz * uprawnienia admchg do kanału.

– CPYMQMCHL, Kopiowanie kanału IBM MQ

  Wymaga to * połączenia i * uprawnienia admcrt do menedżera kolejek, * uprawnienia admdsp do domyślnego typu kanału, który ma być skopiowany, oraz * uprawnienia admcrt do klasy obiektu kanału.

  Na przykład: kopiowanie kanału nadawczego wymaga uprawnienia * admdsp do systemu SYSTEM.DEF.SENDER

– CRTMQMCHL, Tworzenie kanału IBM MQ

  Wymaga to * połączenia i * uprawnienia admcrt do menedżera kolejek, * uprawnienia admdsp do domyślnego typu kanału, który ma zostać utworzony, oraz * uprawnienia admcrt do klasy obiektu kanału.

  Na przykład utworzenie kanału nadawczego wymaga uprawnienia * admdsp do systemu SYSTEM.DEF.SENDER

– DLTMQMCHL, Usunięcie kanału IBM MQ

  Wymaga to * uprawnienia do połączenia z menedżerem kolejek oraz * uprawnienia admdlt do kanału.

– RSVMQMCHL, Rozwiąż kanał IBM MQ

  Wymaga to * połączenia uprawnień do menedżera kolejek i * ctrlx uprawnienia do kanału.

• Wyświetl komendy

  Aby przetworzyć komendy DSP, należy nadać użytkownikowi uprawnienia `*connect` i `*admdsp` do menedżera kolejek, wraz z dowolną konkretną opcją:

  – DSPMQM, Wyświetlenie menedżera kolejek komunikatów
  – DSPMQMAUT, Wyświetlenie uprawnień do obiektu IBM MQ
  – DSPMQMAUTI, Wyświetlenie informacji uwierzytelniających IBM MQ - `*admdsp` do obiektu informacji uwierzytelniającej
  – DSPMQMCHL, Wyświetl kanał IBM MQ - `*admdsp` do kanału
  – DSPMQMCSVR, Wyświetlenie serwera komend IBM MQ
  – DSPMQMNL, Wyświetlenie listy nazw IBM MQ - `*admdsp` na liście nazw
  – DSPMQMOBJN, Wyświetlenie nazw obiektów IBM MQ
  – DSPMQMPRC, Wyświetlanie procesu IBM MQ - `*admdsp` w procesie
  – DSPMQMQ, Wyświetlenie kolejki IBM MQ - `*admdsp` do kolejki
  – DSPMQMTOP, Wyświetl temat IBM MQ - `*admdsp` do tematu

• Praca z komendami

  Aby przetworzyć komendy WRK i wyświetlić panel opcji, należy nadać użytkownikowi uprawnienia `*connect` i `*admdsp` uprawnienia do menedżera kolejek wraz z dowolną konkretną opcją:

  – WRKMQM, Praca z menedżerami kolejek komunikatów
  – WRKMQMAUT, Praca z uprawnieniami do obiektu IBM MQ
  – WRKMQMAUTD, Praca z danymi uprawnień do obiektu IBM MQ
  – WRKMQMAUTI, Praca z informacjami uwierzytelniających IBM MQ
    - `*admchg` dla komendy Zmiana obiektu informacji uwierzytelniającej IBM MQ .
    - `*admcrt` dla komendy Tworzenie i kopiowanie obiektu informacji uwierzytelniającej IBM MQ .
    - `*admdlt` dla komendy Usunięcie obiektu informacji uwierzytelniającej IBM MQ .
    - `*admdsp` dla komendy Wyświetlenie obiektu informacji uwierzytelniającej IBM MQ .
  – WRKMQMCHL, Praca z kanałem IBM MQ

    Wymaga to następujących uprawnień:

- *admchg dla komendy Zmiana kanału IBM MQ .
- *admclr dla komendy Usuwanie zawartości kanału IBM MQ .
- *admcrt dla komendy Tworzenie i kopiowanie kanału IBM MQ .
- *admdlt dla komendy Usuwanie kanału IBM MQ .
- *admdsp dla komendy Wyświetlenie kanału IBM MQ .
- *ctrl dla komendy Uruchomienie kanału IBM MQ .
- *ctrl dla komendy Zakończenie kanału IBM MQ .
- *ctrl dla komendy ping dla kanału IBM MQ .
- *ctrlx dla komendy resetowania kanału IBM MQ .
- *ctrlx dla komendy Rozstrzyganie kanału IBM MQ .

– WRKMQMCHST, Praca ze statusem kanału IBM MQ

  Wymaga to uprawnienia *admdsp do kanału.
– WRKMQMCL, Praca z klastrami IBM MQ
– WRKMQMCLQ, Praca z kolejkami klastrów IBM MQ
– WRKMQMCLQM, Praca z menedżerem kolejek klastra IBM MQ
– WRKMQMLSR, Praca z programem nasłuchującym IBM MQ
– WRKMQMMSG, Praca z komunikatami IBM MQ

  Wymaga to uprawnienia *browse do kolejki.
– WRKMQMNL, Praca z listami nazw IBM MQ

  Wymaga to następujących uprawnień:
  - *admchg for the Change IBM MQ Namelist command.
  - *admcrt dla komendy Tworzenie i kopiowanie listy nazw IBM MQ .
  - *admdlt for the Delete IBM MQ Namelist command.
  - *admdsp for the Display IBM MQ Namelist command.
– WRKMQMPRC, Praca z procesami IBM MQ

  Wymaga to następujących uprawnień:
  - *admchg dla komendy Zmiana procesu IBM MQ .
  - *admcrt dla komendy Tworzenie i kopiowanie IBM MQ procesu.
  - *admdlt dla komendy Usunięcie procesu IBM MQ .
  - *admdsp dla komendy Wyświetlanie IBM MQ procesu.
– WRKMQMQ, Praca z kolejkami IBM MQ

  Wymaga to następujących uprawnień:
  - *admchg for the Change IBM MQ Queue command.
  - *admclr dla komendy Usuwanie zawartości kolejki IBM MQ .
  - *admcrt dla komendy Tworzenie i kopiowanie kolejki IBM MQ .
  - *admdlt for the Delete IBM MQ Queue command.
  - *admdsp for the Display IBM MQ Queue command.
– WRKMQMQSTS, Praca ze statusem kolejki IBM MQ
– WRKMQMTOP, Praca z tematami programu IBM MQ

  Wymaga to następujących uprawnień
  - *admchg dla komendy Zmiana tematu IBM MQ .
  - *admcrt dla komendy Tworzenie i kopiowanie tematu IBM MQ .

- `*admdlt` for the Delete IBM MQ Topic command.
- `*admdsp` for the Display IBM MQ Topic command.

– WRKMQMSUB, Praca z subskrypcjami IBM MQ

- Inne komendy kanału

  Aby przetworzyć komendy kanału, należy nadać użytkownikowi wymienione uprawnienia szczegółowe:

  – ENDMQMCHL, Kanał końcowy IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*allmqi` do kolejki transmisji powiązanej z kanałem.

  – ENDMQMLSR, Zakończenie programu nasłuchującego IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*ctrl` do nazwanego obiektu nasłuchiwania.

  – PNGMQMCHL, Kanał IBM MQ Ping

    Wymaga to uprawnienia `*connect` i `*inq` do menedżera kolejek i uprawnienia `*ctrl` do obiektu kanału.

  – RSTMQMCHL, resetowanie kanału IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek.

  – STRMQMCHL, Uruchamianie kanału IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*ctrl` do obiektu kanału.

  – STRMQMCHLI, Uruchomienie inicjatora kanału IBM MQ

    Wymaga to uprawnień `*connect` i `*inq` do menedżera kolejek, a uprawnienia `*allmqi` do kolejki inicjuj powiązanej z kolejką transmisji kanału.

  – STRMQMLSR, Uruchom program nasłuchujący IBM MQ

    Wymaga to * połączenia uprawnień do menedżera kolejek i * uprawnienia ctrl do nazwanego obiektu nasłuchiwania.

- Inne komendy:

  Aby przetworzyć następujące komendy, należy nadać użytkownikowi wymienione uprawnienia szczegółowe:

  – CCTMQM, Połącz z menedżerem kolejek komunikatów

    Nie wymaga to uprawnień do obiektu IBM MQ .

  – CHGMQM, Zmiana menedżera kolejek komunikatów

    Wymaga to uprawnienia `*connect` i `*admchg` do menedżera kolejek.

  – CHGMQMAUTI, Zmiana Informacji Uwierzytelniania IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek oraz uprawnienia `*admchg` i `*admdsp` do obiektu informacji uwierzytelniających.

  – CHGMQMNL, Zmiana listy nazw IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admchg` do listy nazw.

  – CHGMQMPRC, Zmiana procesu IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admchg` do procesu.

  – CHGMQMQ, Zmiana kolejki IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admchg` do kolejki.

  – CLRMQMQ, Wyczyść kolejkę IBM MQ

Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admclr do kolejki.

- CPYMQMAUTI, Kopiowanie informacji uwierzytelniających IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admdsp do obiektu informacji uwierzytelniających oraz do uprawnienia *admcrt do klasy obiektu informacji uwierzytelniającej.

- CPYMQMNL, Kopiowanie listy nazw IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek.

- CPYMQMPRC, Kopiowanie procesu IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek.

- CPYMQMQ, Kopiowanie kolejki IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek.

- CRTMQMAUTI, Tworzenie Informacji Uwierzytelniania IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admdsp do obiektu informacji uwierzytelniających oraz do uprawnienia *admcrt do klasy obiektu informacji uwierzytelniającej.

- CRTMQMNL, Tworzenie listy nazw IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek i uprawnienia *admdsp do domyślnej listy nazw.

- CRTMQMPRC, Tworzenie procesu IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek i uprawnienia *admdsp do procesu domyślnego.

- CRTMQMQ, Tworzenie kolejki IBM MQ

  Wymaga to uprawnienia *connect i *admcrt do menedżera kolejek i uprawnienia *admdsp do kolejki domyślnej.

- CVTMQMDTA, Konwersja Komendy Typ Danych IBM MQ

  Nie wymaga to uprawnień do obiektu IBM MQ .

- DLTMQMAUTI, Usunięcie Informacji Uwierzytelniania IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *ctrlx do obiektu informacji uwierzytelniających.

- DLTMQMNL, Usunięcie listy nazw IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admdlt do listy nazw.

- DLTMQMPRC, Usuwanie procesu IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admdlt do procesu.

- DLTMQMQ, Usunięcie Kolejki IBM MQ

  Wymaga to uprawnienia *connect do menedżera kolejek i uprawnienia *admdlt do kolejki.

- DSCMQM, Odłącz od menedżera kolejek komunikatów

  Nie wymaga to uprawnień do obiektu IBM MQ .

- RFRMQMAUT, Odśwież zabezpieczenia

  Wymaga to uprawnienia *connect do menedżera kolejek.

- RFRMQMCL, Odśwież klaster

  Wymaga to uprawnienia *connect do menedżera kolejek.

- RSMMQMCLQM, Wznów menedżer kolejek klastra

  Wymaga to uprawnienia *connect do menedżera kolejek.

– RSTMQMCL, Resetowanie klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

– SPDMQMCLQM, Zawieś menedżer kolejek klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

IBM i *Autoryzacje dostępu w systemie IBM i*

Ten temat zawiera informacje na temat komend autoryzacji dostępu.

Autoryzacje zdefiniowane przez słowo kluczowe AUT w komendach GRTMQMAUT i RVKMQMAUT można sklasyfikować w następujący sposób:

- Autoryzacje związane z wywołaniami MQI
- Komendy administracyjne związane z autoryzacją
- Autoryzacje kontekstowe
- Ogólne autoryzacje, to znaczy dla wywołań MQI, dla komend lub obu

Poniższe tabele zawierają listę różnych uprawnień, korzystając z parametru AUT dla wywołań MQI, wywołań kontekstu, komend MQSC i PCF oraz operacji ogólnych.

Tabela 15. Autoryzacje dla wywołań MQI

AUT	Opis
*ALTUSR	Zezwól na użycie uprawnień innego użytkownika na potrzeby wywołań MQOPEN i MQPUT1 .
*BROWSE	Pobierz komunikat z kolejki, wydając wywołanie MQGET z opcją BROWSE.
*CONNECT	Połącz aplikację z określonym menedżerem kolejek, wywołując wywołanie MQCONN.
*GET	Pobierz komunikat z kolejki, wydając wywołanie MQGET.
*INQ	Wprowadź zapytanie w konkretnej kolejce, wydając wywołanie MQINQ.
*PUB	Otwórz temat, aby opublikować komunikat przy użyciu wywołania MQPUT.
*PUT	Umieść komunikat w określonej kolejce, wydając wywołanie MQPUT.
*RESUME	Wznów subskrypcję przy użyciu wywołania MQSUB.
*SET	Ustaw atrybuty w kolejce na podstawie interfejsu MQI, wywołując wywołanie MQSET. Jeśli kolejka jest otwierana dla wielu opcji, użytkownik musi być autoryzowany dla każdego z nich.
*SUB	Utwórz, Alter lub Wznów subskrypcję do tematu za pomocą wywołania MQSUB.

Tabela 16. Autoryzacje dla wywołań kontekstowych

AUT	Opis
*PASSALL	Przekaz cały kontekst w określonej kolejce. Wszystkie pola kontekstu są kopiowane z oryginalnego żądania.
*PASSID	Przekaz kontekst tożsamości w podanej kolejce. Kontekst tożsamości jest taki sam jak kontekst żądania.
*SETALL	Ustaw cały kontekst dla podanej kolejki. Opcja ta jest używana przez specjalne programy narzędziowe systemu.
*SETID	Ustaw kontekst tożsamości dla podanej kolejki. Opcja ta jest używana przez specjalne programy narzędziowe systemu.

Tabela 17. Autoryzacje dla wywołań MQSC i PCF	
AUT	**Opis**
*ADMCHG	Zmiana atrybutów określonego obiektu.
*ADMCLR	Wyczyść określony obiekt (tylko komenda czyszczenia obiektu PCF).
*ADMCRT	Utwórz obiekty określonego typu.
*ADMDLT	Usuń określony obiekt.
*ADMDSP	Wyświetl atrybuty określonego obiektu.

Tabela 18. Autoryzacje dla operacji ogólnych	
AUT	**Opis**
*ALL	Użyj wszystkich operacji mających zastosowanie do obiektu. Uprawnienie `all` jest odpowiednikiem unii uprawnień `alladm`, `allmqi` i `system` odpowiednich dla danego typu obiektu.
*ALLADM	Wykonaj wszystkie operacje administracyjne mające zastosowanie do obiektu.
*ALLMQI	Użyj wszystkich wywołań MQI mających zastosowanie do obiektu.
*CTRL	Sterowanie uruchamianiem i zamykaniem kanałów, programów nasłuchujących i usług.
*CTRLX	Resetuj numer kolejny i rozstrzygnij kanały wątpliwe.

IBM i *Korzystanie z komend autoryzacji dostępu w systemie IBM i*

Te informacje umożliwiają zapoznanie się z komendami autoryzacji dostępu oraz przykłady użycia komend.

Korzystanie z komendy GRTMQMAUT

Jeśli masz wymagane uprawnienia, możesz użyć komendy GRTMQMAUT , aby nadać uprawnienia do profilu użytkownika lub grupy użytkowników w celu uzyskania dostępu do określonego obiektu. W poniższych przykładach przedstawiono sposób użycia komendy GRTMQMAUT :

1. ```
   GRTMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
             AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
   ```

   W tym przykładzie:

   - RED.LOCAL.QUEUE jest nazwą obiektu.
   - *LCLQ (kolejka lokalna) jest typem obiektu.
   - GROUPA to nazwa profilu użytkownika w systemie, dla którego mają zostać zmienione autoryzacje. Ten profil może być używany jako profil grupowy dla innych użytkowników.
   - *BROWSE i *PUT są autoryzacjami nadawanych do określonej kolejki.

     Produkt *BROWSE dodaje autoryzację do przeglądania komunikatów w kolejce (w celu wydania komendy MQGET z opcją przeglądania).

     *PUT dodaje autoryzację do umieszczania (MQPUT) komunikatów w kolejce.
   - `saturn.queue.manager` jest nazwą menedżera kolejek.
2. Następująca komenda nadaje użytkownikom JACK i JILL wszystkie odpowiednie autoryzacje, dla wszystkich definicji procesów, dla domyślnego menedżera kolejek.
   ```

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
```

3. Następująca komenda nadaje użytkownikowi GEORGE uprawnienia do umieszczania komunikatu w kolejce ORDERSw menedżerze kolejek TRENT.

```
GRTMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
GRTMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
```

Korzystanie z komendy RVKMQMAUT

Jeśli masz wymagane uprawnienia, możesz użyć komendy RVKMQMAUT , aby usunąć wcześniej nadane uprawnienia profilu użytkownika lub grupy użytkowników w celu uzyskania dostępu do określonego obiektu. W poniższych przykładach przedstawiono sposób użycia komendy RVKMQMAUT :

1.
```
RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
AUT(*PUT) MQMNAME('saturn.queue.manager')
```

   Uprawnienia do umieszczania komunikatów w określonej kolejce, która została nadana w poprzednim przykładzie, są usuwane dla GROUPA.

2.
```
RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
MQMNAME(PAYROLLQM)
```

   Uprawnienia do pobierania komunikatów z dowolnej kolejki o nazwie rozpoczynający się od znaków PAY, których właścicielem jest menedżer kolejek PAYROLLQM, są usuwane ze wszystkich użytkowników systemu, chyba że lub grupa, do której one należą, zostały autoryzowane oddzielnie.

Korzystanie z komendy DSPMQMAUT

Wyświetlanie uprawnień MQM (DSPMQMAUT) pokazuje, dla podanego obiektu i użytkownika, listę autoryzacji, które użytkownik posiada dla danego obiektu. W poniższym przykładzie przedstawiono sposób użycia komendy:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

Korzystanie z komendy RFRMQMAUT

Odświeżanie zabezpieczeń MQM (RFRMQMAUT) umożliwia natychmiastowe zaktualizowanie informacji o grupie autoryzacji OAM, odzwierciedlając zmiany wprowadzone na poziomie systemu operacyjnego, bez konieczności zatrzymywania i restartowania menedżera kolejek. W poniższym przykładzie przedstawiono sposób użycia komendy:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i Tabele specyfikacji autoryzacji w systemie IBM i

Te informacje umożliwiają określenie, jakie uprawnienia są wymagane do korzystania z określonych wywołań interfejsu API, a także poszczególnych opcji tych wywołań, obiektów kolejek, obiektów procesów i obiektów menedżera kolejek.

Tabele specyfikacji autoryzacji, które rozpoczynają się w programie Tabela 19 na stronie 169 , definiują dokładnie sposób działania autoryzacji 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 dane:

Działanie do wykonania
Opcja MQI, komenda MQSC lub komenda PCF.

Obiekt kontroli dostępu
Kolejka, definicja procesu, menedżer kolejek, lista nazw, kanał, kanał połączenia klienta, obiekt nasłuchiwania, usługa lub obiekt informacji uwierzytelniającej.

Wymagane uprawnienia
Wyrażony jako stała MQZAO_.

W tabelach stałe przedrostki przedrostków MQZAO_ odpowiadają słowom kluczom na liście autoryzacji dla komend **GRTMQMAUT** i **RVKMQMAUT** dla konkretnej jednostki. Na przykład komenda MQZAO_BROWSE odpowiada słowom kluczowym *BROWSE . podobnie, słowo kluczowe MQZAO_SET_ALL_CONTEXT odpowiada słowie kluczowym *SETALL, itd. Te stałe są zdefiniowane w pliku nagłówkowego cmqzc.h, który jest dostarczany razem z produktem.

Autoryzacje MQI

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 wymagają sprawdzenia autoryzacji: MQCONN, MQOPEN, MQPUT1i MQCLOSE.

W przypadku operacji MQOPEN i MQPUT1kontrola uprawnień jest dokonywana na podstawie nazwy otwieranego obiektu, a nie nazwy lub nazw, co spowodowało, że nazwa została rozwiązana. Na przykład można nadać aplikacji uprawnienie do otwarcia kolejki aliasowej bez posiadania uprawnień do otwierania kolejki podstawowej, do której alias jest tłumaczona. Reguła polega na tym, że sprawdzenie jest przeprowadzane na pierwszej definicji napotkanej podczas procesu rozstrzygania nazw, który nie jest aliasem menedżera kolejek, chyba że definicja aliasu menedżera kolejek jest otwierana bezpośrednio, to znaczy, że jej nazwa pojawia się w polu *ObjectName* deskryptora obiektu. Uprawnienia są zawsze wymagane dla danego obiektu otwieranego; w niektórych przypadkach wymagane jest dodatkowe uprawnienie niezależne od kolejki, uzyskane za pomocą autoryzacji dla obiektu menedżera kolejek.

Tabela 19 na stronie 169, Tabela 20 na stronie 169, Tabela 21 na stronie 170i Tabela 22 na stronie 171 podsumowują autoryzacje wymagane dla każdego wywołania.

Uwaga: W tych tabelach nie są wymieniane listy nazw, kanały, kanały połączeń klientów, obiekty nasłuchiwania, usługi lub obiekty 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.

Tabela 19. Autoryzacja zabezpieczeń wymagana dla wywołań MQCONN

Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCONN, opcja	Nie dotyczy	Nie dotyczy	MQZAO_CONNECT

Tabela 20. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN

Wymagana autoryzacja dla:	**Obiekt kolejki (“1” na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_INQUIRE	MQZAO_INQUIRE **(“2” na stronie 171)**	MQZAO_INQUIRE **(“2” na stronie 171)**	MQZAO_INQUIRE **(“2” na stronie 171)**

Tabela 20. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN (kontynuacja)			
Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_BROWSE	MQZAO_PRZEGLĄDANIE	Nie dotyczy	Brak sprawdzenia
MQOO_INPUT_ *	MQZAO_INPUT	Nie dotyczy	Brak sprawdzenia
MQOO_SAVE_ ALL_CONTEXT **("3" na stronie 171)**	MQZAO_INPUT	Nie dotyczy	Nie dotyczy
MQOO_OUTPUT (normalna kolejka) **("4" na stronie 171)**	MQZAO_OUTPUT	Nie dotyczy	Nie dotyczy
MQOO_PASS_ IDENTITY_CONTEXT **("5" na stronie 171)**	MQZAO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	Nie dotyczy	Brak sprawdzenia
MQOO_PASS_ALL_ CONTEXT **("5" na stronie 171, "6" na stronie 171)**	MQZAO_PASS _ALL_CONTEXT	Nie dotyczy	Brak sprawdzenia
MQOO_SET_ IDENTITY_CONTEXT **("5" na stronie 171, "6" na stronie 171)**	MQZAO_SET_ KONTEKST_IDENTYFIKATORA	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("7" na stronie 171)**
MQOO_SET_ ALL_CONTEXT **("5" na stronie 171, "8" na stronie 171)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("7" na stronie 171)**
MQOO_OUTPUT (kolejka transmisji) **("9" na stronie 171)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("7" na stronie 171)**
MQOO_SET	MQZAO_SET	Nie dotyczy	Brak sprawdzenia
MQOO_ALTERNATE_ USER_AUTHORITY	**("10" na stronie 171)**	**("10" na stronie 171)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("10" na stronie 171, "11" na stronie 172)**

Tabela 21. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1			
Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_ TOŻSAMOŚCI_TOŻSAMOŚCI	MQZAO_PASS_ IDENTITY_CONTEXT **("12" na stronie 172)**	Nie dotyczy	Brak sprawdzenia
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **("12" na stronie 172)**	Nie dotyczy	Brak sprawdzenia
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **("12" na stronie 172)**	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("7" na stronie 171)**

Tabela 21. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1 (kontynuacja)			
Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("12" na stronie 172)**	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("7" na stronie 171)**
(Kolejka transmisji) **("9" na stronie 171)**	MQZAO_SET_ ALL_CONTEXT	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("7" na stronie 171)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**("13" na stronie 172)**	Nie dotyczy	MQZAO_ALTERNATE_ USER_AUTHORITY **("11" na stronie 172)**

Tabela 22. Autoryzacja zabezpieczeń wymagana dla wywołań MQCLOSE			
Wymagana autoryzacja dla:	**Obiekt kolejki ("1" na stronie 171)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCO_DELETE	MQZAO_DELETE **("14" na stronie 172)**	Nie dotyczy	Nie dotyczy
MQCO_DELETE _PURGE	MQZAO_DELETE **("14" na stronie 172)**	Nie dotyczy	Nie dotyczy

Uwagi dotyczące tabel:

1. Jeśli otwierana jest kolejka modelowa:
   - 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. Sprawdzany jest obiekt kolejki, procesu, listy nazw lub menedżera kolejek, w zależności od typu otwieranego obiektu.
3. Parametr MQOO_INPUT_ * musi być również określony. Ta opcja jest poprawna dla lokalnej, modelowej lub aliasowej kolejki.
4. To sprawdzenie jest wykonywane dla wszystkich przypadków wyjściowych, z wyjątkiem przypadku określonego w uwadze "9" na stronie 171.
5. Należy również określić parametr MQOO_OUTPUT.
6. Opcja MQOO_PASS_IDENTITY_CONTEXT jest również implikowana przez tę opcję.
7. Uprawnienie to jest wymagane zarówno dla obiektu menedżera kolejek, jak i dla konkretnej kolejki.
8. Opcja ta oznacza również parametr mqoo_pass_identity_context, mqoo_pass_all_context i MQOO_SET_IDENTITY_CONTEXT.
9. 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).
10. Należy również określić co najmniej jedną z następujących wartości: MQOO_INQUIRE (dla dowolnego typu obiektu) lub (dla kolejek): MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET. 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.

11. Ta autoryzacja umożliwia określenie dowolnego identyfikatora *AlternateUser* .
12. Sprawdzenie MQZAO_OUTPUT jest przeprowadzane również wtedy, gdy kolejka nie ma atrybutu kolejki *Użycie* w tabeli MQUS_TRANSMISSION.
13. Przeprowadzone sprawdzenie jest tak, jak w przypadku pozostałych określonych opcji, przy użyciu podanego identyfikatora użytkownika alternatywnego dla nazwanego uprawnienia do kolejki oraz bieżącego uprawnienia do aplikacji dla sprawdzania identyfikatora MQZAO_ALTERNATE_USER_IDENTIFIER.
14. Kontrola jest przeprowadzana tylko wtedy, gdy spełnione są oba poniższe stwierdzenia:
    - Trwała kolejka dynamiczna jest zamykana i usuwana.
    - Kolejka nie została utworzona przez komendę MQOPEN, która zwróciła uchwyt obiektu, który jest używany.

    W przeciwnym razie nie będzie sprawdzania.

Uwagi ogólne:

1. Specjalna autoryzacja MQZAO_ALL_MQI zawiera wszystkie następujące autoryzacje, które są istotne dla danego typu obiektu:
   - MQZAO_CONNECT
   - MQZAO_ZAPYTANIE_O
   - MQZAO_SET
   - MQZAO_PRZEGLĄDANIE
   - MQZAO_INPUT
   - MQZAO_OUTPUT
   - MQZAO_PASS_IDENTITY_CONTEXT
   - MQZAO_PASS_ALL_CONTEXT
   - MQZAO_SET_IDENTITY_CONTEXT
   - MQZAO_SET_ALL_CONTEXT,
   - MQZAO_ALTERNATE_USER_AUTHORITY
2. MQZAO_DELETE (patrz uwaga “14” na stronie 172) i MQZAO_DISPLAY są sklasyfikowane jako autoryzacje administracyjne. W związku z tym nie są one uwzględniane w MQZAO_ALL_MQI.
3. *Brak sprawdzania* oznacza, że sprawdzanie autoryzacji nie jest przeprowadzane.
4. *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie ma znaczenia dla tej operacji. Na przykład nie można wywołać wywołania MQPUT dla obiektu procesu.

IBM i *Autoryzacje komend MQSC w komendach PCF o zmienionym znaczeniu w systemie IBM i*

Te autoryzacje umożliwiają użytkownikowi wydawanie komend administracyjnych w postaci komunikatu o przedwczesnym zakończeniu działania PCF. Metody te pozwalają programowi na wysłanie komendy administracyjnej jako komunikatu do menedżera kolejek w celu wykonania w imieniu tego użytkownika.

W tej sekcji podsumowano autoryzacje wymagane dla każdej komendy MQSC zawartej w programie Escape PCF.

Nie dotyczy oznacza, że sprawdzanie autoryzacji nie ma znaczenia dla tej operacji.

ID użytkownika, pod którym uruchomiony jest program uruchamiający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie DISPLAY w menedżerze kolejek w celu wykonania komend PCF

- Uprawnienie do wydawania komend 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

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

DEFINE *obiekt* NOREPLACE (“1” na stronie 176)

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CREATE **(“2” na stronie 177)**
Temat	MQZAO_CREATE **(“2” na stronie 177)**
Proces	MQZAO_CREATE **(“2” na stronie 177)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(“2” na stronie 177)**
Informacje uwierzytelniające	MQZAO_CREATE **(“2” na stronie 177)**
Kanał	MQZAO_CREATE **(“2” na stronie 177)**
Kanał połączenia klienta	MQZAO_CREATE **(“2” na stronie 177)**

Obiekt	Wymagane uprawnienia
Program nasłuchujący	MQZAO_CREATE **(“2” na stronie 177)**
Usługa	MQZAO_CREATE **(“2” na stronie 177)**

DEFINE *obiekt* REPLACE (“1” na stronie 176, “3” na stronie 177)

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

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

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

Obiekt	Wymagane uprawnienia
Kanał	MQZAO_DISPLAY
Kanał połączenia klienta	MQZAO_DISPLAY
Program nasłuchujący	
Usługa	

KANAŁ PING

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	Nie dotyczy
Usługa	Nie dotyczy

Resetuj kanał

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_EXTENDED
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

Rozstrzyganie kanału

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy

Obiekt	Wymagane uprawnienia
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL_EXTENDED
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

START *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

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

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 GRTMQMAUT .
3. Ta opcja ma zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli tak nie jest, sprawdzanie jest tak, jak w przypadku opcji DEFINE *obiekt* NOREPLACE.

IBM i *Autoryzacje dla komend PCF w systemie IBM i*

Te autoryzacje umożliwiają użytkownikowi wydawanie komend administracyjnych jako komend PCF. Metody te pozwalają programowi na wysłanie komendy administracyjnej jako komunikatu do menedżera kolejek w celu wykonania w imieniu tego użytkownika.

W tej sekcji podsumowano autoryzacje wymagane dla każdej komendy PCF.

Brak sprawdzania oznacza, że sprawdzanie autoryzacji nie jest przeprowadzane; *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie ma znaczenia dla tej operacji.

ID użytkownika, pod którym uruchomiony jest program uruchamiający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie DISPLAY w menedżerze kolejek w celu wykonania komend PCF

Specjalna autoryzacja MQZAO_ALL_ADMIN obejmuje następujące autoryzacje:

- ZMIANA MQZAO_CHANGE
- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_DISPLAY
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

MQZAO_CREATE nie jest uwzględniany, ponieważ 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

Wyczyść *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CLEAR

Obiekt	Wymagane uprawnienia
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

Kopiuj *obiekt* (bez zastępowania) (“1” na stronie 182)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(“2” na stronie 182)**
Temat	MQZAO_CREATE **(“2” na stronie 182)**
Proces	MQZAO_CREATE **(“2” na stronie 182)**
Menedżer kolejek	Nie dotyczy
NamelistMQZAO_CREATE	MQZAO_CREATE **(“2” na stronie 182)**
Informacje uwierzytelniające	MQZAO_CREATE **(“2” na stronie 182)**
Kanał	MQZAO_CREATE **(“2” na stronie 182)**
Kanał połączenia klienta	MQZAO_CREATE **(“2” na stronie 182)**
Program nasłuchujący	MQZAO_CREATE **(“2” na stronie 182)**
Usługa	MQZAO_CREATE **(“2” na stronie 182)**

Kopiowanie obiektu *object* (z zastępem) (“1” na stronie 182, “4” na stronie 183)

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

Utwórz obiekt *obiekt* (bez zastępowania) (“3” na stronie 183)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(“2” na stronie 182)**
Temat	MQZAO_CREATE **(“2” na stronie 182)**
Proces	MQZAO_CREATE **(“2” na stronie 182)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(“2” na stronie 182)**
Informacje uwierzytelniające	MQZAO_CREATE **(“2” na stronie 182)**
Kanał	MQZAO_CREATE **(“2” na stronie 182)**
Kanał połączenia klienta	MQZAO_CREATE **(“2” na stronie 182)**
Program nasłuchujący	ZMIANA MQZAO_CHANGE
Usługa	ZMIANA MQZAO_CHANGE

Utwórz obiekt *obiekt* (z zastąpami) (“3” na stronie 183, “4” na stronie 183)

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

Usuń *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DELETE
Temat	MQZAO_DELETE
Proces	MQZAO_DELETE
Menedżer kolejek	MQZAO_DELETE
Lista nazw	MQZAO_DELETE
Informacje uwierzytelniające	MQZAO_DELETE
Kanał	MQZAO_DELETE
Kanał połączenia klienta	MQZAO_DELETE
Program nasłuchujący	MQZAO_DELETE

Obiekt	Wymagane uprawnienia
Usługa	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

Sprawdź nazwy *obiektu*

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

Kanał ping

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

Obiekt	Wymagane uprawnienia
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

Resetowanie kanału

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_EXTENDED
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

Resetuj statystyki kolejki

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_DISPLAY i MQZAO_CHANGE
Temat	Nie dotyczy
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	
Usługa	

Rozstrzyganie kanału

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy

Obiekt	Wymagane uprawnienia
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL_EXTENDED
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

Uruchom kanał

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	Nie dotyczy
Usługa	Nie dotyczy

Zamknij kanał

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	Nie dotyczy
Usługa	Nie dotyczy

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 GRTMQMAUT .

3. W przypadku komend Create wymagane jest również uprawnienie MQZAO_DISPLAY dla odpowiedniego SYSTEM.DEFAULT.* .
4. Ta opcja ma zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli tak nie jest, sprawdzanie jest tak samo jak w przypadku kopiowania lub tworzenia bez zastępowania.

IBM i Ogólne profile OAM w systemie IBM i

Profile ogólne menedżera uprawnień do obiektów (OAM) umożliwiają ustawienie uprawnień użytkownika na wiele obiektów jednocześnie, a nie konieczności wydawania osobnych komend **GRTMQMAUT** dla każdego pojedynczego obiektu podczas jego tworzenia. Użycie profili ogólnych w komendzie **GRTMQMAUT** umożliwia ustawienie uprawnień ogólnych dla wszystkich tworzonych przyszłych obiektów, które pasują do tego profilu.

W dalszej części tej sekcji opisano bardziej szczegółowe informacje o użyciu profili ogólnych:

- "Korzystanie ze znaków wieloznacznych" na stronie 183
- "Priorytety profilu" na stronie 183

Korzystanie ze znaków wieloznacznych

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 wartość ABC.?EF, autoryzacja, którą podasz temu profilowi, dotyczy wszystkich obiektów utworzonych przy użyciu nazw ABC.DEF, ABC.CEF, ABC.BEFitd.

Dostępne są następujące znaki wieloznaczne:

?

Znak zapytania (?) zastępuje pojedynczy znak. Na przykład: AB.?D będzie mieć 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 nazwie ABC.DEF.GHI kwalifikatorami są ABC, DEF oraz GHI.

  Na przykład: ABC.*.JKL będzie mieć zastosowanie do obiektów ABC.DEF.JKLi ABC.GHI.JKL. (Należy pamiętać, że **nie** będzie mieć zastosowanie 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 będzie mieć zastosowanie do obiektów ABC.DE.JKL, ABC.DEF.JKLi ABC.DEGH.JKL.

******

Użyj dwukrotnego znaku gwiazdki (**) ***jeden raz*** w nazwie profilu jako:

- Nazwa całego profilu, która będzie zgodna ze wszystkimi nazwami obiektów. Jeśli na przykład w celu identyfikowania procesów używany jest parametr OBJTYPE （*PRC）, 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.

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:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

Pierwsza z nich daje uprawnienie do umieszczania wszystkich kolejek dla nazwy użytkownika FRED 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 parametr GRTMQMAUT. 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 poprzednim 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. **

IBM i Określanie zainstalowanej usługi autoryzacji w systemie IBM i

Istnieje możliwość określenia, który komponent usługi autoryzacji ma być używany.

The parameter **Service Component name** on **GRTMQMAUT** and **RVKMQMAUT** allows you to specify the name of the installed authorization service component.

Wybranie opcji **F24** na panelu początkowym, po którym następuje **F9=All parametry** na następnym panelu komendy, umożliwia określenie zainstalowanego komponentu autoryzacji (*DFT) lub nazwy wymaganego komponentu usługi autoryzacji określonego w sekcji Service w pliku qm.ini menedżera kolejek.

Produkt **DSPMQMAUT** ma również ten dodatkowy parametr. Ten parametr umożliwia wyszukiwanie wszystkich zainstalowanych komponentów autoryzacji (*DFT) lub określonej nazwy komponentu usługi autoryzacji, dla określonej nazwy obiektu, typu obiektu i użytkownika.

IBM i Praca z profilami uprawnień i bez nich w systemie IBM i

Ta sekcja zawiera informacje na temat pracy z profilami uprawnień oraz sposobu pracy bez profili uprawnień.

Użytkownik może pracować z profilami uprawnień, zgodnie z wyjaśnieniami w programie “Praca z profilami uprawnień” na stronie 184, lub bez nich, zgodnie z wyjaśnieniami w tym miejscu:

Aby pracować bez profili uprawnień, należy użyć parametru *NONE jako parametru uprawnień w produkcie **GRTMQMAUT** w celu utworzenia profili bez uprawnień. Powoduje to, że wszystkie istniejące profile pozostaną niezmienione.

W systemie **RVKMQMAUT**należy użyć parametru *REMOVE jako parametru uprawnień, aby usunąć istniejący profil uprawnień.

Praca z profilami uprawnień

Z profilowaniem uprawnień powiązane są dwie komendy:

- **WRKMQMAUT**
- **WRKMQMAUTD**

Dostęp do tych komend można uzyskać bezpośrednio z poziomu wiersza komend lub z poziomu panelu WRKMQM:

1. Wpisz nazwę menedżera kolejek i naciśnij klawisz `Enter` , aby uzyskać dostęp do panelu wyników programu **WRKMQM** .
2. Wybranie opcji F23=`More options` na tym panelu.

Opcja 24 wybiera panel wyników dla komendy **WRKMQMAUT** , a opcja 25 powoduje wybranie komendy **WRKMQMAUTI** , która jest używana z warstwą powiązań SSL.

WRKMQMAUT

Ta komenda umożliwia pracę z danymi uprawnień przechowywanych w kolejce uprawnień.

Uwaga: Aby uruchomić tę komendę, użytkownik musi mieć uprawnienia `*connect` i `*admdsp` do menedżera kolejek. Aby jednak utworzyć lub usunąć profil, należy mieć uprawnienie QMQMADM.

Jeśli informacje zostaną wyświetlone na ekranie, zostanie wyświetlona lista nazw profili uprawnień wraz z ich typami. W przypadku drukowania danych wyjściowych zostanie wyświetlona szczegółowa lista wszystkich danych uprawnień, zarejestrowanych użytkowników i ich uprawnień.

Wprowadzenie nazwy obiektu lub profilu na tym panelu i naciśnięcie klawisza ENTER powoduje przejście do panelu wyników dla programu **WRKMQMAUT** .

Jeśli wybierzesz opcję 4=`Delete`, przejdź do nowego panelu, z którego możesz potwierdzić, że chcesz usunąć wszystkie nazwy użytkowników zarejestrowane dla podanej nazwy profilu uprawnień ogólnych. Ta opcja uruchamia program **RVKMQMAUT** z opcją *REMOVE dla wszystkich użytkowników i stosuje **tylko** do ogólnych nazw profili.

Jeśli zostanie wybrana opcja 12=`Work with profile` , przejdź do panelu wyników komendy **WRKMQMAUTD** , zgodnie z opisem w sekcji “WRKMQMAUTD” na stronie 185.

WRKMQMAUTD

Ta komenda umożliwia wyświetlenie wszystkich użytkowników zarejestrowanych przy użyciu określonej nazwy profilu uprawnień i typu obiektu. Aby uruchomić tę komendę, użytkownik musi mieć uprawnienia `*connect` i `*admdsp` do menedżera kolejek. Aby jednak nadać, uruchomić, utworzyć lub usunąć profil, użytkownik musi mieć uprawnienie QMQMADM.

Po wybraniu opcji F24=`More keys` na początkowym panelu wejściowym, po wybraniu opcji F9=`All Parameters` , zostanie wyświetlona nazwa komponentu usługi (Service Component Name), jak w przypadku produktów **GRTMQMAUT** i **RVKMQMAUT**.

Uwaga: Klucz F11=`Display Object Authorizations` przełącza się między następującymi typami uprawnień:

- Autoryzacje obiektów
- Autoryzacje kontekstowe
- Autoryzacje MQI

Opcje na ekranie są następujące:

2=Grant
Powoduje przejście do panelu **GRTMQMAUT** w celu dodania do bieżących uprawnień.

3=Revoke
Powoduje przejście do panelu **RVKMQMAUT** w celu usunięcia niektórych z bieżących definicji.

4=Delete
Powoduje przejście do panelu, który umożliwia usunięcie danych uprawnień dla określonych użytkowników. Spowoduje to uruchomienie **RVKMQMAUT** z opcją *REMOVE.

5=Display
Przenosi użytkownika do istniejącej komendy **DSPMQMAUT** .

F6=Create
Powoduje przejście do panelu **GRTMQMAUT** , który umożliwia utworzenie rekordu uprawnień profilu.

IBM i Wytyczne dotyczące menedżera uprawnień do obiektów w systemie IBM i

Dodatkowe wskazówki i porady dotyczące używania menedżera uprawnień do obiektów (object authority manager-OAM)

Ogranicz dostęp do operacji wrażliwych

Niektóre operacje są objęte szczególną ochroną; należy je ograniczyć do użytkowników uprzywilejowanych. Na przykład składnia

- Uzyskiwanie dostępu do niektórych kolejek specjalnych, takich jak kolejki transmisji lub kolejki komend `SYSTEM.ADMIN.COMMAND.QUEUE`
- Uruchomione programy, które używają pełnych opcji kontekstu MQI
- Tworzenie i kopiowanie kolejek aplikacji

Katalogi menedżera kolejek

Katalogi i biblioteki zawierające kolejki i inne dane menedżera kolejek są prywatne dla produktu. Nie należy używać standardowych komend systemu operacyjnego do nadawania lub odbierania autoryzacji do zasobów MQI.

Kolejki

Uprawnienie do kolejki dynamicznej jest oparte, ale nie musi być takie samo jak uprawnienie kolejki modelowej, z której pochodzi.

W przypadku kolejek aliasowych i kolejek zdalnych autoryzacja dotyczy samego obiektu, a nie kolejki, na którą tłumaczony jest alias lub kolejka zdalna. Możliwe jest autoryzowanie profilu użytkownika w celu uzyskania dostępu do kolejki aliasowej, która jest tłumaczona na kolejkę lokalną, do której profil użytkownika nie ma uprawnień dostępu.

Ogranicz uprawnienia do tworzenia kolejek do użytkowników uprzywilejowanych. W przeciwnym razie użytkownicy mogą pominąć normalną kontrolę dostępu, tworząc alias.

Uprawnienia użytkownika alternatywnego

Alternatywne uprawnienia użytkownika określają, czy profil użytkownika może używać uprawnień innego profilu użytkownika podczas uzyskiwania dostępu do obiektu IBM MQ . Ta technika jest niezbędna w sytuacji, gdy serwer odbiera żądania z programu, a serwer chce mieć pewność, że program ma wymagane uprawnienia do żądania. Serwer może mieć wymagane uprawnienia, ale musi wiedzieć, czy program ma uprawnienia do żądanych działań.

Na przykład:

- Program serwera działający w ramach profilu użytkownika PAYSERV pobiera komunikat żądania z kolejki, która została umieszczona w kolejce przez profil użytkownika USER1.
- Gdy program serwera otrzyma komunikat żądania, przetwarza żądanie i umieszcza odpowiedź z powrotem w kolejce odpowiedzi określonej w komunikacie żądania.
- Zamiast używać własnego profilu użytkownika (PAYSERV) do autoryzowania otwierania kolejki odpowiedzi, serwer może określić inny profil użytkownika, w tym przypadku USER1. W tym przykładzie można użyć uprawnienia alternatywnego użytkownika do określenia, czy PAYSERV może określić USER1 jako alternatywny profil użytkownika podczas otwierania kolejki odpowiedzi.

Profil użytkownika alternatywnego jest określony w polu *AlternateUserId* deskryptora obiektu.

Uwaga: Dla dowolnego obiektu IBM MQ można użyć alternatywnych profili użytkowników. Użycie alternatywnego profilu użytkownika nie ma wpływu na profil użytkownika używany przez inne menedżery zasobów.

Uprawnienie kontekstowe

Kontekst jest informacją, która ma zastosowanie do konkretnego komunikatu i jest zawarty w deskryptorze komunikatu MQMD, który jest częścią komunikatu.

Opisy pól deskryptora komunikatu związanych z kontekstem zawiera sekcja MQMD-przegląd.

Więcej informacji na temat opcji kontekstu zawiera sekcja Kontekst komunikatu.

Uwagi dotyczące zabezpieczeń zdalnych

W przypadku ochrony zdalnej należy wziąć pod uwagę następujące kwestie:

Wstawienie uprawnienia
W celu zapewnienia bezpieczeństwa między menedżerami kolejek można określić uprawnienie do umieszczania, które jest używane, gdy kanał odbiera komunikat wysłany z innego menedżera kolejek.

Ten parametr jest poprawny tylko dla kanałów typu RCVR, RQSTR lub CLUSRCVR. Określ atrybut kanału PUTAUT w następujący sposób:

DEF
Domyślny profil użytkownika. Jest to profil użytkownika QMQM, w którym działa agent kanału komunikatów.

CTX
Profil użytkownika w kontekście komunikatu.

Kolejki transmisji
Menedżery kolejek automatycznie umieszczają komunikaty zdalne w kolejce transmisji. Uprawnienia specjalne nie są wymagane. Jednak umieszczenie komunikatu bezpośrednio w kolejce transmisji wymaga specjalnej autoryzacji.

Wyjścia kanału
Wyjścia kanału mogą być używane w celu zwiększenia bezpieczeństwa.

Rekordy uwierzytelniania kanału
Służy do wykonywania bardziej precyzyjnej kontroli dostępu do systemów łączących na poziomie kanału.

Więcej informacji na temat zabezpieczeń zdalnych zawiera sekcja “Autoryzacja kanału” na stronie 112.

Zabezpieczanie kanałów za pomocą protokołu SSL/TLS

Protokół TLS (Transport Layer Security) zapewnia ochronę kanału przed podsłuchiwaniem, manipulowaniem i imitowaniem. Obsługa protokołu TLS w produkcie IBM MQ umożliwia określenie w definicji kanału, że dany kanał używa zabezpieczeń TLS. Można również określić szczegóły dotyczące ochrony, takie jak algorytm szyfrowania, który ma być używany.

Obsługa protokołu TLS w produkcie IBM MQ używa *obiektu informacji uwierzytelniającej* menedżera kolejek oraz różnych komend CL i MQSC, a także parametrów menedżera kolejek i kanału, które szczegółowo definiują wymaganą obsługę protokołu TLS.

Następujące komendy CL obsługują protokół TLS:

WRKMQMAUTI.
Praca z atrybutami obiektu informacji uwierzytelniającej.

CHGMQMAUTI,
Modyfikowanie atrybutów obiektu informacji uwierzytelniającej.

Komenda CRTMQMAUTI
Utwórz obiekt informacji uwierzytelniającej.

CPYMQMAUTI,
Utwórz obiekt informacji uwierzytelniającej, kopiując istniejący.

DLTMQMAUTI
Usuń obiekt informacji uwierzytelniającej.

Komenda DSPMQMAUTI
Wyświetla atrybuty konkretnego obiektu informacji uwierzytelniającej.

Przegląd zabezpieczeń kanału przy użyciu protokołu TLS znajduje się w sekcji

- Ochrona kanałów za pomocą protokołu TLS

Szczegółowe informacje na temat komend PCF powiązanych z protokołem TLS zawiera sekcja

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

z/OS Konfigurowanie zabezpieczeń w systemie z/OS

Uwagi dotyczące zabezpieczeń specyficzne dla produktu z/OS.

Zabezpieczenia w produkcie IBM MQ for z/OS są kontrolowane za pomocą produktu RACF lub równoważnego zewnętrznego menedżera zabezpieczeń (ESM).

W poniższych instrukcjach przyjęto założenie, że używany jest produkt RACF.

Odsyłacze pokrewne
Scenariusz zabezpieczeń: dwa menedżery kolejek w systemie z/OS
Scenariusz zabezpieczeń: grupa współużytkowania kolejek w systemie z/OS

z/OS Klasy zabezpieczeń produktu RACF

Klasy produktu RACF są używane do przechowywania profili wymaganych do sprawdzania zabezpieczeń produktu IBM MQ . Wiele klas elementów ma równorzędne klasy grupowe. Należy aktywować klasy i włączyć je do akceptowania profili ogólnych.

Każda klasa RACF przechowuje jeden lub więcej profili używanych w pewnym momencie w sekwencji sprawdzania, jak to pokazano na Tabela 23 na stronie 188.

Tabela 23. Klasy RACF używane przez produkt IBM MQ

Klasa elementu	Klasa grupy	Spis treści
MQADMIN	ADMINISTRATOR GMQADMIN	Profile: Używane głównie do przechowywania profili dla funkcji typu administracyjnego. Na przykład: • Profile dla przełączników zabezpieczeń produktu IBM MQ • Profil bezpieczeństwa RESLEVEL • Profile dla alternatywnego zabezpieczenia użytkownika • Profil zabezpieczeń kontekstu • Profile zabezpieczeń zasobów komend

Tabela 23. Klasy RACF używane przez produkt IBM MQ (kontynuacja)		
Klasa elementu	**Klasa grupy**	**Spis treści**
MXADMIN	GMXADMIN	Profile: Używane głównie do przechowywania profili dla funkcji typu administracyjnego. Na przykład: • Profile dla przełączników zabezpieczeń produktu IBM MQ • Profil bezpieczeństwa RESLEVEL • Profile dla alternatywnego zabezpieczenia użytkownika • Profil zabezpieczeń kontekstu • Profile zabezpieczeń zasobów komend Ta klasa może zawierać zarówno wielkie, jak i mieszane profile sprawy RACF .
MQCONN		Profile używane na potrzeby zabezpieczeń połączenia
MQCMDS		Profile używane na potrzeby zabezpieczeń komend
MQQUEUE	GMQQUEUE	Profile używane w zabezpieczeniach zasobów kolejki
MXQUEUE	GMXQUEUE	Mieszane profile wielkości liter i wielkich profili używane w zabezpieczeniach zasobów kolejki
MQPROC	GMQPROC	Profile używane w zabezpieczeniach zasobów procesu
MXPROC	GMXPROC	Mieszane profile wielkości liter i wielkich profili używane w zabezpieczeniach zasobów procesu
MQNLIST	GMQNLIST	Profile używane w zabezpieczeniach zasobów listy nazw
MXNLIST	GMXNLIST	Mieszane profile wielkości liter i wielkich profili używane w zabezpieczeniach zasobów listy nazw
MXTOPIC	GMXTOPIC	Mieszane profile wielkości liter i wielkich liter użyte w zabezpieczeniach tematów

Niektóre klasy mają pokrewny *klasa grupy* , która umożliwia tworzenie grup zasobów o podobnych wymaganiach dotyczących dostępu. Szczegółowe informacje na temat różnic między klasami elementu i grupy oraz w przypadku korzystania z elementu lub klasy grupy zawiera publikacja z/OS Security Server RACF Security Administrator's Guide.

Klasy muszą być aktywowane przed sprawdzeniami zabezpieczeń. Aby aktywować wszystkie klasy produktu IBM MQ , można użyć następującej komendy RACF :

```
SETROPTS CLASSACT(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                  MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

Należy również upewnić się, że zostały skonfigurowane klasy tak, aby mogły akceptować profile ogólne. Można to zrobić również za pomocą komendy SETROPTS komendy RACF , na przykład:

```
SETROPTS GENERIC(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                 MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

z/OS RACF profile

Wszystkie profile produktu RACF używane przez produkt IBM MQ zawierają przedrostek, który jest nazwą menedżera kolejek lub nazwą grupy współużytkowania kolejki. Należy zachować ostrożność, jeśli używany jest znak procentu jako znak wieloznaczny.

Wszystkie profile produktu RACF używane przez produkt IBM MQ zawierają przedrostek. W przypadku zabezpieczeń na poziomie grupy współużytkowania kolejek jest to nazwa grupy współużytkowania kolejki. W przypadku zabezpieczeń na poziomie menedżera kolejek przedrostkiem jest nazwa menedżera kolejek. W przypadku korzystania z połączenia menedżera kolejek i zabezpieczeń na poziomie grupy współużytkowania kolejek profile będą używane z dwoma typami przedrostka. (Zabezpieczenia na poziomie grupy współużytkowania kolejek i menedżera kolejek są opisane w sekcji IBM MQ for z/OS pojęć: security.)

Na przykład, aby chronić kolejkę o nazwie QUEUE_FOR_SUBSCRIBER_LIST w grupie współużytkowania kolejek QSG1 na poziomie grupy współużytkowania kolejki, odpowiedni profil zostanie zdefiniowany jako RACF jako:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Jeśli chcesz chronić kolejkę o nazwie QUEUE_FOR_LOST_CARD_LIST, która należy do menedżera kolejek STCD na poziomie menedżera kolejek, odpowiedni profil zostanie zdefiniowany jako RACF jako:

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

Oznacza to, że różne menedżery kolejek i grupy współużytkowania kolejek mogą współużytkować tę samą bazę danych RACF , a mimo to mają różne opcje zabezpieczeń.

Nie należy używać nazw ogólnych menedżerów kolejek w profilach, aby uniknąć nieprzewidywanego dostępu użytkownika.

IBM MQ zezwala na użycie znaku procentu (%) w nazwach obiektów. Jednak produkt RACF używa znaku% jako znaku wieloznacznego jednoznakowego. Oznacza to, że po zdefiniowaniu nazwy obiektu o znaku% w nazwie należy wziąć pod uwagę to, kiedy zdefiniujesz odpowiedni profil.

Na przykład dla kolejki CREDIT_CARD_ %_RATE_INQUIRY, w menedżerze kolejek CRDP, profil zostanie zdefiniowany dla RACF w następujący sposób:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Ta kolejka nie może być chroniona przez profil ogólny, taki jak CRDP. * *.

Produkt IBM MQ umożliwia użycie znaków mieszanych w nazwach obiektów. Obiekty te można chronić, definiując:

1. Mieszane profile przypadków w odpowiednich klasach RACF z mieszanymi przypadkami, lub
2. Profile ogólne w odpowiednich klasach RACF wielkich liter.

Aby korzystać z mieszanych profili spraw i klas RACF z mieszanymi sprawami, należy wykonać kroki opisane w sekcji “z/OS Migrowanie menedżera kolejek do mieszanego zabezpieczenia elementu pracy” na stronie 276.

Istnieje kilka profili lub części profili, które pozostają wielkimi literami tylko wtedy, gdy wartości są udostępniane przez produkt IBM MQ. Są to:

- Przełącz profile.
- Wszystkie kwalifikatory wysokiego poziomu (HLQ), w tym identyfikatory podsystemu i grupy współużytkowania kolejek.
- Profile dla obiektów SYSTEM.

- Profile dla obiektów domyślnych.
- Klasa **MQCMDS** , więc wszystkie profile komend są tylko wielkimi literami.
- Klasa **MQCONN** , więc wszystkie profile połączeń są tylko wielkimi literami.
- **RESLEVEL** .
- Kwalifikacja `'object'` w profilach zasobów komend, na przykład `hlq.QUEUE.queuename`. Nazwa zasobu jest mieszana tylko z wielkością liter.
- Dynamiczne profile kolejek `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*`i `CSQXCMD.*`.
- `'CONTEXT'` część produktu `hlq.CONTEXT.resourcename`.
- Część `'ALTERNATE.USER'` produktu `hlq.ALTERNATE.USER.userid`.

Na przykład, jeśli istnieje kolejka o nazwie `PAYROLL.Dept1` w menedżerze kolejek `QM01` i używana jest następująca liczba kolejek:

- Mixed case profiles; you can define a profile in the IBM MQ RACF class `MXQUEUE`

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Uppercase profiles; you can define a profile in the IBM MQ RACF class `MQQUEUE`

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

W pierwszym przykładzie, używając mieszanych profili przypadku, można uzyskać bardziej szczegółową kontrolę nad nadawaniem uprawnień do dostępu do zasobu.

z/OS Przełącz profile

Aby sterować sprawdzaniem zabezpieczeń wykonywaną przez produkt IBM MQ, należy użyć *profili przełącznika*. Profil przełącznika to normalny profil produktu RACF , który ma specjalne znaczenie dla produktu IBM MQ. Lista dostępu w profilach przełączników nie jest używana przez produkt IBM MQ.

Produkt IBM MQ obsługuje przełącznik wewnętrzny dla każdego typu przełącznika w tabelach Switch profiles for subsystem level security(Przełącz profile zabezpieczeń na poziomie podsystemu), Switch profiles for queue sharing group or queue manager level security(Przełącz profile dla zabezpieczeń na poziomie menedżera kolejek lub menedżera kolejek) i Switch profiles for resource checking(Przełącz profile na Profile przełączników mogą być utrzymywane na poziomie grupy współużytkowania kolejek lub na poziomie menedżera kolejek albo w kombinacji obu tych elementów. Korzystając z jednego zestawu profili przełącznika zabezpieczeń grupy współużytkowania kolejek, można sterować ochroną wszystkich menedżerów kolejek w grupie współużytkowania kolejek.

Po ustawieniu przełącznika bezpieczeństwa są wykonywane sprawdzenia zabezpieczeń powiązane z przełącznikiem. Po wyłączeniu przełącznika zabezpieczenia powiązane z przełącznikiem są pomijane. Wartością domyślną jest to, że wszystkie przełączniki zabezpieczeń są włączone.

z/OS *Przełączniki i klasy*

Podczas uruchamiania menedżera kolejek lub odświeżania zabezpieczeń program IBM MQ ustawia przełączniki zgodnie ze stanem różnych klas produktu RACF .

Gdy menedżer kolejek jest uruchamiany (lub gdy klasa MQADMIN lub MXADMIN jest odświeżana za pomocą komendy IBM MQ REFRESH SECURITY), program IBM MQ najpierw sprawdza status RACF i odpowiednią klasę:

- Klasa MQADMIN, jeśli używane są wielkie litery
- Klasa MXADMIN, jeśli używany jest profil sprawy mieszanej.

Ustawia wyłącznik bezpieczeństwa podsystemu, jeśli spełniony jest dowolny z następujących warunków:

- RACF jest nieaktywny lub nie jest zainstalowany.

- Nie zdefiniowano klasy MQADMIN lub MXADMIN (klasy te są zawsze definiowane dla RACF , ponieważ są uwzględniane w tabeli definicji klas (CDT)).
- Klasa MQADMIN lub MXADMIN nie została aktywowana.

Jeśli zarówno klasa RACF , jak i klasa MQADMIN lub MXADMIN są aktywne, program IBM MQ sprawdza klasę MQADMIN lub MXADMIN, aby sprawdzić, czy zdefiniowano dowolny z profili przełącznika. Najpierw sprawdzane są profile opisane w sekcji “Profile do sterowania bezpieczeństwem podsystemów” na stronie 193. Jeśli zabezpieczenia podsystemu nie są wymagane, program IBM MQ ustawia wyłączany przełącznik bezpieczeństwa podsystemu wewnętrznego i nie sprawdza żadnych dalszych kontroli.

Profile określają, czy odpowiedni przełącznik IBM MQ jest włączany, czy wyłączony.

- Jeśli przełącznik jest wyłączony, ten typ zabezpieczeń jest dezaktywowany.
- Jeśli dowolny przełącznik IBM MQ jest ustawiony, program IBM MQ sprawdza status klasy RACF powiązanej z typem zabezpieczenia odpowiadonym przełącznikiem IBM MQ . Jeśli klasa nie jest zainstalowana lub jest nieaktywna, przełącznik IBM MQ jest wyłączony. Na przykład sprawdzanie zabezpieczeń procesu nie jest przeprowadzane, jeśli klasa MQPROC lub MXPROC nie została aktywowana. Klasa, która nie jest aktywna, jest równoważna definiowaniu NO.PROCESS.CHECKS profil dla każdego menedżera kolejek i grupy współużytkowania kolejek, który korzysta z tej bazy danych RACF .

z/OS *Sposób działania przełączników*

Aby ustawić przełącznik bezpieczeństwa, zdefiniuj wartość NO.* profil przełącznika dla tego profilu. Można nadpisać wartość NO.* Profil ustawiony na poziomie grupy współużytkowania kolejki, definiując typ YES.* Profil dla menedżera kolejek.

Aby ustawić przełącznik bezpieczeństwa, należy zdefiniować wartość NO.* profil przełącznika dla tego profilu. Istnienie NO.* Profil oznacza, że sprawdzanie zabezpieczeń to **nie** wykonywane dla tego typu zasobu, chyba że zostanie nadpisane ustawienie poziomu grupy współużytkowania kolejki dla konkretnego menedżera kolejek. Jest to opisane w sekcji “Nadpisywanie ustawień poziomu grupy współużytkowania kolejki” na stronie 192.

Jeśli menedżer kolejek nie jest elementem grupy współużytkowania kolejek, nie trzeba definiować żadnych profili poziomu grupy współużytkowania kolejek ani żadnych profili przesłaniania. Należy jednak pamiętać o tym, aby zdefiniować te profile, jeśli menedżer kolejek dołącza do grupy współużytkowania kolejek w późniejszym terminie.

Każdy NO.* Profil przełącznika, który program IBM MQ wykryje, wyłącza sprawdzanie tego typu zasobu. Profile przełączników są aktywowane podczas uruchamiania menedżera kolejek. W przypadku zmiany profili przełącznika w czasie, gdy są uruchomione odpowiednie menedżery kolejek, można uzyskać IBM MQ , aby rozpoznać zmiany, wydając komendę IBM MQ REFRESH SECURITY.

Profile przełączników muszą być zawsze definiowane w klasie MQADMIN lub MXADMIN. Nie należy definiować ich w klasie GMQADMIN lub GMXADMIN. W tabelach Przełącz profile zabezpieczeń na poziomie podsystemu i Przełącz profile na potrzeby sprawdzania zasobów są wyświetlane poprawne profile przełączników i typ zabezpieczeń, który sterują.

Nadpisywanie ustawień poziomu grupy współużytkowania kolejki

Istnieje możliwość nadpisania ustawień zabezpieczeń na poziomie grupy współużytkowania kolejek dla konkretnego menedżera kolejek, który jest członkiem tej grupy. Jeśli menedżer kolejek ma być sprawdzany w pojedynczym menedżerze kolejek, który nie jest wykonywany w innych menedżerach kolejek w grupie, należy użyć komendy (qmgr-name.YES. *). profile przełączników.

Jeśli jednak nie ma potrzeby przeprowadzania pewnych operacji sprawdzania konkretnego menedżera kolejek w grupie współużytkowania kolejek, należy zdefiniować parametr (qmgr-name.NO. *) Profil dla tego konkretnego typu zasobu w menedżerze kolejek i nie definiuj profilu dla grupy współużytkowania kolejek. (IBM MQ sprawdza tylko dla profilu poziomu grupy współużytkowania kolejki, jeśli nie znajduje profilu poziomu menedżera kolejek).

z/OS *Profile do sterowania bezpieczeństwem podsystemów*

Program IBM MQ sprawdza, czy dla podsystemu, dla menedżera kolejek i dla grupy współużytkowania kolejek wymagane są sprawdzenia zabezpieczeń podsystemu.

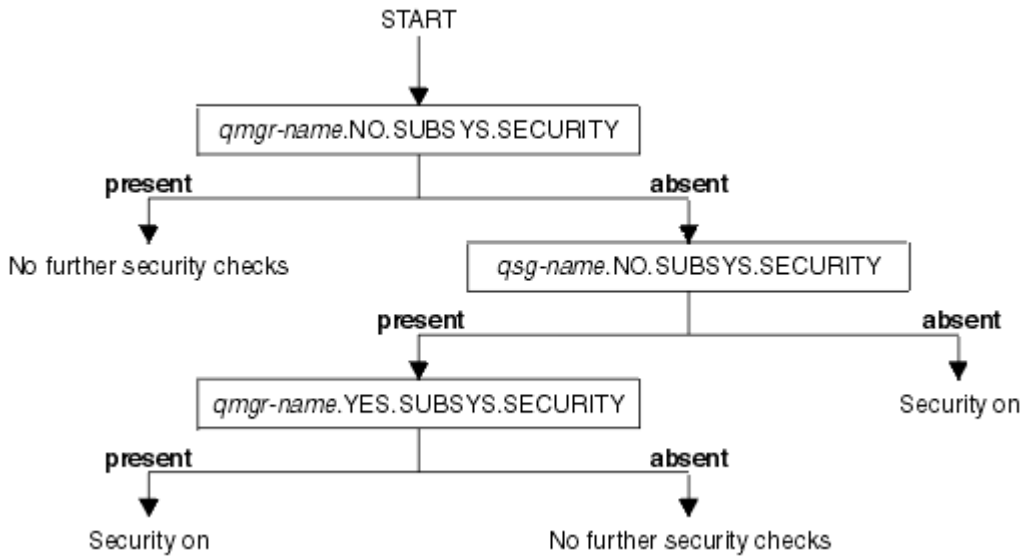
Pierwsza kontrola zabezpieczeń wykonana przez produkt IBM MQ jest używana do określenia, czy wymagane są sprawdzenia zabezpieczeń dla całego podsystemu IBM MQ . W przypadku określenia, że zabezpieczenia podsystemu nie mają być używane, nie są wykonywane żadne dalsze operacje sprawdzania.

Poniższe profile przełączników są sprawdzane w celu określenia, czy wymagane jest bezpieczeństwo podsystemu. Rysunek 14 na stronie 193 pokazuje kolejność, w jakiej są sprawdzane.

Tabela 24. Profile przełączników dla bezpieczeństwa na poziomie podsystemu

Nazwa profilu przełącznika	**Typ zasobu lub sprawdzenia, który jest kontrolowany**
qmgr-name.NO.SUBSYS.SECURITY	Zabezpieczenia podsystemu dla tego menedżera kolejek
qsg-name.NO.SUBSYS.SECURITY	Zabezpieczenia podsystemu dla tej grupy współużytkowania kolejek
qmgr-name.YES.SUBSYS.SECURITY	Przesłonięcie zabezpieczeń podsystemu dla tego menedżera kolejek

Jeśli menedżer kolejek nie należy do grupy współużytkowania kolejek, program IBM MQ sprawdza tylko profil przełącznika qmgr-name.NO.SUBSYS.SECURITY .



Rysunek 14. Sprawdzanie bezpieczeństwa podsystemu

z/OS *Profile do sterowania grupą współużytkowania kolejek lub zabezpieczeniami na poziomie menedżera kolejek*

Jeśli sprawdzanie zabezpieczeń podsystemu jest wymagane, program IBM MQ sprawdza, czy sprawdzanie zabezpieczeń jest wymagane na poziomie grupy współużytkowania kolejek lub menedżera kolejek.

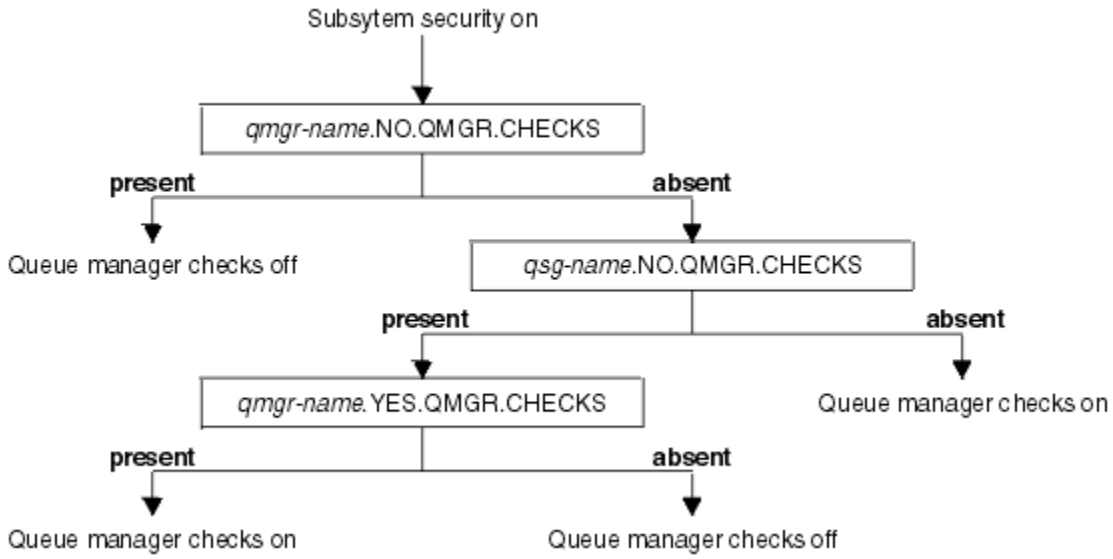
Gdy program IBM MQ określił, że sprawdzanie zabezpieczeń jest wymagane, określa, czy sprawdzanie jest wymagane w grupie współużytkowania kolejek lub na poziomie menedżera kolejek, czy też w obu tych przypadkach. Te sprawdzenia nie są wykonywane, jeśli menedżer kolejek nie jest elementem grupy współużytkowania kolejek.

Poniższe profile przełączników są sprawdzane w celu określenia wymaganego poziomu. Rysunek 15 na stronie 194 i Rysunek 16 na stronie 195 przedstawiają kolejność, w jakiej są sprawdzane.

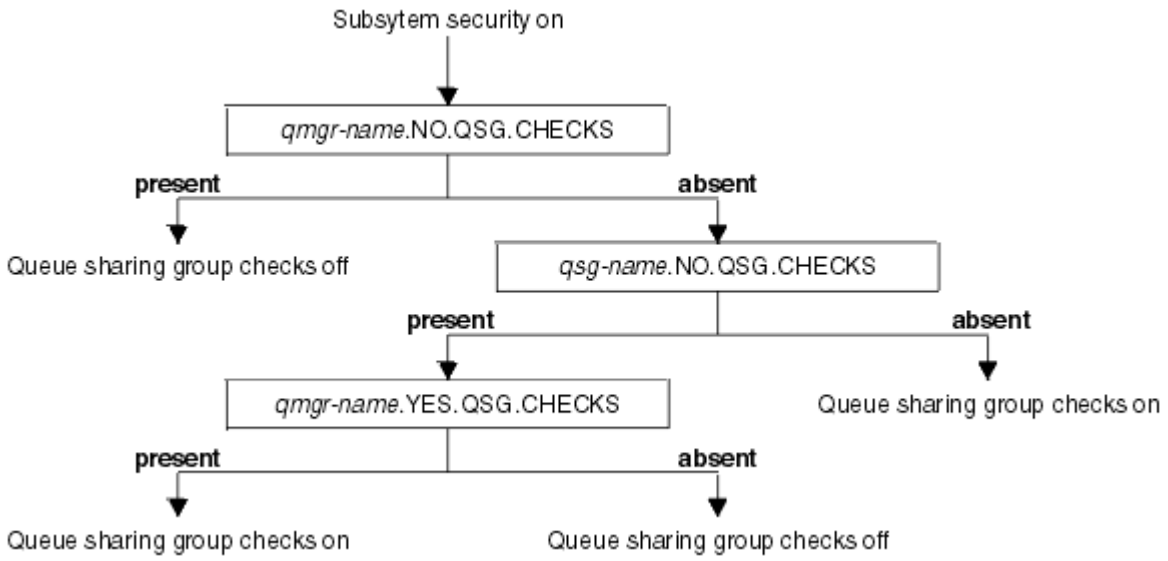
Tabela 25. Przełączanie profili dla grupy współużytkowania kolejek lub zabezpieczeń na poziomie menedżera kolejek

Nazwa profilu przełącznika	**Typ zasobu lub sprawdzenia, który jest kontrolowany**
qmgr-name.NO.QMGR.CHECKS	Brak kontroli na poziomie menedżera kolejek dla tego menedżera kolejek
qsg-name.NO.QMGR.CHECKS	Brak kontroli poziomu menedżera kolejek dla tej grupy współużytkowania kolejek
qmgr-name.YES.QMGR.CHECKS	Nadpisywanie poziomu menedżera kolejek dla tego menedżera kolejek
qmgr-name.NO.QSG.CHECKS	Brak sprawdzania poziomu grupy współużytkowania kolejki dla tego menedżera kolejek
qsg-name.NO.QSG.CHECKS	Brak sprawdzania poziomu grupy współużytkowania kolejki dla tej grupy współużytkowania kolejek
qmgr-name.YES.QSG.CHECKS	Nadpisywanie sprawdzeń poziomu grupy współużytkowania kolejki dla tego menedżera kolejek

Jeśli zabezpieczenia podsystemu są aktywne, nie można wyłączyć zarówno zabezpieczeń na poziomie grupy współużytkowania kolejek, jak i poziomu menedżera kolejek. Jeśli spróbujesz to zrobić, program IBM MQ ustawia sprawdzanie zabezpieczeń na obu poziomach.



Rysunek 15. Sprawdzanie bezpieczeństwa na poziomie menedżera kolejek



Rysunek 16. Sprawdzanie bezpieczeństwa na poziomie grupy współużytkowania kolejek

z/OS *Poprawne kombinacje przełączników zabezpieczeń*

Poprawne są tylko niektóre kombinacje przełączników. Jeśli używana jest kombinacja ustawień przełącznika, które nie są poprawne, wysyłany jest komunikat CSQH026I , a sprawdzanie zabezpieczeń jest ustawione zarówno na poziomie grupy współużytkowania kolejki, jak i na poziomie menedżera kolejek.

Tabela 26 na stronie 195, Tabela 27 na stronie 195, Tabela 28 na stronie 196i Tabela 29 na stronie 196 przedstawiają zestawy kombinacji ustawień przełącznika, które są poprawne dla każdego typu poziomu zabezpieczeń.

Tabela 26. Poprawne kombinacje przełączników zabezpieczeń dla poziomu zabezpieczeń menedżera kolejek

Kombinacje
qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS
qsg-name.NO.QSG.CHECKS qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS

Tabela 27. Poprawne kombinacje przełączników zabezpieczeń dla zabezpieczeń na poziomie grupy współużytkowania kolejek

Kombinacje
qmgr-name.NO.QMGR.CHECKS
qsg-name.NO.QMGR.CHECKS

Tabela 27. Poprawne kombinacje przełączników zabezpieczeń dla zabezpieczeń na poziomie grupy współużytkowania kolejek (kontynuacja)
Kombinacje
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS

Tabela 28. Poprawne kombinacje przełączników zabezpieczeń dla menedżera kolejek i zabezpieczeń na poziomie grupy współużytkowania kolejek
Kombinacje
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Nr QSG.* zdefiniowane profile
No QMGR.* zdefiniowane profile qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS qsg-name.NO.QSG.CHECKS qmgr-name.YES.QSG.CHECKS
Nie zdefiniowano profili dla żadnego przełącznika

*Tabela 29. Inne poprawne kombinacje przełączników, które przełączają się na oba poziomy sprawdzania **włączone**.*
Kombinacje
qmgr-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qmgr-name.NO.QMGR.CHECKS qsg-name.NO.QSG.CHECKS
qsg-name.NO.QMGR.CHECKS qmgr-name.NO.QSG.CHECKS

z/OS *Kontrole na poziomie zasobów*

Do sterowania dostępem do zasobów służy pewna liczba profili przełączników. Niektóre sprawdzanie zatrzymania jest wykonywane w menedżerze kolejek lub w grupie współużytkowania kolejek. Mogą one zostać przesłonięte przez profile, które umożliwiają sprawdzanie konkretnych menedżerów kolejek.

Tabela 30 na stronie 197 przedstawia profile przełączników używane do sterowania dostępem do zasobów produktu IBM MQ .

Jeśli menedżer kolejek jest częścią grupy współużytkowania kolejek, a użytkownik ma aktywny zarówno menedżer kolejek, jak i grupa współużytkowania kolejki, można użyć programu YES.* Profil przełącznika umożliwia przesłonięcie profili poziomu grupy współużytkowania kolejek, a w szczególności włączenie zabezpieczeń dla konkretnego menedżera kolejek.

Niektóre profile mają zastosowanie zarówno do menedżerów kolejek, jak i do grup współużytkowania kolejek. Są one poprzedzane łańcuchem *hlq* , a użytkownik powinien zastąpić nazwę grupy współużytkowania kolejek lub menedżera kolejek, w zależności od przypadku. Nazwy profili wyświetlane z przedrostkiem *qmgr-name* są profilami przesłaniania menedżera kolejek; należy zastąpić nazwę menedżera kolejek.

Tabela 30. Przełączanie profili na potrzeby sprawdzania zasobów

Typ kontroli zasobów, które są kontrolowane	**Nazwa profilu przełącznika**	**Przesłoń profil dla konkretnego menedżera kolejek**
Bezpieczeństwo połączenia	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
Bezpieczeństwo kolejki	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
Zabezpieczenia procesu	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
Zabezpieczenia listy nazw	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
zabezpieczenie kontekstu	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
alternatywne zabezpieczenie użytkownika	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
Bezpieczeństwo komend	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
Zabezpieczenia zasobów komend	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
Zabezpieczenia tematów	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Uwaga: Ogólne profile przełączników, takie jak hlq.NO. * * są ignorowane przez produkt IBM MQ		

Na przykład, aby wykonać sprawdzenia zabezpieczeń procesu w menedżerze kolejek QM01, który jest elementem grupy współużytkowania kolejek QSG3 , ale nie ma być wykonywane sprawdzanie zabezpieczeń procesu dla żadnego z pozostałych menedżerów kolejek w grupie, należy zdefiniować następujące profile przełączników:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Jeśli wymagane jest przeprowadzenie kontroli bezpieczeństwa kolejki dla wszystkich menedżerów kolejek w grupie współużytkowania kolejek z wyjątkiem QM02, należy zdefiniować następujący profil przełącznika:

```
QM02.NO.QUEUE.CHECKS
```

(Nie ma potrzeby definiowania profilu dla grupy współużytkowania kolejek, ponieważ sprawdzanie jest włączane automatycznie, jeśli nie zdefiniowano żadnego profilu).

z/OS *Przykład definiowania przełączników*

Różne podsystemy IBM MQ mają różne wymagania dotyczące zabezpieczeń, które mogą być implementowane przy użyciu różnych profili przełączników.

Zdefiniowano cztery podsystemy IBM MQ :

- MQP1 (system produkcyjny)
- MQP2 (system produkcyjny)
- MQD1 (system programistycznym)
- MQT1 (system testowy)

Wszystkie cztery menedżery kolejek są elementami grupy współużytkowania kolejek QS01. Wszystkie klasy IBM MQ RACF zostały zdefiniowane i aktywowane.

Podsystemy te mają różne wymagania dotyczące bezpieczeństwa:

- Systemy produkcyjne wymagają, aby na poziomie grupy współużytkowania kolejki w obu systemach była aktywna pełna kontrola zabezpieczeń serwera IBM MQ .

  W tym celu należy określić następujący profil:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Ustawia to sprawdzanie poziomu grupy współużytkowania kolejki dla wszystkich menedżerów kolejek w grupie współużytkowania kolejek. Nie ma potrzeby definiowania żadnych innych profili przełączników dla menedżerów kolejek produkcyjnych, ponieważ użytkownik chce sprawdzić wszystko, co w tych systemach.
- Menedżer kolejek testowych MQT1 wymaga również pełnego sprawdzenia zabezpieczeń. Jednak z uwagi na to, że można to później zmienić, można zdefiniować zabezpieczenia na poziomie menedżera kolejek, aby można było zmienić ustawienia zabezpieczeń dla tego menedżera kolejek bez wpływu na innych członków grupy współużytkowania kolejek.

  W tym celu należy zdefiniować wartość NO.QSG.CHECKS dla MQT1 w następujący sposób:

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```
- Menedżer kolejek programistycznym MQD1 ma inne wymagania dotyczące zabezpieczeń od reszty grupy współużytkowania kolejek. Wymagane jest, aby aktywne było tylko połączenie i zabezpieczenia kolejki.

  W tym celu należy zdefiniować profil produktu `MQD1.YES.QMGR.CHECKS` dla tego menedżera kolejek, a następnie zdefiniować następujące profile w celu wyłączenia sprawdzania zabezpieczeń dla zasobów, które nie muszą być sprawdzane:

  ```
  RDEFINE MQADMIN MQD1.NO.CMD.CHECKS
  RDEFINE MQADMIN MQD1.NO.CMD.RESC.CHECKS
  RDEFINE MQADMIN MQD1.NO.PROCESS.CHECKS
  RDEFINE MQADMIN MQD1.NO.NLIST.CHECKS
  RDEFINE MQADMIN MQD1.NO.CONTEXT.CHECKS
  RDEFINE MQADMIN MQD1.NO.ALTERNATE.USER.CHECKS
  ```

Gdy menedżer kolejek jest aktywny, można wyświetlić bieżące ustawienia zabezpieczeń, wydając komendę DISPLAY SECURITY MQSC.

Można również zmienić ustawienia przełącznika, gdy menedżer kolejek jest uruchomiony, definiując lub usuwając odpowiedni profil przełącznika w klasie MQADMIN. Aby zmiany wprowadzone w ustawieniach przełącznika były aktywne, należy wprowadzić komendę REFRESH SECURITY dla klasy MQADMIN.

Więcej informacji na temat komend DISPLAY SECURITY i REFRESH SECURITY można znaleźć w sekcji “Odświeżanie zabezpieczeń menedżera kolejek w systemie z/OS” na stronie 256 .

z/OS Profile używane do sterowania dostępem do zasobów produktu IBM MQ

Należy zdefiniować profile produktu RACF , aby sterować dostępem do zasobów produktu IBM MQ , oprócz profili przełącznika, które mogły zostać zdefiniowane. Ta kolekcja tematów zawiera informacje na temat profili produktu RACF dla różnych typów zasobów produktu IBM MQ .

Jeśli dla konkretnego sprawdzenia zabezpieczeń nie zdefiniowano profilu zasobu, a użytkownik zgłosi żądanie, które wiązałoby się z dokonaniem tego sprawdzenia, program IBM MQ odmawia dostępu. Nie ma potrzeby definiowania profili dla typów zabezpieczeń odnoszących się do wszystkich przełączników zabezpieczeń, które zostały zdezaktywowane.

z/OS *Profile zabezpieczeń połączenia*

Jeśli zabezpieczenia połączenia są aktywne, należy zdefiniować profile w klasie MQCONN i zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników, tak aby mogły one łączyć się z produktem IBM MQ.

Aby umożliwić nawiązawanie połączenia, należy nadać użytkownikom uprawnienia do odczytu RACF (READ) do odpowiedniego profilu. (Jeśli żaden profil poziomu menedżera kolejek nie istnieje, a menedżer kolejek jest elementem grupy współużytkowania kolejek, może być przeprowadzane sprawdzanie profili poziomu grupy współużytkowania kolejek, jeśli zabezpieczenia zostały skonfigurowane w taki sposób, aby to zrobić.)

Profil połączenia kwalifikowany przy użyciu nazwy menedżera kolejek steruje dostępem do konkretnego menedżera kolejek, a użytkownicy z dostępem do tego profilu mogą łączyć się z tym menedżerem kolejek. Profil połączenia kwalifikowany z nazwą grupy współużytkowania kolejki steruje dostępem do wszystkich menedżerów kolejek w ramach grupy współużytkowania kolejek dla tego typu połączenia. Na przykład użytkownik z dostępem do produktu `QS01.BATCH` może użyć połączenia wsadowego z dowolnym menedżerem kolejek w grupie współużytkowania kolejek QS01 , który nie ma zdefiniowanego profilu poziomu menedżera kolejek.

Uwaga:

1. Więcej informacji na temat identyfikatorów użytkowników sprawdzanych pod kątem różnych żądań zabezpieczeń zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244.
2. Sprawdzanie bezpieczeństwa na poziomie zasobów (RESLEVEL) jest również wykonywane w czasie połączenia. Szczegółowe informacje na ten temat zawiera sekcja “Profil bezpieczeństwa RESLEVEL” na stronie 237.

Zabezpieczenia produktu IBM MQ rozpoznają następujące typy połączeń:

- Połączenia wsadowe (i typu zadania wsadowego), które obejmują:
  - z/OS Zadania wsadowe
  - Aplikacje TSO
  - Podpisy USS
  - Db2Procedury składowane
- Połączenia serwera CICS
- Połączenia IMS z regionów sterowania i przetwarzania aplikacji
- Inicjator kanału IBM MQ

z/OS *Profile zabezpieczeń połączenia dla połączeń wsadowych*

Profile służące do sprawdzania połączeń typu zadania wsadowego składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *BATCH*. Podaj identyfikator użytkownika powiązany z dostępem do przestrzeni adresowej łączenia (READ) do profilu połączenia.

Profile do sprawdzania połączeń typu wsadowego i typu wsadowego mają następującą postać:

```
hlq.BATCH
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używane są zarówno zabezpieczenia na poziomie grupy, jak i menedżera kolejek, program IBM MQ sprawdza, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki. Jeśli znalezienie profilu nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączeń typu batch lub batch-type należy zezwolić na dostęp do profilu połączenia z identyfikatorem użytkownika powiązanym z przestrzenią adresową łączącą. Na przykład następująca komenda RACF umożliwia użytkownikom z grupy CONNTQM1 łączenie się z menedżerem kolejek TQM1; te identyfikatory użytkowników będą mogły korzystać z dowolnego połączenia wsadowego lub typu zadania wsadowego.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS *Korzystanie z produktu **CHCKLOCL** w lokalnie powiązanych aplikacjach*

Produkt **CHCKLOCL** ma zastosowanie tylko do połączeń, które są wykonywane za pośrednictwem połączeń BATCH i nie ma zastosowania do połączeń wykonanych z produktu CICS lub IMS. Połączenia wykonywane za pośrednictwem inicjatora kanału są sterowane przez produkt **CHCKCLNT**.

Przegląd

Aby skonfigurować menedżer kolejek produktu z/OS do sprawdzania ID użytkownika i hasła dla niektórych, ale nie wszystkich, lokalnie powiązanych aplikacji, należy wykonać dodatkową konfigurację.

Wynika to z tego, że po skonfigurowaniu produktu **CHCKLOCL** (*REQUIRED*) wcześniejsze aplikacje wsadowe, które korzystają z wywołania API MQCONN, nie mogą już łączyć się z menedżerem kolejek.

W przypadku produktu z/OS można użyć bardziej szczegółowego mechanizmu opartego na zabezpieczeniach połączenia przestrzeni adresowej w celu obniżenia globalnej konfiguracji CHCKLOCL (REQUIRED) na wartość CHCKLOCL (OPTIONAL) dla specjalnie zdefiniowanych identyfikatorów użytkowników. Zastosowany mechanizm opisany jest w poniższym tekście, wraz z przykładem.

Aby umożliwić większą granulację w systemie **CHCKLOCL** (*WYMAGANE*) niż tylko EVERYONE, należy zmodyfikować **CHCKLOCL** w taki sam sposób, w jaki zmodyfikujesz poziom dostępu dla ID użytkownika powiązanego z przestrzenią adresową łączącą do profili połączeń produktu `hlq.batch` w klasie MQCONN.

Jeśli identyfikator użytkownika przestrzeni adresowej ma tylko dostęp z prawem do odczytu (READ), który jest minimalnym wymaganiem, aby można było połączyć się w ogóle, konfiguracja produktu **CHCKLOCL** ma zastosowanie w formie pisemnej.

Jeśli identyfikator użytkownika przestrzeni adresowej ma dostęp UPDATE (lub wyższy), wówczas konfiguracja produktu **CHCKLOCL** działa w trybie *OPTIONAL* . Oznacza to, że użytkownik nie musi udostępniać identyfikatora użytkownika i hasła, ale jeśli zostanie podany, identyfikator użytkownika i hasło muszą być poprawnymi parą.

Zabezpieczenia połączenia zostały już skonfigurowane dla menedżera kolejek produktu z/OS .

Jeśli dla menedżera kolejek produktu z/OS skonfigurowano zabezpieczenia połączenia i wymagane jest, aby produkt **CHCKLOCL** (*WYMAGANY*) miał zastosowanie do lokalnie powiązanych aplikacji serwera WAS, a także nie ma innych, wykonaj następujące kroki:

1. Zacznij od **CHCKLOCL** (*OPCJONALNE*) jako konfiguracji. Oznacza to, że wszystkie podane ID użytkownika i hasła są sprawdzane pod względem ważności, ale nie są wymagane.
2. Wyświetl listę wszystkich użytkowników, którzy mają dostęp do profili zabezpieczeń połączenia, wydając komendę:

   ```
   RLIST MQCONN MQ23.BATCH AUTHUSER
   ```

   Ta komenda jest wyświetlana, na przykład:

   ```
   CLASS    NAME
   -----    ----
   MQCONN   MQ23.BATCH

   USER     ACCESS  ACCESS COUNT
   ----     ------  ------ -----
   JOHNDOE  READ    000009
   JDOE1    READ    000003
   WASUSER  READ    000000
   ```

3. Dla każdego identyfikatora użytkownika, który ma dostęp z prawem do odczytu, zmień dostęp do

   ```
   UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
   ```

4. Zaktualizuj konfigurację produktu IBM MQ na wartość **CHCKLOCL** (*REQUIRED*).

   Kombinacja dostępu UPDATE do produktu `MQ23.BATCH` i bieżącego ustawienia oznacza, że używany jest produkt **CHCKLOCL** (*OPCJONALNY*).
5. Teraz należy zastosować zachowanie **CHCKLOCL** (*REQUIRED*) do jednego konkretnego identyfikatora użytkownika, na przykład WASUSER, tak aby wszystkie połączenia przychodzące z tego regionu musiały podać identyfikator użytkownika i hasło.

   W tym celu należy cofnąć zmiany dokonane wcześniej, wydając komendę:

   ```
   PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
   ```

Zabezpieczenia połączenia nie są skonfigurowane dla menedżera kolejek produktu z/OS .

W takiej sytuacji należy:

1. Utwórz profile połączenia dla produktu `hlq.BATCH` w klasie MQCONN, wydając komendę:

   ```
   RDEFINE MQCONN MQ23.BATCH UACC(NONE)
   ```

2. Autoryzuj wszystkie identyfikatory użytkowników, które tworzą połączenia wsadowe z menedżerem kolejek, tak aby miały dostęp UPDATE do tego profilu. Spowoduje to pominięcie wymagania **CHCKLOCL** (*REQUIRED*) dla identyfikatora użytkownika i hasła w czasie połączenia.

   W tym celu wydając komendę:

   ```
   PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
   ```

   Należą do nich identyfikatory użytkowników:

   a. Używane w przypadku paneli CSQUTIL, ISPF i innych lokalnie powiązanych narzędzi.

b. Powiązane z zadaniami wsadowymi, takimi jak połączenia z menedżerem kolejek. Rozważmy na przykład procedury składowane Advanced Message Security, IBM Integration Bus, Db2 , użytkowników USS i TSO oraz aplikacje produktu Java .

3. Usuń profil przełącznika dla menedżera kolejek, wydając komendę:

```
hlq.NO.CONNECT.CHECKS
```

4. Teraz należy zastosować zachowanie **CHCKLOCL** (*REQUIRED*) do jednego konkretnego identyfikatora użytkownika, na przykład WASUSER, tak aby wszystkie połączenia przychodzące z tego regionu musiały podać identyfikator użytkownika i hasło.

   W tym celu należy cofnąć zmiany dokonane wcześniej, wydając komendę:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS *Profile zabezpieczeń połączenia dla połączeń produktu CICS*

Profile służące do sprawdzania połączeń produktu CICS składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *CICS* . Należy podać identyfikator użytkownika powiązany z przestrzenią adresową CICS READ do profilu połączenia.

Profile służące do sprawdzania połączeń z produktu CICS mają następującą postać:

```
hlq.CICS
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używane są zarówno zabezpieczenia na poziomie grupy, jak i menedżera kolejek, program IBM MQ sprawdza, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki. Jeśli znalezienie profilu nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączeń przez produkt CICSwymagane jest tylko zezwolenie na dostęp do profilu połączenia z ID użytkownika przestrzeni adresowej CICS .

Na przykład następujące komendy produktu RACF zezwalają użytkownikowi przestrzeni adresowej CICS KCBCICS na nawiązanie połączenia z menedżerem kolejek TQM1:

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

z/OS *Profile zabezpieczeń połączenia dla połączeń produktu IMS*

Profile służące do sprawdzania połączeń produktu IMS składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *IMS* . Nadaj identyfikatorom użytkowników regionu sterującego IMS i regionowi zależnym dostęp z uprawnieniami do odczytu do profilu połączenia.

Profile służące do sprawdzania połączeń z produktu IMS mają następującą postać:

```
hlq.IMS
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używane są zarówno zabezpieczenia na poziomie grupy, jak i menedżera kolejek, program IBM MQ sprawdza, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek.

Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki. Jeśli znalezienie profilu nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączeń przez produkt IMS, należy zezwolić na dostęp do profilu połączenia dla identyfikatorów użytkowników regionu sterującego IMS i regionu zależnego.

Na przykład następujące komendy produktu RACF zezwalają na:

- ID użytkownika regionu IMS , IMSREG, w celu nawiązania połączenia z menedżerem kolejek TQM1.
- Użytkownicy w grupie BMPGRP do wprowadzania zadań BMP.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

z/OS *Profile zabezpieczeń połączenia dla inicjatora kanału*

Profile służące do sprawdzania połączeń z inicjatora kanału składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejki, po której następuje słowo *CHIN*. Podaj identyfikator użytkownika używany przez inicjator kanału, który uruchomił dostęp do przestrzeni adresowej zadania READ do profilu połączenia.

Profile służące do sprawdzania połączeń z inicjatora kanału mają następującą postać:

```
hlq.CHIN
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używane są zarówno zabezpieczenia na poziomie grupy, jak i menedżera kolejek, program IBM MQ sprawdza, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki. Jeśli znalezienie profilu nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączenia przez inicjatora kanału należy zdefiniować dostęp do profilu połączenia dla identyfikatora użytkownika używanego przez przestrzeń adresową uruchomionego zadania inicjatora kanału.

Na przykład następujące komendy produktu RACF zezwalają na połączenie przestrzeni adresowej inicjatora kanału z identyfikatorem użytkownika DQCTRL w celu nawiązania połączenia z menedżerem kolejek TQM1:

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS *Profile dla bezpieczeństwa kolejki*

Jeśli zabezpieczenia kolejki są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników. Profile zabezpieczeń kolejki są nazywane po menedżerze kolejek lub grupie współużytkowania kolejek i kolejką, która ma zostać otwarta.

Jeśli zabezpieczenia kolejki są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach **MQQUEUE** lub **GMQQUEUE** , jeśli używane są wielkie profile.
- Zdefiniuj profile w klasach **MXQUEUE** lub **GMXQUEUE** , jeśli używane są mieszane profile spraw.
- Należy zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników, tak aby mogły one wydawać żądania API IBM MQ , które korzystają z kolejek.

Profile dotyczące zabezpieczeń kolejki mają następującą postać:

```
hlq.queuename
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `queuename` jest nazwą otwartej kolejki, która została określona w deskryptorze obiektu w wywołaniu komendy `MQOPEN` lub `MQPUT1` .

Profil poprzedzony przez nazwę menedżera kolejek steruje dostępem do jednej kolejki w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje dostępem do jednej lub większej liczby kolejek z tą nazwą kolejki we wszystkich menedżerach kolejek w grupie współużytkowania kolejek lub dostępem do kolejki współużytkowanej przez dowolny menedżer kolejek w grupie. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tej kolejki w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

Jeśli używane są kolejki współużytkowane, zalecane jest użycie zabezpieczeń na poziomie grupy współużytkowania kolejek.

Szczegółowe informacje na temat działania zabezpieczeń kolejki w przypadku, gdy nazwa kolejki jest nazwą aliasu lub kolejki modelowej z/OS, patrz “Uwagi dotyczące kolejek aliasowych” na stronie 206 i “Uwagi dotyczące kolejek modelowych” na stronie 207 .

Dostęp do kolejki RACF wymagany do otwarcia kolejki zależy od podanych opcji `MQOPEN` lub `MQPUT1` . Jeśli zakodowana jest więcej niż jedna z opcji MQOO_ * i MQPMO_ *, to sprawdzanie zabezpieczeń kolejki jest wykonywane dla najwyższego wymaganego uprawnienia RACF .

Tabela 31. Poziomy dostępu dla zabezpieczeń kolejki za pomocą wywołań MQOPEN lub MQPUT1

MQOPEN lub MQPUT1 -opcja	**Wymagany poziom dostępu RACF do hlq.queuename**
MQOO_BROWSE	ODCZYT
MQOO_INQUIRE	ODCZYT
MQOO_BIND_ *	TEMPERATURY
MQOO_INPUT_ *	TEMPERATURY
MQOO_OUTPUT lub MQPUT1	TEMPERATURY
MQOO_PASS_ALL_CONTEXT, MQPMO_PASS_ALL_CONTEXT	TEMPERATURY
MQOO_PASS_IDENTITY_CONTEXT, MQPMO_PASS_IDENTITY_CONTEXT	TEMPERATURY
MQOO_SAVE_ALL_CONTEXT	TEMPERATURY
MQOO_SET_IDENTITY_CONTEXT, MQPMO_SET_IDENTITY_CONTEXT	TEMPERATURY
MQOO_SET_ALL_CONTEXT, MQPMO_SET_ALL_CONTEXT	TEMPERATURY
MQOO_SET	Zmień

Na przykład w menedżerze kolejek IBM MQ QM77wszystkie identyfikatory użytkowników w grupie RACF PAYGRP mają mieć dostęp do pobierania komunikatów z lub umieszczania komunikatów do wszystkich

kolejek o nazwach rozpoczynających się od 'PAY.'. Można to zrobić za pomocą następujących komend produktu RACF :

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Ponadto wszystkie identyfikatory użytkowników w grupie PAYGRP muszą mieć dostęp do umieszczania komunikatów w kolejkach, które nie są zgodne z konwencją nazewnictwa PAY. Na przykład:

```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```

Można to zrobić, definiując profile dla tych kolejek w klasie GMQQUEUE i nadając dostęp do tej klasy w następujący sposób:

```
RDEFINE GMQQUEUE PAYROLL.EXTRAS UACC(NONE)
        ADDMEM(QM77.REQUEST_QUEUE_FOR_PAYROLL,
               QM77.SALARY.INCREASE.SERVER,
               QM77.REPLIES.FROM.SALARY.MODEL)
PERMIT PAYROLL.EXTRAS CLASS(GMQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Uwaga:

1. Jeśli zmieniany jest poziom dostępu aplikacji RACF do profilu zabezpieczeń kolejki, zmiany są wprowadzane tylko dla wszystkich nowo uzyskanych uchwytów obiektów (czyli nowych MQOPEN) dla tej kolejki. Te uchwyty, które już istnieją w momencie zmiany, zachowują istniejący dostęp do kolejki. Jeśli aplikacja jest wymagana do korzystania z jej zmienionego poziomu dostępu do kolejki, a nie do istniejącego poziomu dostępu, musi zamknąć i ponownie otworzyć kolejkę dla każdego uchwytu obiektu, który wymaga zmiany.
2. W tym przykładzie nazwą menedżera kolejek QM77 może być także nazwa grupy współużytkowania kolejek.

Inne typy sprawdzeń zabezpieczeń mogą również występować w momencie otwarcia kolejki, w zależności od podanych opcji otwartych oraz typów aktywnych zabezpieczeń. z/OS Patrz także “Profile zabezpieczeń kontekstu” na stronie 221 i “Profile dla alternatywnego zabezpieczenia użytkownika” na stronie 219. W przypadku tabeli podsumowania przedstawiających opcje otwarcia oraz autoryzację zabezpieczeń, która jest wymagana w przypadku, gdy wszystkie aktywne są kolejki, kontekst i alternatywne zabezpieczenia użytkownika, patrz Tabela 36 na stronie 212.

W przypadku korzystania z funkcji publikowania/subskrypcji należy wziąć pod uwagę następujące kwestie. Gdy żądanie MQSUB jest przetwarzane, wykonywane jest sprawdzenie zabezpieczeń, aby upewnić się, że ID użytkownika udostępniający żądanie ma wymagany dostęp do umieszczenia komunikatów w docelowej kolejce IBM MQ oraz wymagany dostęp do subskrybowania tematu IBM MQ .

Tabela 32. Poziomy dostępu dla zabezpieczeń kolejki przy użyciu wywołania MQSUB

MQSUB, opcja	**Wymagany poziom dostępu RACF do hlq.queuename**
MQSO_ALTER, MQSO_CREATE i MQSO_RESUME	TEMPERATURY

Uwaga:

1. `hlq.queuename` jest kolejką docelową dla publikacji. Jeśli jest to kolejka zarządzana, wymagany jest dostęp do odpowiedniej kolejki modelowej, która ma być używana dla kolejki zarządzanej i utworzonej kolejki dynamicznej.
2. Można użyć takiej techniki dla kolejki docelowej udostępnianej w wywołaniu API MQSUB, jeśli użytkownik chce odróżnić użytkowników dokonających subskrypcji, a użytkownicy pobierający publikacje z kolejki docelowej.

z/OS *Uwagi dotyczące kolejek aliasowych*

Po wywołaniu wywołania MQOPEN lub MQPUT1 dla kolejki aliasowej program IBM MQ sprawdza, czy w wywołaniu znajduje się nazwa kolejki określona w deskryptorze obiektu (MQOD). Nie sprawdza, czy użytkownik ma dostęp do nazwy kolejki docelowej.

Na przykład: kolejka aliasowa o nazwie PAYROLL.REQUEST jest rozstrzygane do kolejki docelowej o wartości PAY.REQUEST. Jeśli zabezpieczenia kolejki są aktywne, użytkownik musi mieć uprawnienia tylko do uzyskania dostępu do kolejki PAYROLL.REQUEST. Sprawdzenie, czy użytkownik jest uprawniony do uzyskania dostępu do kolejki PAY.REQUEST.

z/OS *Używanie kolejek aliasowych do rozróżniania żądań MQGET i MQPUT*

Zakres wywołań MQI dostępnych na jednym poziomie dostępu może powodować problemy, jeśli dostęp do kolejki ma być ograniczony tylko do wywołania **MQPUT** lub tylko wywołania **MQGET** . Kolejkę można zabezpieczyć, definiując dwa aliasy, które są tłumaczone na tę kolejkę: jeden, który umożliwia aplikacjom pobieranie komunikatów z kolejki i drugi, który umożliwia aplikacjom umieszczanie komunikatów w kolejce.

Poniższy tekst przedstawia przykład definiowania kolejek w programie IBM MQ:

```
DEFINE QLOCAL(MUST_USE_ALIAS_TO_ACCESS) GET(ENABLED)
       PUT(ENABLED)

DEFINE QALIAS(USE_THIS_ONE_FOR_GETS) GET(ENABLED)
       PUT(DISABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)

DEFINE QALIAS(USE_THIS_ONE_FOR_PUTS) GET(DISABLED)
       PUT(ENABLED) TARGET(MUST_USE_ALIAS_TO_ACCESS)
```

Należy również utworzyć następujące definicje RACF :

```
RDEFINE MQQUEUE hlq.MUST_USE_ALIAS_TO_ACCESS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_GETS UACC(NONE)
RDEFINE MQQUEUE hlq.USE_THIS_ONE_FOR_PUTS UACC(NONE)
```

Następnie upewnij się, że żaden użytkownik nie ma dostępu do kolejki hlq.MUST_USE_ALIAS_TO_ACCESSi nadaj odpowiednim użytkownikom lub grupom dostęp do tego aliasu. Można to zrobić za pomocą następujących komend RACF :

```
PERMIT hlq.USE_THIS_ONE_FOR_GETS CLASS(MQQUEUE)
       ID(GETUSER,GETGRP) ACCESS(UPDATE)
PERMIT hlq.USE_THIS_ONE_FOR_PUTS CLASS(MQQUEUE)
       ID(PUTUSER,PUTGRP) ACCESS(UPDATE)
```

Oznacza to, że ID użytkownika GETUSER i ID użytkownika w grupie GETGRP mogą tylko uzyskiwać komunikaty w MUST_USE_ALIAS_TO_ACCESS za pośrednictwem kolejki aliasowej USE_THIS_ONE_FOR_GETS; a ID użytkownika PUTUSER i ID użytkownika w grupie PUTGRP mogą tylko umieszczać komunikaty w kolejce aliasowej USE_THIS_ONE_FOR_PUTS.

Uwaga:

1. Aby użyć takiej techniki, należy poinformować o tym twórców aplikacji, tak aby mogli oni odpowiednio zaprojektować swoje programy.

2. Takiej techniki można użyć dla kolejki docelowej, która została określona w żądaniu funkcji API MQSUB, aby odróżnić użytkowników dokonujących subskrypcji od użytkowników pobierających publikacje z kolejki docelowej.

z/OS *Uwagi dotyczące kolejek modelowych*

Aby otworzyć kolejkę modelową, należy być w stanie otworzyć zarówno samą kolejkę modelową, jak i kolejkę dynamiczną, do której jest ona tłumaczona. Definiowanie ogólnych profili produktu RACF dla kolejek dynamicznych, w tym kolejek dynamicznych używanych przez programy narzędziowe produktu IBM MQ .

Po otwarciu kolejki modelowej zabezpieczenia produktu IBM MQ sprawdzają dwie operacje sprawdzania zabezpieczeń kolejki:

1. Czy masz uprawnienia do uzyskiwania dostępu do kolejki modelowej?
2. Czy użytkownik jest uprawniony do uzyskiwania dostępu do kolejki dynamicznej, do której jest rozstrzygana kolejka modelowa?

Jeśli nazwa kolejki dynamicznej zawiera znak gwiazdki (*), to znak * jest zastępowany łańcuchem znakowym wygenerowanym przez produkt IBM MQ, aby utworzyć kolejkę dynamiczną o unikalnej nazwie. Jednak ze względu na to, że cała nazwa, w tym wygenerowany łańcuch, jest używana do sprawdzania uprawnień, należy zdefiniować profile ogólne dla tych kolejek.

Na przykład wywołanie MQOPEN korzysta z nazwy kolejki modelowej o nazwie CREDIT.CHECK.REPLY.MODEL i nazwa kolejki dynamicznej CREDIT.REPLY.* w menedżerze kolejek (lub grupie współużytkowania kolejek) MQSP.

W tym celu należy wprowadzić następujące komendy produktu RACF , aby zdefiniować wymagane profile kolejek:

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Aby zezwolić użytkownikowi na dostęp do tych profili, należy również wprowadzić odpowiednie komendy programu RACF PERMIT.

Typowa nazwa kolejki dynamicznej utworzona przez komendę MQOPEN jest taka sama jak CREDIT.REPLY.A346EF00367849A0. Dokładna wartość ostatniego kwalifikatora jest nieprzewidywalna; dlatego należy używać profili ogólnych dla takich nazw kolejek.

Liczba programów narzędziowych IBM MQ , które umieszczają komunikaty w kolejkach dynamicznych. Należy zdefiniować profile dla następujących dynamicznych nazw kolejek i zapewnić RACF dostęp UPDATE do odpowiednich identyfikatorów użytkowników (więcej informacji na ten temat zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244 , aby uzyskać odpowiednie identyfikatory użytkowników):

```
SYSTEM.CSQUTIL.*  (used by CSQUTIL)
SYSTEM.CSQOREXX.* (used by the operations and control panels)
SYSTEM.CSQXCMD.*  (used by the channel initiator when processing CSQINPX)
CSQ4SAMP.*        (used by the IBM MQ supplied samples)
```

Można również rozważyć zdefiniowanie profilu w celu kontrolowania użycia nazwy kolejki dynamicznej używanej domyślnie w elementach kopii programowania aplikacji. Pliki copybook dostarczane przez produkt IBM MQzawierają domyślną wartość *DynamicQName*, która jest CSQ. *. Umożliwia to ustanawianie odpowiedniego profilu produktu RACF .

Uwaga: Nie należy zezwalać programistom aplikacji na określenie pojedynczego znaku * dla nazwy kolejki dynamicznej. Jeśli to zrobisz, musisz zdefiniować hlq. * * Profil w klasie MQQUEUE, a użytkownik musiałby nadać mu szeroki dostęp. Oznacza to, że ten profil może być również używany dla innych kolejek

niedynamicznych, które nie mają bardziej konkretnego profilu produktu RACF . Użytkownicy mogą więc uzyskać dostęp do kolejek, których nie mają do nich dostęp.

z/OS *Zamknij opcje dla trwałych kolejek dynamicznych*

Jeśli aplikacja otwiera trwałą kolejkę dynamiczną, która została utworzona przez inną aplikację, a następnie próbuje usunąć tę kolejkę za pomocą opcji MQCLOSE , podczas próby wykonania tej próby zostaną zastosowane dodatkowe sprawdzenia zabezpieczeń.

Tabela 33. Poziomy dostępu dla opcji zamykania w stałych kolejkach dynamicznych

MQCLOSE, opcja	**Wymagany poziom dostępu RACF do hlq.queuename**
MQCO_DELETE	Zmień
MQCO_DELETE_PURGE	Zmień

z/OS *Bezpieczeństwo i kolejki zdalne*

Gdy komunikat jest umieszczany w kolejce zdalnej, zabezpieczenia kolejki implementowane przez lokalny menedżer kolejek zależą od sposobu, w jaki kolejka zdalna jest określona podczas otwierania.

Stosowane są następujące reguły:

1. Jeśli kolejka zdalna została zdefiniowana w lokalnym menedżerze kolejek za pomocą komendy IBM MQ DEFINE QREMOTE, kolejka, która jest sprawdzona, jest nazwą kolejki zdalnej. Na przykład, jeśli kolejka zdalna jest zdefiniowana w menedżerze kolejek MQS1 w następujący sposób:

   ```
   DEFINE QREMOTE(BANK7.CREDIT.REFERENCE)
          RNAME(CREDIT.SCORING.REQUEST)
          RQMNAME(BNK7)
          XMITQ(BANK1.TO.BANK7)
   ```

   W tym przypadku profil dla BANK7.CREDIT.REFERENCE musi być zdefiniowana w klasie MQQUEUE.
2. Jeśli nazwa *ObjectQMgrName* dla żądania nie jest rozstrzygana w lokalnym menedżerze kolejek, to sprawdzenie zabezpieczeń jest wykonywane w odniesieniu do rozwiązanej (zdalnej) nazwy menedżera kolejek z wyjątkiem przypadku kolejki klastra, w której wykonywane jest sprawdzenie nazwy kolejki klastra.

   Na przykład kolejka transmisji BANK1.TO.BANK7 jest zdefiniowany w menedżerze kolejek MQS1. Żądanie MQPUT1 jest następnie wysyłane w produkcie MQS1 , określając parametr *ObjectName* jako BANK1.INTERBANK.TRANSFERS i *ObjectQMgrName* z BANK1.TO.BANK7. W takim przypadku użytkownik wykonujący żądanie musi mieć dostęp do BANK1.TO.BANK7.
3. Jeśli żądanie MQPUT zostanie wysłane do kolejki, a parametr *ObjectQMgrName* zostanie określony jako alias lokalnego menedżera kolejek, tylko nazwa kolejki zostanie sprawdzona pod kątem zabezpieczeń, a nie dla menedżera kolejek.

Gdy komunikat zostanie wysłany do zdalnego menedżera kolejek, może on zostać poddany dodatkowym przetwarzaniu zabezpieczeń. Więcej informacji na ten temat zawiera “Zabezpieczenia dla zdalnego przesyłania komunikatów” na stronie 97.

z/OS *Zabezpieczenia kolejki niedostarczanych komunikatów*

Uwagi specjalne mają zastosowanie do kolejki niedostarczonych komunikatów, ponieważ wielu użytkowników musi mieć możliwość umieszczania na nim komunikatów, ale dostęp do pobierania komunikatów musi być ściśle ograniczony. Można to osiągnąć, stosując różne uprawnienia RACF do kolejki niedostarczonych komunikatów i do kolejki aliasowej.

Niedostarczone komunikaty mogą być umieszczane w specjalnej kolejce zwanej kolejką niedostarczonych komunikatów. Jeśli istnieją poufne dane, które mogą być prawdopodobnie zakończone w tej kolejce, należy wziąć pod uwagę ich konsekwencje, ponieważ użytkownik nie chce, aby nieuprawnieni użytkownicy mogli pobrać te dane.

Aby możliwe było umieszczanie komunikatów w kolejce niedostarczonych komunikatów, muszą być dozwolone następujące działania:

- Programy użytkowe.
- Przestrzeń adresowa inicjatora kanału i wszystkie identyfikatory użytkownika MCA. (Jeśli profil RESLEVEL nie jest obecny lub jest zdefiniowany w taki sposób, że sprawdzane są identyfikatory użytkowników kanału, identyfikator użytkownika kanału musi także mieć uprawnienia do umieszczania komunikatów w kolejce niedostarczonych komunikatów).
- CKTI, inicjator zadania CICS dostarczony przez CICS.
- CSQQTRMN, IBM MQ-dostarczony monitor wyzwalacza IMS .

Jedyną aplikacją, która może pobierać komunikaty z kolejki niedostarczonych komunikatów, powinna być aplikacją specjalną, która przetwarza te komunikaty. Jednak pojawia się problem, jeśli użytkownik poda aplikacjom RACF uprawnienie UPDATE do kolejki niedostarczonych komunikatów dla MQPUT , ponieważ mogą one następnie automatycznie pobierać komunikaty z kolejki za pomocą wywołań MQGET . Nie można wyłączyć kolejki niedostarczonych komunikatów dla operacji pobierania, ponieważ w przeciwnym razie nawet aplikacje specjalne nie pobierają komunikatów.

Jednym z rozwiązań tego problemu jest skonfigurowanie dwupoziomowego dostępu do kolejki niedostarczonych komunikatów. CKTI, transakcje agenta kanału komunikatów lub przestrzeń adresowa inicjatora kanału oraz aplikacje 'specjalne' mają bezpośredni dostęp; inne aplikacje mogą uzyskać dostęp do kolejki niewysłanych wiadomości tylko przez kolejkę aliasową. Ten alias jest zdefiniowany, aby umożliwić aplikacjom umieszczanie komunikatów w kolejce niedostarczonych komunikatów, ale nie w celu pobierania z niego komunikatów.

W ten sposób może działać:

1. Zdefiniuj rzeczywistą kolejkę niedostarczonych komunikatów z atrybutami PUT (ENABLED) i GET (ENABLED), tak jak pokazano to w przykładowym thlqual.SCSQPROC(CSQ4INYG).
2. Nadaj uprawnienie RACF UPDATE dla kolejki niedostarczonych komunikatów do następujących identyfikatorów użytkowników:
   - Identyfikatory użytkowników, których przestrzeń adresowa CKTI i MCAs lub inicjator kanału są uruchamiane w ramach.
   - Identyfikatory użytkowników powiązane z aplikacją do przetwarzania niewysłanych wiadomości w ramach specjalnego pliku.
3. Zdefiniuj kolejkę aliasową, która jest tłumaczona na rzeczywistą kolejkę niedostarczonych komunikatów, ale podaj kolejkę aliasową dla następujących atrybutów: PUT (ENABLED) i GET (DISABLED). Nadaj kolejce aliasowej nazwę z tym samym rdzeniem, co nazwa kolejki niedostarczonych komunikatów, ale dopisz znaki ". PUT" do tego rdzenia. Na przykład, jeśli nazwa kolejki niedostarczonych komunikatów to hlq.DEAD.QUEUE, nazwą kolejki aliasowej jest hlq.DEAD.QUEUE.PUT.
4. Aby umieścić komunikat w kolejce niedostarczonych komunikatów, aplikacja korzysta z kolejki aliasowej. To jest to, co aplikacja musi wykonać:
   - Pobiera nazwę rzeczywistej kolejki niedostarczonych komunikatów. W tym celu otwiera obiekt menedżera kolejek za pomocą komendy MQOPEN , a następnie wysyła komendę MQINQ , aby uzyskać nazwę kolejki niedostarczonych komunikatów.
   - Zbuduj nazwę kolejki aliasowej, dodając znaki '.PUT' do tej nazwy, w tym przypadku hlq.DEAD.QUEUE.PUT.
   - Otwórz kolejkę aliasową hlq.DEAD.QUEUE.PUT.
   - Umieść komunikat w rzeczywistej kolejce niedostarczonych komunikatów, wydając komendę MQPUT dla kolejki aliasowej.
5. Podaj identyfikator użytkownika powiązany z uprawnieniem UPDATE RACF aplikacji do aliasu, ale nie ma dostępu (uprawnienie NONE) do rzeczywistej kolejki niedostarczonych komunikatów. Oznacza to, że:

- Aplikacja może umieszczać komunikaty w kolejce niedostarczonych komunikatów przy użyciu kolejki aliasowej.
- Aplikacja nie może pobrać komunikatów z kolejki niedostarczonych komunikatów przy użyciu kolejki aliasowej, ponieważ kolejka aliasowa jest wyłączona w celu uzyskania operacji pobierania.

Aplikacja nie może pobrać żadnych komunikatów z rzeczywistej kolejki niedostarczonych komunikatów, ponieważ ma on poprawne uprawnienia RACF .

Tabela 34 na stronie 210 podsumowuje uprawnienia RACF wymagane dla różnych uczestników tego rozwiązania.

Tabela 34. Uprawnienie RACF do kolejki niedostarczonych komunikatów i jej aliasu

Powiązane identyfikatory użytkowników	**Rzeczywista kolejka niedostarczonych komunikatów (hlq.DEAD.QUEUE)**	**Kolejka niedostarczonych komunikatów (hlq.DEAD.QUEUE.PUT)**
Przestrzeń adresowa MCA lub inicjatora kanału oraz CKTI	UPDATE	BRAK
Aplikacja "Special" (dla przetwarzania w kolejce niedostarczonych komunikatów)	UPDATE	BRAK
Identyfikatory użytkowników aplikacji napisanych przez użytkownika	BRAK	UPDATE

Jeśli używana jest ta metoda, aplikacja nie może określić maksymalnej długości komunikatu (MAXMSGL) dla kolejki niedostarczonych komunikatów. Wynika to z faktu, że atrybut MAXMSGL nie może zostać pobrany z kolejki aliasowej. Dlatego w aplikacji należy przyjąć, że maksymalna długość komunikatu wynosi 100 MB, a maksymalna wielkość obsługiwana przez IBM MQ for z/OS . Rzeczywista kolejka niedostarczonych komunikatów powinna być również zdefiniowana z atrybutem MAXMSGL o wielkości 100 MB.

Uwaga: Programy użytkowe napisane przez użytkownika zwykle nie używają alternatywnych uprawnień użytkownika do umieszczania komunikatów w kolejce niedostarczonych komunikatów. Zmniejsza to liczbę identyfikatorów użytkowników, którzy mają dostęp do kolejki niedostarczonych komunikatów.

z/OS *Bezpieczeństwo kolejki systemowej*

Aby umożliwić niektórym użytkownikom dostęp do konkretnych kolejek systemowych, należy skonfigurować dostęp do produktu RACF .

Dostęp do wielu kolejek systemowych uzyskuje się przez dodatkowe części produktu IBM MQ:

- Program narzędziowy CSQUTIL
- Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL)
- Panele kontrolne i operacje
- Przestrzeń adresowa inicjatora kanału (łącznie z umieszczonym w kolejce demonem publikowania/subskrypcji)
- V 9.1.0 Serwer mqweb, używany przez produkty MQ Console i REST API.

Identyfikatory użytkowników, pod którymi te uruchomienie muszą mieć dostęp RACF do tych kolejek, jak to pokazano w Tabela 35 na stronie 211.

Tabela 35. Dostęp wymagany do kolejek SYSTEM przez IBM MQ

SYSTEM, kolejka	CSQUTIL	CSQ0UTIL	serwer mqweb	Operacje i panele kontrolne	Inicjator kanału dla rozproszonego kolejkowania
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	UPDATE
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	UPDATE	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	Zmień
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	Zmień
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	Zmień
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	UPDATE
SYSTEM.CHANNEL.INITQ	-	-	-	-	UPDATE
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	UPDATE
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	Zmień
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	UPDATE
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	Zmień
SYSTEM.COMMAND.INPUT	UPDATE	-	-	UPDATE	UPDATE
SYSTEM.COMMAND.REPLY.*	-	-	-	-	UPDATE
SYSTEM.COMMAND.REPLY.MODEL	UPDATE	-	-	UPDATE	UPDATE
SYSTEM.CSQOREXX.*	-	-	-	UPDATE	-
SYSTEM.CSQUTIL.*	UPDATE	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	UPDATE
SYSTEM.HIERARCHY.STATE	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	UPDATE
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	UPDATE
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	UPDATE
SYSTEM.PROTECTION.POLICY.QUEUE	-	Aktualizacja“1” na stronie 212	-	-	READ
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	UPDATE
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	UPDATE
SYSTEM.REST.REPLY.QUEUE	-	-	UPDATE	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	UPDATE

Uwagi:

1. Użytkownik przestrzeni adresowej Advanced Message Security wymaga również dostępu z uprawnieniami READ do tej kolejki.

z/OS *Interfejs API-szybki przegląd dostępu do zabezpieczeń zasobów*

Podsumowanie opcji **MQOPEN**, **MQPUT1**, **MQSUB**i **MQCLOSE** oraz dostęp wymagany przez różne typy zabezpieczeń zasobów.

Tabela 36. Opcje MQOPEN, MQPUT1, MQSUB i MQCLOSE oraz wymagane autoryzacje zabezpieczeń. Wywołania pokazywane w ten sposób **(1)** odnoszą się do uwag następujących po tej tabeli.

	Wymagany jest minimalny poziom dostępu RACF			
RACF Klasa:	**MXTOPIC**	**MQQUEUE lub MXQUEUE (1)**	**MQADMIN lub MXADMIN**	**MQADMIN lub MXADMIN**
RACF Profil:	**(15 lub 16)**	**(2)**	**(3)**	**(4)**
Opcja MQOPEN				
MQOO_INQUIRE		ODCZYT **(5)**	Brak sprawdzenia	Brak sprawdzenia
MQOO_BROWSE		READ	Brak sprawdzenia	Brak sprawdzenia
MQOO_INPUT_ *		UPDATE	Brak sprawdzenia	Brak sprawdzenia
MQOO_SAVE_ALL_CONTEXT **(6)**		UPDATE	Brak sprawdzenia	Brak sprawdzenia
MQOO_OUTPUT (USAGE = NORMAL) **(7)**		UPDATE	Brak sprawdzenia	Brak sprawdzenia
MQOO_PASS_IDENTITY_CONTEXT **(8)**		UPDATE	READ	Brak sprawdzenia
MQOO_PASS_ALL_CONTEXT **(8) (9)**		UPDATE	READ	Brak sprawdzenia
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		UPDATE	UPDATE	Brak sprawdzenia
MQOO_SET_ALL_CONTEXT **(8) (10)**		UPDATE	CONTROL	Brak sprawdzenia
MQOO_OUTPUT (USAGE (XMITQ) **(11)**		UPDATE	CONTROL	Brak sprawdzenia
MQOO_OUTPUT (obiekt tematu)	UPDATE **(16)**			
MQOO_OUTPUT (kolejka aliasowa do obiektu tematu)	UPDATE **(16)**	UPDATE		
MQOO_SET		Zmień	Brak sprawdzenia	Brak sprawdzenia
MQOO_ALTERNATE_USER_AUTHORITY		**(12)**	**(12)**	UPDATE
Opcja MQPUT1				
Umieszczanie w normalnej kolejce **(7)**		UPDATE	Brak sprawdzenia	Brak sprawdzenia

Tabela 36. Opcje MQOPEN, MQPUT1, MQSUB i MQCLOSE oraz wymagane autoryzacje zabezpieczeń. Wywołania pokazywane w ten sposób **(1)** odnoszą się do uwag następujących po tej tabeli. *(kontynuacja)*

	Wymagany jest minimalny poziom dostępu RACF			
RACF Klasa:	**MXTOPIC**	**MQQUEUE lub MXQUEUE (1)**	**MQADMIN lub MXADMIN**	**MQADMIN lub MXADMIN**
RACF Profil:	**(15 lub 16)**	**(2)**	**(3)**	**(4)**
MQPMO_PASS_IDENTITY_CONTEXT		UPDATE	READ	Brak sprawdzenia
MQPMO_PASS_ALL_CONTEXT		UPDATE	READ	Brak sprawdzenia
MQPMO_SET_IDENTITY_CONTEXT		UPDATE	UPDATE	Brak sprawdzenia
MQPMO_SET_ALL_CONTEXT		UPDATE	CONTROL	Brak sprawdzenia
MQOO_OUTPUT Umieszczanie w kolejce transmisji **(11)**		UPDATE	CONTROL	Brak sprawdzenia
MQOO_OUTPUT (obiekt tematu)	UPDATE **(16)**			
MQOO_OUTPUT (kolejka aliasowa do obiektu tematu)	UPDATE **(16)**	UPDATE		
MQPMO_ALTERNATE_USER_AUTHORITY		**(13)**	**(13)**	UPDATE
Opcja `MQCLOSE`				
MQCO_DELETE **(14)**		Zmień	Brak sprawdzenia	Brak sprawdzenia
MQCO_DELETE_PURGE **(14)**		Zmień	Brak sprawdzenia	Brak sprawdzenia
MQCO_REMOVE_SUB	ALTER **(15)**			
Opcja `MQSUB`				
MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER	ALTER **(15)**	**(17)**	**(18)**	
MQSO_RESUME	ODCZYT **(15)**	**(17)**	Brak sprawdzenia	
MQSO_ALTERNATE_USER_AUTHORITY				UPDATE
MQSO_SET_IDENTITY_CONTEXT			**(18)**	

Uwaga:

1. Ta opcja nie jest ograniczona do kolejek. Użyj klasy MQNLIST lub MXNLIST dla list nazw, a także klasy MQPROC lub MXPROC dla procesów.
2. Użyj profilu RACF : hlq.resourcename
3. Użyj profilu RACF : hlq.CONTEXT.queuename
4. Użyj profilu RACF : hlq.ALTERNATE.USER. `alternateuserid`

alternateuserid to identyfikator użytkownika określony w polu *AlternateUserId* deskryptora obiektu. Należy pamiętać, że do tego sprawdzenia używane są maksymalnie 12 znaków w polu *AlternateUserId* , w przeciwieństwie do innych sprawdzeń, w których używane są tylko pierwsze 8 znaków identyfikatora użytkownika.

5. Podczas otwierania menedżera kolejek na potrzeby zapytań nie jest wykonywane żadne sprawdzenie.
6. Parametr MQOO_INPUT_ * musi być również określony. Jest to poprawne dla lokalnej, modelu lub kolejki aliasowej.
7. To sprawdzenie jest wykonywane dla lokalnej lub modelowej kolejki, która ma atrybut kolejki **Usage** MQUS_NORMAL, a także dla aliasu lub zdalnej kolejki (która jest zdefiniowana dla połączonego menedżera kolejek). Jeśli kolejka jest kolejką zdalną, która jest otwierana, określając jawnie *ObjectQMgrName* (nie nazwę połączonego menedżera kolejek) jawnie, to sprawdzenie jest wykonywane względem kolejki o takiej samej nazwie jak *ObjectQMgrName* (która musi być kolejką lokalną z atrybutem kolejki **Usage** o wartości MQUS_TRANSMISSION).
8. Należy również określić parametr MQOO_OUTPUT.
9. Opcja MQOO_PASS_IDENTITY_CONTEXT jest implikowana również przez tę opcję.
10. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT i MQOO_SET_IDENTITY_CONTEXT są również rozumiane przy użyciu tej opcji.
11. To sprawdzenie jest wykonywane dla lokalnej lub modelowej kolejki, która ma atrybut kolejki produktu **Usage** o wartości MQUS_TRANSMISSION, i jest otwierana bezpośrednio na potrzeby danych wyjściowych. Nie ma zastosowania, jeśli kolejka zdalna jest otwierana.
12. Należy również określić co najmniej jedną z następujących wartości: MQOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET. Przeprowadzone sprawdzenie jest takie samo, jak w przypadku pozostałych określonych opcji.
13. Przeprowadzone sprawdzenie jest takie samo, jak w przypadku pozostałych określonych opcji.
14. Dotyczy to tylko trwałych kolejek dynamicznych, które zostały otwarte bezpośrednio, czyli nie są otwierane w kolejce modelowej. Do usunięcia tymczasowej kolejki dynamicznej nie jest wymagane żadne zabezpieczenia.
15. Użyj profilu RACF hlq.SUBSCRIBE.topicname.
16. Użyj profilu RACF hlq.PUBLISH.topicname.
17. Jeśli w żądaniu MQSUB określono kolejkę docelową dla publikacji, do których mają zostać wysłane publikacje, to w tej kolejce wykonywane jest sprawdzenie zabezpieczeń, aby upewnić się, że użytkownik umieł uprawnienie do tej kolejki.
18. Jeśli w żądaniu MQSUB określono opcje MQSO_CREATE lub MQSO_ALTER, konieczne jest ustawienie dowolnego z pól kontekstu tożsamości w strukturze MQSD. Należy również określić opcję MQSO_SET_IDENTITY_CONTEXT, a także odpowiednie uprawnienia do profilu kontekstu dla kolejki docelowej.

z/OS *Profile dla zabezpieczeń tematów*

Jeśli zabezpieczenia tematów są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników.

Pojęcie zabezpieczeń tematu w drzewie tematów jest opisane w sekcji Zabezpieczenia publikowania/subskrypcji.

Jeśli zabezpieczenia tematów są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach **MXTOPIC** lub **GMXTOPIC** .
- Należy zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników, tak aby mogły one wydawać żądania API IBM MQ , które korzystają z tematów.

Profile dotyczące zabezpieczeń tematów mają następującą postać:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

where

- `hlq` to `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek).
- `topicname` to nazwa węzła administracyjnego tematu w drzewie tematów, powiązana z tematem subskrybowanym za pomocą wywołania MQSUB lub publikowana w wywołaniu MQOPEN.

Profil poprzedzony przez nazwę menedżera kolejek steruje dostępem do pojedynczego tematu w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje dostępem do jednego lub większej liczby tematów z tą nazwą tematu we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tego tematu w menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

Subskrybowanie

Aby zasubskrybować temat, wymagany jest dostęp do tematu, który ma zostać zasubskrybowany, oraz do kolejki docelowej dla publikacji.

Po wydaniu żądania MQSUB wykonywane są następujące sprawdzenia zabezpieczeń:

- Określa, czy użytkownik ma odpowiedni poziom dostępu do subskrybowania tego tematu, a także czy kolejka docelowa (jeśli została określona) jest otwarta dla danych wyjściowych
- Określa, czy użytkownik ma odpowiedni poziom dostępu do tej kolejki docelowej.

Tabela 37. Poziom dostępu wymagany w celu zasubskrybowania zabezpieczeń tematów

MQSUB, opcja	**RACF access required to `hlq.SUBSCRIBE.topicname` profile in MXTOPIC class**
MQSO_CREATE i MQSO_ALTER	Zmień
MQSO_RESUME	ODCZYT

Tabela 38. Dodatkowe uprawnienia wymagane do subskrypcji przy użyciu niezarządzanej kolejki docelowej

MQSUB, opcja	**Dostęp do produktu RACF wymagany do profilu produktu `hlq.CONTEXT.queuename` w klasie MQADMIN lub MXADMIN**
MQSO_CREATE, MQSO_ALTER i MQSO_RESUME	TEMPERATURY
	RACF dostęp wymagany do profilu `hlq.queuename` w klasie MQQUEUE lub MXQUEUE
MQSO_CREATE i MQSO_ALTER	TEMPERATURY
	RACF wymagany dostęp do profilu produktu `hlq.ALTERNATE.USER.alternateuserid` w klasie MQADMIN lub MXADMIN
MQSO_ALTERNATE_USER_AUTHORITY	TEMPERATURY

Uwagi dotyczące kolejek zarządzanych dla subskrypcji

Sprawdzenie zabezpieczeń jest wykonywane w celu sprawdzenia, czy użytkownik jest uprawniony do subskrybowania tematu. Jednak podczas tworzenia kolejki zarządzanej nie są przeprowadzane

żadne sprawdzenia zabezpieczeń lub w celu określenia, czy użytkownik ma dostęp do umieszczania komunikatów w tej kolejce docelowej.

Nie można zamknąć usuwania kolejki zarządzanej.

Używane kolejki modelowe to: SYSTEM.DURABLE.MODEL.QUEUE i SYSTEM.NDURABLE.MODEL.QUEUE.

Kolejki zarządzane utworzone z tych kolejek modelowych mają postać SYSTEM.MANAGED.DURABLE.A346EF00367849A0 i SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0 , gdzie ostatni kwalifikator jest nieprzewidywalny.

Nie należy nadawać użytkownikowi dostępu do tych kolejek. Kolejki mogą być chronione za pomocą profili ogólnych w postaci SYSTEM.MANAGED.DURABLE.* i SYSTEM.MANAGED.NDURABLE.* bez żadnych uprawnień.

Komunikaty mogą być pobierane z tych kolejek za pomocą uchwytu zwróconego w żądaniu MQSUB.

Jeśli użytkownik jawnie wyda wywołanie MQCLOSE dla subskrypcji z określoną opcją MQCO_REMOVE_SUB, a użytkownik nie utworzył subskrypcji, która jest zamykana pod tym uchwytem, to w momencie zamknięcia jest wykonywane sprawdzenie zabezpieczeń, aby upewnić się, że użytkownik ma odpowiednie uprawnienia do wykonania operacji.

Tabela 39. Poziom dostępu wymagany do profili zabezpieczeń tematów w celu zamknięcia operacji subskrypcji.

MQCLOSE, opcja	**RACF access required to hlq.SUBSCRIBE.topicname profile in MXTOPIC class**
MQCO_REMOVE_SUB	Zmień

Publikowanie

Aby opublikować w temacie, należy uzyskać dostęp do tematu, a jeśli używane są kolejki aliasowe, również do kolejki aliasowej.

Tabela 40. Poziom dostępu wymagany dla zabezpieczeń tematów do opublikowania

MQOPEN lub MQPUT1 -opcja	**RACF access required to hlq.PUBLISH.topicname profile in MXTOPIC class**
MQOO_OUTPUT lub MQPUT1	TEMPERATURY

Tabela 41. Poziom dostępu wymagany do otwarcia kolejki aliasowej, która jest tłumaczona na dany temat

MQOPEN lub MQPUT1 -opcja	**Dostęp do bazy danych RACF wymagany do profilu hlq.queuename w klasie MQQUEUE lub MXQUEUE dla kolejki aliasowej**
MQOO_OUTPUT lub MQPUT1	TEMPERATURY

Szczegółowe informacje na temat działania zabezpieczeń tematów w przypadku, gdy kolejka aliasowa tłumaczona na nazwę tematu jest otwierana do publikowania, zawiera sekcja “Uwagi dotyczące kolejek aliasowych rozstrzyganych w tematach dotyczących operacji publikowania” na stronie 217.

W przypadku rozważenia kolejek aliasowych używanych dla kolejek docelowych dla ograniczeń PUT lub GET, patrz “Uwagi dotyczące kolejek aliasowych” na stronie 206.

Jeśli poziom dostępu aplikacji RACF do profilu zabezpieczeń tematu zostanie zmieniony, zmiany zostaną uwzględnione tylko dla wszystkich nowo uzyskanych uchwytów obiektów (czyli nowego obiektu MQSUB lub MQOPEN) dla tego tematu. Te uchwyty, które już istnieją w momencie zmiany, zachowują istniejący dostęp do tematu. Również dotychczasowi subskrybenci zachowują swój dostęp do wszelkich subskrypcji, które już dokonali.

Uwagi dotyczące kolejek aliasowych rozstrzyganych w tematach dotyczących operacji publikowania

Po wywołaniu wywołania MQOPEN lub MQPUT1 dla kolejki aliasowej, która jest tłumaczona na dany temat, program IBM MQ sprawdza, czy dwa zasoby są sprawdzane:

- Pierwszy z nazwą kolejki aliasowej określoną w deskryptorze obiektu (MQOD) w wywołaniu MQOPEN lub MQPUT1 .
- Drugi w odniesieniu do tematu, do którego rozstrzygana jest kolejka aliasowa

Należy pamiętać, że to zachowanie różni się od zachowania, które można uzyskać, gdy kolejki aliasowe są rozstrzygane do innych kolejek. Aby działanie publikowania było kontynuowane, wymagany jest poprawny dostęp do obu profili.

Zabezpieczenia tematów systemowych

Przestrzeń adresowa inicjatora kanału uzyskuje dostęp do następujących tematów systemowych.

The user IDs under which this runs must be given RACF access to these queues, as shown in Tabela 42 na stronie 217.

Tabela 42. Dostęp wymagany do tematów SYSTEM

Temat SYSTEM	Profil	Inicjator kanału dla rozproszonego kolejkowania
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	TEMPERATURY
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	Zmień

z/OS *Profile dla procesów*

Jeśli zabezpieczenia procesu są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników.

Jeśli zabezpieczenia procesu są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach **MQPROC** lub **GMQPROC** , jeśli używane są wielkie profile.
- Zdefiniuj profile w klasach **MXPROC** lub **GMXPROC** , jeśli używane są mieszane profile spraw.
- Należy zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników, tak aby mogły one wydawać żądania API IBM MQ , które korzystają z procesów.

Profile dla procesów mają następującą postać:

```
hlq.processname
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `processname` to nazwa otwieranego procesu.

Profil poprzedzony przez nazwę menedżera kolejek steruje dostępem do pojedynczej definicji procesu w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje dostępem do jednej lub większej liczby definicji procesów o tej nazwie we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tej definicji procesu w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ

sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

W poniższej tabeli przedstawiono dostęp wymagany do otwarcia procesu.

Tabela 43. Poziomy dostępu dla zabezpieczeń procesu

MQOPEN, opcja	**Wymagany jest poziom dostępu RACF do hlq.processname**
MQOO_INQUIRE	READ

Na przykład w menedżerze kolejek MQS9, grupa RACF INQVPRC musi mieć możliwość zapytania (`MQINQ`) we wszystkich procesach, począwszy od litery V. Definicje RACF dla tego typu to:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

Alternatywne zabezpieczenia użytkownika mogą być również aktywne, w zależności od otwartych opcji określonych podczas otwierania obiektu definicji procesu.

z/OS *Profile dla list nazw*

Jeśli zabezpieczenia listy nazw są aktywne, należy zdefiniować profile w odpowiednich klasach i nadać niezbędne grupy lub identyfikatory użytkowników do tych profili.

Jeśli zabezpieczenia listy nazw są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach **MQNLIST** lub **GMQNLIST** , jeśli używane są wielkie profile.
- Zdefiniuj profile w klasach **MXNLIST** lub **GMXNLIST** , jeśli używane są mieszane profile spraw.
- Zezwól na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników.

Profile dla list nazw mają następującą postać:

```
hlq.namelistname
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `namelistname` to nazwa otwieranej listy nazw.

Profil poprzedzony przez nazwę menedżera kolejek steruje dostępem do pojedynczej listy nazw w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje dostępem do jednego lub większej liczby list nazw z tą nazwą we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tej listy nazw w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

W poniższej tabeli przedstawiono dostęp wymagany do otwarcia listy nazw.

Tabela 44. Poziomy dostępu dla zabezpieczeń listy nazw

MQOPEN, opcja	**Wymagany jest poziom dostępu RACF do hlq.namelistname**
MQOO_INQUIRE	READ

Na przykład w menedżerze kolejek (lub grupie współużytkowania kolejek) PQM3, grupa RACF DEPT571 musi mieć możliwość zapytania (`MQINQ`) na tych listach nazw:

- Wszystkie listy nazw rozpoczynają się od "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/ŻĄDANIE/KOLEJKI
- WAREHOUSE.BROADCAST

Definicje produktu RACF , które mają być używane, są następujące:

```
RDEFINE MQNLIST PQM3.DEPT571.** UACC(NONE)
PERMIT PQM3.DEPT571.** CLASS(MQNLIST) ID(DEPT571) ACCESS(READ)

RDEFINE GMQNLIST NLISTS.FOR.DEPT571 UACC(NONE)
        ADDMEM(PQM3.PRINTER/DESTINATIONS/DEPT571,
               PQM3.AGENCY/REQUEST/QUEUES,
               PQM3.WAREHOUSE.BROADCAST)
PERMIT NLISTS.FOR.DEPT571 CLASS(GMQNLIST) ID(DEPT571) ACCESS(READ)
```

Alternatywne zabezpieczenia użytkownika mogą być aktywne, w zależności od opcji określonych podczas otwierania obiektu listy nazw.

Zabezpieczenia listy nazw systemów

Wiele list nazw systemów jest używanych przez dodatkowe części produktu IBM MQ:

- Program narzędziowy CSQUTIL
- Panele kontrolne i operacje
- Przestrzeń adresowa inicjatora kanału (w tym umieszczana w kolejce demon publikowania/subskrypcji)

Identyfikatory użytkowników, pod którymi są one uruchamiane, muszą mieć dostęp RACF do tych list nazw, jak to pokazano w Tabela 45 na stronie 219.

Tabela 45. Dostęp wymagany do list nazw SYSTEM przez IBM MQ

Systemowa lista nazw	CSQUTIL	Operacje i panele kontrolne	Inicjator kanału dla rozproszonego kolejkowania
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ

z/OS *Profile dla alternatywnego zabezpieczenia użytkownika*

Jeśli alternatywne zabezpieczenia użytkownika są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników.

Więcej informacji na temat produktu *AlternateUserId*zawiera sekcja Identyfikator użytkownikaAlternateUser(MQCHAR12).

Jeśli alternatywne zabezpieczenia użytkownika są aktywne, należy:

- Zdefiniuj profile w klasach MQADMIN lub GMQADMIN, jeśli używane są wielkie profile.
- Zdefiniuj profile w klasach MXADMIN lub GMXADMIN, jeśli używane są profile mieszanych przypadków.

Należy zezwolić na dostęp do tych profili przez niezbędne grupy lub identyfikatory użytkowników, aby umożliwić im korzystanie z opcji ALTERNATE_USER_AUTHORITY podczas otwierania obiektu.

Profile dla alternatywnych zabezpieczeń użytkownika można określić na poziomie podsystemu lub na poziomie grupy współużytkowania kolejki i przyjąć następujący formularz:

```
hlq.ALTERNATE.USER.alternateuserid
```

Gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `alternateuserid` to wartość pola *AlternateUserId* w deskryptorze obiektu.

Profil poprzedzony przez nazwę menedżera kolejek steruje użyciem alternatywnego identyfikatora użytkownika w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje użyciem alternatywnego identyfikatora użytkownika we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten alternatywny identyfikator użytkownika może być używany w dowolnym menedżerze kolejek w ramach grupy współużytkowania kolejek przez użytkownika, który ma poprawny dostęp. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tego alternatywnego identyfikatora użytkownika w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

W poniższej tabeli przedstawiono dostęp podczas określania alternatywnej opcji użytkownika.

Tabela 46. Poziomy dostępu dla alternatywnych zabezpieczeń użytkownika

MQOPEN, MQSUB lub MQPUT1 -opcja	**Wymagany poziom dostępu RACF**
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	UPDATE

Oprócz innych sprawdzeń zabezpieczeń użytkownika, można również wprowadzić inne sprawdzenia zabezpieczeń dla kolejki, procesu, listy nazw i zabezpieczeń kontekstu. Alternatywny identyfikator użytkownika, jeśli został podany, jest używany tylko do sprawdzania zabezpieczeń w kolejkach, definicjach procesów lub zasobach listy nazw. W przypadku alternatywnych sprawdzeń zabezpieczeń użytkownika i kontekstu identyfikator użytkownika żądającego sprawdzenia jest używany. Szczegółowe informacje na temat sposobu obsługi identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244. W przypadku tabeli podsumowania przedstawiających otwarte opcje oraz sprawdzenia zabezpieczeń wymagane w przypadku, gdy kolejka, kontekst i alternatywne zabezpieczenia użytkownika są aktywne, patrz Tabela 36 na stronie 212.

Alternatywny profil użytkownika nadaje użytkownikowi żądającego dostępu do zasobów powiązanych z identyfikatorem użytkownika określonym w alternatywnym identyfikatorze użytkownika. Na przykład serwer płac działający w ramach ID użytkownika PAYSERV w menedżerze kolejek QMPY przetwarza żądania od identyfikatorów użytkowników personelu, z których wszystkie rozpoczynają się od PS. Aby spowodować, że praca wykonywana przez serwer płac zostanie wykonana zgodnie z identyfikatorem użytkownika wysyłającego żądanie, zostanie użyte alternatywne uprawnienie użytkownika. Serwer payroll wie, który ID użytkownika określa się jako alternatywny ID użytkownika, ponieważ programy wysyłające komunikaty generują komunikaty przy użyciu opcji komunikatu umieszczonego w tabeli MQPMO_DEFAULT_CONTEXT. Więcej informacji na temat miejsca uzyskania alternatywnych identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244 .

W poniższym przykładzie przedstawiono definicje RACF , które umożliwiają serwerowi określenie alternatywnych identyfikatorów użytkowników, zaczynając od znaków PS:

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

Uwaga:

1. Pola *AlternateUserId* w deskryptorze obiektu i deskryptorze subskrypcji mają długość 12 bajtów. W kontrolach profilu używane są wszystkie 12 bajtów, ale jako ID użytkownika przez IBM MQużywane są tylko pierwsze 8 bajtów. Jeśli obcięcie tego identyfikatora użytkownika nie jest pożądane, programy aplikacji tworające żądanie muszą przetłumaczyć dowolny alternatywny ID użytkownika o więcej niż 8 bajtów w coś bardziej odpowiedniego.
2. Jeśli użytkownik określi opcję MQOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY lub MQPMO_ALTERNATE_USER_AUTHORITY, a w deskryptorze obiektu nie zostanie określone pole *AlternateUserId* , zostanie użyty identyfikator użytkownika odstępów. Na potrzeby alternatywnego sprawdzenia zabezpieczeń użytkownika ID użytkownika użyty dla kwalifikatora *AlternateUserId* jest -BLANK-. Na przykład `RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-`.

   Jeśli użytkownik może uzyskać dostęp do tego profilu, wszystkie dalsze operacje sprawdzania są wykonywane przy użyciu identyfikatora użytkownika odstępów. Szczegółowe informacje na temat pustych identyfikatorów użytkowników zawiera sekcja “Puste identyfikatory użytkowników i poziomy UACC” na stronie 253.

Administrowanie alternatywnymi identyfikatorami użytkowników jest łatwiejsze, jeśli istnieje konwencja nazewnictwa dla identyfikatorów użytkowników, która umożliwia korzystanie z ogólnych alternatywnych profili użytkowników. Jeśli nie, można użyć opcji RACF RACVARS. Szczegółowe informacje na temat korzystania z RACVARS można znaleźć w publikacji *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

Gdy komunikat jest umieszczany w kolejce, która została otwarta z alternatywnym uprawnieniem użytkownika, a kontekst komunikatu został wygenerowany przez menedżer kolejek, pole MQMD_USER_IDENTIFIER jest ustawione na alternatywny identyfikator użytkownika.

z/OS *Profile zabezpieczeń kontekstu*

Produkt IBM MQ korzysta z profili w celu kontrolowania dostępu do informacji kontekstowych specyficznych dla konkretnego komunikatu. Kontekst jest zawarty w deskryptorze komunikatu (MQMD).

Korzystanie z profili dla zabezpieczeń kontekstu

Jeśli zabezpieczenia kontekstu są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profil w klasie **MQADMIN** , jeśli używane są wielkie profile.
- Zdefiniuj profil w klasie **MXADMIN** , jeśli używany jest mieszany profil sprawy.

Profil nosi nazwę `hlq.CONTEXT.queuename` lub `hlq.CONTEXT.topicname`, gdzie:

HLQ
Może to być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek).

queueName
Może to być pełna nazwa kolejki, dla której ma zostać zdefiniowany profil kontekstu, lub profil ogólny.

nazwa_topicName
Może to być pełna nazwa tematu, dla którego ma zostać zdefiniowany profil kontekstu, lub profil ogólny.

Profil poprzedzony nazwą menedżera kolejek oraz z nazwą ** określoną jako nazwa kolejki lub tematu umożliwia sterowanie zabezpieczeniami kontekstu we wszystkich kolejkach i tematach należących do tego menedżera kolejek. Tę opcję można przesłonić w pojedynczej kolejce lub w poszczególnych tematach, definiując konkretny profil dla kontekstu w danej kolejce lub temacie.

Profil poprzedzony nazwą grupy współużytkowania kolejki oraz z ** określonym jako nazwa kolejki lub tematu umożliwia sterowanie kontekstem dla wszystkich kolejek i tematów należących do menedżerów kolejek w ramach grupy współużytkowania kolejek. Można to przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla kontekstu w tym menedżerze kolejek, określając profil z przedrostkiem nazwy menedżera kolejek. Można go także przesłonić w pojedynczej kolejce lub tematu, określając profil z przyrostkiem kolejki lub nazwą tematu.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

Należy podać niezbędne grupy lub identyfikatory użytkowników do tego profilu. W poniższej tabeli przedstawiono wymagany poziom dostępu, w zależności od specyfikacji opcji kontekstu, gdy kolejka jest otwarta.

Tabela 47. Poziomy dostępu dla zabezpieczeń kontekstu

MQOPEN lub MQPUT1 -opcja	**Wymagany poziom dostępu RACF do pliku hlq.CONTEXT.queuename lub hlq.CONTEXT.topicname**
MQPMO_NO_CONTEXT	Brak sprawdzania zabezpieczeń kontekstu
MQPMO_DEFAULT_CONTEXT	Brak sprawdzania zabezpieczeń kontekstu
MQOO_SAVE_ALL_CONTEXT	Brak sprawdzania zabezpieczeń kontekstu
MQOO_PASS_IDENTITY_CONTEXT, MQPMO_PASS_IDENTITY_CONTEXT	ODCZYT
MQOO_PASS_ALL_CONTEXT, MQPMO_PASS_ALL_CONTEXT	ODCZYT
MQOO_SET_IDENTITY_CONTEXT, MQPMO_SET_IDENTITY_CONTEXT	TEMPERATURY
MQOO_SET_ALL_CONTEXT, MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT lub MQPUT1(USAGE (XMITQ))	CONTROL
MQSUB, opcja	
MQSO_SET_IDENTITY_CONTEXT **(Uwaga 2)**	TEMPERATURY

Uwaga:

1. Identyfikatory użytkowników używane do rozproszonego kolejkowania wymagają dostępu CONTROL do programu `hlq.CONTEXT.queuename` w celu umieszczenia komunikatów w kolejce docelowej. Informacje na temat używanych identyfikatorów użytkowników znajdują się w sekcji “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 247 .
2. Jeśli w żądaniu MQSUB określono opcje MQSO_CREATE lub MQSO_ALTER, należy ustawić dowolny z pól kontekstu tożsamości w strukturze MQSD. W tym celu należy określić opcję MQSO_SET_IDENTITY_CONTEXT. Wymagane są również odpowiednie uprawnienia do profilu kontekstu dla kolejki docelowej.

Jeśli komendy zostały umieszczone w kolejce wejściowej komend systemowych, należy użyć opcji domyślnego komunikatu umieszczonego w kontekście w celu powiązania poprawnego ID użytkownika z komendą.

Na przykład program narzędziowy CSQUTIL dostarczany z produktem IBM MQmoże być używany do odciążania i przeładowywania komunikatów w kolejkach. Gdy przenoszone komunikaty są odtwarzane do kolejki, program narzędziowy CSQUTIL korzysta z opcji MQOO_SET_ALL_CONTEXT w celu zwrócenia komunikatów do ich stanu początkowego. Oprócz zabezpieczeń kolejki wymaganych przez tę otwartą opcję wymagane jest również uprawnienie kontekstu. Na przykład, jeśli ten organ jest wymagany przez grupę BACKGRP w menedżerze kolejek MQS1, zostanie on zdefiniowany przez:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

W zależności od podanych opcji oraz typów wykonywanych zabezpieczeń, podczas otwierania kolejki mogą być również wykonywane inne typy sprawdzeń zabezpieczeń. Należą do nich zabezpieczenia kolejki (patrz “Profile dla bezpieczeństwa kolejki” na stronie 203) i alternatywne zabezpieczenia użytkowników (patrz “Profile dla alternatywnego zabezpieczenia użytkownika” na stronie 219). W przypadku tabeli podsumowania przedstawiających otwarte opcje oraz sprawdzenia zabezpieczeń wymagane w przypadku, gdy kolejka, kontekst i alternatywne zabezpieczenia użytkownika są aktywne, patrz Tabela 36 na stronie 212.

Zabezpieczenia kontekstu kolejki systemowej

Dostęp do wielu kolejek systemowych uzyskuje się przez dodatkowe części produktu IBM MQ, na przykład przestrzeń adresową inicjatora kanału V 9.1.0 oraz serwer mqweb używany przez serwery IBM MQ Console i REST API.

The user IDs under which these run under must be given RACF access to these queues, as shown in Tabela 48 na stronie 223.

Tabela 48. Dostęp wymagany do kolejek SYSTEM w operacjach kontekstu

SYSTEM, kolejka	**Inicjator kanału dla rozproszonego kolejkowania**	**serwer mqweb**
SYSTEM.ADMIN.COMMAND.QUEUE	-	CONTROL
SYSTEM.BROKER.CONTROL.QUEUE	CONTROL	-
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	CONTROL	-
SYSTEM.CHANNEL.SYNCQ	CONTROL	-
SYSTEM.CLUSTER.COMMAND.QUEUE	CONTROL	-
SYSTEM.CLUSTER.TRANSMIT.QUEUE	CONTROL	-

z/OS *Profile zabezpieczeń komend*

Aby włączyć sprawdzanie zabezpieczeń dla komend, dodaj profile do klasy MQCMDS. Nazwy profili są oparte na komendach MQSC, ale kontrolują zarówno komendy MQSC, jak i PCF. Profile mogą mieć zastosowanie do menedżera kolejek lub grupy współużytkowania kolejek.

Jeśli wymagane jest sprawdzenie zabezpieczeń dla komend (nie zdefiniowano profilu przełącznika zabezpieczeń komend hlq.NO.CMD.CHECKS), należy dodać profile do klasy MQCMDS.

Te same profile zabezpieczeń kontrolują zarówno komendy MQSC, jak i PCF. Nazwy profili produktu RACF na potrzeby sprawdzania zabezpieczeń komend są oparte na samych nazwach komend MQSC. Te profile mają następującą postać:

```
hlq.verb.pkw
```

Gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), `verb` jest częścią komendy o nazwie, na przykład ALTER, a `pkw` jest typem obiektu, na przykład QLOCAL dla kolejki lokalnej.

W związku z tym nazwa profilu komendy ALTER QLOCAL w podsystemie CSQ1 jest następująca:

```
CSQ1.ALTER.QLOCAL
```

Profili ogólnych można używać do zabezpieczania zestawów komend w taki sposób, aby posiadały mniej profili do zachowania, a co za tym samym, mniej list dostępu. Rozważ utworzenie profilu ogólnego, który ma zastosowanie do wszystkich komend, które nie są chronione przez bardziej konkretny profil. Należy zdefiniować ten profil przy użyciu atrybutu UACC (NONE) i nadać uprawnienia ALTER tylko do

grup produktu RACF zawierających administratorów. Następnie można utworzyć profil ogólny mający zastosowanie do wszystkich komend DISPLAY i nadać mu dostęp do szerokiego dostępu. Między tymi skrajnościami można zidentyfikować grupy użytkowników wymagające dostępu do określonych zestawów komend. W takim przypadku można utworzyć profile dla tych zestawów i przyznać dostęp do grup produktu RACF reprezentujących te klasy użytkowników. Unikaj nadawania użytkownikom dostępu do komend, których nie wymagają: Zastosuj zasadę najmniejszych uprawnień, aby użytkownicy mieli dostęp tylko do komend, które są wymagane dla ich zadań.

Profil poprzedzony przez nazwę menedżera kolejek steruje użyciem komendy w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje użyciem komendy we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tej komendy w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

Przez konfigurowanie profili komend na poziomie menedżera kolejek użytkownik może być ograniczony do wydawania komend w określonym menedżerze kolejek. Alternatywnie można zdefiniować jeden profil dla grupy współużytkowania kolejek dla każdej komendy komendy, a wszystkie sprawdzenia zabezpieczeń mają miejsce dla tego profilu, a nie dla poszczególnych menedżerów kolejek.

Jeśli zabezpieczenia podsystemu i grupy współużytkowania kolejek są aktywne, a profil lokalny nie został znaleziony, wykonywane jest sprawdzenie zabezpieczeń komendy w celu sprawdzenia, czy użytkownik ma dostęp do profilu grupy współużytkowania kolejek.

Jeśli do kierowania komendy do innych menedżerów kolejek w grupie współużytkowania kolejek jest używany atrybut CMDSCOPE, to zabezpieczenia są sprawdzane w każdym menedżerze kolejek, w którym uruchamiana jest komenda, ale niekoniecznie w menedżerze kolejek, w którym wpisano komendę.

Tabela 49 na stronie 224 pokazuje, dla każdej komendy MQSC IBM MQ , profile wymagane do sprawdzania zabezpieczeń komend i odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

Tabela 50 na stronie 230 pokazuje, dla każdej komendy IBM MQ PCF, profile wymagane dla sprawdzania zabezpieczeń komend, które mają zostać przeprowadzone, oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu

Komenda	**Profil komendy dla MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla produktu MQADMIN lub MXADMIN**	**Poziom dostępu dla produktu MQADMIN lub MXADMIN**
ALTER AUTHINFO	hlq.ALTER.AUTHINFO	Zmień	hlq.AUTHINFO.resourcenam e	Zmień
ALTER BUFFPOOL	hlq.ALTER.BUFFPOOL	Zmień	Brak sprawdzenia	-
ALTER CFSTRUCT	hlq.ALTER.CFSTRUCT	Zmień	Brak sprawdzenia	-
ZMIEŃ KANAŁ	hlq.ALTER.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
ALTER NAMELIST	hlq.ALTER.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
ALTER PROCESS	hlq.ALTER.PROCESS	Zmień	hlq.PROCESS.process	Zmień
ALTER PSID	hlq.ALTER.PSID	Zmień	Brak sprawdzenia	-
ALTER QALIAS	hlq.ALTER.QALIAS	Zmień	hlq.QUEUE.queue	Zmień

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
ALTER QLOCAL	hlq.ALTER.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
ALTER QMGR	hlq.ALTER.QMGR	Zmień	Brak sprawdzenia	-
ALTER QMODEL	hlq.ALTER.QMODEL	Zmień	hlq.QUEUE.queue	Zmień
ALTER QREMOTE	hlq.ALTER.QREMOTE	Zmień	hlq.QUEUE.queue	Zmień
ZMIEŃ ZABEZPIECZENIA	hlq.ALTER.SECURITY	Zmień	Brak sprawdzenia	-
ALTER SMDS	hlq.ALTER.SMDS	Zmień	Brak sprawdzenia	-
ALTER STGCLASS	hlq.ALTER.STGCLASS	Zmień	Brak sprawdzenia	-
ALTER SUB	hlq.ALTER.SUB	Zmień	Brak sprawdzenia	-
ALTER TOPIC	hlq.ALTER.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
ZMIANA ŚLEDZENIA	hlq.ALTER.TRACE	Zmień	Brak sprawdzenia	-
DZIENNIK ARCHIWUM	hlq.ARCHIVE.LOG	CONTROL	Brak sprawdzenia	-
BACKUP CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Brak sprawdzenia	-
CLEAR QLOCAL	hlq.CLEAR.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
CLEAR TOPICSTR “3” na stronie 230	hlq.CLEAR.TOPICSTR	Zmień	hlq.TOPIC.topic	Zmień
DEFINE AUTHINFO	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
DEFINIOWANIE BUFETU	hlq.DEFINE.BUFFPOOL	Zmień	Brak sprawdzenia	-
DEFINE CFSTRUCT	hlq.DEFINE.CFSTRUCT	Zmień	Brak sprawdzenia	-
Zdefiniowanie kanału	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
ZDEFINIUJ DZIENNIK	hlq.DEFINE.LOG	Zmień	Brak sprawdzenia	-
DEFINE MAXSMSGS	hlq.DEFINE.MAXSMSGS	Zmień	Brak sprawdzenia	-
DEFINIUJ LISTĘ NAZW	hlq.DEFINE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
ZDEFINIUJ PROCES	hlq.DEFINE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
DEFINE PSID	hlq.DEFINE.PSID	Zmień	Brak sprawdzenia	-
ZDEFINIUJ ALIAS QALIAS	hlq.DEFINE.QALIAS	Zmień	hlq.QUEUE.queue	Zmień
DEFINE QLOCAL	hlq.DEFINE.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
DEFINE QMODEL	hlq.DEFINE.QMODEL	Zmień	hlq.QUEUE.queue	Zmień
ZDEFINIUJ QREMOTE	hlq.DEFINE.QREMOTE	Zmień	hlq.QUEUE.queue	Zmień

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
DEFINE STGCLASS	hlq.DEFINE.STGCLASS	Zmień	Brak sprawdzenia	-
DEFINE SUB	hlq.DEFINE.SUB	Zmień	Brak sprawdzenia	-
ZDEFINIUJ TEMAT	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
USUŃ INFORMACJE O AUTORYZACJI	hlq.DELETE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
USUŃ BUFFPOOL	hlq.DELETE.BUFFPOOL	Zmień	Brak sprawdzenia	-
USUŃ CFSTRUCT	hlq.DELETE.CFSTRUCT	Zmień	Brak sprawdzenia	-
Usuń kanał	hlq.DELETE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
USUŃ NAZWĘ LISTY	hlq.DELETE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Usuń proces	hlq.DELETE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
USUŃ IDENTYFIKATOR PSID	hlq.DELETE.PSID	Zmień	Brak sprawdzenia	-
USUŃ QALIAS	hlq.DELETE.QALIAS	Zmień	hlq.QUEUE.queue	Zmień
USUŃ QLOCAL	hlq.DELETE.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
USUŃ QMODEL	hlq.DELETE.QMODEL	Zmień	hlq.QUEUE.queue	Zmień
USUŃ QREMOTE	hlq.DELETE.QREMOTE	Zmień	hlq.QUEUE.queue	Zmień
USUŃ KLASĘ STGCLASS	hlq.DELETE.STGCLASS	Zmień	Brak sprawdzenia	-
USUŃ SUB	hlq.DELETE.SUB	Zmień	Brak sprawdzenia	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
WYŚWIETL ARCHIWUM “1” na stronie 229	hlq.DISPLAY.ARCHIVE	READ	Brak sprawdzenia	-
WYŚWIETLENIE INFORMACJI UWIERZYTELNIAJĄCYCH	hlq.DISPLAY.AUTHINFO	READ	Brak sprawdzenia	-
WYŚWIETL STATUS CFSTATUS	hlq.DISPLAY.CFSTATUS	READ	Brak sprawdzenia	-
WYŚWIETL CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ	Brak sprawdzenia	-
WYŚWIETL KANAŁ	hlq.DISPLAY.CHANNEL	READ	Brak sprawdzenia	-
WYŚWIETL CHINIT	hlq.DISPLAY.CHINIT	READ	Brak sprawdzenia	-
WYŚWIETL CHLAUTH	hlq.DISPLAY.CHLAUTH	READ	Brak sprawdzenia	-
WYŚWIETL STATUS CHSTATUS	hlq.DISPLAY.CHSTATUS	READ	Brak sprawdzenia	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
WYŚWIETL CLUSQMGR	hlq.DISPLAY.CLUSQMGR	READ	Brak sprawdzenia	-
WYŚWIETLAJ CMDSERV	hlq.DISPLAY.CMDSERV	READ	Brak sprawdzenia	-
WYŚWIETLANIE CONN “1” na stronie 229	hlq.DISPLAY.CONN	READ	Brak sprawdzenia	-
WYŚWIETL GRUPĘ	hlq.DISPLAY.GROUP	READ	Brak sprawdzenia	-
WYŚWIETL DZIENNIK “1” na stronie 229	hlq.DISPLAY.LOG	READ	Brak sprawdzenia	-
WYŚWIETLAJ MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ	Brak sprawdzenia	-
WYŚWIETLANIE LISTY NAZW	hlq.DISPLAY.NAMELIST	READ	Brak sprawdzenia	-
WYŚWIETL PROCES	hlq.DISPLAY.PROCESS	READ	Brak sprawdzenia	-
WYŚWIETL PUBSUB	hlq.DISPLAY.PUBSUB	READ	Brak sprawdzenia	-
WYŚWIETL ALIAS QALIAS	hlq.DISPLAY.QALIAS	READ	Brak sprawdzenia	-
WYŚWIETLANIE KLASTRA QCLUSTER	hlq.DISPLAY.QCLUSTER	READ	Brak sprawdzenia	-
WYŚWIETL QLOCAL	hlq.DISPLAY.QLOCAL	READ	Brak sprawdzenia	-
WYŚWIETL QMGR	hlq.DISPLAY.QMGR	READ	Brak sprawdzenia	-
WYŚWIETLANIE MODELU QMODEL	hlq.DISPLAY.QMODEL	READ	Brak sprawdzenia	-
WYŚWIETL QREMOTE	hlq.DISPLAY.QREMOTE	READ	Brak sprawdzenia	-
WYŚWIETL STATUS QSTATUS	hlq.DISPLAY.QSTATUS	READ	Brak sprawdzenia	-
WYŚWIETL KOLEJKĘ	hlq.DISPLAY.QUEUE	READ	Brak sprawdzenia	-
WYŚWIETL STATUS SBSTATUS	hlq.DISPLAY.SBSTATUS	READ	Brak sprawdzenia	-
Wyświetlanie zestawu SMDS	hlq.DISPLAY.SMDS	READ	Brak sprawdzenia	-
WYŚWIETLAJ SMDSCONN	hlq.DISPLAY.SMDSCONN	READ	Brak sprawdzenia	-
WYŚWIETL SUB	hlq.DISPLAY.SUB	READ	Brak sprawdzenia	-
WYŚWIETL ZABEZPIECZENIA	hlq.DISPLAY.SECURITY	READ	Brak sprawdzenia	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
WYŚWIETL KLASĘ STGCLASS	hlq.DISPLAY.STGCLASS	READ	Brak sprawdzenia	-
WYŚWIETL SYSTEM “1” na stronie 229	hlq.DISPLAY.SYSTEM	READ	Brak sprawdzenia	-
WYŚWIETL WĄTEK	hlq.DISPLAY.THREAD	READ	Brak sprawdzenia	-
WYŚWIETL STATUS TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	Brak sprawdzenia	-
WYŚWIETL TEMAT	hlq.DISPLAY.TOPIC	READ	Brak sprawdzenia	-
WYŚWIETL STATUS TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	Brak sprawdzenia	-
WYŚWIETL ŚLEDZENIE	hlq.DISPLAY.TRACE	READ	Brak sprawdzenia	-
WYŚWIETL WYKORZYSTANIE “1” na stronie 229	hlq.DISPLAY.USAGE	READ	Brak sprawdzenia	-
MOVE QLOCAL	hlq.MOVE.QLOCAL	Zmień	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	Zmień
KANAŁ PING	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ODZYSKIWANIE BSDS	hlq.RECOVER.BSDS	CONTROL	Brak sprawdzenia	-
ODZYSKIWANIE CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	Brak sprawdzenia	-
ODŚWIEŻ KLASTER	hlq.REFRESH.CLUSTER	Zmień	Brak sprawdzenia	-
ODŚWIEŻ MENEDŻERA KOLEJEK	hlq.REFRESH.QMGR	Zmień	Brak sprawdzenia	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	Zmień	Brak sprawdzenia	-
RESET CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	Brak sprawdzenia	-
Resetuj kanał	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Resetowanie klastra	hlq.RESET.CLUSTER	CONTROL	Brak sprawdzenia	-
RESETOWANIE MENEDŻERA KOLEJEK	hlq.RESET.QMGR	CONTROL	Brak sprawdzenia	-
ZRESETUJ QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
ZRESETUJ SMDS	hlq.RESET.SMDS	CONTROL	Brak sprawdzenia	-
RESETUJ POTOK TPIPE	hlq.RESET.TPIPE	CONTROL	Brak sprawdzenia	-
Rozstrzyganie kanału	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
ROZSTRZYGNIJ WĄTPLIWOŚĆ	hlq.RESOLVE.INDOUBT	CONTROL	Brak sprawdzenia	-
WZNÓW MENEDŻERA KOLEJEK	hlq.RESUME.QMGR	CONTROL	Brak sprawdzenia	-
ZABEZPIECZENIA RVERIFY	hlq.RVERIFY.SECURITY	Zmień	Brak sprawdzenia	-
USTAW ARCHIWUM	hlq.SET.ARCHIVE	CONTROL	Brak sprawdzenia	-
USTAW WARTOŚĆ CHLAUTH	hlq.SET.CHLAUTH	CONTROL	Brak sprawdzenia	-
USTAW DZIENNIK	hlq.SET.LOG	CONTROL	Brak sprawdzenia	-
USTAW SYSTEM	hlq.SET.SYSTEM	CONTROL	Brak sprawdzenia	-
KANAŁ POCZĄTKOWY	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
START CHINIT “4” na stronie 230	hlq.START.CHINIT	CONTROL	Brak sprawdzenia	-
START CMDSERV	hlq.START.CMDSERV	CONTROL	Brak sprawdzenia	-
Uruchom proces nasłuchujący	hlq.START.LISTENER	CONTROL	Brak sprawdzenia	-
START QMGR	brak“2” na stronie 230	-	-	-
START SMDSCONN	hlq.START.SMDSCONN	CONTROL	Brak sprawdzenia	-
URUCHOMIENIE ŚLEDZENIA	hlq.START.TRACE	CONTROL	Brak sprawdzenia	-
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ZATRZYMAJ CHINIT	hlq.STOP.CHINIT	CONTROL	Brak sprawdzenia	-
STOP CMDSERV	hlq.STOP.CMDSERV	CONTROL	Brak sprawdzenia	-
Zatrzymaj proces nasłuchujący	hlq.STOP.LISTENER	CONTROL	Brak sprawdzenia	-
STOP QMGR	hlq.STOP.QMGR	CONTROL	Brak sprawdzenia	-
STOP SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	Brak sprawdzenia	-
ZATRZYMAJ ŚLEDZENIE	hlq.STOP.TRACE	CONTROL	Brak sprawdzenia	-
Menedżer kolejki zawieszony	hlq.SUSPEND.QMGR	CONTROL	Brak sprawdzenia	-

Uwagi:

1. Te komendy mogą być wydawane wewnętrznie przez menedżer kolejek; w tych przypadkach nie są sprawdzane żadne uprawnienia.

2. Program IBM MQ nie sprawdza uprawnień użytkownika, który wydaje komendę START QMGR. Można jednak użyć programu RACFlub alternatywnych zabezpieczeń w celu kontrolowania dostępu do komendy START xxxxMSTR , która jest wydawana w wyniku komendy START QMGR. W tym celu należy kontrolować dostęp do profilu MVS.START.STC.xxxxMSTR w klasie komend operatora RACF (OPERCMDS). Szczegółowe informacje na temat tej procedury można znaleźć w publikacji *z/OS SecureWay Security Server RACF Security Administrator's Guide*. Jeśli używana jest ta technika, a nieautoryzowany użytkownik podejmie próbę uruchomienia menedżera kolejek, zostanie on zakończony z kodem przyczyny 00F30216.
3. Zasób **hlq.TOPIC.topic** odwołuje się do obiektu tematu pochodzącego z TOPICSTR. Więcej informacji na ten temat zawiera sekcja "Zabezpieczenia publikowania/subskrypcji" na stronie 480
4. W wersjach wcześniejszych niż IBM MQ for z/OS V6, sprawdzanie zabezpieczeń miało miejsce dla MVS.START.STC.CSQ1CHIN. W wersji IBM MQ for z/OS V6 i nowszych nazwa zasobu zawiera dodatkowy kwalifikator JOBNAME, do którego dopisano. Może to powodować problemy podczas uruchamiania inicjatora kanału.

   Aby rozwiązać problem, zastąp obiekt MVS.START.STC. *ssid* CHIN z profilem dla zasobu o nazwie MVS.START.STC. *ssid* CHIN **.*** lub MVS.START.STC. *ssid* CHIN. *ssid* CHIN, gdzie *ssid* jest identyfikatorem podsystemu dla menedżera kolejek. Wymaga to uprawnienia UPDATE RACF . Więcej informacji na ten temat zawiera publikacja Dokumentacja produktu z/OS for *Operation planning, MVS Commands, RACF Access Authorities, and Resource Names*.

   Parametr START dla *ssid* MSTR nie zawiera parametru JOBNAME=. W celu zapewnienia spójności można zaktualizować profil dla MVS.START.STC.ssidMSTR do MVS.START.STC.ssidMSTR. *.

Tabela 50. Komendy PCF, profile i ich poziomy dostępu

Komenda	**Profil komendy dla MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla produktu MQADMIN lub MXADMIN**	**Poziom dostępu dla produktu MQADMIN lub MXADMIN**
Utwórz kopię zapasową struktury CF	hlq.BACKUP.CFSTRUCT	CONTROL	Brak sprawdzenia	-
Zmień obiekt informacji uwierzytelniającej	hlq.ALTER.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Zmiana struktury CF	hlq.ALTER.CFSTRUCT	Zmień	Brak sprawdzenia	-
Zmień kanał	hlq.ALTER.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Zmień listę nazw	hlq.ALTER.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Zmień proces	hlq.ALTER.PROCESS	Zmień	hlq.PROCESS.process	Zmień
Zmiana kolejki	hlq.ALTER.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Zmiana menedżera kolejek	hlq.ALTER.QMGR	Zmień	Brak sprawdzenia	-
Zmiana zabezpieczeń	hlq.ALTER.SECURITY	Zmień	Brak sprawdzenia	-
Zmiana SMDS	hlq.ALTER.SMDS	Zmień	Brak sprawdzenia	-
Zmień klasę pamięci masowej	hlq.ALTER.STGCLASS	Zmień	Brak sprawdzenia	-
Zmień subskrypcję	hlq.ALTER.SUB	Zmień	Brak sprawdzenia	-
Zmień temat	hlq.ALTER.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Wyczyść kolejkę	hlq.CLEAR.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
Wyczyść łańcuch tematu "1" na stronie 234	hlq.CLEAR.TOPICSTR	Zmień	hlq.TOPIC.topic	Zmień

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
Kopiuj obiekt informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Kopiuj strukturę CF	hlq.DEFINE.CFSTRUCT	Zmień	Brak sprawdzenia	-
Kopiuj kanał	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Kopiuj listę nazw	hlq.DEFINE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Kopiuj proces	hlq.DEFINE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
Kopiuj kolejkę	hlq.DEFINE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Kopiuj subskrypcję	hlq.DEFINE.SUB	Zmień	Brak sprawdzenia	-
Kopiuj klasę pamięci masowej	hlq.DEFINE.STGCLASS	Zmień	Brak sprawdzenia	-
Kopiuj temat	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Tworzenie obiektu informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Utwórz strukturę CF	hlq.DEFINE.CFSTRUCT	Zmień	Brak sprawdzenia	-
Utwórz kanał	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Utwórz listę nazw	hlq.DEFINE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Utwórz proces	hlq.DEFINE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
Tworzenie kolejki	hlq.DEFINE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Utwórz klasę pamięci masowej	hlq.DEFINE.STGCLASS	Zmień	Brak sprawdzenia	-
Utwórz subskrypcję	hlq.DEFINE.SUB	Zmień	Brak sprawdzenia	-
Utwórz temat	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Usuń obiekt informacji uwierzytelniającej	hlq.DELETE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Usuń strukturę CF	hlq.DELETE.CFSTRUCT	Zmień	Brak sprawdzenia	-
Usuń kanał	hlq.DELETE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Usuń listę nazw	hlq.DELETE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Usuń proces	hlq.DELETE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
Usuń kolejkę	hlq.DELETE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Usuń klasę pamięci masowej	hlq.DELETE.STGCLASS	Zmień	Brak sprawdzenia	-
Usuń subskrypcję	hlq.DELETE.SUB	Zmień	Brak sprawdzenia	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Sprawdź archiwum	hlq.DISPLAY.ARCHIVE	READ	Brak sprawdzenia	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
Zapytanie o obiekt informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	READ	Brak sprawdzenia	-
Sprawdź nazwy obiektów informacji uwierzytelniających	hlq.DISPLAY.AUTHINFO	READ	Brak sprawdzenia	-
Sprawdź strukturę CF	hlq.DISPLAY.CFSTRUCT	READ	Brak sprawdzenia	-
Sprawdź nazwy struktury CF	hlq.DISPLAY.CFSTRUCT	READ	Brak sprawdzenia	-
Sprawdź status struktury CF	hlq.DISPLAY.CFSTATUS	READ	Brak sprawdzenia	-
Sprawdź kanał	hlq.DISPLAY.CHANNEL	READ	Brak sprawdzenia	-
Zapytaj o rekordy uwierzytelniania kanału	hlq.DISPLAY.CHLAUTH	READ	Brak sprawdzenia	-
Sprawdź inicjator kanału	hlq.DISPLAY.CHINIT	READ	Brak sprawdzenia	-
Sprawdź nazwy kanałów	hlq.DISPLAY.CHANNEL	READ	Brak sprawdzenia	-
Sprawdź status kanału	hlq.DISPLAY.CHSTATUS	READ	Brak sprawdzenia	-
Zapytanie o menedżer kolejek klastra	hlq.DISPLAY.CLUSQMGR	READ	Brak sprawdzenia	-
Sprawdź połączenie	hlq.DISPLAY.CONNPCF	READ	Brak sprawdzenia	-
Sprawdź grupę	hlq.DISPLAY.GROUP	READ	Brak sprawdzenia	-
Sprawdź dziennik	hlq.DISPLAY.LOG	READ	Brak sprawdzenia	-
Sprawdź listę nazw	hlq.DISPLAY.NAMELIST	READ	Brak sprawdzenia	-
Sprawdź nazwy listy nazw	hlq.DISPLAY.NAMELIST	READ	Brak sprawdzenia	-
Sprawdź proces	hlq.DISPLAY.PROCESS	READ	Brak sprawdzenia	-
Sprawdź nazwy procesów	hlq.DISPLAY.PROCESS	READ	Brak sprawdzenia	-
Sprawdź status publikowania/ subskrypcji	hlq.DISPLAY.PUBSUB	READ	Brak sprawdzenia	-
Sprawdź kolejkę	hlq.DISPLAY.QUEUE	READ	Brak sprawdzenia	-
Zapytaj menedżera kolejek	hlq.DISPLAY.QMGR	READ	Brak sprawdzenia	-
Sprawdź nazwy kolejek	hlq.DISPLAY.QUEUE	READ	Brak sprawdzenia	-
Sprawdź status kolejki	hlq.DISPLAY.QSTATUS	READ	Brak sprawdzenia	-
Sprawdź zabezpieczenia	hlq.DISPLAY.SECURITY	READ	Brak sprawdzenia	-
Sprawdź SMDS	hlq.DISPLAY.SMDS	READ	Brak sprawdzenia	-
Zapytaj SMDSCONN	hlq.DISPLAY.SMDSCONN	READ	Brak sprawdzenia	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
Sprawdź klasę pamięci masowej	hlq.DISPLAY.STGCLASS	READ	Brak sprawdzenia	-
Sprawdź nazwy klas pamięci masowej	hlq.DISPLAY.STGCLASS	READ	Brak sprawdzenia	-
Sprawdź subskrypcję	hlq.INQUIRE.SUB	READ	Brak sprawdzenia	-
Sprawdź status subskrypcji	hlq.INQUIRE.SBSTATUS	READ	Brak sprawdzenia	-
Zapytaj o system	hlq.DISPLAY.SYSTEM	READ	Brak sprawdzenia	-
Sprawdź temat	hlq.DISPLAY.TOPIC	READ	Brak sprawdzenia	-
Sprawdź nazwy tematów	hlq.DISPLAY.TOPIC	READ	Brak sprawdzenia	-
Sprawdź status tematu	hlq.DISPLAY.TPSTATUS	READ	Brak sprawdzenia	-
Sprawdź składnię	hlq.DISPLAY.USAGE	READ	Brak sprawdzenia	-
Przenieś kolejkę	hlq.MOVE.QLOCAL	Zmień	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	Zmień
Kanał ping	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Odzyskaj strukturę CF	hlq.RECOVER.CFSTRUCT	CONTROL	Brak sprawdzenia	-
Odśwież klaster	hlq.REFRESH.CLUSTER	Zmień	Brak sprawdzenia	-
Odśwież menedżera kolejek	hlq.REFRESH.QMGR	Zmień	Brak sprawdzenia	-
Odśwież zabezpieczenia	hlq.REFRESH.SECURITY	Zmień	Brak sprawdzenia	-
Resetuj strukturę CF	hlq.RESET.CFSTRUCT	CONTROL	Brak sprawdzenia	-
Resetowanie kanału	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Resetowanie klastra	hlq.RESET.CLUSTER	CONTROL	Brak sprawdzenia	-
Resetowanie menedżera kolejek	hlq.RESET.QMGR	CONTROL	Brak sprawdzenia	-
Resetuj statystyki kolejki	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Zresetuj SMDS	hlq.RESET.SMDS	CONTROL	Brak sprawdzenia	-
Rozstrzyganie kanału	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Wznów menedżer kolejek	hlq.RESUME.QMGR	CONTROL	Brak sprawdzenia	-
Wznów klaster menedżera kolejek	hlq.RESUME.QMGR	CONTROL	Brak sprawdzenia	-
Ponowne weryfikowanie zabezpieczeń	hlq.RVERIFY.SECURITY	Zmień	Brak sprawdzenia	-
Ustaw archiwum	hlq.SET.ARCHIVE	CONTROL	Brak sprawdzenia	-
Ustaw rekord uwierzytelniania kanału	hlq.SET.CHLAUTH	CONTROL	Brak sprawdzenia	-
Ustaw dziennik	hlq.SET.LOG	CONTROL	Brak sprawdzenia	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)				
Komenda	**Profil komendy dla MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla produktu MQADMIN lub MXADMIN**	**Poziom dostępu dla produktu MQADMIN lub MXADMIN**
Ustaw system	hlq.SET.SYSTEM	CONTROL	Brak sprawdzenia	-
Uruchom kanał	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Uruchom inicjator kanału	hlq.START.CHINIT	CONTROL	Brak sprawdzenia	-
Uruchom program nasłuchujący kanału	hlq.START.LISTENER	CONTROL	Brak sprawdzenia	-
Uruchom połączenie SMDS	hlq.START.SMDSCONN	CONTROL	Brak sprawdzenia	-
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Zatrzymaj inicjator kanału	hlq.STOP.CHINIT	CONTROL	Brak sprawdzenia	-
Zatrzymaj proces nasłuchujący kanału	hlq.STOP.LISTENER	CONTROL	Brak sprawdzenia	-
Zatrzymaj połączenie SMDS	hlq.STOP.SMDSCONN	CONTROL	Brak sprawdzenia	-
Menedżer kolejki - SUSPEND	hlq.SUSPEND.QMGR	CONTROL	Brak sprawdzenia	-
Zawieś klaster menedżera kolejek	hlq.SUSPEND.QMGR	CONTROL	Brak sprawdzenia	-

Uwagi:

1. Zasób **hlq.TOPIC.topic** odwołuje się do obiektu tematu pochodzącego z TOPICSTR. Więcej informacji na ten temat zawiera sekcja “Zabezpieczenia publikowania/subskrypcji” na stronie 480

V 9.1.0 Szczegółowe informacje na temat wymaganych profili PCF w programie IBM MQ można znaleźć w sekcji “IBM MQ Console -wymagane profile zabezpieczeń komend” na stronie 234 , jeśli używany jest IBM MQ Console.

z/OS V 9.1.0 *IBM MQ Console -wymagane profile zabezpieczeń komend*

Operacje wykonywane w produkcie IBM MQ Console przez użytkownika w produkcie `MQWebAdmin`lub `MQWebAdminRO`roli mają miejsce w kontekście zabezpieczeń dla identyfikatora użytkownika uruchomionego zadania serwera mqweb. Jeśli ma być używany produkt IBM MQ Console, identyfikator użytkownika uruchomionego zadania serwera mqweb wymaga autoryzacji do wydawania określonych komend PCF.

Tabela 51 na stronie 235 pokazuje, dla każdej komendy IBM MQ PCF, wymagane profile zabezpieczeń komend oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS, który jest wymagany przez IBM MQ Console.

Tabela 51. IBM MQ Console Komendy PCF, profile i ich poziomy dostępu

Komenda	Profil komendy dla MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla produktu MQADMIN lub MXADMIN	Poziom dostępu dla produktu MQADMIN lub MXADMIN
Zmień obiekt informacji uwierzytelniającej	hlq.ALTER.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Zmień kanał	hlq.ALTER.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Zmiana kolejki	hlq.ALTER.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Zmiana menedżera kolejek	hlq.ALTER.QMGR	Zmień	Brak sprawdzenia	-
Zmień temat	hlq.ALTER.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Wyczyść kolejkę	hlq.CLEAR.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
Tworzenie obiektu informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Utwórz kanał	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Tworzenie kolejki	hlq.DEFINE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Utwórz subskrypcję	hlq.DEFINE.SUB	Zmień	Brak sprawdzenia	-
Utwórz temat	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Usuń obiekt informacji uwierzytelniającej	hlq.DELETE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Usuń kanał	hlq.DELETE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Usuń kolejkę	hlq.DELETE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Usuń subskrypcję	hlq.DELETE.SUB	Zmień	Brak sprawdzenia	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Zapytanie o obiekt informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	READ	Brak sprawdzenia	-
Sprawdź nazwy obiektów informacji uwierzytelniających	hlq.DISPLAY.AUTHINFO	READ	Brak sprawdzenia	-
Sprawdź kanał	hlq.DISPLAY.CHANNEL	READ	Brak sprawdzenia	-
Zapytaj o rekordy uwierzytelniania kanału	hlq.DISPLAY.CHLAUTH	READ	Brak sprawdzenia	-
Sprawdź inicjator kanału	hlq.DISPLAY.CHINIT	READ	Brak sprawdzenia	-
Sprawdź nazwy kanałów	hlq.DISPLAY.CHANNEL	READ	Brak sprawdzenia	-
Sprawdź status kanału	hlq.DISPLAY.CHSTATUS	READ	Brak sprawdzenia	-
Sprawdź kolejkę	hlq.DISPLAY.QUEUE	READ	Brak sprawdzenia	-
Zapytaj menedżera kolejek	hlq.DISPLAY.QMGR	READ	Brak sprawdzenia	-
Sprawdź nazwy kolejek	hlq.DISPLAY.QUEUE	READ	Brak sprawdzenia	-
Sprawdź status kolejki	hlq.DISPLAY.QSTATUS	READ	Brak sprawdzenia	-

Tabela 51. IBM MQ Console Komendy PCF, profile i ich poziomy dostępu (kontynuacja)				
Komenda	**Profil komendy dla MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla produktu MQADMIN lub MXADMIN**	**Poziom dostępu dla produktu MQADMIN lub MXADMIN**
Sprawdź subskrypcję	hlq.INQUIRE.SUB	READ	Brak sprawdzenia	-
Sprawdź status subskrypcji	hlq.INQUIRE.SBSTATUS	READ	Brak sprawdzenia	-
Sprawdź temat	hlq.DISPLAY.TOPIC	READ	Brak sprawdzenia	-
Sprawdź nazwy tematów	hlq.DISPLAY.TOPIC	READ	Brak sprawdzenia	-
Sprawdź status tematu	hlq.DISPLAY.TPSTATUS	READ	Brak sprawdzenia	-
Kanał ping	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Odśwież klaster	hlq.REFRESH.CLUSTER	Zmień	Brak sprawdzenia	-
Odśwież zabezpieczenia	hlq.REFRESH.SECURITY	Zmień	Brak sprawdzenia	-
Resetowanie kanału	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Rozstrzyganie kanału	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Ustaw rekord uwierzytelniania kanału	hlq.SET.CHLAUTH	CONTROL	Brak sprawdzenia	-
Uruchom kanał	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

z/OS *Profile zabezpieczeń zasobów komend*

Jeśli profil przełącznika bezpieczeństwa zasobów komend nie został zdefiniowany, ponieważ wymagane jest sprawdzanie zabezpieczeń dla zasobów powiązanych z komendami, należy dodać profile zasobów dla każdego zasobu do odpowiedniej klasy. Te same profile zabezpieczeń kontrolują zarówno komendy MQSC, jak i PCF.

Jeśli profil przełącznika zabezpieczeń zasobów komend nie został zdefiniowany, `hlq.NO.CMD.RESC.CHECKS`, ponieważ sprawdzanie zabezpieczeń dla zasobów powiązanych z komendami ma być wymagane, należy:

- Należy dodać profil zasobu w klasie **MQADMIN** , jeśli dla każdego zasobu używane są wielkie litery.
- Dodaj profil zasobu w klasie **MXADMIN** , jeśli używany jest mieszany profil sprawy dla każdego zasobu.

Te same profile zabezpieczeń kontrolują zarówno komendy MQSC, jak i PCF.

Profile służące do sprawdzania zabezpieczeń zasobów komendy mają następującą postać:

```
hlq.type.resourcename
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek).

Profil poprzedzony przez nazwę menedżera kolejek steruje dostępem do zasobów powiązanych z komendami w tym menedżerze kolejek. Profil poprzedzony przez nazwę grupy współużytkowania kolejki steruje dostępem do zasobów powiązanych z komendami we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w przypadku pojedynczego menedżera kolejek, definiując profil poziomu menedżera kolejek dla tego zasobu komendy w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ

sprawdza najpierw, czy profil jest poprzedzony przedrostkiem nazwy menedżera kolejek. Jeśli nie jest on wyszukiany, wyszukuje profil z przedrostkiem nazwy grupy współużytkowania kolejki.

Na przykład nazwa profilu RACF dla sprawdzania zabezpieczeń zasobu komendy względem kolejki modelowej CREDIT.WORTHY w podsystemie CSQ1 to:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Ponieważ profile dla wszystkich typów zasobów komend są przechowywane w klasie MQADMIN, w profilu wymagana jest część "type" nazwy profilu w celu odróżnienia zasobów różnych typów o takiej samej nazwie. Częścią "type" nazwy profilu może być CHANNEL, QUEUE, TOPIC, PROCESS lub NAMELIST. Na przykład użytkownik może mieć uprawnienia do definiowania parametru hlq.QUEUE.PAYROLL.ONE, ale nie ma uprawnień do definiowania hlq.PROCESS.PAYROLL.ONE

Jeśli typem zasobu jest kolejka, a profil jest profilem grupowym współużytkowania kolejki, steruje on dostępem do jednej lub większej liczby kolejek lokalnych w grupie współużytkowania kolejek lub dostępem do pojedynczej kolejki współużytkowanej z dowolnego menedżera kolejek w grupie współużytkowania kolejek.

z/OS Komendy MQSC, profile i ich poziomy dostępu pokazują, dla każdej komendy MQSC IBM MQ , profile wymagane do sprawdzania zabezpieczeń komend i odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

z/OS Komendy PCF, profile i ich poziomy dostępu wyświetla dla każdej komendy IBM MQ PCF profile wymagane do przeprowadzenia sprawdzania zabezpieczeń komend oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

z/OS *Sprawdzanie zabezpieczeń zasobów komend dla kolejek aliasowych i kolejek zdalnych*
Zarówno kolejka aliasowa, jak i kolejki zdalne zapewniają kierowanie do innej kolejki. Dodatkowe punkty mają zastosowanie w przypadku sprawdzania uprawnień dla tych kolejek.

Kolejki aliasowe

Podczas definiowania kolejki aliasowej sprawdzanie zabezpieczeń zasobów komend jest wykonywane tylko na podstawie nazwy kolejki aliasowej, a nie na podstawie nazwy kolejki docelowej, do której alias jest tłumaczona.

Kolejki aliasowe mogą być rozstrzygane zarówno w kolejkach lokalnych, jak i zdalnych. Jeśli użytkownik nie chce zezwalać użytkownikom na dostęp do niektórych kolejek lokalnych lub zdalnych, należy wykonać obie czynności:

1. Nie zezwalaj użytkownikom na dostęp do tych kolejek lokalnych i zdalnych.
2. Ogranicz użytkowników z możliwości definiowania aliasów dla tych kolejek. Oznacza to, że uniemożliwiają one wydawanie komend DEFINE QALIAS i ALTER QALIAS.

Kolejki zdalne

Podczas definiowania kolejki zdalnej sprawdzanie zabezpieczeń zasobów komend jest wykonywane tylko w odniesieniu do nazwy kolejki zdalnej. Nie są wykonywane żadne sprawdzenia dla nazw kolejek określonych w atrybutach RNAME lub XMITQ w definicji obiektu kolejki zdalnej.

z/OS Profil bezpieczeństwa RESLEVEL

Istnieje możliwość zdefiniowania profilu specjalnego w klasie MQADMIN lub MXADMIN w celu kontrolowania liczby identyfikatorów użytkowników sprawdzanych pod kątem zabezpieczeń zasobów API. Profil ten nosi nazwę profilu RESLEVEL. Sposób, w jaki ten profil wpływa na bezpieczeństwo interfejsu API, zależy od sposobu uzyskiwania dostępu do produktu IBM MQ.

Gdy aplikacja próbuje połączyć się z produktem IBM MQ, produkt IBM MQ sprawdza dostęp, jaki identyfikator użytkownika powiązany z połączeniem ma do profilu w klasie MQADMIN lub MXADMIN wywołanej:

```
hlq.RESLEVEL
```

Gdzie `hlq` może być `ssid` (ID podsystemu) lub `qsg` (identyfikator grupy współużytkowania kolejki).

Identyfikatory użytkowników powiązane z każdym typem połączenia są następujące:

- Identyfikator użytkownika zadania łączącego dla połączeń wsadowych.
- Identyfikator użytkownika przestrzeni adresowej CICS dla połączeń CICS
- Identyfikator użytkownika przestrzeni adresowej regionu produktu IMS dla połączeń produktu IMS
- Identyfikator użytkownika przestrzeni adresowej inicjatora kanału dla połączeń inicjatora kanału

Ostrzeżenie: RESLEVEL jest bardzo potężną opcją; może spowodować ominięcie wszystkich sprawdzeń bezpieczeństwa zasobów dla określonego połączenia.

Jeśli nie zdefiniowano profilu RESLEVEL, należy uważać, aby żaden inny profil w klasie MQADMIN nie był zgodny z rozszerzeniem hlq.RESLEVEL. Jeśli na przykład istnieje profil w tabeli MQADMIN o nazwie hlq. * * i nie ma profilu hlq.RESLEVEL , należy uważać na konsekwencje hlq. * * profilu, ponieważ jest on używany do sprawdzania RESLEVEL.

Zdefiniuj profil hlq.RESLEVEL i ustaw wartość UACC na NONE, a nie w ogóle nie mieć profilu RESLEVEL. Na liście dostępu należy jak najmniejszej liczby użytkowników lub grup. Szczegółowe informacje na temat kontroli dostępu RESLEVEL można znaleźć w sekcji “Zagadnienia dotyczące kontroli w systemie z/OS” na stronie 265.

Jeśli używane są tylko zabezpieczenia na poziomie menedżera kolejek, produkt IBM MQ przeprowadza sprawdzanie RESLEVEL względem profilu `qmgr-name.RESLEVEL` . Jeśli używane są tylko zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ przeprowadza sprawdzanie RESLEVEL względem profilu produktu `qsg-name.RESLEVEL` . Jeśli używane jest połączenie zarówno menedżera kolejek, jak i zabezpieczenia poziomu grupy współużytkowania kolejki, produkt IBM MQ sprawdza najpierw istnienie profilu RESLEVEL na poziomie menedżera kolejek. Jeśli nie jest on używany, sprawdza profil RESLEVEL na poziomie grupy współużytkowania kolejki.

Jeśli nie można znaleźć profilu RESLEVEL, produkt IBM MQ włącza sprawdzanie zarówno zadania, jak i zadania (lub alternatywnego użytkownika) dla połączenia CICS lub IMS . W przypadku połączenia wsadowego program IBM MQ umożliwia sprawdzanie ID użytkownika zadania (lub zastępcy). W przypadku inicjatora kanału program IBM MQ umożliwia sprawdzanie identyfikatora użytkownika kanału oraz identyfikatora użytkownika MCA (lub alternatywnego).

Jeśli istnieje profil RESLEVEL, to poziom sprawdzania zależy od środowiska i poziomu dostępu dla profilu.

Należy pamiętać, że jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i nie zostanie zdefiniowany ten profil na poziomie menedżera kolejek, może istnieć jeden zdefiniowany na poziomie grupy współużytkowania kolejki, który będzie miał wpływ na poziom checking.To aktywowania sprawdzania dwóch identyfikatorów użytkowników, należy zdefiniować profil RESLEVEL (poprzedzony nazwą menedżera kolejek o nazwie grupy współużytkowania kolejek) z identyfikatorem UACC (NONE) i upewnić się, że odpowiedni użytkownicy nie mają dostępu przyznanego dla tego profilu.

Jeśli użytkownik uzna, że identyfikator użytkownika inicjatora kanału ma wartość RESLEVEL, należy pamiętać, że połączenie nawiązane przez inicjatora kanału jest również połączeniem używanym przez kanały. Ustawienie, które powoduje ominięcie wszystkich sprawdzeń zabezpieczeń zasobów dla identyfikatora użytkownika inicjatora kanału, jest efektywnie omijane sprawdzeniami zabezpieczeń dla wszystkich kanałów. Jeśli identyfikator użytkownika RESLEVEL inicjatora kanału ma wartość inną niż NONE, to dla dostępu sprawdzany jest tylko jeden identyfikator użytkownika (dla poziomu dostępu READ lub UPDATE) lub żaden ID użytkownika (dla poziomu dostępu CONTROL lub ALTER). Jeśli identyfikator użytkownika inicjatora kanału zostanie ustawiony na wartość RESLEVEL na poziomie innym niż NONE, należy pamiętać o tym, że to ustawienie jest zrozumiane dla sprawdzeń zabezpieczeń, które zostały wykonane dla kanałów.

Użycie profilu RESLEVEL oznacza, że nie są podejmowane normalne rekordy kontroli bezpieczeństwa. Jeśli na przykład użytkownik umiesz UAUDIT na użytkownika, dostęp do profilu hlq.RESLEVEL w produkcie MQADMIN nie jest kontrolowany.

Jeśli w profilu hlq.RESLEVEL zostanie użyta opcja OSTRZEŻENIE RACF , dla profili w klasie RESLEVEL nie będą generowane żadne komunikaty ostrzegawcze produktu RACF .

Sprawdzanie zabezpieczeń dla komunikatów raportów, takich jak COD, jest kontrolowane przez profil RESLEVEL powiązany z aplikacją inicjują. Na przykład, jeśli ID użytkownika zadania wsadowego ma uprawnienie CONTROL lub ALTER do profilu RESLEVEL, pomijane są wszystkie operacje sprawdzania zasobów wykonywane przez zadanie wsadowe, w tym sprawdzanie bezpieczeństwa komunikatów raportu.

Jeśli zmienisz profil RESLEVEL, użytkownicy muszą się rozłączyć i połączyć się ponownie, zanim nastąpi zmiana. (obejmuje to zatrzymywanie i restartowanie inicjatora kanału, jeśli zmieniony zostanie dostęp do profilu RESLEVEL dla identyfikatora użytkownika przestrzeni adresowej rozproszonego kolejkowania).

Aby wyłączyć kontrolę RESLEVEL, należy użyć parametru systemu RESAUDIT.

z/OS *RESLEVEL i połączenia wsadowe*

Domyślnie, gdy dostęp do zasobu IBM MQ jest uzyskiwany za pośrednictwem zadań wsadowych i połączeń typu wsadowego, użytkownik musi mieć uprawnienia do dostępu do tego zasobu dla konkretnej operacji. Sprawdzenie zabezpieczeń można pominąć, ustawiając odpowiednią definicję RESLEVEL.

Określa, czy użytkownik jest sprawdzany, czy nie jest oparty na ID użytkownika używanym w czasie połączenia, tym samym ID użytkownika, który jest używany do sprawdzania połączenia.

Można na przykład skonfigurować RESLEVEL w taki sposób, aby w sytuacji, w której użytkownik zaufał dostęp do określonych zasobów za pośrednictwem połączenia wsadowego, nie wykonano sprawdzania zabezpieczeń zasobów interfejsu API; ale gdy użytkownik, którego nie ufasz, próbuje uzyskać dostęp do tych samych zasobów, kontrole bezpieczeństwa są przeprowadzane normalnie. Należy skonfigurować sprawdzanie RESLEVEL w taki sposób, aby pomijanie sprawdzania zabezpieczeń interfejsu API było możliwe tylko wtedy, gdy użytkownik jest wystarczająco zaufany, a programy są uruchamiane przez tego użytkownika.

Poniższa tabela zawiera informacje o kontrolach wykonanych dla połączeń wsadowych.

Tabela 52. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń wsadowych

RACF poziom dostępu	**Poziom kontroli**
BRAK	Przeprowadzone sprawdzenia zasobów
READ	Przeprowadzone sprawdzenia zasobów
UPDATE	Przeprowadzone sprawdzenia zasobów
CONTROL	Brak sprawdzenia.
Zmień	Brak sprawdzenia.

z/OS *RESLEVEL i funkcje systemowe*

Zastosowanie RESLEVEL do paneli operacyjno-sterujących, a do CSQUTIL.

Panele operacji i sterowania oraz program narzędziowy CSQUTIL to aplikacje typu wsadowego, które generują żądania do serwera komend menedżera kolejek, a więc są one objęte uwagami opisanymi w sekcji “RESLEVEL i połączenia wsadowe” na stronie 239. Można użyć RESLEVEL do pominięcia sprawdzania zabezpieczeń dla SYSTEM.COMMAND.INPUT i SYSTEM.COMMAND.REPLY.MODEL kolejek, których używają, ale nie w przypadku kolejek dynamicznych SYSTEM.CSQXCMD. *, SYSTEM.CSQOREXX.*, i SYSTEM.CSQUTIL. *.

Serwer komend jest integralną częścią menedżera kolejek, dlatego nie jest z nim powiązany sprawdzanie połączenia ani RESLEVEL. Aby zachować bezpieczeństwo, serwer komend musi potwierdzić, że ID użytkownika aplikacji wysyłającej żądanie ma uprawnienie do otwarcia kolejki używanej w odpowiedziach.

W przypadku paneli operacji i sterowania jest to SYSTEM.CSQOREXX. *. Dla CSQUTIL jest to SYSTEM.CSQUTIL. *. Użytkownicy muszą być uprawnieni do korzystania z tych kolejek, zgodnie z opisem w sekcji “Bezpieczeństwo kolejki systemowej” na stronie 210, oprócz autoryzacji RESLEVEL, które są im nadawane.

W przypadku innych aplikacji korzystających z serwera komend jest to kolejka, której nazwa jest kolejką zwrotną. Takie inne aplikacje mogą oszukać serwer komend w celu umieszczania komunikatów w nieautoryzowanych kolejkach, przekazując (w kontekście komunikatu) bardziej zaufany identyfikator użytkownika niż jego własny, do serwera komend. Aby temu zapobiec, należy użyć profilu CONTEXT, aby chronić kontekst tożsamości komunikatów umieszczonych w systemie SYSTEM.COMMAND.INPUT.

z/OS *Połączenia RESLEVEL i CICS*

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API w połączeniu z produktem CICS sprawdzane są dwa identyfikatory użytkowników. Można zmienić, które identyfikatory użytkowników są sprawdzane, ustawiając profil RESLEVEL.

Pierwszym sprawdzonym identyfikatorem użytkownika jest przestrzeń adresowa CICS . Jest to identyfikator użytkownika na karcie pracy zadania CICS lub identyfikator użytkownika przypisany do uruchomionego zadania CICS za pomocą klasy z/OS STARTED lub tabeli uruchomionych procedur. (To nie jest CICS DFLTUSER.)

Drugim sprawdzonym identyfikatorem użytkownika jest identyfikator użytkownika powiązany z transakcją CICS .

Jeśli jeden z tych identyfikatorów użytkownika nie ma dostępu do zasobu, żądanie nie powiedzie się i zostanie złożony kod zakończenia MQRC_NOT_AUTHORIZED. Zarówno identyfikator użytkownika przestrzeni adresowej CICS , jak i identyfikator użytkownika uruchamiający transakcję CICS , muszą mieć dostęp do zasobu na poprawnym poziomie.

W jaki sposób RESLEVEL może mieć wpływ na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL, można zmienić identyfikatory użytkowników, które są sprawdzane podczas uzyskiwania dostępu do zasobu. Więcej informacji można znaleźć w sekcji Tabela 53 na stronie 240.

Sprawdzane identyfikatory użytkowników zależą od ID użytkownika używanego w czasie połączenia, tj. identyfikatora użytkownika przestrzeni adresowej CICS . Ten element sterujący umożliwia pominięcie sprawdzania zabezpieczeń interfejsu API dla żądań IBM MQ pochodzących z jednego systemu (na przykład systemu testowego, testuCICS,), ale w celu zaimplementowania ich dla innego systemu (na przykład systemu produkcyjnego, PRODCICS).

Uwaga: Jeśli ID użytkownika przestrzeni adresowej CICS zostanie skonfigurowany z atrybutem "zaufany" w klasie STARTED lub ICHRIN03w tabeli procedur uruchomionych w produkcie RACF , nadpisuje ono wszystkie sprawdzenia ID użytkownika dla przestrzeni adresowej CICS ustanowione przez profil RESLEVEL dla danego menedżera kolejek (to znaczy menedżer kolejek nie wykona sprawdzenia zabezpieczeń dla przestrzeni adresowej CICS). Więcej informacji na ten temat zawiera publikacja *CICS Transaction Server for z/OS V3.2 RACF Security Guide*.

W poniższej tabeli przedstawiono sprawdzenia dotyczące połączeń produktu CICS .

Tabela 53. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń produktu CICS

RACF poziom dostępu	**Poziom kontroli**
BRAK	Program IBM MQ sprawdza identyfikator użytkownika przestrzeni adresowej CICS oraz identyfikator użytkownika transakcji.
READ	IBM MQ sprawdza tylko identyfikator użytkownika przestrzeni adresowej CICS .

Tabela 53. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń produktu CICS (kontynuacja)	
RACF poziom dostępu	**Poziom kontroli**
UPDATE	Jeśli transakcja została zdefiniowana na serwerze CICS z wartością RESSEC (YES), produkt IBM MQ sprawdza identyfikator użytkownika przestrzeni adresowej CICS i identyfikator użytkownika transakcji.
UPDATE	Jeśli transakcja jest zdefiniowana dla CICS z RESSEC (NO), IBM MQ sprawdza tylko identyfikator użytkownika przestrzeni adresowej CICS .
CONTROL lub ALTER	Program IBM MQ nie sprawdza żadnych identyfikatorów użytkowników.

z/OS *Połączenia RESLEVEL i IMS*

Domyślnie, gdy dla połączenia IMS wykonywane jest sprawdzenie zabezpieczeń interfejsu API, sprawdzane są dwa identyfikatory użytkowników. Można zmienić, które identyfikatory użytkowników są sprawdzane, ustawiając profil RESLEVEL.

Domyślnie, gdy dla połączenia IMS wykonywane jest sprawdzenie zabezpieczeń interfejsu API, sprawdzane są dwa identyfikatory użytkowników, aby sprawdzić, czy dostęp do zasobu jest dozwolony.

Pierwszym sprawdzonym identyfikatorem użytkownika jest przestrzeń adresowa w regionie IMS . Jest to pobierane z pola USER z karty pracy lub z identyfikatora użytkownika przypisanego do regionu z klasy z/OS STARTED lub z tabeli uruchomionych procedur (SPT).

Drugi sprawdzany identyfikator użytkownika jest powiązany z pracą wykonanego w regionie zależnym. Jest on określany w zależności od typu regionu zależnego, jak pokazano w sekcji Jak określono drugi identyfikator użytkownika dla połączenia IMS(tm).

Jeśli pierwszy lub drugi identyfikator użytkownika produktu IMS nie ma dostępu do zasobu, żądanie nie powiedzie się i zostanie złożony kod zakończenia MQRC_NOT_AUTHORIZED.

Ustawienie profili RESLEVEL produktu IBM MQ nie może zmienić identyfikatora użytkownika, w ramach którego transakcje IMS są zaplanowane na podstawie dostarczonego przez IBMprogramu MQ-IMS programu Monitor wyzwalacza CSQQTRMN. Ten ID użytkownika to PSBNAME tego monitora wyzwalacza, który domyślnie jest CSQQTRMN.

W jaki sposób RESLEVEL może mieć wpływ na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL, można zmienić identyfikatory użytkowników, które są sprawdzane podczas uzyskiwania dostępu do zasobu. Możliwe są następujące sprawdzenia:

- Sprawdź identyfikator użytkownika przestrzeni adresowej regionu produktu IMS oraz drugi identyfikator użytkownika lub alternatywny identyfikator użytkownika.
- Sprawdź tylko identyfikator użytkownika obszaru adresu regionu IMS .
- Nie sprawdzaj identyfikatorów użytkowników.

W poniższej tabeli przedstawiono sprawdzenia dotyczące połączeń produktu IMS .

Tabela 54. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń produktu IMS	
RACF poziom dostępu	**Poziom kontroli**
BRAK	Sprawdź identyfikator użytkownika przestrzeni adresowej IMS oraz drugi identyfikator użytkownika programu IMS lub alternatywny identyfikator użytkownika.
READ	Sprawdź identyfikator użytkownika przestrzeni adresowej IMS .
UPDATE	Sprawdź identyfikator użytkownika przestrzeni adresowej IMS .
CONTROL	Brak sprawdzenia.

Tabela 54. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń produktu IMS (kontynuacja)	
RACF poziom dostępu	**Poziom kontroli**
Zmień	Brak sprawdzenia.

z/OS *RESLEVEL i połączenie inicjatora kanału*

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API przez inicjatora kanału sprawdzane są dwa identyfikatory użytkowników. Można zmienić, które identyfikatory użytkowników są sprawdzane, ustawiając profil RESLEVEL.

Domyślnie, gdy inicjator kanału jest sprawdzany przez funkcję API-kontrola zasobu, sprawdzane są dwa identyfikatory użytkowników, aby sprawdzić, czy dostęp do zasobu jest dozwolony.

Sprawdzane identyfikatory użytkowników mogą być określone za pomocą atrybutu kanału MCAUSER, który został odebrany z sieci, przestrzeni adresowej inicjatora kanału lub alternatywnego identyfikatora użytkownika dla deskryptora komunikatu. To, które identyfikatory użytkowników są sprawdzane, zależy od używanego przez użytkownika protokołu komunikacyjnego i ustawienia atrybutu kanału PUTAUT. Więcej informacji zawiera sekcja “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 247.

Jeśli jeden z tych identyfikatorów użytkownika nie ma dostępu do zasobu, żądanie nie powiedzie się i zostanie złożony kod zakończenia MQRC_NOT_AUTHORIZED.

W jaki sposób RESLEVEL może mieć wpływ na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL można zmienić identyfikatory użytkowników, które są sprawdzane podczas uzyskiwania dostępu do zasobu, oraz liczbę sprawdzanych.

W poniższej tabeli przedstawiono kontrole połączenia inicjatora kanału oraz wszystkie kanały, które są używane przez te połączenia.

Tabela 55. Kontrole wykonane na różnych poziomach dostępu RACF dla połączeń inicjatora kanału	
RACF poziom dostępu	**Poziom kontroli**
BRAK	Sprawdź dwa identyfikatory użytkowników.
READ	Sprawdź jeden ID użytkownika.
UPDATE	Sprawdź jeden ID użytkownika.
CONTROL	Brak sprawdzenia.
Zmień	Brak sprawdzenia.
Uwaga: Więcej informacji na temat sprawdzania identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 247 .	

z/OS *Kolejkowanie RESLEVEL i kolejkowanie wewnątrz grupy*

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API przez wewnątrzgrupowy agent kolejkowania sprawdzane są dwa identyfikatory użytkowników, aby sprawdzić, czy dostęp do zasobu jest dozwolony. Użytkownik może zmienić, które identyfikatory użytkowników są sprawdzane, ustawiając profil RESLEVEL.

Sprawdzane identyfikatory użytkowników mogą być identyfikatorem użytkownika określonym za pomocą atrybutu IGQUSER odbierającego menedżera kolejek, ID użytkownika menedżera kolejek w grupie współużytkowania kolejki, który umieł komunikat w systemie SYSTEM.QSG.TRANSMIT.QUEUElub alternatywny identyfikator użytkownika określony w polu *UserIdentifier* deskryptora komunikatu. Więcej informacji zawiera temat “Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania” na stronie 252.

Ponieważ wewnątrzgrupowy agent kolejkowania jest wewnętrznym zadaniem menedżera kolejek, nie wydaje on jawnego żądania połączenia i działa pod ID użytkownika menedżera kolejek. Wewnątrzgrupowy agent kolejkowania jest uruchamiany przy inicjowaniu menedżera kolejek. Podczas inicjowania wewnątrzgrupowego agenta kolejkowania program IBM MQ sprawdza dostęp, jaki identyfikator użytkownika powiązany z menedżerem kolejek ma do profilu w klasie MQADMIN o nazwie:

```
hlq.RESLEVEL
```

To sprawdzenie jest zawsze wykonywane, chyba że został ustawiony przełącznik hlq.NO.SUBSYS.SECURITY .

Jeśli nie ma profilu RESLEVEL, produkt IBM MQ włącza sprawdzanie dwóch identyfikatorów użytkowników. Jeśli istnieje profil RESLEVEL, to poziom sprawdzania zależy od poziomu dostępu przyznanego ID użytkownika menedżera kolejek dla profilu. Kontrole wykonane na różnych poziomach dostępu RACF(r) dla agenta kolejkowania wewnątrz grupy przedstawiają sprawdzenia dla agenta kolejkowania wewnątrz grupy.

Tabela 56. Kontrole wykonane na różnych poziomach dostępu RACF dla wewnątrzgrupowego agenta kolejkowania

RACF poziom dostępu	**Poziom kontroli**
BRAK	Sprawdź dwa identyfikatory użytkowników.
READ	Sprawdź jeden ID użytkownika.
UPDATE	Sprawdź jeden ID użytkownika.
CONTROL	Brak sprawdzenia.
Zmień	Brak sprawdzenia.
Uwaga: Więcej informacji na temat sprawdzania identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania” na stronie 252 .	

Jeśli uprawnienia nadane profilowi RESLEVEL dla ID użytkownika menedżera kolejek zostały zmienione, należy zatrzymać i zrestartować wewnątrzgrupowy agent kolejkowania w celu pobrania nowych uprawnień. Ponieważ nie ma możliwości samodzielnego zatrzymania i zrestartowania wewnątrzgrupowego agenta kolejkowania, menedżer kolejek musi zostać zatrzymany i zrestartowany, aby to osiągnąć.

z/OS *RESLEVEL i sprawdzane identyfikatory użytkowników*

Przykład ustawiania profilu RESLEVEL i nadawania dostępu do niego.

Identyfikator użytkownika sprawdzający nazwę profilu dla połączeń wsadowych za pomocą opcji Identyfikatory użytkowników sprawdzane z nazwą profilu dla LU 6.2 i kanałów połączeń serwera TCP/IP pokazują, w jaki sposób RESLEVEL ma wpływ na to, które identyfikatory użytkowników są sprawdzane pod kątem różnych żądań MQI.

Na przykład menedżer kolejek o nazwie QM66 musi spełniać następujące wymagania:

- Użytkownik WS21B ma być zwolniony z zabezpieczeń zasobów.
- CICS uruchomione zadanie WXNCICS działające pod kontrolą identyfikatora użytkownika przestrzeni adresowej CICSWXN ma wykonywać pełne sprawdzanie zasobów tylko dla transakcji zdefiniowanych za pomocą komendy RESSEC (YES).

Aby zdefiniować odpowiedni profil RESLEVEL, wydaj następującą komendę RACF :

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Następnie należy nadać użytkownikom dostęp do tego profilu, korzystając z następujących komend:

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```

Jeśli te zmiany zostaną wprowadzone w czasie, gdy identyfikatory użytkowników są połączone z menedżerem kolejek QM66, użytkownicy muszą się rozłączyć i ponownie nawiązać połączenie przed zmianą.

Jeśli zabezpieczenia podsystemu nie są aktywne, gdy użytkownik połączy się, ale ten użytkownik jest nadal połączony, zabezpieczenia podsystemu stają się aktywne, pełne sprawdzanie zabezpieczeń zasobów jest stosowane do użytkownika. Aby uzyskać poprawne przetwarzanie RESLEVEL, użytkownik musi ponownie nawiązać połączenie.

z/OS Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS

Produkt IBM MQ inicjuje sprawdzenia zabezpieczeń na podstawie identyfikatorów użytkowników powiązanych z użytkownikami, terminalami, aplikacjami i innymi zasobami. Ta kolekcja tematów zawiera listę identyfikatorów użytkowników, które są używane dla każdego typu sprawdzenia zabezpieczeń.

z/OS *Identyfikatory użytkowników dla zabezpieczeń połączenia*

Identyfikator użytkownika używany na potrzeby zabezpieczeń połączenia zależy od typu połączenia.

Typ połączenia	Zawartość ID użytkownika
Połączenie wsadowe	Identyfikator użytkownika zadania łączącego. Na przykład: • Identyfikator użytkownika TSO • Identyfikator użytkownika przypisany do zadania wsadowego za pomocą parametru USER JCL • Identyfikator użytkownika przypisany do uruchomionego zadania przez klasę STARTED lub tabelę uruchomionych procedur.
CICSconnection	Identyfikator użytkownika przestrzeni adresowej CICS .
IMSconnection	Identyfikator użytkownika przestrzeni adresowej regionu produktu IMS .
Połączenie inicjatora kanału	Identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

z/OS *Identyfikatory użytkowników dla zabezpieczeń zasobów komend i komend*

Identyfikator użytkownika używany na potrzeby zabezpieczeń komendy lub zabezpieczenia zasobów komendy zależy od miejsca, z którego komenda jest uruchamiana.

Wydane z ...	Zawartość ID użytkownika
CSQINP1, CSQINP2lub CSQINPT	Nie jest wykonywane żadne sprawdzenie.
Systemowa kolejka wejściowa komend	Identyfikator użytkownika znaleziony w *UserIdentifier* deskryptora komunikatu, który zawiera komendę. Jeśli komunikat nie zawiera *UserIdentifier*, do menedżera zabezpieczeń przekazywany jest identyfikator użytkownika odstępów.
Konsola	Identyfikator użytkownika podpisany na konsoli. Jeśli konsola nie jest podpisana, domyślnym identyfikatorem użytkownika ustawionym przez parametr systemowy CMDUSER jest CSQ6SYSP. Aby można było wydawać komendy z poziomu konsoli, konsola musi mieć atrybut z/OS SYS AUTHORITY.

Wydane z ...	Zawartość ID użytkownika
Konsola SDSF/TSO	TSO lub ID użytkownika zadania.
Operacje i panele kontrolne	ID użytkownika TSO. Jeśli zamierzasz korzystać z paneli sterowania i operacji, musisz mieć odpowiednie uprawnienia do wydawania poleceń odpowiadających działaniom, które wybierzesz. Ponadto użytkownik musi mieć dostęp z prawem do odczytu do wszystkich obiektów hlq.DISPLAY. Profile *object* w klasie MQCMDS, ponieważ panele używają różnych komend DISPLAY w celu zebrania informacji, które są obecne.
MGCRE	Jeśli parametr MGCRE jest używany z elementem UTOKEN, to identyfikator użytkownika w znaczniku UTOKEN. Jeśli MGCRE jest wydawana bez znacznika UTOKEN, używany jest system TSO lub identyfikator użytkownika zadania.
CSQ0UTIL	ID użytkownika zadania.
CSQUTIL	ID użytkownika zadania.
CSQINPX	ID użytkownika przestrzeni adresowej inicjatora kanału.

z/OS *Identyfikatory użytkowników dla zabezpieczeń zasobów (MQOPEN, MQSUB i MQPUT1)*

Te informacje przedstawiają zawartość identyfikatorów użytkowników dla zwykłych i alternatywnych identyfikatorów użytkowników dla każdego typu połączenia. Liczba sprawdzeń jest definiowana przez profil RESLEVEL. Sprawdzany identyfikator użytkownika jest używany w przypadku wywołań **MQOPEN**, **MQSUB**lub **MQPUT1** .

Uwaga: Wszystkie pola identyfikatora użytkownika są sprawdzane dokładnie w miarę ich odbierania. Żadne konwersje nie mają miejsca, a na przykład trzy pola ID użytkownika zawierające "Boba", "BOB"i "bob" nie są równoważne.

z/OS *Identyfikatory użytkowników sprawdzane pod kątem połączeń wsadowych*

Identyfikator użytkownika sprawdzany dla połączenia wsadowego jest zależny od sposobu uruchomienia zadania oraz od tego, czy został określony alternatywny identyfikator użytkownika.

Tabela 57. Sprawdzanie ID użytkownika w odniesieniu do nazwy profilu dla połączeń wsadowych

Czy alternatywny ID użytkownika został określony przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Nie	-	JOB	JOB
Tak	JOB	JOB	ALT

Klucz:

ALT
Alternatywny ID użytkownika.

JOB

- Identyfikator użytkownika wpisania się do systemu TSO lub USS.
- Identyfikator użytkownika przypisany do zadania wsadowego.
- Identyfikator użytkownika przypisany do uruchomionego zadania przez klasę STARTED lub tabelę uruchomionych procedur.

- Identyfikator użytkownika powiązany z wykonaną procedurą składowaną Db2

Zadanie wsadowe wykonuje MQPUT1 w kolejce o nazwie Q1 z ustawioną RESLEVEL ustawioną na READ i wyłączone sprawdzanie ID użytkownika.

Kontrole wykonane na różnych poziomach dostępu RACF(r) dla połączeń wsadowych i Sprawdzanie identyfikatora użytkownika dla połączeń wsadowych pokazują, że ID użytkownika zadania jest porównany z profilem hlq.Q1.

z/OS *Identyfikatory użytkowników sprawdzane pod kątem połączeń z produktem CICS*

Identyfikatory użytkowników sprawdzane pod kątem połączeń z produktem CICS zależą od tego, czy mają być przeprowadzane kontrole, czy też określony jest alternatywny ID użytkownika.

Tabela 58. Sprawdzanie ID użytkownika względem nazwy profilu dla identyfikatorów użytkowników typu CICS

Czy alternatywny ID użytkownika został określony przy otwarciu?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Nie, 1 sprawdź	-	ADS	ADS
Nie, 2 kontrole	-	ADS + TXN	ADS + TXN
Tak, 1 sprawdzenie	ADS	ADS	ADS
Tak, 2 kontrole	ADS + TXN	ADS + TXN	ADS + ALT

Klucz:

ALT
Alternatywne ID użytkownika

ADS
Identyfikator użytkownika powiązany z zadaniem wsadowym CICS lub, jeśli program CICS jest uruchomiony jako zadanie uruchomione, przez klasę STARTED lub tabelę uruchomionych procedur.

TXN
Identyfikator użytkownika powiązany z transakcją CICS . Zwykle jest to identyfikator użytkownika terminalu, który uruchomił transakcję. Może to być użytkownik CICS DFLTUSER, terminal bezpieczeństwa PRESET lub ręcznie podpisany użytkownik.

Sprawdź, czy identyfikatory użytkowników zostały sprawdzone pod kątem następujących warunków:

- Poziom dostępu RACF do profilu RESLEVEL, dla ID użytkownika przestrzeni adresowej CICS , jest ustawiony na wartość NONE.
- Wywołanie MQOPEN dla kolejki z parametrem MQOO_OUTPUT i MQOO_PASS_IDENTITY_CONTEXT jest wykonywane w kolejce.

Najpierw należy sprawdzić, ile identyfikatorów użytkowników produktu CICS jest sprawdzanych w oparciu o ID użytkownika przestrzeni adresowej CICS , który ma dostęp do profilu RESLEVEL. W produkcie Tabela 53 na stronie 240 w temacie “Połączenia RESLEVEL i CICS” na stronie 240sprawdzane są dwa identyfikatory użytkowników, jeśli profil RESLEVEL jest ustawiony na wartość NONE. Następnie od Tabela 58 na stronie 246 są wykonywane następujące operacje sprawdzania:

- Wartość hlq.ALTERNATE.USER.userid nie jest sprawdzany.
- Profil hlq.CONTEXT.queuename jest sprawdzany zarówno z identyfikatorem użytkownika przestrzeni adresowej CICS , jak i z identyfikatorem użytkownika transakcji CICS .
- Profil hlq.resourcename jest sprawdzany zarówno z identyfikatorem użytkownika przestrzeni adresowej CICS , jak i z identyfikatorem użytkownika transakcji CICS .

Oznacza to, że dla tego wywołania MQOPEN wykonywane są cztery sprawdzenia zabezpieczeń.

z/OS *Identyfikatory użytkowników sprawdzane pod kątem połączeń z produktem IMS*

Identyfikatory użytkowników sprawdzane pod kątem połączeń z programem IMS zależą od tego, czy ma być wykonywane jedno lub dwa sprawdzenia oraz czy określony jest alternatywny ID użytkownika. Jeśli zostanie sprawdzony drugi identyfikator użytkownika, to zależy on od typu regionu zależnego i od tego, które identyfikatory użytkowników są dostępne.

Tabela 59. Sprawdzanie ID użytkownika względem nazwy profilu dla identyfikatorów użytkowników typu IMS

Czy alternatywny ID użytkownika został określony przy otwarciu?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Nie, 1 sprawdź	-	REG	REG
Nie, 2 kontrole	-	REG + SEC	REG + SEC
Tak, 1 sprawdzenie	REG	REG	REG
Tak, 2 kontrole	REG + SEC	REG + SEC	REG + ALT

Klucz:

ALT
Alternatywny ID użytkownika.

REG
Identyfikator użytkownika jest zwykle ustawiany za pomocą klasy STARTED lub tabeli uruchomionych procedur lub, jeśli program IMS jest uruchomiony, z wprowadzonego zadania, przez parametr USER JCL.

sek.
Drugi identyfikator użytkownika jest powiązany z pracą wykonanego w regionie zależnym. Jest on określany zgodnie z Tabela 60 na stronie 247.

Tabela 60. Określa, w jaki sposób drugi identyfikator użytkownika jest określany dla połączenia IMS

Typy regionów zależnych	**Hierarchia do określania drugiego ID użytkownika**
• Komunikat BMP sterowany i pomyślnie wydany GET UNIQUE. • Wydano IFP i GET UNIQUE. • MPP.	Identyfikator użytkownika powiązany z transakcją IMS , jeśli użytkownik jest zalogowany. Nazwa LTERM, jeśli jest dostępna. PSBNAME.
• Komunikat BMP został sterowany i nie został wydany pomyślnie GET UNIQUE. • BMP nie jest sterowane komunikatami. • Nie wydano IFP i GET UNIQUE.	Identyfikator użytkownika powiązany z przestrzenią adresową regionu zależnego IMS , jeśli nie jest to wszystkie odstępy lub wszystkie zera. PSBNAME.

z/OS *Identyfikatory użytkowników używane przez inicjatora kanału*

Ta kolekcja tematów opisuje identyfikatory użytkowników używane i sprawdzone w celu odbierania kanałów oraz żądań MQI klienta wydanych za pośrednictwem kanałów połączenia z serwerem. Informacje są udostępniane dla TCP/IP i dla LU6.2

Aby określić typ używanego sprawdzania zabezpieczeń, można użyć parametru PUTAUT definicji kanału odbierającego. Aby uzyskać spójne sprawdzanie zabezpieczeń w całej sieci produktu IBM MQ , można użyć opcji ONLYMCA i ALTMCA.

Do określenia identyfikatora użytkownika używanego przez agenta MCA można użyć komendy DISPLAY CHSTATUS.

z/OS *Odbieranie kanałów za pomocą protokołu TCP/IP*

Sprawdzane identyfikatory użytkowników zależą od opcji PUTAUT kanału i od tego, czy ma być wykonana jedna lub dwie operacje sprawdzania.

Tabela 61. Identyfikatory użytkowników sprawdzane pod względem nazwy profilu dla kanałów TCP/IP

Opcja PUTAUT określona dla kanału odbiorczego lub requestera	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Sprawdzanie DEF, 1	-	CHL	CHL
kontrole DEF, 2	-	CHL + MCA	CHL + MCA
Sprawdzanie CTX, 1	CHL	CHL	CHL
sprawdzanie CTX, 2	CHL + MCA	CHL + MCA	CHL + ALT
Sprawdzanie ONLYMCA, 1	-	MCA	MCA
ONLYMCA, 2 kontrole	-	MCA	MCA
Sprawdzanie ALTMCA, 1	MCA	MCA	MCA
kontrole ALTMCA, 2	MCA	MCA	MCA + ALT

Klucz:

MCA (ID użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER w odbiorniku. Jeśli pole to jest puste, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału dla strony odbiornika lub requestera.

CHL (ID użytkownika kanału)
W przypadku protokołu TCP/IP zabezpieczenia nie są obsługiwane przez system komunikacji dla kanału. Jeśli używany jest protokół TLS (Transport Layer Security), a od partnera został wywiązany certyfikat cyfrowy, używany jest identyfikator użytkownika powiązany z tym certyfikatem (jeśli jest zainstalowany) lub identyfikator użytkownika powiązany z filtrem zgodnym z użyciem filtru nazw certyfikatów RACF (CNF). Jeśli nie zostanie znaleziony powiązany identyfikator użytkownika lub jeśli nie jest używany protokół TLS, jako identyfikator użytkownika kanału w kanałach zdefiniowanych z parametrem PUTAUT ustawionym na DEF lub CTX używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

Uwaga: Użycie funkcji filtrowania nazw certyfikatów (CNF- RACF Certificate Name Filtering) umożliwia przypisanie tego samego identyfikatora użytkownika produktu RACF do wielu zdalnych użytkowników, na przykład wszystkich użytkowników należących do tej samej jednostki organizacyjnej, którzy w sposób naturalny mają te same uprawnienia zabezpieczeń. Oznacza to, że serwer nie musi mieć kopii certyfikatu każdego z możliwych zdalnych użytkowników na całym świecie, a także znacznie upraszcza zarządzanie certyfikatami i dystrybucją.

Jeśli parametr PUTAUT jest ustawiony na wartość ONLYMCA lub ALTMCA dla kanału, identyfikator użytkownika kanału jest ignorowany, a używany jest identyfikator użytkownika agenta MCA odbiornika lub requestera. Dotyczy to również kanałów TCP/IP korzystających z protokołu TLS.

ALT (alternatywny ID użytkownika)
Identyfikator użytkownika z informacji kontekstowych (to znaczy pole *UserIdentifier*) w deskryptorze komunikatu. Ten identyfikator użytkownika jest przenoszony do pola

AlternateUserID w deskryptorze obiektu przed wywołaniem wywołania **MQOPEN** lub **MQPUT1** dla docelowej kolejki docelowej.

z/OS *Odbieranie kanałów za pomocą jednostki logicznej 6.2*

Sprawdzane identyfikatory użytkowników zależą od opcji PUTAUT kanału i od tego, czy ma być wykonana jedna lub dwie operacje sprawdzania.

Tabela 62. Identyfikatory użytkowników sprawdzane pod względem nazwy profilu dla kanałów LU 6.2

Opcja PUTAUT określona dla kanału odbiorczego lub requestera	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Sprawdzanie DEF, 1	-	CHL	CHL
kontrole DEF, 2	-	CHL + MCA	CHL + MCA
Sprawdzanie CTX, 1	CHL	CHL	CHL
sprawdzanie CTX, 2	CHL + MCA	CHL + MCA	CHL + ALT
Sprawdzanie ONLYMCA, 1	-	MCA	MCA
ONLYMCA, 2 kontrole	-	MCA	MCA
Sprawdzanie ALTMCA, 1	MCA	MCA	MCA
kontrole ALTMCA, 2	MCA	MCA	MCA + ALT

Klucz:

MCA (ID użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER w odbiorniku. Jeśli pole to jest puste, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału dla strony odbiornika lub requestera.

CHL (ID użytkownika kanału)

Kanał requestera - kanał serwera
Jeśli kanał jest uruchamiany od requestera, nie ma możliwości odebrania identyfikatora użytkownika sieci (ID użytkownika kanału).

Jeśli parametr PUTAUT jest ustawiony na wartość DEF lub CTX w kanale requestera, ID użytkownika kanału jest identyfikatorem przestrzeni adresowej inicjatora kanału requestera, ponieważ żaden identyfikator użytkownika nie jest odbierany z sieci.

Jeśli parametr PUTAUT jest ustawiony na wartość ONLYMCA lub ALTMCA, identyfikator użytkownika kanału jest ignorowany, a identyfikator użytkownika agenta MCA requestera jest używany.

Inne typy kanałów
Jeśli parametr PUTAUT jest ustawiony na wartość DEF lub CTX na kanale odbiornika lub requestera, identyfikator użytkownika kanału to ID użytkownika otrzymany z systemu komunikacyjnego podczas inicjowania kanału.

- Jeśli kanał nadawczy znajduje się w systemie z/OS, otrzymany identyfikator użytkownika kanału jest identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału nadawcy.
- Jeśli kanał nadawczy znajduje się na innej platformie (na przykład AIX), otrzymany identyfikator użytkownika kanału jest zwykle udostępniany przez parametr USERID definicji kanału.

Jeśli odebrany identyfikator użytkownika jest pusty lub nie zostanie odebrany żaden identyfikator użytkownika, zostanie użyty identyfikator użytkownika kanału pusty.

ALT (alternatywny ID użytkownika)
Identyfikator użytkownika z informacji kontekstowych (to znaczy pole *UserIdentifier*) w deskryptorze komunikatu. Ten identyfikator użytkownika jest przenoszony do pola *AlternateUserID* w deskryptorze obiektu przed wywołaniem wywołania MQOPEN lub MQPUT1 dla docelowej kolejki docelowej.

z/OS *Żądania MQI klienta*

W zależności od tego, które identyfikatory użytkowników i zmienne środowiskowe zostały ustawione, można użyć różnych identyfikatorów użytkowników. Te identyfikatory użytkowników są sprawdzane pod kątem różnych profili, w zależności od używanej opcji PUTAUT oraz od tego, czy został określony alternatywny identyfikator użytkownika.

W tej sekcji opisano identyfikatory użytkowników sprawdzane pod kątem żądań MQI klienta wydanych za pośrednictwem kanałów połączenia z serwerem dla TCP/IP i LU 6.2. Identyfikator użytkownika MCA i ID użytkownika kanału są takie, jak w przypadku kanałów TCP/IP i LU 6.2 opisanych w poprzednich sekcjach.

W przypadku kanałów połączenia z serwerem identyfikator użytkownika otrzymany od klienta jest używany, jeśli atrybut MCAUSER jest pusty.

Więcej informacji zawiera sekcja “Kontrola dostępu dla klientów” na stronie 99.

W przypadku żądań klienta **MQOPEN**, **MQSUB**i **MQPUT1** należy użyć następujących reguł w celu określenia profilu, który jest sprawdzany:

- Jeśli żądanie określa uprawnienia użytkownika alternatywnego, wykonywane jest sprawdzenie za pomocą komendy *hlq*.ALTERNATE.USER. Profil *userid* .
- Jeśli żądanie określa uprawnienie do kontekstu, wykonywane jest sprawdzenie za pomocą komendy *hlq*.KONTEKST. Profil *queuename* .
- W przypadku wszystkich żądań **MQOPEN**, **MQSUB**i **MQPUT1** jest wykonywane sprawdzenie profilu *hlq.resourcename* .

Po określeniu, które profile są sprawdzane, należy skorzystać z poniższej tabeli, aby określić, które identyfikatory użytkowników są sprawdzane pod kątem tych profili.

Tabela 63. Identyfikatory użytkowników sprawdzane pod kątem nazwy profilu dla jednostek logicznych LU 6.2 i kanałów połączeń serwera TCP/IP

Opcja PUTAUT określona dla kanału połączenia z serwerem	Czy alternatywny ID użytkownika został określony przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Sprawdzanie DEF, 1	Nie	-	CHL	CHL
Sprawdzanie DEF, 1	Tak	CHL	CHL	CHL
kontrole DEF, 2	Nie	-	CHL + MCA	CHL + MCA
kontrole DEF, 2	Tak	CHL + MCA	CHL + MCA	CHL + ALT

Tabela 63. Identyfikatory użytkowników sprawdzane pod kątem nazwy profilu dla jednostek logicznych LU 6.2 i kanałów połączeń serwera TCP/IP (kontynuacja)

Opcja PUTAUT określona dla kanału połączenia z serwerem	Czy alternatywny ID użytkownika został określony przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Sprawdzanie ONLYMCA, 1	Nie	-	MCA	MCA
Sprawdzanie ONLYMCA, 1	Tak	MCA	MCA	MCA
ONLYMCA, 2 kontrole	Nie	-	MCA	MCA
ONLYMCA, 2 kontrole	Tak	MCA	MCA	MCA + ALT

Klucz:

MCA (ID użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER na serwerze-connection; jeśli jest pusty, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

CHL (ID użytkownika kanału)
W przypadku protokołu TCP/IP zabezpieczenia nie są obsługiwane przez system komunikacji dla kanału. Jeśli używany jest protokół TLS (Transport Layer Security), a od partnera został wywiązany certyfikat cyfrowy, używany jest identyfikator użytkownika powiązany z tym certyfikatem (jeśli jest zainstalowany) lub identyfikator użytkownika powiązany z filtrem zgodnym z użyciem filtru nazw certyfikatów RACF (CNF). Jeśli nie zostanie znaleziony powiązany identyfikator użytkownika lub jeśli nie jest używany protokół TLS, identyfikator użytkownika przestrzeni adresowej inicjatora kanału jest używany jako identyfikator użytkownika kanału w kanałach zdefiniowanych za pomocą parametru PUTAUT ustawionego na DEF lub CTX.

Uwaga: Użycie funkcji filtrowania nazw certyfikatów (CNF- RACF Certificate Name Filtering) umożliwia przypisanie tego samego identyfikatora użytkownika produktu RACF do wielu zdalnych użytkowników, na przykład wszystkich użytkowników należących do tej samej jednostki organizacyjnej, którzy w sposób naturalny mają te same uprawnienia zabezpieczeń. Oznacza to, że serwer nie musi mieć kopii certyfikatu każdego z możliwych zdalnych użytkowników na całym świecie, a także znacznie upraszcza zarządzanie certyfikatami i dystrybucją.

Jeśli parametr PUTAUT jest ustawiony na wartość ONLYMCA lub ALTMCA dla kanału, identyfikator użytkownika kanału jest ignorowany, a używany jest identyfikator użytkownika MCA kanału połączenia z serwerem. Dotyczy to również kanałów TCP/IP korzystających z protokołu TLS.

ALT (alternatywny ID użytkownika)
Identyfikator użytkownika z informacji kontekstowych (to znaczy pole *UserIdentifier*) w deskryptorze komunikatu. Ten identyfikator użytkownika jest przenoszony do pola *AlternateUserID* w deskryptorze obiektu lub subskrypcji przed wywołaniem wywołania **MQOPEN**, **MQSUB** lub **MQPUT1** w imieniu aplikacji klienckiej.

z/OS *Przykład inicjatora kanału*

Przykład sprawdzania identyfikatorów użytkowników względem profili produktu RACF .

Użytkownik wykonuje operację **MQPUT1** do kolejki w menedżerze kolejek QM01 , która jest tłumaczona na kolejkę o nazwie QB w menedżerze kolejek QM02. Komunikat jest wysyłany w kanale TCP/IP o nazwie QM01.TO.QM02. Wartość RESLEVEL jest ustawiona na NONE, a operacja otwierania jest wykonywana z alternatywnym identyfikatorem użytkownika i sprawdzaniem kontekstu. Definicja kanału odbiorczego ma wartość PUTAUT (CTX), a ID użytkownika agenta MCA jest ustawiony. Które identyfikatory użytkowników są używane w kanale odbierającym w celu umieszczenia komunikatu w kolejce QB?

Odpowiedź: Tabela 55 na stronie 242 pokazuje, że sprawdzane są dwa identyfikatory użytkowników, ponieważ wartość RESLEVEL jest ustawiona na NONE.

Tabela 61 na stronie 248 pokazuje, że z parametrem PUTAUT ustawionym na CTX i 2 sprawdzane są następujące identyfikatory użytkowników:

- Identyfikator użytkownika inicjatora kanału i ID użytkownika MCAUSER są sprawdzane pod kątem wartości hlq.ALTERNATE.USER.userid .
- Identyfikator użytkownika inicjatora kanału i ID użytkownika MCAUSER są sprawdzane pod kątem profilu hlq.CONTEXT.queuename .
- Identyfikator użytkownika inicjatora kanału oraz alternatywny identyfikator użytkownika określony w deskryptorze komunikatu (MQMD) są sprawdzane pod kątem profilu hlq.Q2 .

z/OS *Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania*

Identyfikatory użytkowników, które są sprawdzane podczas otwierania kolejek docelowych przez agenta kolejkowania wewnątrz grupy, są określane przez wartości atrybutów menedżera kolejek IGQAUT i IGQUSER.

Możliwe identyfikatory użytkowników to:

ID użytkownika kolejkowania wewnątrz grupy (IGQ)
Identyfikator użytkownika określony za pomocą atrybutu IGQUSER odbierającego menedżera kolejek. Jeśli wartość ta jest pusta, używany jest identyfikator użytkownika odbierającego menedżera kolejek. Jednak ponieważ odbierający menedżer kolejek ma uprawnienia do uzyskiwania dostępu do wszystkich zdefiniowanych kolejek, nie są wykonywane sprawdzenia zabezpieczeń dla identyfikatora użytkownika odbierającego menedżera kolejek. W tym przypadku:

- Jeśli ma być sprawdzany tylko jeden identyfikator użytkownika, a ID użytkownika jest taki sam, jak w przypadku odbierającego menedżera kolejek, nie są przeprowadzane żadne sprawdzenia zabezpieczeń. Taka operacja może wystąpić, gdy parametr IGQAUT jest ustawiony na ONLYIGQ lub ALTIGQ.
- Jeśli mają być sprawdzane dwa identyfikatory użytkowników, a jednym z identyfikatorów użytkowników jest odbierający menedżer kolejek, to sprawdzanie zabezpieczeń ma miejsce tylko dla innego ID użytkownika. Taka operacja może wystąpić, gdy parametr IGQAUT jest ustawiony na wartość DEF, CTX lub ALTIGQ.
- Jeśli mają być sprawdzane dwa identyfikatory użytkowników, a oba identyfikatory użytkowników są identyfikatorami użytkownika odbierającego menedżera kolejek, nie są przeprowadzane żadne sprawdzenia zabezpieczeń. Taka możliwość może wystąpić, gdy parametr IGQAUT jest ustawiony na wartość ONLYIGQ.

Wysyłanie ID użytkownika menedżera kolejek (SND)
Identyfikator użytkownika menedżera kolejek w grupie współużytkowania kolejek, który umieł komunikat w systemie SYSTEM.QSG.TRANSMIT.QUEUE.

Alternatywny ID użytkownika (ALT)
Identyfikator użytkownika określony w polu *UserIdentifier* w deskryptorze komunikatu komunikatu.

Tabela 64. Identyfikatory użytkowników sprawdzane pod względem nazwy profilu w kolejkach wewnątrz grupy			
Opcja IGQAUT określona w odbierającym menedżerze kolejek	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Sprawdzanie DEF, 1	-	SND	SND
kontrole DEF, 2	-	SND + IGQ	SND + IGQ
Sprawdzanie CTX, 1	SND	SND	SND
sprawdzanie CTX, 2	SND + IGQ	SND + IGQ	SND + ALT
Sprawdzanie ONLYIGQ, 1	-	IGQ	IGQ
ONLYIGQ, 2 kontrole	-	IGQ	IGQ
Sprawdzanie ALTIGQ, 1	-	IGQ	IGQ
kontrole ALTIGQ, 2	IGQ	IGQ	IGQ + ALT

Klucz:

ALT
Alternatywny ID użytkownika.

IGQ
Identyfikator użytkownika IGQ.

SND
Wysyłanie ID użytkownika menedżera kolejek.

z/OS *Puste identyfikatory użytkowników i poziomy UACC*

Jeśli wystąpi pusty identyfikator użytkownika, wówczas zostanie wpisany niezdefiniowany użytkownik RACF . Nie należy udzielać szerokich praw dostępu do niezdefiniowanego użytkownika.

Puste identyfikatory użytkowników mogą istnieć, gdy użytkownik manipuluje komunikatami przy użyciu kontekstu lub alternatywnym zabezpieczeniem użytkownika, lub gdy IBM MQ jest przekazywany pusty identyfikator użytkownika. Na przykład, pusty identyfikator użytkownika jest używany, gdy komunikat jest zapisywany w kolejce wejściowej komend systemowych bez kontekstu.

Uwaga: Identyfikator użytkownika " * " (oznacza to, że znak gwiazdki, po którym następuje siedem spacji), jest traktowany jako niezdefiniowany identyfikator użytkownika.

Program IBM MQ przekazuje pusty identyfikator użytkownika do programu RACF , a użytkownik o niezdefiniowanym identyfikatorze RACF jest zalogowany. Wszystkie sprawdzenia bezpieczeństwa korzystają następnie z powszechnego dostępu (UACC) dla odpowiedniego profilu. W zależności od sposobu ustawienia poziomów dostępu, jednostka UACC może nadać niezdefiniowanym użytkownikowi szeroki zakres dostępu.

Na przykład, jeśli zostanie wydana komenda RACF z TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

Użytkownik definiuje profil, który włącza zarówno identyfikatory użytkowników zdefiniowane w produkcie z/OS(które nie zostały umieszczone na liście dostępu), jak i niezdefiniowany identyfikator użytkownika produktu RACF w celu umieszczania komunikatów w kolejce i pobierania komunikatów z tej kolejki.

W celu ochrony przed pustymi identyfikatorami użytkowników należy dokładnie zaplanować poziomy dostępu, a także ograniczyć liczbę osób, które mogą korzystać z kontekstu i zabezpieczenia alternatywnego użytkownika. Aby uzyskać dostęp do zasobów, do których nie mogą uzyskać

dostępu, należy uniemożliwić użytkownikom korzystanie z niezdefiniowanego identyfikatora użytkownika w produkcie RACF . Jednocześnie należy jednak zezwolić na dostęp do osób ze zdefiniowanymi identyfikatorami użytkowników. W tym celu można określić ID użytkownika gwiazdki (*) w komendzie RACF PERMIT, nadając dostęp do zasobów dla wszystkich zdefiniowanych identyfikatorów użytkowników. Dlatego wszystkie niezdefiniowane identyfikatory użytkowników (takie jak " * ") Odmowa dostępu.
Na przykład komendy RACF uniemożliwiają uzyskanie przez RACF niezdefiniowanego identyfikatora użytkownika w celu uzyskania dostępu do kolejki w celu umieszczenia lub pobrania komunikatów:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY UACC(NONE)
PERMIT Q.AVAILABLE.TO.RACF.DEFINED.USERS.ONLY CLASS(MQQUEUE) ACCESS(UPDATE) ID(*)
```

z/OS Identyfikatory użytkowników z/OS i uwierzytelnianie wieloskładnikowe (MFA)

IBM Uwierzytelnianie wieloskładnikowe dla systemu z/OS umożliwia administratorom zabezpieczeń systemu z/OS rozszerzenie uwierzytelniania SAF przez wymaganie od zidentyfikowanych użytkowników użycia wielu elementów uwierzytelniania (na przykład zarówno hasła, jak i tokenu szyfrującego) w celu zalogowania się do systemu z/OS . IBM MFA zapewnia również obsługę opartych na czasie technologii generowania haseł jednorazowych, takich jak RSA SecureId.

W większości przypadków produkt IBM MQ nie ma informacji o tym, w jaki sposób użytkownicy "zalogowali się" do systemu CICS lub systemu wsadowego, które sterują pracą IBM MQ , informacje autoryzacyjne zalogowanego identyfikatora użytkownika są powiązane z zadaniem z/OS lub przestrzenią adresową, a produkt IBM MQ używa ich do sprawdzania autoryzacji zasobów. Identyfikatory użytkowników, dla których włączono uwierzytelnianie wieloskładnikowe, mogą być używane do autoryzacji zasobów IBM MQ i uwierzytelniania za pomocą biletów tranzytowego używanych z mostkami CICS i IMS .

Ważne: Jednak w przypadku korzystania z aplikacji, takich jak IBM MQ Explorer, które przekazują identyfikator użytkownika i referencje hasła w wywołaniu funkcji API MQCONNX z opcją *MQCSP_AUTH_USER_ID_AND_PWD* , mają zastosowanie specjalne uwagi. IBM MQ nie ma narzędzia do przekazywania dodatkowych informacji autoryzacyjnych dla tego żądania API.

W poniższym tekście opisano ograniczenia i potencjalne sposoby ich obejścia.

IBM MQ Explorer

Nie można użyć IBM MQ Explorer do zalogowania się w systemie z/OS z ID użytkownika, dla którego włączono uwierzytelnianie MFA, ponieważ nie ma możliwości przekazania dodatkowego elementu uwierzytelniania z IBM MQ Explorer do z/OS.

Dodatkowo istnieją dwa różne mechanizmy używane przez IBM MQ Explorer do ponownego wykorzystania identyfikatora użytkownika i hasła, które wymagają szczególnej uwagi, gdy używane są hasła jednorazowe:

1. IBM MQ Explorer ma możliwość przechowywania haseł w formacie zaciemnionego na komputerze lokalnym w celu późniejszego zalogowania się. Tę możliwość należy wyłączyć, wyświetlając zapytanie eksploratora o hasło za każdym razem, gdy nawiązywane jest połączenie z menedżerem kolejek produktu z/OS .

   W tym celu należy wykonać następującą procedurę:

   a. Wybierz opcję **Menedżery kolejek**.
   b. Z wyświetlonej listy wybierz żądany menedżer kolejek i kliknij go prawym przyciskiem myszy.
   c. Z wyświetlonej listy menu wybierz opcję **Connection Details** (Szczegóły połączenia).
   d. Wybierz opcję **Właściwości** z następnej listy menu i wybierz kartę **ID użytkownika** .

      Upewnij się, że wybrano przełącznik **prompt for password** (pytaj o hasło).

2. Różne operacje w programie IBM MQ Explorer, takie jak przeglądanie komunikatów w kolejkach, testowanie subskrypcji itp. uruchamiają nowy wątek, który uwierzytelnia się w programie IBM MQ przy użyciu referencji używanych po raz pierwszy podczas logowania. Ponieważ nie można ponownie użyć informacji autoryzacyjnych hasła, nie można użyć tych operacji.

Istnieją dwa możliwe sposoby obejścia tych problemów na poziomie konfiguracji MFA:

- Użycie identyfikatora aplikacji z wykluczeniem MFA w celu całkowitego wykluczenia zadań IBM MQ z przetwarzania MFA.

  W tym celu należy wydać następujące komendy:

  1. `RDEFINE MFADEF MFABYPASS.USERID.chinuser`

     gdzie *chinuser* jest identyfikatorem użytkownika na poziomie przestrzeni adresowej inicjatora kanału (powiązanym z inicjatorem kanału za pośrednictwem klasy STC)

  2. `PERMIT MFABYPASS.USERID.chinuser CLASS MFADEF ACCESS(READ) ID(explorer user)`

  Więcej informacji na temat tej metody zawiera sekcja Pomijanie IBM dla aplikacji.
- Użyj obsługi pozapasmowej dla uwierzytelniania wieloskładnikowego (MFA), który został wprowadzony w wersji IBM MFA 1.2. W takim przypadku należy wstępnie uwierzytelnić się na serwerze WWW IBM MFA, a oprócz identyfikatora użytkownika i hasła podać dodatkowe uwierzytelnianie określone przez strategię. IBM generuje informacje autoryzacyjne tokenu pamięci podręcznej, które są następnie określane w oknie dialogowym uwierzytelniania IBM MQ Explorer . Administrator zabezpieczeń może zezwolić na powtarzanie tych informacji autoryzacyjnych przez rozsądny czas, tak aby umożliwić normalne użycie IBM MQ Explorer .

Więcej informacji na temat tego podejścia zawiera sekcja Wprowadzenie do produktu IBM MFA.

z/OS Zarządzanie zabezpieczeniami produktu IBM MQ for z/OS

Produkt IBM MQ używa tabeli w pamięci masowej do przechowywania informacji dotyczących każdego użytkownika i żądań dostępu wykonanych przez każdego użytkownika. Aby sprawnie zarządzać tą tabelą i zmniejszyć liczbę żądań wykonanych z produktu IBM MQ do zewnętrznego menedżera zabezpieczeń (ESM), dostępna jest pewna liczba elementów sterujących.

Te elementy sterujące są dostępne zarówno na panelach operacji, jak i w panelach sterujących i w komendach IBM MQ .

z/OS *Ponowna weryfikacja identyfikatora użytkownika*

Jeśli definicja RACF użytkownika korzystaącego z zasobów produktu IBM MQ została zmieniona, na przykład przez połączenie użytkownika z nową grupą, można powiadomić menedżera kolejek o tym, aby ponownie podpisał ten użytkownik podczas następnego próby uzyskania dostępu do zasobu IBM MQ . W tym celu należy użyć komendy IBM MQ RVERIFY SECURITY.

- Użytkownik HX0804 otrzymuje i wprowadza komunikaty do kolejek PAYROLL w menedżerze kolejek PRD1. Jednak HX0804 wymaga teraz dostępu do niektórych kolejek PENSION w tym samym menedżerze kolejek (PRD1).
- Administrator zabezpieczeń danych łączy użytkownika HX0804 z grupą RACF , która umożliwia dostęp do kolejek PENSION.
- Tak więc HX0804 może natychmiast uzyskać dostęp do kolejek PENSION (czyli bez zamykania menedżera kolejek PRD1 lub oczekiwania na przekroczenie limitu czasu przez HX0804), należy użyć komendy IBM MQ :

```
RVERIFY SECURITY(HX0804)
```

Uwaga: W przypadku wyłączenia limitu czasu identyfikatora użytkownika przez długi czas (dni lub nawet tygodnie), gdy menedżer kolejek jest uruchomiony, należy pamiętać, aby uruchomić komendę RVERIFY SECURITY dla wszystkich użytkowników, którzy zostali odwołani lub usunięci w tym czasie.

z/OS *Limity czasu dla ID użytkownika*

Po upływie okresu nieaktywności można utworzyć użytkownika z menedżera kolejek przy użyciu programu IBM MQ .

Gdy użytkownik uzyskuje dostęp do zasobu IBM MQ , menedżer kolejek próbuje podpisać tego użytkownika w menedżerze kolejek (jeśli zabezpieczenia podsystemu są aktywne). Oznacza to, że użytkownik jest uwierzytelniany w ESM. Ten użytkownik pozostaje zalogowany do programu IBM MQ do czasu wyłączenia menedżera kolejek lub do czasu, gdy identyfikator użytkownika będzie miał wartość *Przekroczenie limitu czasu* (lapses uwierzytelniania) lub ponownie zweryfikowany (ponownie uwierzytelniony).

Gdy użytkownik przekroczył limit czasu, identyfikator użytkownika ma wartość *wylogowany* w menedżerze kolejek, a wszelkie informacje związane z bezpieczeństwem przechowywane dla tego użytkownika są usuwane. Wpisywanie się i wyłączanie użytkownika w menedżerze kolejek nie jest widoczne dla programu użytkowego ani dla użytkownika.

Użytkownicy kwalifikują się do przekroczenia limitu czasu, jeśli nie używali żadnych zasobów IBM MQ przez określony czas. Ten okres jest ustawiany za pomocą komendy MQSC ALTER SECURITY.

W komendzie ALTER SECURITY można podać dwie wartości:

TIMEOUT
Czas (w minutach), przez który nieużywany ID użytkownika i powiązane z nim zasoby mogą pozostać w menedżerze kolejek produktu IBM MQ .

INTERVAL
Wyrażony w minutach przedział czasu między sprawdzeniami identyfikatorów użytkowników i powiązanymi z nimi zasobami, w celu określenia, czy limit czasu *LIMIT_CZASU* utracił ważność.

Na przykład, jeśli wartość *TIMEOUT* wynosi 30, a wartość *INTERVAL* to 10, to co 10 minut program IBM MQ sprawdza identyfikatory użytkowników i powiązane z nimi zasoby w celu określenia, czy nie zostały one użyte przez 30 minut. Jeśli zostanie znalezione nieważne ID użytkownika, to ID użytkownika jest wypisywane z menedżera kolejek. Jeśli zostaną znalezione jakiekolwiek informacje o zasobach z przekroczonym limitem czasu, które są powiązane z identyfikatorami użytkowników, które nie przekroczono limitu czasu, informacje o zasobach są usuwane. Jeśli identyfikatory użytkowników nie mają być czasochłonne, należy ustawić wartość *INTERVAL* na zero. Jeśli jednak wartość *INTERVAL* wynosi zero, pamięć zajmowana przez identyfikatory użytkowników i powiązane z nimi zasoby nie są zwalniane do czasu wydania komendy **REFRESH SECURITY** lub **RVERIFY SECURITY** .

Strojenie tej wartości może być istotne, jeśli istnieje wiele jednorazowych użytkowników. Jeśli zostanie ustawiony mały odstęp czasu i wartości limitu czasu, zasoby, które nie są już wymagane, zostaną zwolnione.

Uwaga: Jeśli używane są wartości *INTERVAL* lub *TIMEOUT* inne niż wartości domyślne, należy ponownie wprowadzić komendę przy każdym uruchomieniu menedżera kolejek. Tę opcję można wykonać automatycznie, umieszczając komendę **ALTER SECURITY** w zestawie danych CSQINP1 dla tego menedżera kolejek.

z/OS *Odświeżanie zabezpieczeń menedżera kolejek w systemie z/OS*

IBM MQ for z/OS buforuje dane RACF w celu zwiększenia wydajności. Po zmianie niektórych klas zabezpieczeń należy odświeżyć te informacje w pamięci podręcznej. W razie problemów z wydajnością należy często odświeżać zabezpieczenia. Można również odświeżyć tylko informacje o zabezpieczeniach TLS.

Gdy kolejka jest otwierana po raz pierwszy (lub po raz pierwszy od momentu odświeżenia zabezpieczeń), program IBM MQ sprawdza RACF w celu uzyskania praw dostępu użytkownika i umieszcza te informacje w pamięci podręcznej. Buforowane dane obejmują identyfikatory użytkowników i zasoby, dla których wykonano sprawdzanie zabezpieczeń. Jeśli kolejka jest ponownie otwierana przez tego samego użytkownika, obecność buforowanych danych oznacza, że produkt IBM MQ nie musi wydawać RACF sprawdzania, co zwiększa wydajność. Działanie odświeżania zabezpieczeń polega na odrzucaniu wszystkich buforowanych informacji o zabezpieczeniach i tak wymuszonej IBM MQ w celu dokonania nowego sprawdzenia w odniesieniu do produktu RACF. W przypadku dodawania, zmiany lub usuwania

profilu zasobu produktu RACF znajdującego się w klasie MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST lub MXTOPIC należy poinformować menedżery kolejek, które używają tej klasy, do odświeżenia informacji o zabezpieczeniach, które przechowują. W tym celu należy wprowadzić następujące komendy:

- Komenda REFRESH RACF SETROPTS RACLIST (classname) REFRESH w celu odświeżenia na poziomie RACF .
- Komenda IBM MQ REFRESH SECURITY służy do odświeżania informacji o zabezpieczeniach przechowywanych przez menedżer kolejek. Ta komenda musi być wywołana przez każdy menedżer kolejek, który uzyskuje dostęp do tych profili, które uległy zmianie. Jeśli istnieje grupa współużytkowania kolejek, można użyć atrybutu zasięgu komendy w celu skierowania komendy do wszystkich menedżerów kolejek w grupie.

  Uwaga: Jeśli do istniejącej grupy nawiązano połączenie nowego użytkownika, należy uruchomić komendę IBM MQ RVERIFY SECURITY(ID użytkownika). Komenda REFRESH SECURITY (*) nie pozwala menedżerowi kolejek wpisywać tego użytkownika ponownie, przy następnym próbie uzyskania dostępu do zasobu IBM MQ .

Jeśli w dowolnej z klas produktu IBM MQ używane są profile ogólne, należy również wprowadzić normalne komendy odświeżania produktu RACF , jeśli zostaną zmienione, dodane lub usunięte wszystkie profile ogólne. Na przykład: SETROPTS GENERIC (classname) ODŚWIEŻ.

Jeśli jednak profil zasobu produktu RACF zostanie dodany, zmieniony lub usunięty, a zasób, do którego ma on zastosowanie, nie został jeszcze uzyskany (w związku z tym żadne informacje nie są buforowane), produkt IBM MQ użyje nowej informacji RACF bez wydania komendy REFRESH SECURITY.

Jeśli kontrola RACF jest włączona (na przykład za pomocą komendy RACF RALTER AUDIT (access-próbie (audit_access_level))), buforowanie nie odbywa się, a więc IBM MQ odnosi się bezpośrednio do przestrzeni danych RACF dla każdego sprawdzenia. Zmiany są więc pobierane natychmiast, a REFRESH SECURITY nie jest konieczne w celu uzyskania dostępu do zmian. Za pomocą komendy RACF RLIST można sprawdzić, czy kontrola RACF jest włączona. Na przykład można wydać komendę

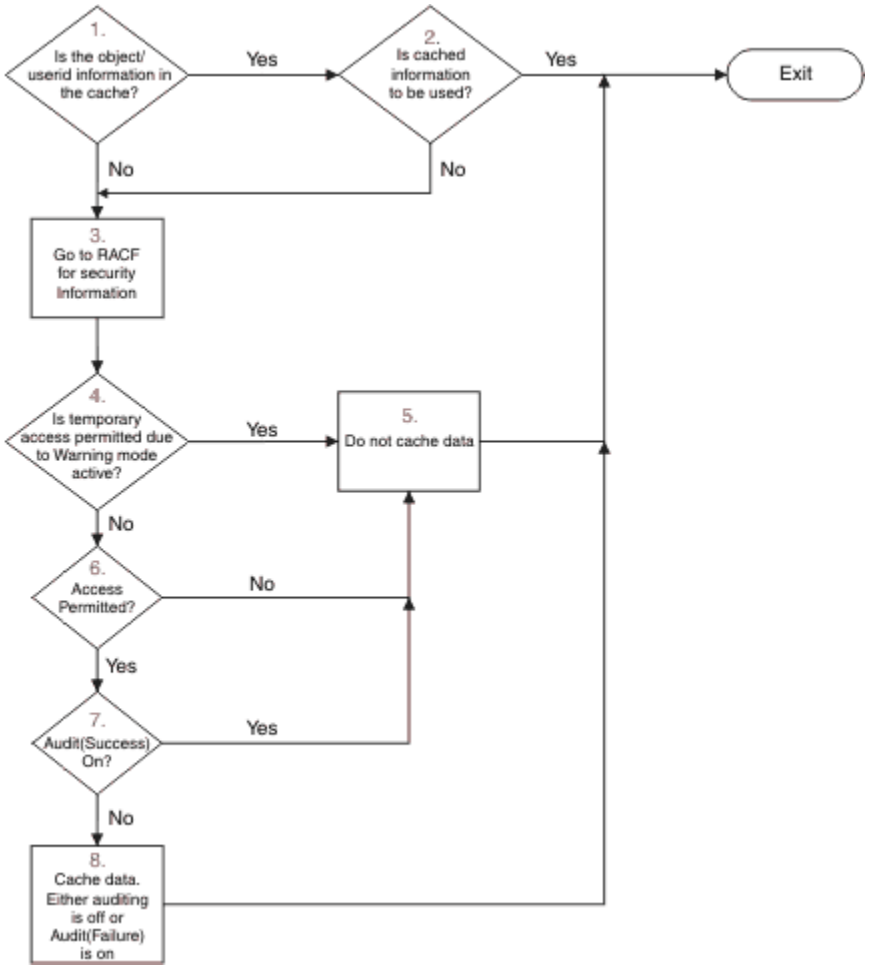
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

i otrzymać wyniki

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

Wskazuje na to, że kontrola jest włączona. Więcej informacji na ten temat zawiera publikacja *z/OS Security Server RACF Auditor's Guide* oraz podręcznik *z/OS Security Server RACF Command Language Reference*.

Rysunek 17 na stronie 258 podsumowuje sytuacje, w których informacje o zabezpieczeniach są buforowane i w których wykorzystywane są informacje buforowane.



Rysunek 17. Przepływ logiki dla buforowania zabezpieczeń produktu IBM MQ

Jeśli ustawienia zabezpieczeń zostaną zmienione przez dodanie lub usunięcie profili przełącznika w klasach MQADMIN lub MXADMIN, należy użyć jednej z następujących komend, aby dokonać dynamicznego wyboru następujących zmian:

ODŚWIEŻ ZABEZPIECZENIA (*)
ODŚWIEŻ ZABEZPIECZENIA (MQADMIN)
ODŚWIEŻ ZABEZPIECZENIA (MXADMIN)

Oznacza to, że można aktywować nowe typy zabezpieczeń lub dezaktywować je bez konieczności restartowania menedżera kolejek.

Ze względu na wydajność są to jedyne klasy, na które ma wpływ komenda REFRESH SECURITY. W przypadku zmiany profilu w klasach MQCONN lub MQCMDS nie ma potrzeby używania opcji REFRESH SECURITY.

Uwaga: Odświeżenie klasy MQADMIN lub MXADMIN nie jest wymagane, jeśli zmieniany jest profil bezpieczeństwa RESLEVEL.

Ze względu na wydajność należy używać funkcji REFRESH SECURITY możliwie jak najczęstej, najlepiej w godzinach poza szczytem. Użytkownik może zminimalizować liczbę odświeżeń zabezpieczeń, łącząc użytkowników z grupami RACF , które znajdują się już na liście dostępu dla profili produktu IBM MQ , a nie umieszczając poszczególnych użytkowników na listach dostępu. W ten sposób można zmienić użytkownika, a nie profil zasobu. Zamiast odświeżania zabezpieczeń można również użyć komendy RVERIFY SECURITY, która jest odpowiednim użytkownikiem.

Na przykład: REFRESH SECURITY, załóżmy, że definiuje się nowe profile w celu ochrony dostępu do kolejek, zaczynając od INSURANCE.LIFE w menedżerze kolejek PRMQ. Można użyć następujących komend produktu RACF :

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Należy wydać następującą komendę, aby poinformować program RACF o odświeżeniu informacji o zabezpieczeniach, które są przechowywane, na przykład:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Ponieważ te profile są ogólne, należy poinformować produkt RACF , aby odświeżyć profile ogólne dla MQQUEUE. Na przykład:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Następnie należy użyć tej komendy w celu poinformowania menedżera kolejek PRMQ o zmianie profili kolejek:

```
REFRESH SECURITY(MQQUEUE)
```

Odświeżanie zabezpieczeń SSL/TLS

Aby odświeżyć buforowany widok repozytorium kluczy TLS, wydaj komendę REFRESH SECURITY z opcją TYPE (SSL). Dzięki temu można zaktualizować niektóre ustawienia TLS bez konieczności restartowania inicjatora kanału.

z/OS *Wyświetlanie statusu zabezpieczeń*

Aby wyświetlić status przełączników zabezpieczeń i inne elementy sterujące zabezpieczeniami, należy wprowadzić komendę MQSC DISPLAY SECURITY.

Na poniższym rysunku przedstawiono typowe dane wyjściowe komendy DISPLAY SECURITY ALL.

```
CSQH015I +CSQ1 Security timeout = 54 MINUTES
CSQH016I +CSQ1 Security interval = 12 MINUTES
CSQH030I +CSQ1 Security switches ...
CSQH034I +CSQ1 SUBSYSTEM: ON, 'SQ05.NO.SUBSYS.SECURITY' not found
CSQH032I +CSQ1 QMGR: ON, 'CSQ1.YES.QMGR.CHECKS' found
CSQH031I +CSQ1 QSG: OFF, 'SQ05.NO.QSG.CHECKS' found
CSQH031I +CSQ1 CONNECTION: OFF, 'CSQ1.NO.CONNECT.CHECKS' found
CSQH034I +CSQ1 COMMAND: ON, 'CSQ1.NO.COMMAND.CHECKS' not found
CSQH031I +CSQ1 CONTEXT: OFF, 'CSQ1.NO.CONTEXT.CHECKS' found
CSQH034I +CSQ1 ALTERNATE USER: ON, 'CSQ1.NO.ALTERNATE.USER.CHECKS' not found
CSQH034I +CSQ1 PROCESS: ON, 'CSQ1.NO.PROCESS.CHECKS' not found
CSQH034I +CSQ1 NAMELIST: ON, 'CSQ1.NO.NLIST.CHECKS' not found
CSQH034I +CSQ1 QUEUE: ON, 'CSQ1.NO.QUEUE.CHECKS' not found
CSQH034I +CSQ1 TOPIC: ON, 'CSQ1.NO.TOPIC.CHECKS' not found
CSQH031I +CSQ1 COMMAND RESOURCES: OFF, 'CSQ1.NO.CMD.RESC.CHECKS' found
CSQ9022I +CSQ1 CSQHPDTC ' DISPLAY SECURITY' NORMAL COMPLETION
```

Rysunek 18. Typowe dane wyjściowe komendy DISPLAY SECURITY

W przykładzie przedstawiono, że menedżer kolejek, który odpowiedział na komendę, zawiera podsystem, komendę, alternatywny użytkownik, proces, listę nazw i bezpieczeństwo kolejek na poziomie menedżera kolejek, ale nie na poziomie grupy współużytkowania kolejek. Połączenie, zasób komendy i zabezpieczenia kontekstu nie są aktywne. Wyświetlane są również informacje o tym, że limity czasu dla ID użytkownika są aktywne i co 12 minut menedżer kolejek sprawdza identyfikatory użytkowników, które nie były używane w tym menedżerze kolejek przez 54 minuty, a następnie usuwa je.

Uwaga: Ta komenda wyświetla bieżący status zabezpieczeń. Nie musi on odzwierciedlać bieżącego statusu profili przełącznika zdefiniowanych dla produktu RACFlub statusu klas RACF . Na przykład profile przełączników mogły zostać zmienione od czasu ostatniego restartu tego menedżera kolejek lub komendy REFRESH SECURITY.

z/OS Zadania instalacji zabezpieczeń dla produktu z/OS

Po zainstalowaniu i dostosowaniu produktu IBM MQautoryzuj uruchomione procedury zadań w programie RACF, autoryzuj dostęp do różnych zasobów i skonfiguruj definicje produktu RACF . Opcjonalnie skonfiguruj system pod kątem protokołu TLS.

Po pierwszym zainstalowaniu i dostosowaniu produktu IBM MQ należy wykonać następujące zadania związane z bezpieczeństwem:

1. Skonfiguruj zestaw danych IBM MQ i zabezpieczenia systemu przez:
   - Autoryzowanie procedury uruchomionego zadania menedżera kolejek xxxxMSTR i procedury uruchomionego zadania kolejkowania rozproszonego xxxxCHIN w celu uruchomienia w ramach produktu RACF.
   - Autoryzowanie dostępu do zestawów danych menedżera kolejek.
   - Autoryzowanie dostępu do zasobów dla tych identyfikatorów użytkowników, którzy będą korzystać z menedżera kolejek i programów narzędziowych.
   - Autoryzowanie dostępu dla tych menedżerów kolejek, które będą korzystały ze struktur listy narzędzia CF.
   - Autoryzowanie dostępu dla tych menedżerów kolejek, które będą używać produktu Db2.
2. Skonfiguruj definicje RACF dla zabezpieczeń produktu IBM MQ .
3. Jeśli chcesz używać protokołu TLS (Transport Layer Security), przygotuj system do korzystania z certyfikatów i kluczy.

z/OS *Konfigurowanie zabezpieczeń zestawu danych produktu IBM MQ for z/OS*

Istnieje wiele typów użytkowników produktu IBM MQ . Produkt RACF służy do sterowania dostępem do zestawów danych systemowych.

Potencjalnymi użytkownikami zestawów danych produktu IBM MQ są następujące obiekty:

- Sam menedżer kolejek.
- Inicjator kanału
- Administratorzy produktu IBM MQ , którzy muszą tworzyć zestawy danych programu IBM MQ , uruchamiać programy narzędziowe i podobne zadania.
- Programiści aplikacji, którzy muszą korzystać z dostarczonych przez produkt IBM MQstruktury copybook, obejmują zestawy danych, makra i podobne zasoby.
- Wnioski obejmujące jeden lub więcej spośród:
  - Zadania wsadowe
  - Użytkownicy TSO
  - CICS regiony
  - IMS regiony
- Zestawy danych CSQOUTX i CSQSNAP
- Kolejki dynamiczne SYSTEM.CSQXCMD.*

Dla wszystkich tych potencjalnych użytkowników należy chronić zestawy danych produktu IBM MQ za pomocą produktu RACF.

Musisz także kontrolować dostęp do wszystkich zestawów danych 'CSQINP'.

z/OS *Autoryzacja RACF dla procedur uruchomionych zadań*

Niektóre zestawy danych produktu IBM MQ są przeznaczone do wyłącznego użycia menedżera kolejek. Jeśli zestawy danych produktu IBM MQ są zabezpieczane przy użyciu produktu RACF, należy również autoryzować procedurę uruchomionego zadania menedżera kolejek xxxxMSTRoraz procedurę uruchomionego zadania kolejkowania rozproszonego xxxxCHINprzy użyciu programu RACF. W tym celu należy użyć klasy STARTED. Alternatywnie można użyć tabeli uruchomionych procedur (ICHRIN03), ale przed rozpoczęciem wprowadzania zmian należy wykonać IPL systemu z/OS .

Aby uzyskać więcej informacji, zapoznaj się z podręcznikiem *z/OS Security Server RACF System Programmer's Guide*.

Zidentyfikowany identyfikator użytkownika produktu RACF musi mieć wymagany dostęp do zestawów danych w procedurze uruchomionego zadania. Jeśli na przykład uruchomiono procedurę zadania uruchomionego menedżera kolejek o nazwie CSQ1MSTR z identyfikatorem użytkownika RACF o identyfikatorze QMGRCSQ1, identyfikator użytkownika QMGRCSQ1 musi mieć dostęp do zasobów z/OS , do których uzyskuje dostęp menedżer kolejek CSQ1 .

Ponadto treść pola GROUP w identyfikatorze użytkownika menedżera kolejek musi być taka sama, jak treść pola GROUP w profilu STARTED dla tego menedżera kolejek. Jeśli treść w poszczególnych polach GROUP nie jest zgodna, do systemu nie można wprowadzić odpowiedniego ID użytkownika. Ta sytuacja powoduje, że program IBM MQ jest uruchamiany z niezdefiniowanym identyfikatorem użytkownika i w związku z tym z powodu naruszenia zabezpieczeń.

Identyfikatory użytkowników programu RACF powiązane z procedurami zadania menedżera kolejek i inicjatora kanału nie mogą mieć ustawionego atrybutu TRUSTED.

z/OS *Autoryzowanie dostępu do zestawów danych*

Zestawy danych produktu IBM MQ powinny być chronione w taki sposób, aby nieautoryzowany użytkownik mógł uruchamiać instancję menedżera kolejek lub uzyskiwać dostęp do żadnych danych menedżera kolejek. Aby to zrobić, należy użyć normalnego zabezpieczenia zestawu danych z/OS RACF .

Tabela 65 na stronie 261 podsumowuje dostęp produktu RACF do różnych zestawów danych, które muszą być dostępne dla procedury uruchomionej przez menedżer kolejek.

Tabela 65. Dostęp do produktu RACF do zestawów danych powiązanych z menedżerem kolejek

RACF dostęp	**Zestawy danych**
READ	• `thlqual.SCSQAUTH` i `thlqual.SCSQANLx` (gdzie x jest literą języka dla danego języka narodowego). • Zestawy danych, do których odwołuje się CSQINP1, CSQINP2 i CSQXLIB, w procedurze uruchomionej zadania menedżera kolejek. • Zestawy danych SMDS należące do innych menedżerów kolejek w grupie. • Dziennik, BSDS i archiwalne zestawy danych dziennika dla innych menedżerów kolejek w grupie.
UPDATE	• Wszystkie zestawy stron oraz zestawy danych dziennika i BSDS. • Zestawy danych SMDS, których właścicielem jest menedżer kolejek
Zmień	• Wszystkie zestawy danych dziennika archiwalnego.

Tabela 66 na stronie 262 podsumowuje dostęp produktu RACF , że procedura uruchomionego zadania dla rozproszonego kolejkowania musi mieć do różnych zestawów danych.

Tabela 66. RACF dostęp do zestawów danych powiązanych z kolejkowaniem rozproszonym	
RACF dostęp	**Zestawy danych**
READ	• thlqual.SCSQAUTH, thlqual.SCSQANLx (gdzie x jest literą języka dla danego języka narodowego) i thlqual.SCSQMVR1. • Zestawy danych biblioteki LE. • Zestawy danych, do których odwołuje się CSQXLIB i CSQINPX, w procedurze uruchomionego zadania initator kanału.
UPDATE	• Zestawy danych CSQOUTX i CSQSNAP

Więcej informacji na ten temat zawiera publikacja *z/OS Security Server RACF Security Administrator's Guide*.

z/OS V 9.1.4 *Szyfrowanie zestawów danych*

Zestawy danych produktu IBM MQ mogą być szyfrowane przy użyciu szyfrowania zestawu danych z/OS , dzięki czemu dane są chronione lub ze względów regulacyjnych.

Można chronić wszystkie zestawy stron, aktywny dziennik, dziennik archiwalny i zestawy danych programu startowego (BSDS) z szyfrowaniem zestawu danych z/OS .

Ostrzeżenie: Nie można chronić współużytkowanych zestawów danych komunikatów (SMDS) z szyfrowaniem zestawu danych z/OS przez produkt IBM MQ for z/OS 9.1.3 lub wcześniejszy.

Patrz sekcja poufność danych w produkcie IBM MQ for z/OS przy użyciu szyfrowania zestawu danych. :NONE.

z/OS *Konfigurowanie zabezpieczeń zasobów produktu IBM MQ for z/OS*

Istnieje wiele typów użytkowników produktu IBM MQ . Produkt RACF służy do sterowania dostępem do zasobów produktu IBM MQ .

Potencjalnymi użytkownikami zasobów produktu IBM MQ , takimi jak kolejki i kanały, są następujące obiekty:

- Sam menedżer kolejek.
- Inicjator kanału
- Administratorzy produktu IBM MQ , którzy muszą tworzyć zestawy danych programu IBM MQ , uruchamiać programy narzędziowe i podobne zadania.
- Programiści aplikacji, którzy muszą korzystać z dostarczonych przez produkt IBM MQstruktury copybook, obejmują zestawy danych, makra i podobne zasoby.
- Wnioski obejmujące jeden lub więcej spośród:
  - Zadania wsadowe
  - Użytkownicy TSO
  - CICS regiony
  - IMS regiony
- Zestawy danych CSQOUTX i CSQSNAP
- Kolejki dynamiczne SYSTEM.CSQXCMD.*

Dla wszystkich tych potencjalnych użytkowników należy chronić zasoby produktu IBM MQ przy użyciu produktu RACF. W szczególności należy pamiętać, że inicjator kanału musi mieć dostęp do różnych zasobów, zgodnie z opisem w sekcji “Zagadnienia związane z zabezpieczeniami dla inicjatora kanału w systemie z/OS” na stronie 269, a więc identyfikator użytkownika, pod którym działa, musi być autoryzowany do uzyskania dostępu do tych zasobów.

Jeśli używana jest grupa współużytkowania kolejek, menedżer kolejek może wydawać wewnętrznie różne komendy, dlatego identyfikator użytkownika, którego używa, musi być autoryzowany do wydawania takich komend. Dostępne są następujące komendy:

- DEFINE, ALTER i DELETE dla każdego obiektu, który ma QSGDISP (GROUP)
- START i STOP CHANNEL dla każdego kanału używanego z CHLDISP (SHARED)

z/OS *Konfigurowanie systemu z/OS do używania protokołu TLS*

W tym temacie opisano sposób konfigurowania produktu IBM MQ for z/OS przy użyciu protokołu TLS (Transport Layer Security) przy użyciu komend produktu RACF .

Jeśli ma być używany protokół TLS w celu zabezpieczenia kanału, w systemie istnieje wiele zadań, które należy wykonać. Szczegółowe informacje na temat używania komend RACF dla certyfikatów i repozytoriów kluczy (key rings) zawiera sekcja Praca z protokołem TLS w systemie z/OS .

1. Utwórz plik kluczy w programie RACF , aby przechowywać wszystkie klucze i certyfikaty dla systemu, za pomocą komendy RACF RACDCERT. Na przykład:

   ```
   RACDCERT ID(CHINUSER) ADDRING(QM1RING)
   ```

   Identyfikator musi być identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału lub identyfikatorem użytkownika, który ma być właścicielem pliku kluczy, jeśli ma to być współużytkowany pierścień kluczy.

2. Utwórz certyfikat cyfrowy dla każdego menedżera kolejek, korzystając z komendy RACF RACDCERT.

   Etykieta certyfikatu musi być wartością atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartością domyślną `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek lub grupy współużytkowania kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych . W tym przykładzie jest to `ibmWebSphereMQQM1`.

   Na przykład:

   ```
   RACDCERT ID(USERID) GENCERT
   SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
   WITHLABEL('ibmWebSphereMQQM1')
   ```

3. Połącz certyfikat w RACF z pierścieniem kluczy, korzystając z komendy RACF RACDCERT. Na przykład:

   ```
   RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
   CONNECT ID(CHINUSER)
   ```

   Konieczne jest również połączenie wszystkich odpowiednich certyfikatów osoby podpisującej (z ośrodka certyfikacji) do pliku kluczy. Oznacza to, że wszystkie uprawnienia do certyfikatów TLS dla tego menedżera kolejek i wszystkich ośrodków certyfikacji dla wszystkich certyfikatów TLS, z którymi komunikuje się ten menedżer kolejek, są wymagane. Na przykład:

   ```
   RACDCERT ID(CHINUSER)
   CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
   ```

4. Na każdym z menedżerów kolejek należy użyć komendy IBM MQ ALTER QMGR, aby określić repozytorium kluczy, do którego należy wskazać menedżer kolejek. Na przykład, jeśli właścicielem pliku kluczy jest przestrzeń adresowa inicjatora kanału:

```
ALTER QMGR SSLKEYR(QM1RING)
```

lub jeśli używany jest współużytkowany pierścień kluczy:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

gdzie *id_użytkownika* jest identyfikatorem użytkownika, który jest właścicielem współużytkowanego pliku kluczy.

5. Listy odwołań certyfikatów (Certificate Revocation Lists-CRLs) umożliwiają organom certyfikacji unieważnienie certyfikatów, których nie można już ufać. Listy CRL są przechowywane na serwerach LDAP. Aby uzyskać dostęp do tej listy na serwerze LDAP, należy najpierw utworzyć obiekt AUTHINFO o wartości AUTHTYPE CRLLDAP, korzystając z komendy IBM MQ DEFINE AUTHINFO. Na przykład:

```
DEFINE AUTHINFO(LDAP1)
AUTHTYPE(CRLLDAP)
CONNAME(ldap.server(389))
LDAPUSER('')
LDAPPWD('')
```

W tym przykładzie lista odwołań certyfikatów jest przechowywana w publicznym obszarze serwera LDAP, dlatego pola LDAPUSER i LDAPPWD nie są konieczne.

Następnie należy umieścić obiekt AUTHINFO na liście nazw, używając komendy IBM MQ DEFINE NAMELIST. Na przykład:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Na koniec należy powiązać listę nazw z każdym menedżerem kolejek za pomocą komendy IBM MQ ALTER QMGR. Na przykład:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Skonfiguruj menedżer kolejek, aby uruchamiać wywołania TLS, używając komendy IBM MQ ALTER QMGR. Definiuje podzadania serwera, które obsługują tylko wywołania SSL, co pozostawia normalne programy rozsyłające, aby kontynuować przetwarzanie w normalny sposób, bez wpływu na połączenia SSL. Użytkownik musi mieć co najmniej dwa z tych podzadań. Na przykład:

```
ALTER QMGR SSLTASKS(8)
```

Ta zmiana jest używana tylko wtedy, gdy inicjator kanału jest restartowany.

7. Określ specyfikację szyfru, która ma być używana dla każdego kanału, przy użyciu komendy IBM MQ DEFINE CHANNEL lub ALTER CHANNEL. Na przykład:

```
ALTER CHANNEL(LDAPCHL)
CHLTYPE(SDR)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

Oba końce kanału muszą określać tę samą specyfikację szyfru.

z/OS Zarządzanie rekordami uwierzytelniania kanału w QSG

Rekordy uwierzytelniania kanału mają zastosowanie do menedżera kolejek, w którym są tworzone, nie są one współużytkowane w całej grupie współużytkowania kolejki (QSG). Dlatego też, jeśli wszystkie menedżery kolejek w grupie współużytkowania kolejek muszą mieć te same reguły, należy przeprowadzić pewne zarządzanie, aby zachować spójność wszystkich reguł.

1. Zawsze należy dodać opcję `CMDSCOPE(*)` do wszystkich komend produktu `SET CHLAUTH`. Spowoduje to wysłanie komendy do wszystkich działających menedżerów kolejek w grupie współużytkowania kolejek.
2. Użyj komendy `DISPLAY CHLAUTH` z opcją `CMDSCOPE(*)`, a następnie przeanalizuj odpowiedzi, aby sprawdzić, czy rekordy są takie same we wszystkich menedżerach kolejek. Jeśli niespójność zostanie znaleziona, można wydać komendę `SET CHLAUTH` zawierającą tę samą regułę z produktem `CMDSCOPE(*)` lub `CMDSCOPE(`*qmgr-name*`)`.
3. Dodaj element do konkatenacji CSQINP2 menedżera kolejek (szczegółowe informacje zawiera sekcja Komendy inicjalizacji), która zawiera pełny zestaw reguł. Te elementy zostaną odczytane jako część procesu inicjowania menedżera kolejek. Jeśli komenda `SET CHLAUTH` używa `ACTION(ADD)`, reguła zostanie dodana tylko wtedy, gdy nie istnieje. Użycie produktu `ACTION(REPLACE)` spowoduje zastąpienie istniejącej reguły, jeśli już istnieje, lub ją doda, jeśli nie. Ten sam element może następnie zostać umieszczony w konkatenacji CSQINP2 wszystkich menedżerów kolejek w grupie współużytkowania kolejek.
4. Aby wyodrębnić reguły z jednego menedżera kolejek przy użyciu opcji `MAKEDEF` lub `MAKEREP`, należy użyć programu narzędziowego CSQUTIL (szczegółowe informacje na ten temat można znaleźć w sekcji Wydawanie komend do komendy IBM MQ (COMMAND)). Następnie należy odtworzyć dane wyjściowe za pomocą komendy CSQUTIL w docelowym menedżerze kolejek.

Pojęcia pokrewne

Rekordy uwierzytelniania kanału

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

z/OS Zagadnienia dotyczące kontroli w systemie z/OS

W celu przeprowadzenia kontroli bezpieczeństwa menedżera kolejek dostępne są standardowe elementy sterujące RACF kontroli. Produkt IBM MQ nie gromadzi żadnych danych statystycznych dotyczących bezpieczeństwa. Jedynymi statystykami są te, które mogą być tworzone na podstawie kontroli.

Kontrola produktu RACF może być oparta na:

- Identyfikatory użytkownika
- Klasy zasobów
- Profile

Więcej informacji na ten temat zawiera podręcznik *z/OS Security Server RACF Auditor's Guide*.

Uwaga: Kontrola pogarsza wydajność; im więcej kontroli jest implementowana, tym większa wydajność jest zdegradowana. Jest to również rozważenie użycia opcji RACF WARNING.

z/OS *POZIOM KONTROLI RESLEVEL*

Za pomocą parametru systemowego RESAUDIT można sterować produkcją rekordów kontroli RESLEVEL. RACF tworzone są rekordy kontroli ogólnej.

Tworzenie rekordów kontroli RESLEVEL poprzez ustawienie parametru systemu RESAUDIT na YES. Jeśli parametr RESAUDIT jest ustawiony na NO, rekordy kontroli nie są generowane. Więcej szczegółowych informacji na temat ustawiania tego parametru zawiera sekcja Korzystanie z komendy CSQ6SYSP.

Jeśli wartość RESAUDIT jest ustawiona na YES, nie są wykonywane żadne normalne rekordy kontroli produktu RACF , gdy zostanie sprawdzony dostęp do profilu hlq.RESLEVEL , który ma dostęp do identyfikatora użytkownika przestrzeni adresowej. Zamiast tego IBM MQ żąda, aby program RACF utworzył rekord kontroli ogólnej (zdarzenie o numerze 27). Te sprawdzenia są wykonywane tylko w czasie połączenia, a więc koszt wydajności jest minimalny.

Ogólne rekordy kontroli produktu IBM MQ można zgłaszać za pomocą programu piszącego raport RACF (RACFRW). Aby zgłosić dostęp do RESLEVEL, można użyć następujących komend RACFRW:

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

Przykładowy raport z tabeli RACFRW, z wyłączeniem pól *Date*, *Time*i *SYSID* , jest wyświetlany w produkcie Rysunek 19 na stronie 266.

```
       RACF REPORT - LISTING OF PROCESS RECORDS                                  PAGE   4
                                E
                                V  Q
                                E  U
*JOB/USER *STEP/  --TERMINAL--  N  A
   NAME    GROUP     ID    LVL  T  L

 WS21B    MQMGRP IGJZM000   0   27 0  JOBID=(WS21B 05.111 09:44:57),USERDATA=()
    TRUSTED USER                      AUTH=(NONE),REASON=(NONE)
                                 SESSION=TSOLOGON,TERMINAL=IGJZM000,
                                 LOGSTR='CSQH RESLEVEL CHECK PERFORMED AGAINST
PROFILE(QM66.RESLEVEL),
                                 CLASS(MQADMIN), ACCESS EQUATES TO
(CONTROL)',RESULT=SUCCESS,MQADMIN
```

Rysunek 19. Przykładowe dane wyjściowe z RACFRW przedstawiające ogólne rekordy kontroli RESLEVEL

Po sprawdzeniu danych LOGSTR w tym przykładzie można zauważyć, że użytkownik TSO WS21B ma dostęp CONTROL do katalogu QM66.RESLEVEL. Oznacza to, że wszystkie sprawdzenia zabezpieczeń zasobów są pomijane, gdy użytkownik WS21B uzyskuje dostęp do zasobów QM66 .

Więcej informacji na temat korzystania z RACFRW można znaleźć w publikacji *z/OS Security Server RACF Auditor's Guide*.

z/OS Dostosowywanie zabezpieczeń

Aby zmienić sposób działania zabezpieczeń produktu IBM MQ , należy wykonać to działanie za pomocą wyjścia SAF (ICHRFR00) lub wyjść z zewnętrznego menedżera zabezpieczeń.

Więcej informacji na temat wyjść produktu RACF można znaleźć w podręczniku *z/OS Security Server RACROUTE Macro Reference* .

Uwaga: Ponieważ program IBM MQ optymalizuje wywołania ESM, żądania RACROUTE mogą nie być wykonywane na przykład w przypadku wszystkich otwartych dla konkretnej kolejki przez konkretnego użytkownika.

z/OS Komunikaty o naruszaniu zabezpieczeń w systemie z/OS

Naruszenie zabezpieczeń jest wskazyane przez kod powrotu MQRC_NOT_AUTHORIZED w aplikacji lub przez komunikat w protokole zadania.

Kod powrotu MQRC_NOT_AUTHORIZED może zostać zwrócony do aplikacji z następujących powodów:

- Użytkownik nie ma uprawnień do łączenia się z menedżerem kolejek. W tym przypadku wyświetlany jest komunikat ICH408I w protokole zadania wsadowego/TSO, CICSlub IMS .
- Logowanie użytkownika do menedżera kolejek nie powiodło się, ponieważ na przykład ID użytkownika zadania jest niepoprawny lub odpowiedni, albo ID użytkownika zadania lub alternatywny identyfikator użytkownika nie jest poprawny. Co najmniej jeden z tych identyfikatorów użytkowników może nie być poprawny, ponieważ zostały odwołane lub usunięte. W takim przypadku w protokole zadania menedżera kolejek zostanie wyświetlony komunikat ICHxxxx i prawdopodobnie zostanie wyświetlony komunikat IRRxxxx zawierający przyczynę niepowodzenia wpisania się. Na przykład:

```
ICH408I USER(NOTDFND ) GROUP(        ) NAME(???                 )
  LOGON/JOB INITIATION - USER AT TERMINAL          NOT RACF-DEFINED
IRR012I  VERIFICATION FAILED. USER PROFILE NOT FOUND
```

- Zażądano innego użytkownika, ale identyfikator użytkownika zadania lub zadania nie ma dostępu do alternatywnego identyfikatora użytkownika. W przypadku tego niepowodzenia w protokole zadania odpowiedniego menedżera kolejek zostanie wyświetlony komunikat o naruszaniu.
- Opcja kontekstu została użyta lub jest domniemana przez otwarcie kolejki transmisji dla danych wyjściowych, ale identyfikator użytkownika zadania lub, w razie potrzeby, zadanie lub alternatywny identyfikator użytkownika nie mają dostępu do opcji kontekstu. W tym przypadku komunikat o naruszaniu jest umieszczany w protokole zadania odpowiedniego menedżera kolejek.
- Nieautoryzowany użytkownik podjął próbę uzyskania dostępu do zabezpieczonego obiektu menedżera kolejek, na przykład do kolejki. W tym przypadku komunikat ICH408I dla naruszenia jest umieszczany w protokole zadania odpowiedniego menedżera kolejek. To naruszenie może być spowodowane przez zadanie lub, jeśli ma to zastosowanie, z zadaniem lub alternatywnym ID użytkownika.

Komunikaty o naruszaniu bezpieczeństwa komend i zabezpieczeń zasobów komend można również znaleźć w protokole zadania menedżera kolejek.

Jeśli komunikat naruszenia ICH408I wyświetla nazwę zadania menedżera kolejek, a nie ID użytkownika, zwykle jest to wynik podania pustego alternatywnego ID użytkownika. Na przykład:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          INSUFFICIENT ACCESS AUTHORITY
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

Użytkownik może sprawdzić, kto może używać pustych alternatywnych identyfikatorów użytkowników, sprawdzając listę dostępu do profilu MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Komunikat o naruszaniu funkcji ICH408I może być również wygenerowany przez:

- Komenda przesyłana do kolejki wejściowej komend systemowych bez kontekstu. Programy napisane przez użytkownika, które zapisują do kolejki wejściowej systemu, powinny zawsze używać opcji kontekstu. Więcej informacji na ten temat zawiera “Profile zabezpieczeń kontekstu” na stronie 221.
- Gdy zadanie uzyskające dostęp do zasobu IBM MQ nie ma powiązanego identyfikatora użytkownika lub gdy adapter IBM MQ nie może wyodrębnić identyfikatora użytkownika ze środowiska adaptera.

Komunikaty o naruszaniu mogą być również wysyłane, jeśli używane są zarówno grupy współużytkowania kolejek, jak i zabezpieczenia na poziomie menedżera kolejek. Mogą zostać wyświetlone komunikaty wskazujące, że żaden profil nie został znaleziony na poziomie menedżera kolejek, ale nadal ma nadany dostęp ze względu na profil poziomu grupy współużytkowania kolejki.

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

z/OS Co zrobić, jeśli dostęp jest niedozwolony lub niedozwolony

Oprócz kroków szczegółowo określonych w *z/OS Security Server RACF -Podręcznik administratora bezpieczeństwa*należy użyć tej listy kontrolnej, jeśli dostęp do zasobu wydaje się być nieprawidłowo kontrolowany.

- Czy profile przełączników są poprawnie ustawione?
  - Czy RACF jest aktywne?
  - Czy klasy IBM MQ RACF są zainstalowane i aktywne?

    Aby to sprawdzić, należy użyć komendy RACF (SETROPTS LIST).
  - Aby wyświetlić bieżący status przełącznika z menedżera kolejek, należy użyć komendy IBM MQ DISPLAY SECURITY.
  - Sprawdź profile przełącznika w klasie MQADMIN.

    W tym celu należy użyć komend RACF , SEARCH i RLIST.
  - Ponownie sprawdź profile przełączników RACF , wydając komendę IBM MQ REFRESH SECURITY (MQADMIN).
- Czy profil zasobu RACF został zmieniony? Czy na przykład zmienił się uniwersalny dostęp do profilu lub czy lista dostępu do profilu została zmieniona?
  - Czy profil jest ogólny?

    Jeśli jest, wydaj komendę RACF , SETROPTS GENERIC (nazwa_klasy) ODŚWIEŻ.
  - Czy odświeżono zabezpieczenia w tym menedżerze kolejek?

    Jeśli jest to wymagane, wydaj komendę RACF SETROPTS RACLIST (classname) ODŚWIEŻ.

    Jeśli jest to wymagane, wydaj komendę IBM MQ REFRESH SECURITY (*).
- Czy zmieniono definicję użytkownika RACF ? Na przykład, czy użytkownik został połączony z nową grupą lub czy uprawnienie dostępu użytkownika zostało odwołane?
  - Czy ponownie zweryfikowano użytkownika, wydając komendę IBM MQ RVERIFY SECURITY (userid)?
- Czy kontrole bezpieczeństwa są pomijane ze względu na RESLEVEL?
  - Sprawdź, czy ID użytkownika nawiązanego połączenia ma dostęp do profilu RESLEVEL. Użyj rekordów kontroli RACF , aby określić, do czego ma zostać ustawiony parametr RESLEVEL.
  - W przypadku kanałów należy pamiętać, że poziom dostępu, który identyfikator użytkownika inicjatora kanału ma do RESLEVEL, jest dziedziczony przez wszystkie kanały, więc poziom dostępu, taki jak ALTER, który powoduje, że wszystkie sprawdzenia są pomijane, powoduje ominięcie kontroli zabezpieczeń dla wszystkich kanałów.
  - Jeśli program CICSjest uruchomiony, sprawdź ustawienie RESSEC transakcji.
  - Jeśli wartość RESLEVEL została zmieniona w czasie, gdy użytkownik jest połączony, muszą one rozłączyć się i ponownie nawiązać połączenie, zanim nowe ustawienie RESLEVEL zostanie zastosowane.
- Czy są używane grupy współużytkowania kolejek?
  - Jeśli używana jest zarówno grupa współużytkowania kolejek, jak i zabezpieczenia na poziomie menedżera kolejek, należy sprawdzić, czy zdefiniowano wszystkie poprawne profile. Jeśli profil menedżera kolejek nie jest zdefiniowany, do dziennika wysyłany jest komunikat informujący o tym, że nie znaleziono profilu.

- Czy użyto kombinacji ustawień przełącznika, które nie są poprawne, tak aby było włączone pełne sprawdzanie zabezpieczeń?
- Czy chcesz zdefiniować przełączniki bezpieczeństwa, aby przesłonić niektóre ustawienia grupy współużytkowania kolejek dla menedżera kolejek?
- Czy profil na poziomie menedżera kolejek ma pierwszeństwo przed profilem poziomu grupy współużytkowania kolejki?

z/OS Zagadnienia związane z zabezpieczeniami dla inicjatora kanału w systemie z/OS

Jeśli zabezpieczenia zasobów są używane w rozproszonym środowisku kolejkowania, przestrzeń adresowa inicjatora kanału musi mieć odpowiedni dostęp do różnych zasobów produktu IBM MQ . Za pomocą narzędzia Integrated Cryptographic Support Facility (ICSF) można zainicjować algorytm ochrony hasła.

Korzystanie z zabezpieczeń zasobów

Jeśli używane są zabezpieczenia zasobów, należy wziąć pod uwagę następujące kwestie, jeśli używane jest kolejkowanie rozproszone:

kolejki systemowe
The channel initiator address space needs RACF UPDATE access to the system queues listed at “Bezpieczeństwo kolejki systemowej” na stronie 210, and to all the user destination queues and the dead-letter queue (but see “Zabezpieczenia kolejki niedostarczanych komunikatów” na stronie 208).

Kolejki transmisji
Przestrzeń adresowa inicjatora kanału wymaga dostępu ALTER do wszystkich kolejek transmisji użytkownika.

zabezpieczenie kontekstu
Identyfikator użytkownika kanału (oraz ID użytkownika agenta MCA, jeśli został określony), wymaga dostępu do komponentu RACF CONTROL do profili hlq.CONTEXT.queuename w klasie MQADMIN. W zależności od profilu RESLEVEL, identyfikator użytkownika kanału może również potrzebować dostępu CONTROL do tych profili.

Wszystkie kanały muszą mieć dostęp CONTROL do obiektu MQADMIN hlq.CONTEXT. martwy-profil kolejki niewysłanych wiadomości. Wszystkie kanały (inicjujące lub udzielające odpowiedzi) mogą generować raporty, a w konsekwencji muszą mieć dostęp CONTROL do profilu hlq.CONTEXT.reply-q .

Kanały SENDER, CLUSSDR i SERVER wymagają dostępu CONTROL do profili hlq.CONTEXT.xmit-queue-name , ponieważ komunikaty mogą być umieszczane w kolejce transmisji w celu zbudzenia kanału w celu zakończenia wdzięku.

Uwaga: Jeśli ID użytkownika kanału lub grupa RACF , z którą powiązany jest identyfikator użytkownika kanału, ma dostęp CONTROL lub ALTER do pliku hlq.RESLEVEL, to nie ma żadnych sprawdzeń zasobów dla inicjatora kanału ani żadnego z jego kanałów.

Więcej informacji na ten temat zawierają “Profile zabezpieczeń kontekstu” na stronie 221 “RESLEVEL i połączenie inicjatora kanału” na stronie 242 i “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244 .

CSQINPX
Jeśli używany jest zestaw danych wejściowych CSQINPX, inicjator kanału musi również mieć dostęp z prawem do odczytu CSQINPX, a dostęp UPDATE do zestawu danych CSQOUTX i kolejek dynamicznych SYSTEM.CSQXCMD. *.

Bezpieczeństwo połączenia
Żądania połączenia z przestrzenią adresową inicjatora kanału używają typu połączenia CHIN, dla którego należy ustawić odpowiednie zabezpieczenia dostępu, patrz “Profile zabezpieczeń połączenia dla inicjatora kanału” na stronie 203.

Zestawy danych
Przestrzeń adresowa inicjatora kanału wymaga odpowiedniego dostępu do zestawów danych menedżera kolejek, patrz “Autoryzowanie dostępu do zestawów danych” na stronie 261.

Komendy
Rozproszone komendy kolejkowania (na przykład DEFINE CHANNEL, START CHINIT, START LISTENER i inne komendy kanału) muszą mieć odpowiednie ustawione zabezpieczenia komend, patrz Tabela 49 na stronie 224.

Jeśli używana jest grupa współużytkowania kolejek, inicjator kanału może wewnętrznie wydawać różne komendy, dlatego identyfikator użytkownika, którego używa, musi być autoryzowany do wydawania takich komend. Te komendy to START i STOP CHANNEL dla każdego kanału używanego z CHLDISP (SHARED).

Jeśli tryb PSMODE menedżera kolejek nie jest WYŁĄCZONY, inicjator kanału musi mieć dostęp z prawem do odczytu komendy DISPLAY PUBSUB.

Bezpieczeństwo kanału
Kanały, w szczególności dzienniki i połączenia z serwerem, wymagają skonfigurowania odpowiednich zabezpieczeń; więcej informacji na ten temat zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 244 .

Można również użyć protokołu TLS (Transport Layer Security) w celu zapewnienia bezpieczeństwa na kanałach. Więcej informacji na temat używania protokołu TLS z produktem IBM MQzawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24 .

Patrz także “Kontrola dostępu dla klientów” na stronie 99 , aby uzyskać informacje na temat zabezpieczeń połączenia z serwerem.

Identyfikatory użytkownika
Identyfikatory użytkowników opisane w produktach “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 247 i “Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania” na stronie 252 muszą mieć następujący dostęp:

- RACF UPDATE dostęp do odpowiednich kolejek docelowych i kolejki niedostarczonych komunikatów
- RACF kontrola dostępu do profilu `hlq.CONTEXT.queuename` , jeśli sprawdzanie kontekstu jest wykonywane na odbiorniku
- Odpowiedni dostęp do pliku hlq.ALTERNATE.USER.userid profile, które mogą być używane.
- W przypadku klientów odpowiedni RACF dostęp do zasobów, które mają być używane.

Bezpieczeństwo APPC
Należy ustawić odpowiednie zabezpieczenia APPC, jeśli używany jest protokół transmisji LU 6.2 . (Na przykład należy użyć klasy APPCLU RACF). Informacje na temat konfigurowania zabezpieczeń dla komunikacji APPC można znaleźć w następujących podręcznikach:

- *z/OS V1R2.0 Planowanie MVS: Zarządzanie APPC*
- Publikacja *Multiplatform APPC Configuration Guide*, publikacja IBM Redbooks

Transmisje wychodzące korzystają z opcji APPC "SECURITY (SAME)" . Oznacza to, że identyfikator użytkownika przestrzeni adresowej inicjatora kanału i jego profil domyślny (RACF GROUP) są przepływowane przez sieć do odbiornika ze wskaźnikiem, który został już zweryfikowany (ALREADYV).

Jeśli stroną odbierającą jest również z/OS, identyfikator i profil użytkownika są weryfikowane przez APPC, a identyfikator użytkownika jest prezentowany w kanale odbiorczym i używany jako identyfikator użytkownika kanału.

W środowisku, w którym menedżer kolejek używa APPC do komunikowania się z innym menedżerem kolejek w tym samym lub innym systemie z/OS , należy upewnić się, że:

- Definicja VTAM dla komunikacji LU określa SETACPT (ALREADYV)
- Istnieje profil APPCLU produktu RACF dla połączenia między jednostkami logicznymi, które określa parametr CONVSEC (ALREADYV).

zmiana ustawień zabezpieczeń
Jeśli poziom dostępu RACF , który albo identyfikator użytkownika kanału lub identyfikator użytkownika agenta MCA ma do kolejki docelowej, zostanie zmieniony, to zmiana ta obowiązuje tylko dla nowych uchwytów obiektów (czyli nowych MQOPEN) dla kolejki docelowej. Czasy, gdy kolejki otwarte i zamknięte są zmienne; jeśli kanał jest już uruchomiony podczas dokonywania takiej zmiany dostępu, agent MCA może kontynuować umieszczanie komunikatów w kolejce docelowej przy użyciu istniejącego dostępu zabezpieczeń identyfikatorów użytkowników, a nie zaktualizowanego dostępu do zabezpieczeń. Zatrzymywanie i restartowanie kanałów w celu wymuszenia zaktualizowanego poziomu dostępu pozwala uniknąć tego scenariusza.

automatyczne restartowanie
Jeśli do restartowania inicjatora kanału jest używany program z/OS Automatic Restart Manager (ARM), to ID użytkownika powiązany z przestrzenią adresową XCFAS musi być autoryzowany do wydania komendy IBM MQ START CHINIT.

Korzystanie z narzędzia Integrated Cryptographic Service Facility (ICSF)

Inicjator kanału może użyć funkcji ICSF w celu wygenerowania liczby losowej podczas inicjowania algorytmu ochrony hasła w celu zacieślenia haseł przepływających przez kanały klienta, jeśli protokół TLS nie jest używany. Proces generowania liczby losowej nosi nazwę *entropia*.

Jeśli zainstalowano składnik z/OS , ale nie uruchomiono ICSF, zostanie wyświetlony komunikat CSQX213E , a inicjator kanału używa STCK dla entropii.

Komunikat CSQX213E ostrzega, że algorytm ochrony hasła nie jest tak bezpieczny, jak może być. Można jednak kontynuować proces; nie ma innego wpływu na środowisko wykonawcze.

Jeśli opcja z/OS nie jest zainstalowana, inicjator kanału automatycznie użyje STCK.

Uwagi:

1. Użycie ICSF dla entropii generuje bardziej losowe sekwencje niż przy użyciu STCK.
2. Jeśli uruchamiasz ICSF, musisz zrestartować inicjator kanału.
3. ICSF jest wymagane w przypadku niektórych specyfikacji CipherSpecs. Jeśli zostanie podjęta próba użycia jednej z tych specyfikacji CipherSpecs i nie zainstalowano ICSF, zostanie wyświetlony komunikat CSQX629E.

z/OS Zabezpieczenia w klastrach menedżerów kolejek w systemie z/OS

Uwagi dotyczące zabezpieczeń dla klastrów są takie same dla menedżerów kolejek i kanałów, które nie są zgrupowane. Inicjator kanału musi mieć dostęp do dodatkowych kolejek systemowych, a niektóre dodatkowe komendy wymagają odpowiedniego zestawu bezpieczeństwa.

Do uwierzytelniania kanałów klastra (tak jak w przypadku konwencjonalnych kanałów) można używać identyfikatora użytkownika MCA, rekordów uwierzytelniania kanału, protokołu TLS i wyjść zabezpieczeń. Rekordy uwierzytelniania kanału lub wyjście zabezpieczeń odnoszące się do kanału odbierającego klastry muszą sprawdzić, czy zdalny menedżer kolejek ma dostęp do kolejek klastra menedżera kolejek serwera. Obsługa klastrów produktu IBM MQ może być używana bez zmiany istniejących zabezpieczeń dostępu do kolejki. Należy jednak zezwolić innym menedżerom kolejek w klastrze na zapis w systemie SYSTEM.CLUSTER.COMMAND.QUEUE , jeśli mają one zostać przyłączone do klastra.

Obsługa klastrów w systemie IBM MQ nie udostępnia mechanizmu ograniczający tylko element klastra do roli klienta. W związku z tym należy upewnić się, że wszystkie menedżery kolejek, które zostały dozwolone w klastrze, są zaufane. Jeśli dowolny menedżer kolejek w klastrze tworzy kolejkę o określonej nazwie, może odbierać komunikaty dla tej kolejki, niezależnie od tego, czy aplikacja umieszczała komunikaty w tej kolejce, czy nie.

Aby ograniczyć przypisanie do klastra, należy wykonać to samo działanie, aby zapobiec łączeniu menedżerów kolejek z kanałami odbiorcze. Przynależność do klastra można ograniczyć, używając rekordów uwierzytelniania kanału lub pisząc program obsługi wyjścia zabezpieczeń na kanale odbiorczym. Można również napisać program obsługi wyjścia, aby uniemożliwić osobom nieautoryzowanym menedżerom kolejek zapisywanie w systemie SYSTEM.CLUSTER.COMMAND.QUEUE.

Uwaga: Nie zaleca się zezwalania aplikacjom na otwieranie systemu SYSTEM.CLUSTER.TRANSMIT.QUEUE bezpośrednio. Nie zaleca się również zezwalania aplikacji na otwarcie innej kolejki transmisji bezpośrednio.

Jeśli używane są zabezpieczenia zasobów, oprócz uwag dotyczących produktu "Zagadnienia związane z zabezpieczeniami dla inicjatora kanału w systemie z/OS" na stronie 269należy wziąć pod uwagę następujące kwestie:

kolejki systemowe
Inicjator kanału wymaga dostępu RACF ALTER do następujących kolejek systemowych:

- SYSTEM.CLUSTER.COMMAND
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

i UPDATE, aby uzyskać dostęp do SYSTEM.CLUSTER.REPOSITORY.QUEUE

Musi również mieć dostęp z prawem do odczytu do wszystkich list nazw używanych do łączenia w klastry.

Komendy
Ustaw odpowiednie zabezpieczenia komend (zgodnie z opisem w sekcji Tabela 49 na stronie 224) dla komend obsługi klastra (REFRESH i RESET CLUSTER, SUSPEND i RESUME QMGR).

z/OS Uwagi dotyczące zabezpieczeń dotyczące używania produktu IBM MQ z produktem CICS

Wszystkie wersje produktu CICS obsługiwane przez produkt IBM MQ 9.0.0i nowsze wersje korzystają z dostarczonej wersji adaptera i mostu w wersji CICS .

Szczegółowe informacje na temat zabezpieczeń można znaleźć w sekcji:

- Zabezpieczenia dla adaptera CICS-IBM MQ.
- Zabezpieczenia mostu CICS-IBM MQ.

z/OS Uwagi dotyczące zabezpieczeń dotyczące używania produktu IBM MQ z produktem IMS

W tej sekcji opisano sposób planowania wymagań dotyczących bezpieczeństwa podczas używania produktu IBM MQ z produktem IMS.

Korzystanie z klasy OPERCMDS

Jeśli produkt RACF jest używany do ochrony zasobów w klasie OPERCMDS, należy się upewnić, że identyfikator użytkownika powiązany z przestrzenią adresową menedżera kolejek produktu IBM MQ ma uprawnienia do wydawania komendy MODIFY do dowolnego systemu IMS , z którym może się on łączyć.

Uwagi dotyczące zabezpieczeń mostu IMS

Podczas określania wymagań dotyczących zabezpieczeń dla mostu IMS należy wziąć pod uwagę cztery aspekty:

- Jakie uprawnienia zabezpieczeń są wymagane do połączenia produktu IBM MQ z produktem IMS
- Ilość sprawdzanych zabezpieczeń dla aplikacji korzystających z mostu w celu uzyskania dostępu do produktu IMS
- Które zasoby produktu IMS mogą być używane przez te aplikacje
- Jakie uprawnienia ma być używane w przypadku komunikatów umieszczonych i odebranych przez most

Podczas definiowania wymagań dotyczących zabezpieczeń dla mostu IMS należy wziąć pod uwagę następujące kwestie:

- Komunikaty przechodzących przez most mogły pochodzić z aplikacji na platformach, które nie oferują silnych zabezpieczeń.
- Komunikaty przechodzących przez most mogły pochodzić z aplikacji, które nie są kontrolowane przez to samo przedsiębiorstwo lub organizację.

z/OS *Uwagi dotyczące zabezpieczeń dotyczące nawiązywania połączenia z produktem IMS*

Nadaj identyfikatorowi użytkownika dostęp do przestrzeni adresowej menedżera kolejek produktu IBM MQ do grupy OTMA.

Most IMS jest klientem OTMA. Połączenie z serwerem IMS działa pod ID użytkownika w przestrzeni adresowej menedżera kolejek produktu IBM MQ . Jest on zwykle zdefiniowany jako członek uruchomionej grupy zadań. Ten identyfikator użytkownika musi mieć nadany dostęp do grupy OTMA (chyba, że ustawienie /SECURE OTMA nie ma wartości NONE).

Aby to zrobić, należy zdefiniować następujący profil w klasie FACILITY:

```
IMSXCF.xcfgname.mqxcfmname
```

Gdzie `xcfgname` to nazwa grupy XCF, a `mqxcfmname` to nazwa elementu XCF IBM MQ.

Należy nadać temu profilowi uprawnienia do odczytu identyfikatora użytkownika menedżera kolejek produktu IBM MQ .

Uwaga:

1. Jeśli uprawnienia zostaną zmienione w klasie FACILITY, należy wydać komendę RACF SETROPTS RACLIST (FACILITY) REFRESH w celu aktywowania zmian.
2. Jeśli profil hlq.NO.SUBSYS.SECURITY istnieje w klasie MQADMIN, żaden identyfikator użytkownika nie jest przekazywany do produktu IMS , a połączenie nie powiedzie się, chyba że ustawienie /SECURE OTMA nie ma wartości NONE.

z/OS *Kontrola dostępu do aplikacji dla mostu IMS*

Zdefiniuj profil RACF w klasie FACILITY dla każdego systemu IMS . Nadaj odpowiedni poziom dostępu do identyfikatora użytkownika menedżera kolejek produktu IBM MQ .

Dla każdego systemu IMS , z którym łączy się most IMS , można zdefiniować następujący profil RACF w klasie FACILITY, aby określić, ile jest wykonywane sprawdzanie zabezpieczeń dla każdego komunikatu przekazanego do systemu IMS .

```
IMSXCF.xcfgname.imsxcfmname
```

Gdzie `xcfgname` to nazwa grupy XCF, a `imsxcfmname` to nazwa elementu XCF dla IMS. (Należy zdefiniować osobny profil dla każdego systemu IMS).

Poziom dostępu dla identyfikatora użytkownika menedżera kolejek produktu IBM MQ w tym profilu jest zwracany do programu IBM MQ , gdy most IMS łączy się z serwerem IMSi wskazuje poziom zabezpieczeń wymagany dla kolejnych transakcji. W przypadku kolejnych transakcji produkt IBM MQ żąda odpowiednich usług z produktu RACF , a w przypadku gdy identyfikator użytkownika jest autoryzowany, przekazuje komunikat do produktu IMS.

OTMA nie obsługuje komendy IMS /SIGN; jednak program IBM MQ umożliwia ustawienie sprawdzania dostępu dla każdego komunikatu w celu umożliwienia implementacji niezbędnego poziomu kontroli.

Mogą zostać zwrócone następujące informacje o poziomie dostępu:

BRAK lub NIE ZNALEZIONO PROFILU

Te wartości wskazują, że wymagane jest maksymalne bezpieczeństwo, czyli uwierzytelnianie jest wymagane dla każdej transakcji. Należy sprawdzić, czy identyfikator użytkownika określony w polu *UserIdentifier* struktury MQMD, a także hasło lub PassTicket w polu *Authenticator* struktury MQIIH są znane RACFi są poprawną kombinacją. Element UTOKEN jest tworzony z hasłem lub PassTicketi przekazywany do produktu IMS ; Element UTOKEN nie jest buforowany.

Uwaga: Jeśli profil hlq.NO.SUBSYS.SECURITY istnieje w klasie MQADMIN, ten poziom zabezpieczeń nadpisuje wszystkie zdefiniowane w profilu.

READ

Ta wartość wskazuje, że takie samo uwierzytelnianie ma być wykonywane, jak dla parametru `NONE` , w następujących okolicznościach:

- Pierwszy raz, gdy napotkano konkretny identyfikator użytkownika
- Gdy identyfikator użytkownika został napotkany, ale buforowany element UTOKEN nie został utworzony przy użyciu hasła lub opcji PassTicket

Produkt IBM MQ żąda wartości UTOKEN, jeśli jest to wymagane, i przekazuje go do produktu IMS.

Uwaga: Jeśli żądanie ponownego zweryfikowania zabezpieczeń zostało wykonane, wszystkie informacje w pamięci podręcznej są tracone, a znacznik UTOKEN jest wymagany przy pierwszym napotkaniu każdego identyfikatora użytkownika.

UPDATE

Upewnij się, że identyfikator użytkownika w polu *UserIdentifier* struktury MQMD jest znany w produkcie RACF.

Obiekt UTOKEN został zbudowany i przekazany do produktu IMS . Element UTOKEN jest buforowany.

CONTROL/ALTER

Te wartości wskazują, że dla identyfikatorów użytkowników dla tego systemu IMS nie ma potrzeby podawania żadnych zabezpieczeń UTOKENs. (Ta opcja jest prawdopodobnie używana tylko w przypadku systemów programistycznych i testowych).

Ostrzeżenie: Należy pamiętać, że identyfikator użytkownika zawarty w polu *UserIdentifier* struktury MQMD jest nadal przekazywany do produktu **CONTROL/ALTER**.

Uwaga:

1. Ten dostęp jest definiowany, gdy program IBM MQ łączy się z serwerem IMSi trwa przez czas trwania połączenia. Aby zmienić poziom zabezpieczeń, należy zmienić dostęp do profilu zabezpieczeń, a następnie zatrzymać i restartować most (na przykład zatrzymując i restartując OTMA).
2. Jeśli uprawnienia zostaną zmienione w klasie FACILITY, należy wydać komendę RACF SETROPTS RACLIST (FACILITY) REFRESH w celu aktywowania zmian.
3. Możliwe jest użycie hasła lub PassTicket, ale należy pamiętać, że most IMS nie szyfruje danych. Więcej informacji na temat korzystania z opcji PassTicketszawiera sekcja “Korzystanie z opcji RACF PassTickets w nagłówku IMS” na stronie 276.
4. Niektóre z tych wyników mogą mieć wpływ na ustawienia zabezpieczeń w programie IMSprzy użyciu komendy /SECURE OTMA.
5. Informacje przechowywane w pamięci podręcznej UTOKEN są przechowywane przez czas trwania zdefiniowany przez parametry INTERVAL i TIMEOUT komendy IBM MQ ALTER SECURITY.
6. Opcja RACF OSTRZEŻENIE nie ma wpływu na profil IMSXCF.xcfgname.imsxcfmname . Jego użycie nie ma wpływu na poziom dostępu i nie są generowane żadne komunikaty ostrzegawcze serwera RACF .

z/OS *Sprawdzanie zabezpieczeń w systemie IMS*

Komunikaty, które przechodzą przez most, zawierają informacje o zabezpieczeniach. Sprawdzenia zabezpieczeń zależą od ustawienia komendy IMS /SECURE OTMA.

Każdy komunikat IBM MQ , który przechodzi przez most, zawiera następujące informacje o zabezpieczeniach:

- Identyfikator użytkownika zawarty w polu *UserIdentifier* w strukturze MQMD.
- Zasięg zabezpieczeń zawarty w polu *SecurityScope* w strukturze MQIIH (jeśli struktura MQIIH jest obecna)
- UTOKEN (chyba, że podsystem IBM MQ ma dostęp CONTROL lub ALTER do odpowiedniego profilu `IMSXCF.xcfgname.imsxcfmname`)

Sprawdzenia zabezpieczeń zależą od ustawienia komendy IMS /SECURE OTMA, w następujący sposób:

/SECURE OTMA NONE
Dla transakcji nie są wykonywane żadne sprawdzenia zabezpieczeń.

/BEZPIECZNA KONTROLA OTMA
Pole *UserIdentifier* struktury MQMD jest przekazywane do IMS w celu sprawdzenia uprawnień transakcji lub komend.

Element ACEE (Accessor Environment Element) jest budowany w regionie sterującym IMS .

/BEZPIECZNA OTMA PEŁNA
Pole *UserIdentifier* struktury MQMD jest przekazywane do IMS w celu sprawdzenia uprawnień transakcji lub komend.

Produkt ACEE jest budowany w regionie zależnym od produktu IMS , a także w regionie sterującym IMS .

/BEZPIECZNY PROFIL OTMA
Pole *UserIdentifier* struktury MQMD jest przekazywane do produktu IMS na potrzeby sprawdzania uprawnień do transakcji lub komend.

Pole *SecurityScope* w strukturze MQIIH jest używane do określenia, czy ma być kompilowana ACEE w zależnym regionie IMS , jak również w regionie sterującym.

Uwaga:

1. Jeśli użytkownik zmieni uprawnienia w klasie TIMS lub CIMS lub powiązanych klasach grupy GIMS lub DIMS, należy wydać następujące komendy IMS w celu aktywacji zmian:
   - /MODIFY PREPARE RACF
   - /MODIFY COMMIT
2. Jeśli nie jest używany /SECURE OTMA PROFILE, każda wartość określona w polu *SecurityScope* struktury MQIIH jest ignorowana.

z/OS *Sprawdzanie zabezpieczeń wykonywane przez most IMS*

W zależności od wykonywanego działania używane są różne uprawnienia.

Gdy most umieszcza lub pobiera komunikat, używane są następujące uprawnienia:

Pobieranie komunikatu z kolejki mostu
Nie są wykonywane żadne sprawdzenia zabezpieczeń.

Umieszczanie wyjątku lub komunikatu raportu COA
Korzysta z uprawnień identyfikatora użytkownika w polu *UserIdentifier* struktury MQMD.

Umieszczanie komunikatu odpowiedzi
Korzysta z uprawnień identyfikatora użytkownika w polu *UserIdentifier* struktury MQMD oryginalnego komunikatu.

Umieszczanie komunikatu w kolejce niedostarczonych komunikatów
Nie są wykonywane żadne sprawdzenia zabezpieczeń.

Uwaga:

1. Jeśli profile klas produktu IBM MQ zostaną zmienione, należy wprowadzić komendę IBM MQ REFRESH SECURITY (*), aby aktywować zmiany.
2. Jeśli użytkownik zmieni uprawnienia użytkownika, należy wydać komendę MQSC RVERIFY SECURITY, aby aktywować zmianę.

z/OS *Korzystanie z opcji RACF PassTickets w nagłówku IMS*

Istnieje możliwość użycia PassTicket w miejsce hasła w nagłówku IMS .

Aby użyć parametru PassTicket zamiast hasła w nagłówku IMS (MQIIH), należy określić nazwę aplikacji, dla której jest sprawdzana poprawność PassTicket w atrybucie PASSTKTA definicji STGCLASS kolejki mostu IMS , do której komunikat ma być kierowany.

Jeśli wartość PASSTKTA pozostanie pusta, należy ją utworzyć, aby została wygenerowana PassTicket . Nazwa aplikacji w tym przypadku musi mieć postać MVSxxxx, gdzie xxxx jest identyfikatorem SMFID systemu z/OS , na którym jest uruchomiony docelowy menedżer kolejek.

Obiekt PassTicket jest tworzony na podstawie identyfikatora użytkownika, docelowej nazwy aplikacji i klucza tajnego. Jest to 8-bajtowa wartość zawierająca wielkie litery i cyfry. Może być używany tylko raz i jest ważny przez 20 minut. Jeśli PassTicket jest generowany przez lokalny system RACF , program RACF sprawdza tylko, czy profil istnieje, a nie czy użytkownik ma uprawnienia do profilu. Jeśli parametr PassTicket został wygenerowany w systemie zdalnym, program RACF sprawdza poprawność dostępu identyfikatora użytkownika do profilu. Pełne informacje na temat PassTicketszawiera publikacja *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

PassTickets w nagłówkach IMS są nadawane RACF przez IBM MQ, a nie IMS.

z/OS z/OS Migrowanie menedżera kolejek do mieszanego zabezpieczenia elementu pracy

Aby przeprowadzić migrację menedżera kolejek z zabezpieczeniami mieszanymi, należy wykonać następujące kroki. Użytkownik dokonuje przeglądu poziomu produktu zabezpieczeń, który jest używany, i aktywuje nowe zewnętrzne klasy monitora zabezpieczeń produktu IBM MQ . Uruchom komendę **REFRESH SECURITY** , aby aktywować profile mieszanych spraw.

Zanim rozpoczniesz

1. Upewnij się, że wszystkie zewnętrzne klasy monitora zabezpieczeń produktu IBM MQ są aktywowane.
2. Upewnij się, że menedżer kolejek jest uruchomiony.

O tym zadaniu

Wykonaj poniższe kroki, aby przekształcić menedżer kolejek w zabezpieczenia mieszanego elementu pracy.

Procedura

1. Skopiuj wszystkie istniejące profile i poziomy dostępu z wielkich klas do równoważnej klasy monitora zabezpieczeń zewnętrznych przypadku mieszanego.
   a) `MQADMIN` do `MXADMIN`.
   b) `MQPROC` do `MXPROC`.
   c) `MQNLIST` do `MXNLIST`.
   d) `MQQUEUE` do `MXQUEUE`.
2. Zmień wartość atrybutu `SCYCASE` na `MIXED`.

```
ALTER QMGR SCYCASE(MIXED)
```

3. Aktywuj istniejące profile zabezpieczeń.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. Sprawdź, czy profile zabezpieczeń działają poprawnie.

Co dalej

Przejrzyj definicje obiektów i utwórz nowe, odpowiednio, mieszane profile spraw, używając programu **REFRESH SECURITY** zgodnie z wymaganiami w celu aktywowania profili.

Konfigurowanie zabezpieczeń produktu IBM MQ MQI client

Należy wziąć pod uwagę bezpieczeństwo systemu IBM MQ MQI client , 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 produkcie IBM MQ 8.0uwierzytelnianie jest udostępniane przez jedną z dwóch opcji:

  – Funkcja uwierzytelniania połączenia.

    Więcej informacji na temat uwierzytelniania połączenia zawiera sekcja “Uwierzytelnianie połączenia” na stronie 68.

  – Korzystanie z uwierzytelniania wzajemnego w ramach protokołu TLS.

    Więcej informacji na temat protokołu TLS można znaleźć w sekcji “Praca z protokołem SSL/TLS” na stronie 282.

- 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 361.

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 klienta na identyfikator użytkownika MCAUSER” na stronie 400.

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 50.

Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.

Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

Aby zapewnić zgodność ze standardem FIPS w czasie wykonywania, repozytoria kluczy muszą być utworzone i zarządzane tylko przy użyciu oprogramowania zgodnego ze standardem FIPS, takiego jak runmqakm z opcją -fips.

Można określić, że kanał TLS musi używać tylko CipherSpecs z certyfikatem FIPS na trzy sposoby, wymienione w kolejności wykonywania operacji:

1. W polu FipsRequired w strukturze MQSCO ustaw wartość MQSSL_FIPS_YES.
2. Ustaw zmienną środowiskową MQSSLFIPS na wartość YES.
3. Ustaw atrybut SSLFipsRequired w pliku konfiguracyjnym klienta na wartość YES.

Domyślnie specyfikacje szyfrowania CipherSpecs z certyfikatem FIPS nie są wymagane.

Wartości te mają takie samo znaczenie jak równoważne wartości parametrów w komendzie ALTER QMGR SSLFIPS (patrz ALTER QMGR). Jeśli proces klienta nie ma obecnie aktywnych połączeń TLS, a wartość FipsRequired jest poprawnie określona dla MQCONNX SSL, wszystkie kolejne połączenia TLS powiązane z tym procesem muszą używać tylko CipherSpecs powiązanych z tą wartością. Ma to zastosowanie do momentu zatrzymania tego i wszystkich innych połączeń TLS. Na tym etapie kolejna operacja MQCONNX może udostępnić nową wartość dla atrybutu FipsRequired.

Jeśli sprzęt szyfrujący jest obecny, moduły szyfrujące używane przez produkt IBM MQ można skonfigurować w taki sposób, aby były modułami udostępnianymi przez produkt sprzętowy. Moduły te mogą mieć certyfikat FIPS na określonym poziomie. Konfigurowalne moduły i to, czy mają certyfikat FIPS, zależy od używanego produktu sprzętowego.

Tam, gdzie jest to możliwe, jeśli skonfigurowano CipherSpecs tylko dla FIPS, klient MQI odrzuca połączenia, które określają specyfikację szyfrowania CipherSpec z opcją MQRC_SSL_INITIALIZATION_ERROR. IBM MQ nie gwarantuje odrzucenia wszystkich takich połączeń i jest odpowiedzialny za określenie, czy konfiguracja IBM MQ jest zgodna ze standardami FIPS.

Pojęcia pokrewne

“Standardy FIPS (Federal Information Processing Standards) dla UNIX, Linux, and Windows” na stronie 33

Jeśli szyfrowanie jest wymagane w kanale SSL/TLS w systemach Windowsi UNIX and Linux , IBM MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach Windowsi UNIX and Linux oprogramowanie ICC przeszło program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program) amerykańskiego National Institute of Standards and Technology na poziomie 140-2.

Sekcja SSL pliku konfiguracyjnego klienta

Odsyłacze pokrewne

FipsRequired (MQLONG)

MQSSLFIPS

AIX Uruchamianie aplikacji klienckich TLS z wieloma instalacjami pakietu GSKit V8.0 w systemie AIX

Aplikacje klienckie TLS na serwerze AIX mogą doświadczyć MQRC_CHANNEL_CONFIG_ERROR i błędów AMQ6175 podczas pracy w systemach AIX z wieloma instalacjami GSKit w wersji V8.0 .

Podczas uruchamiania aplikacji klienckich w systemie AIX z wieloma instalacjami pakietu GSKit V8.0 wywołania połączenia klienta mogą zwracać MQRC_CHANNEL_CONFIG_ERROR podczas korzystania z protokołu 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 MQ załadował mieszany zestaw bibliotek z dwóch różnych instalacji pakietu GSKit V8.0 . Ten błąd może być przyczyną wykonania aplikacji klienckiej IBM MQ w środowisku Db2 .

Aby uniknąć tego błędu, należy dołączyć katalogi bibliotek produktu IBM MQ z przodu ścieżki do biblioteki, aby mieć pierwszeństwo przed bibliotekami produktu IBM 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** zawiera sekcja setmqenv (set IBM MQ environment) .

IBM i Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie IBM i

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 niektórych systemach operacyjnych można wykonać testy z samopodpisanymi certyfikatami. Jednak w systemie IBM ikonieczne jest użycie certyfikatów osobistych podpisanych przez lokalny ośrodek CA.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL/TLS w systemie IBM i” na stronie 282.

W tej kolekcji tematów przedstawiono niektóre zadania związane z konfigurowaniem komunikacji SSL lub TLS oraz zawierają wskazówki dotyczące wykonywania tych zadań.

Użytkownik może również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalnymi częściami protokołów SSL i TLS. Podczas uzgadniania protokołu SSL lub TLS klient SSL lub TLS zawsze pobiera i sprawdza poprawność certyfikatu cyfrowego z serwera. W przypadku implementacji IBM MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemie IBM iklient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie IBM MQ :

- W przypadku menedżera kolejek `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek, została zmieniona na małe litery. Na przykład: `QM1`, `ibmwebspheremqqm1`.
- W przypadku klienta IBM MQ C dla produktu IBM i `ibmwebspheremq` , po którym następuje zmiana ID użytkownika logowania na małe litery, na przykład `ibmwebspheremqmyuserid`.

Produkt IBM 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 SSL lub TLS 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 ten temat zawiera sekcja Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS.

ULW Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemach UNIX, Linux lub 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.

Ostrzeżenie: Nie jest możliwe użycie kombinacji certyfikatów podpisanych z krzywą eliptyczną i certyfikatów podpisanych przez RSA w menedżerach kolejek, które mają być połączone za pomocą kanałów obsługujących protokół TLS.

Menedżery kolejek używające kanałów z włączoną obsługą protokołu TLS muszą używać certyfikatów podpisanych przez RSA lub wszystkich certyfikatów podpisanych przez EC, a nie mieszaniną obu tych certyfikatów.

Więcej informacji zawiera sekcja “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45.

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/TLS w systemie UNIX, Linux, and Windows” na stronie 294.

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 MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemie UNIX, Linux, and Windowsklient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie IBM 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 MQ `ibmwebspheremq` , po którym następuje zmiana identyfikatora użytkownika na małe litery, na przykład `ibmwebspheremqmyuserid`.

Produkt IBM 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.

z/OS Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie z/OS

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 systemie z/OS można wykonywać testy z samopodpisanymi certyfikatami lub certyfikatami osobistymi podpisanymi przez lokalny ośrodek certyfikacji (CA).

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/TLS w systemie z/OS” na stronie 327.

W tej kolekcji tematów przedstawiono niektóre zadania związane z konfigurowaniem komunikacji SSL lub TLS, a także szczegółowe wskazówki dotyczące 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 MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemie z/OS klient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma jeden z następujących certyfikatów:

- Tylko w przypadku współużytkowanego kanału-certyfikat z etykietą w formacie `ibmWebSphereMQ` , po którym następuje nazwa grupy współużytkowania kolejek, na przykład `ibmWebSphereMQQSG1`
- Certyfikat z etykietą w formacie`ibmWebSphereMQ` , po którym następuje nazwa menedżera kolejek, na przykład `ibmWebSphereMQQM1`
- Certyfikat domyślny (który może być certyfikatem `ibmWebSphereMQ`).

Jeśli kanał jest współużytkowany, kanał najpierw próbuje znaleźć certyfikat dla grupy współużytkowania kolejek. Jeśli nie znajdzie certyfikatu dla grupy współużytkowania kolejki, próbuje znaleźć certyfikat dla menedżera kolejek.

W systemie z/OSprodukt IBM MQ używa przedrostka `ibmWebSphereMQ` na etykiecie, aby uniknąć nieporozumień z certyfikatami dla innych produktów.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli taki certyfikat jest wysyłany. Jeśli klient SSL lub TLS 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 ten temat zawiera sekcja Łączenie dwóch menedżerów kolejek za pomocą protokołu SSL lub TLS.

Praca z protokołem SSL/TLS

W tych tematach znajdują się instrukcje dotyczące wykonywania pojedynczych zadań związanych z używaniem protokołu TLS z produktem IBM MQ.

Wiele z nich jest używanych jako kroki w zadaniach wyższego poziomu opisanych w następujących sekcjach:

- “Identyfikowanie i uwierzytelnianie użytkowników” na stronie 340
- “Autoryzowanie dostępu do obiektów” na stronie 361
- “Poufność komunikatów” na stronie 432
- “Integralność danych komunikatów” na stronie 472
- “Zabezpieczanie klastrów” na stronie 473

IBM i Praca z protokołem SSL/TLS w systemie IBM i

Ta kolekcja tematów zawiera instrukcje dotyczące poszczególnych zadań pracujących z protokołem TLS (Transport Layer Security) w produkcie IBM MQ for IBM i.

W przypadku systemu operacyjnego IBM i obsługa protokołu TLS jest integralna dla systemu operacyjnego. Upewnij się, że zostały zainstalowane wymagania wstępne wymienione w sekcji Wymagania sprzętowe i programowe produktu IBM i.

W systemie IBM imożna zarządzać kluczami i certyfikatami cyfrowymi za pomocą narzędzia Digital Certificate Manager (DCM).

Dostęp do DCM

Aby uzyskać dostęp do interfejsu programu DCM, należy wykonać poniższe instrukcje.

O tym zadaniu

Wykonaj następujące kroki w przeglądarce WWW, która obsługuje ramki.

Procedura

1. Przejdź do katalogu `http://machine.domain:2001` lub `https://machine.domain:2010`, gdzie *komputer* jest nazwą komputera.
2. Wpisz poprawny profil użytkownika i hasło podczas żądania.

   Upewnij się, że profil użytkownika ma uprawnienia specjalne *ALLOBJ i *SECADM, aby umożliwić tworzenie nowych baz certyfikatów. Jeśli użytkownik nie ma uprawnień specjalnych, może zarządzać tylko certyfikatami osobistymi lub wyświetlać podpisy obiektów dla obiektów, do których użytkownik jest uprawniony. Jeśli użytkownik ma uprawnienia do korzystania z aplikacji podpisującej obiekty, może również podpisywać obiekty z programu DCM.
3. Na stronie Konfiguracje internetowe kliknij opcję **Cyfrowy Certificate Manager**.

   Zostanie wyświetlona strona Digital Certificate Manager (Menedżer certyfikatów).

Przypisywanie certyfikatu do menedżera kolejek w systemie IBM i

Użyj programu DCM, aby przypisać certyfikat do menedżera kolejek.

Aby przypisać certyfikat do menedżera kolejek, należy użyć tradycyjnego zarządzania certyfikatami cyfrowymi produktu IBM i . Oznacza to, że można określić, że menedżer kolejek korzysta ze składnicy certyfikatów systemu i że menedżer kolejek jest zarejestrowany do użycia jako aplikacja z programem

Digital Certificate Manager. Aby to zrobić, zmień wartość atrybutu **SSLKEYR** menedżera kolejek na *SYSTEM.

Gdy parametr **SSLKEYR** zostanie zmieniony na *SYSTEM, program IBM MQ zarejestruje menedżera kolejek jako aplikację serwera z unikalną etykietą aplikacji QIBM_WEBSPHERE_MQ_QMGRNAME i etykietą z opisem Qmgrname (WMQ). Należy zauważyć, że atrybuty kanału **CERTLABL** nie są używane, jeśli używana jest baza certyfikatów *SYSTEM. Następnie menedżer kolejek jest wyświetlany jako aplikacja serwera w programie Digital Certificate Manager, a użytkownik może przypisać do tej aplikacji dowolny certyfikat serwera lub klienta w składnicy systemu.

Ponieważ menedżer kolejek jest rejestrowany jako aplikacja, można wykonać zaawansowane funkcje programu DCM, takie jak definiowanie list zaufanych ośrodków CA.

Jeśli parametr **SSLKEYR** zostanie zmieniony na wartość inną niż *SYSTEM, program IBM MQ wyrejestrowuje menedżer kolejek jako aplikację z programem Digital Certificate Manager. Jeśli usuwany jest menedżer kolejek, jest on również wyrejestrowany z programu DCM. Użytkownik z odpowiednim uprawnieniem *SECADM może także ręcznie dodawać lub usuwać aplikacje z programu DCM.

Konfigurowanie repozytorium kluczy w systemie IBM i

Repozytorium kluczy musi być skonfigurowane na obu końcach połączenia. Domyślne bazy certyfikatów mogą być używane lub można utworzyć własne.

Połączenie TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek i produkt IBM MQ MQI client muszą mieć dostęp do repozytorium kluczy. Aby uzyskać dostęp do repozytorium kluczy przy użyciu nazwy pliku i hasła (to znaczy, że nie jest używana opcja *SYSTEM), należy upewnić się, że profil użytkownika QMQM ma następujące uprawnienia:

- Uprawnienie do wykonywania dla katalogu zawierającego repozytorium kluczy
- Uprawnienie do odczytu dla pliku zawierającego repozytorium kluczy

Więcej informacji zawiera sekcja “Repozytorium kluczy SSL/TLS” na stronie 25. Należy zauważyć, że atrybuty kanału **CERTLABL** nie są używane, jeśli używana jest baza certyfikatów *SYSTEM.

W systemie IBM icertyfikaty cyfrowe są przechowywane w bazie certyfikatów, która jest zarządzana za pomocą programu DCM. Te certyfikaty cyfrowe mają etykiety, które wiążą certyfikat z menedżerem kolejek lub z produktem IBM MQ MQI client. Protokół TLS korzysta z certyfikatów do celów uwierzytelniania.

Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem logowania użytkownika produktu IBM MQ MQI client (małymi literami). Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Nazwa menedżera kolejek lub bazy certyfikatów produktu IBM MQ MQI client zawiera ścieżkę i nazwę macierzystą. Domyślna ścieżka to `/QIBM/UserData/ICSS/Cert/Server/` , a domyślna nazwa rdzenia to `Default`. W systemie IBM idomyślna baza certyfikatów `/QIBM/UserData/ICSS/Cert/Server/Default.kdb`jest znana również pod nazwą *SYSTEM. Opcjonalnie można zdefiniować własną ścieżkę i nazwę macierzystą.

Jeśli zdefiniujesz własną ścieżkę lub nazwę pliku, ustaw uprawnienia do tego pliku, aby ściśle kontrolować dostęp do niego.

“Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie IBM i” na stronie 285 zawiera informacje na temat określania nazwy bazy certyfikatów. Nazwę bazy certyfikatów można określić przed utworzeniem bazy certyfikatów lub po jej utworzeniu.

Uwaga: Operacje, które można wykonać za pomocą programu DCM, mogą być ograniczone przez uprawnienia profilu użytkownika. Na przykład, wymagane są uprawnienia *ALLOBJ i *SECADM, aby utworzyć certyfikat ośrodka CA.

Tworzenie bazy certyfikatów w systemie IBM i

Jeśli nie chcesz używać domyślnej bazy certyfikatów, wykonaj tę procedurę, aby utworzyć własną.

O tym zadaniu

Nową bazę certyfikatów należy utworzyć tylko wtedy, gdy nie ma być używana domyślna baza certyfikatów produktu IBM i .

Aby określić, że baza certyfikatów systemu IBM i ma być używana, należy zmienić wartość atrybutu SSLKEYR menedżera kolejek na *SYSTEM. Ta wartość wskazuje, że menedżer kolejek korzysta ze składnicy certyfikatów systemu, a menedżer kolejek jest rejestrowany do użycia jako aplikacja z programem Digital Certificate Manager (DCM).

Procedura

1. Dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282
2. Na panelu nawigacyjnym kliknij opcję **Create New Certificate Store**(Utwórz nową bazę certyfikatów).

   W ramce zadań zostanie wyświetlona strona Tworzenie nowej bazy certyfikatów.
3. W ramce zadań wybierz opcję **Inny system certyfikatów systemowych** , a następnie kliknij przycisk **Kontynuuj**.

   W ramce zadań zostanie wyświetlona strona Tworzenie certyfikatu w nowej składnicy certyfikatów.
4. Wybierz opcję **Nie-nie twórz certyfikatu w bazie certyfikatów** , a następnie kliknij przycisk **Kontynuuj**.

   W ramce zadań zostanie wyświetlona strona Nazwa i hasło bazy certyfikatów.
5. W polu **Ścieżka i nazwa pliku bazy certyfikatów** wpisz ścieżkę IFS i nazwę pliku, na przykład `/QIBM/UserData/mqm/qmgrs/qm1/key.kdb` .
6. Wpisz hasło w polu **Hasło** i wpisz je ponownie w polu **Potwierdź hasło** . Kliknij opcję **Continue**.

   Zanotuj hasło (w takim przypadku jest rozróżniana wielkość liter), ponieważ jest ono potrzebne podczas ukrycia klucza repozytorium.
7. Aby wyjść z programu DCM, zamknij okno przeglądarki.

Co dalej

Po utworzeniu bazy certyfikatów za pomocą programu DCM upewnij się, że hasło jest ukryte, zgodnie z opisem w sekcji “Ukrycie hasła bazy certyfikatów w systemach IBM i” na stronie 284 .

Zadania pokrewne

“Importowanie certyfikatu do repozytorium kluczy w systemie IBM i” na stronie 290
Aby zaimportować certyfikat, należy wykonać następującą procedurę.

Ukrycie hasła bazy certyfikatów w systemach IBM i

Zeskładuj hasło bazy certyfikatów za pomocą komend CL.

Poniższe instrukcje dotyczą ukrytego hasła bazy certyfikatów w produkcie IBM i dla menedżera kolejek. Alternatywnie, dla partycji IBM MQ MQI client, jeśli nie jest używana baza certyfikatów *SYSTEM (czyli środowisko MQSSLKEYR jest ustawione na wartość inną niż *SYSTEM), należy wykonać procedurę opisaną w sekcji “Ukryj hasło bazy certyfikatów” na stronie 293 produktu “IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla IBM i” na stronie 292.

Jeśli określono, że baza certyfikatów *SYSTEM ma być używana (zmieniając wartość atrybutu SSLKEYR menedżera kolejek na *SYSTEM), nie należy wykonywać tych kroków.

Jeśli baza certyfikatów została utworzona za pomocą programu DCM, użyj następujących komend, aby zeskładować hasło:

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

W haśle jest rozróżniana wielkość liter. Należy ją wprowadzić w apostrofach dokładnie tak, jak zostało to wprowadzone w kroku 6 produktu “Tworzenie bazy certyfikatów w systemie IBM i” na stronie 283.

Uwaga: Jeśli nie jest używana domyślna baza certyfikatów systemu, a hasło nie jest ukryte, próby uruchomienia kanałów TLS nie powiodą się, ponieważ nie mogą uzyskać hasła wymaganego do uzyskania dostępu do bazy certyfikatów.

Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie IBM i

Ta procedura służy do uzyskania miejsca położenia bazy certyfikatów menedżera kolejek.

Procedura

1. Wyświetl atrybuty menedżera kolejek za pomocą następującej komendy:

```
DSPMQM MQMNAME('queue manager name')
```

2. Sprawdź dane wyjściowe komendy dla ścieżki i nazwy macierzystej bazy certyfikatów.

   Na przykład: `/QIBM/UserData/ICSS/Cert/Server/Default`, gdzie `/QIBM/UserData/ICSS/Cert/Server` jest ścieżką, a `Default` jest nazwą rdzenia.

Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie IBM i

Zmień położenie bazy certyfikatów menedżera kolejek przy użyciu komendy CHGMQM lub ALTER QMGR.

Procedura

Użyj komendy CHGMQM lub ALTER QMGR MQSC, aby ustawić atrybut repozytorium kluczy menedżera kolejek.

a) Korzystanie z komendy CHGMQM: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

b) Używanie instrukcji ALTER QMGR: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

W obu przypadkach baza certyfikatów ma pełną nazwę pliku: `/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb`

Co dalej

Po zmianie położenia bazy certyfikatów menedżera kolejek certyfikaty nie są przesyłane ze starej lokalizacji. Jeśli certyfikaty ośrodka CA wstępnie zainstalowane podczas tworzenia bazy certyfikatów są niewystarczające, należy zapełnić nową bazę certyfikatów certyfikatami, zgodnie z opisem w sekcji “Importowanie certyfikatu do repozytorium kluczy w systemie IBM i” na stronie 290. Należy także zeskładować hasło dla nowej lokalizacji, zgodnie z opisem w sekcji “Ukrycie hasła bazy certyfikatów w systemach IBM i” na stronie 284.

Tworzenie ośrodka certyfikacji i certyfikatu do testowania w systemie IBM i

Ta procedura służy do tworzenia lokalnego certyfikatu ośrodka CA w celu podpisywania żądań certyfikatów oraz do tworzenia i instalowania certyfikatu ośrodka CA.

Zanim rozpoczniesz

W instrukcjach w tym temacie przyjęto założenie, że lokalny ośrodek certyfikacji (CA) nie istnieje. Jeśli lokalny ośrodek CA istnieje, przejdź do sekcji “Żądanie certyfikatu serwera w systemie IBM i” na stronie 286.

O tym zadaniu

Certyfikaty ośrodka CA, które są udostępniane podczas instalowania protokołu TLS, są podpisywane przez wydający ośrodek CA. W systemie IBM imożna wygenerować lokalny ośrodek certyfikacji, który będzie mógł podpisywać certyfikaty serwera na potrzeby testowania komunikacji TLS w systemie. Aby utworzyć lokalny certyfikat ośrodka CA, wykonaj następujące kroki w przeglądarce WWW:

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji "Dostęp do DCM" na stronie 282.
2. Na panelu nawigacyjnym kliknij opcję **Create a Certificate Authority**(Utwórz ośrodek certyfikacji).
   W ramce zadań zostanie wyświetlona strona Tworzenie ośrodka certyfikacji.
3. Wpisz hasło w polu **Hasło bazy certyfikatów** i wpisz je ponownie w polu **Potwierdź hasło** .
4. Wpisz nazwę w polu **Certificate Authority (CA) name** (Ośrodek certyfikacji), na przykład `TLS Test Certificate Authority`.
5. Wpisz odpowiednie wartości w polach **Nazwa zwykła** i **Organizacja** , a następnie wybierz kraj.
   W przypadku pozostałych pól opcjonalnych wpisz wymagane wartości.
6. W polu **Okres ważności** wpisz okres ważności dla lokalnego ośrodka CA.
   Wartość domyślna to 1095 dni.
7. Kliknij opcję **Continue**.
   Ośrodek CA jest tworzony, a program DCM tworzy bazę certyfikatów i certyfikat ośrodka CA dla lokalnego ośrodka CA.
8. Kliknij opcję **Zainstaluj certyfikat**.
   Zostanie wyświetlone okno dialogowe menedżera pobierania.
9. Wpisz pełną nazwę ścieżki do pliku tymczasowego, w którym ma zostać zapisany certyfikat ośrodka CA, a następnie kliknij przycisk **Zapisz**.
10. Po zakończeniu pobierania kliknij przycisk **Otwórz**.
    Zostanie wyświetlone okno Certyfikat.
11. Kliknij opcję **Zainstaluj certyfikat**.
    Zostanie wyświetlony kreator importowania certyfikatów.
12. Kliknij przycisk **Dalej**.
13. Wybierz opcję **Automatycznie wybierz bazę certyfikatów w oparciu o typ certyfikatu** i kliknij przycisk **Dalej**.
14. Kliknij opcję **Zakończ**.
    Zostanie wyświetlone okno z potwierdzeniem.
15. Kliknij przycisk **OK**.
16. W oknie Certificate (Certyfikat) kliknij przycisk **OK**.
17. Kliknij opcję **Continue**.
    Strona Strategia ośrodka certyfikacji jest wyświetlana w ramce zadań.
18. W polu **Zezwalaj na tworzenie certyfikatów użytkowników** wybierz wartość **Tak**.
19. W polu **Okres ważności** wpisz okres ważności certyfikatów wydawanych przez lokalny ośrodek CA.
    Wartość domyślna to 365 dni.
20. Kliknij opcję **Continue**.
    W ramce zadań zostanie wyświetlona strona Tworzenie certyfikatu w nowej składnicy certyfikatów.
21. Upewnij się, że żadna z aplikacji nie została wybrana.
22. Kliknij przycisk **Continue** (Kontynuuj), aby zakończyć konfigurowanie lokalnego ośrodka CA.

Żądanie certyfikatu serwera w systemie IBM i

Certyfikaty cyfrowe chronią przed imitowaniem, poświadczając, że klucz publiczny należy do określonej jednostki. Certyfikat nowego serwera można zażądać od ośrodka certyfikacji za pomocą programu Digital Certificate Manager (DCM).

O tym zadaniu

Wykonaj następujące kroki w przeglądarce WWW:

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji "Dostęp do DCM" na stronie 282.
2. Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.
3. Wybierz bazę certyfikatów, która ma być używana, i kliknij przycisk **Kontynuuj**.
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło magazynu systemowego, a następnie kliknij przycisk **Kontynuuj**.
5. Opcjonalne: Jeśli w kroku 3 wybrano opcję **Inny system certyfikatów systemowych** , w polu **Ścieżka i nazwa pliku bazy certyfikatów** wpisz ścieżkę IFS i nazwę pliku, który został ustawiony podczas tworzenia bazy certyfikatów. Wpisz także hasło w polu **Hasło bazy certyfikatów** . Następnie kliknij przycisk **Kontynuuj** .
6. Na panelu nawigacyjnym kliknij opcję **Create Certificate**(Utwórz certyfikat).
7. W ramce zadań wybierz przełącznik **Certyfikat serwera lub klienta** , a następnie kliknij przycisk **Kontynuuj**.

   W ramce zadań zostanie wyświetlona strona Wybór ośrodka certyfikacji (CA).
8. Jeśli na stacji roboczej znajduje się lokalny ośrodek certyfikacji (CA), należy wybrać lokalny ośrodek certyfikacji (CA) lub handlowy ośrodek CA, aby podpisać certyfikat. Wybierz przełącznik dla wybranego ośrodka CA i kliknij przycisk **Kontynuuj**.

   W ramce zadań zostanie wyświetlona strona Tworzenie certyfikatu.
9. Opcjonalne: W przypadku menedżera kolejek, w polu **Etykieta certyfikatu** wprowadź etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z dodanym nazwą menedżera kolejek (małymi literami). Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

   Na przykład w przypadku menedżera kolejek QM1, wpisz `ibmwebspheremqqm1` , aby użyć wartości domyślnej.
10. Opcjonalne: W przypadku IBM MQ MQI client, w polu **Etykieta certyfikatu** wpisz `ibmwebspheremq` , a po nim identyfikator użytkownika logowania złożony z małych liter.
    Wpisz na przykład: `ibmwebspheremqmyuserID`
11. Wpisz odpowiednie wartości w polach **Nazwa zwykła** i **Organizacja** , a następnie wybierz kraj.
    W przypadku pozostałych pól opcjonalnych wpisz wymagane wartości.

Wyniki

Jeśli do podpisania certyfikatu został wybrany handlowy ośrodek CA, program DCM utworzy żądanie certyfikatu w formacie PEM (Privacy-Enhanced Mail). Prześlij żądanie do wybranego ośrodka CA.

Jeśli certyfikat został podpisany przez lokalny ośrodek certyfikacji (CA), program DCM informuje, że certyfikat został utworzony w bazie certyfikatów i może być używany.

Żądanie certyfikatu serwera dla programu IBM Key Manager w systemie IBM i

Wykonaj tę procedurę, aby utworzyć certyfikat podpisany przez lokalny ośrodek certyfikacji (CA) lub złożyć wniosek o certyfikat serwera podpisany przez komercyjny ośrodek certyfikacji (CA) do zaimportowania do programu narzędziowego IBM Key Management (iKeyman).

O tym zadaniu

Certyfikat użytkownika musi być używany, gdy program Digital Certificate Manager (DCM) pełni rolę menedżera certyfikatów dla produktu IBM MQ na wielu platformach. W przypadku certyfikatów osobistych dystrybuowanych do innych platform i importowania do programu narzędziowego iKeyman , wykonaj następujące kroki w przeglądarce WWW:

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji "Dostęp do DCM" na stronie 282.
2. W panelu **nawigacyjnym** kliknij opcję **Utwórz certyfikat**.

   Strona **Utwórz certyfikat** jest wyświetlana w ramce zadania.
3. Na panelu **Create Certificate** (Utwórz certyfikat) zaznacz przełącznik **User certificate** (Certyfikat użytkownika) i kliknij przycisk **Continue**(Kontynuuj).

   Zostanie wyświetlona strona **Tworzenie certyfikatu użytkownika** (Create User Certificate).
4. Na panelu **Create User Certificate** (Utwórz certyfikat użytkownika) wypełniaj wymagane pola w sekcji Informacje o certyfikacie w polach **Nazwa organizacji**, **Stan** lub **województwo**, **Kraj** lub **region**. Opcjonalnie można umieścić wartości w polach **Jednostka organizacyjna** i **Miejscowość** lub **Miasto** . Kliknij opcję **Continue**.

   Opcja **Nazwa zwykła** jest automatycznie ustawiana na identyfikator użytkownika, z którym użytkownik jest zalogowany w systemie iSeries .
5. Na panelu **Create User Certificate** (Utwórz certyfikat użytkownika) kliknij opcję **Install certificate** (Zainstaluj certyfikat) i kliknij przycisk **Continue**(Kontynuuj).

   Zostanie wyświetlony komunikat z informacją o tym, że certyfikat osobisty `został zainstalowany. Należy zachować kopię zapasową tego certyfikatu.`
6. Kliknij przycisk **OK**.
7. W zależności od przeglądarki internetowej używanej do uzyskania dostępu do programu DCM, wykonaj następujące czynności:
   a) W przypadku opcji Microsoft Edge wybierz kolejno opcje: **Narzędzia > Opcje internetowe > Karta Treść > Przycisk Certyfikaty > Karta Osobista >**. Wybierz certyfikat i kliknij przycisk **Eksportuj**.
   b) W przypadku przeglądarki Mozilla Firefox wybierz kolejno opcje: **Narzędzia > Opcje > Zaawansowana karta szyfrowania > Przycisk Wyświetl certyfikaty > Karta Certyfikaty >**. Wybierz certyfikat i kliknij opcję **Utwórz kopię zapasową**. Wybierz ścieżkę i nazwę pliku, a następnie kliknij przycisk **OK**.
8. Prześlij wyeksportowany certyfikat do systemu zdalnego za pomocą protokołu FTP w formacie binarnym.
9. Dodaj wyeksportowany certyfikat z kroku 7 do programu narzędziowego iKeyman w bazie danych kluczy.
   a) Jeśli certyfikat został zapisany za pomocą programu Microsoft Edge, należy skorzystać z instrukcji opisanych w sekcji Importowanie z pliku Microsoft `.pfx` .
   b) Jeśli certyfikat został zapisany przy użyciu przeglądarki Mozilla Firefox, należy skorzystać z instrukcji opisanych w sekcji Importowanie certyfikatu osobistego do repozytorium kluczy.

   Podczas importowania upewnij się, że nazwa etykiety certyfikatu osobistego i certyfikatu osoby podpisującej zostały zmienione na to, co IBM MQ oczekuje. Etykieta musi być wartością atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartością domyślną `ibmwebspheremq` z dodanym nazwą menedżera kolejek, a wszystko to małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Dodawanie certyfikatów serwera do repozytorium kluczy w systemie IBM i

Wykonaj tę procedurę, aby dodać żądany certyfikat do repozytorium kluczy.

O tym zadaniu

Po wysłaniu przez ośrodek CA nowego certyfikatu serwera, należy dodać go do bazy certyfikatów, z której wygenerowano żądanie. Jeśli ośrodek CA wyśle certyfikat jako część wiadomości e-mail, skopiuj certyfikat do osobnego pliku.

Uwaga:

- Jeśli certyfikat serwera jest podpisany przez lokalny ośrodek CA, nie ma potrzeby wykonywania tej procedury.
- Przed zaimportowanie certyfikatu serwera w formacie PKCS #12 do programu DCM, należy najpierw zaimportować odpowiedni certyfikat ośrodka CA.

Aby odebrać certyfikat serwera do bazy certyfikatów menedżera kolejek, należy wykonać następującą procedurę:

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282.
2. W kategorii zadań **Zarządzanie certyfikatami** na panelu nawigacyjnym kliknij opcję **Importuj certyfikat**.

   W ramce zadań zostanie wyświetlona strona Importowanie certyfikatu.
3. Wybierz przełącznik dla typu certyfikatu i kliknij przycisk **Continue**(Kontynuuj).

   W ramce zadań zostanie wyświetlona strona Importowanie certyfikatu serwera lub certyfikatu klienta albo strona Importowanie certyfikatu ośrodka certyfikacji (CA).
4. W polu **Plik importu** wpisz nazwę pliku certyfikatu, który ma zostać zaimportowany, a następnie kliknij przycisk **Kontynuuj**.

   Program DCM automatycznie określa format pliku.
5. Jeśli certyfikat jest certyfikatem **Serwer lub klient** , wpisz hasło w ramce zadania i kliknij przycisk **Kontynuuj**.

   Program DCM informuje, że certyfikat został zaimportowany.

Eksportowanie certyfikatu z repozytorium kluczy w systemie IBM i

Eksportowanie certyfikatu eksportuje zarówno klucz publiczny, jak i prywatny. To działanie powinno być podejmowane z dużą ostrożnością, ponieważ przekazanie klucza prywatnego całkowicie zagroziłoby bezpieczeństwu.

Zanim rozpoczniesz

Jeśli certyfikat użytkownika zostanie udostępniony do współużytkowania dla innego użytkownika, należy wymieniać klucze publiczne. Ten proces został opisany w **zadaniu 5. Współużytkowanie certyfikatów** w Podręcznik Szybki start dla produktu AMS w systemie UNIX. Podczas eksportowania certyfikatu zgodnie z opisem w tym miejscu należy wyeksportować zarówno klucz publiczny, jak i prywatny. To działanie powinno być podejmowane z dużą ostrożnością, ponieważ przekazanie klucza prywatnego całkowicie zagroziłoby bezpieczeństwu.

O tym zadaniu

Wykonaj następujące kroki na komputerze, na podstawie którego chcesz wyeksportować certyfikat:

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282.
2. Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.
3. Wybierz bazę certyfikatów, która ma być używana, i kliknij przycisk **Kontynuuj**.
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło magazynu systemowego, a następnie kliknij przycisk **Kontynuuj**.
5. Opcjonalne: Jeśli w kroku 3 wybrano opcję **Inna baza certyfikatów systemu** , w polu **Ścieżka i nazwa pliku bazy certyfikatów** wpisz ścieżkę i nazwę pliku IFS, która została ustawiona podczas

tworzenia bazy certyfikatów, i wpisz hasło w polu **Hasło bazy certyfikatów** . Następnie kliknij przycisk **Kontynuuj** .

6. W kategorii zadań **Zarządzanie certyfikatami** na panelu nawigacyjnym kliknij opcję **Eksportuj certyfikat**.

   Strona Eksport certyfikatu jest wyświetlana w ramce zadań.
7. Wybierz przełącznik dla typu certyfikatu i kliknij przycisk **Continue**(Kontynuuj).

   W ramce zadań zostanie wyświetlona strona Eksport certyfikatu serwera lub klienta albo strona Certyfikat eksportu ośrodka certyfikacji (CA).
8. Wybierz certyfikat, który chcesz wyeksportować.
9. Wybierz przełącznik, aby określić, czy certyfikat ma zostać wyeksportowany do pliku, czy też bezpośrednio do innej bazy certyfikatów.
10. Jeśli wybrano opcję eksportowania certyfikatu serwera lub klienta do pliku, należy podać następujące informacje:
    - Ścieżka i nazwa pliku, w którym ma zostać zapisany wyeksportowany certyfikat.
    - W przypadku certyfikatu osobistego hasło, które jest używane do szyfrowania eksportowanego certyfikatu i wydania docelowego. W przypadku certyfikatów CA nie ma potrzeby określania hasła.
11. Jeśli wybrano opcję eksportowania certyfikatu bezpośrednio do innej bazy certyfikatów, należy określić docelową bazę certyfikatów i jego hasło.
12. Kliknij opcję **Continue**.

Importowanie certyfikatu do repozytorium kluczy w systemie IBM i

Aby zaimportować certyfikat, należy wykonać następującą procedurę.

Zanim rozpoczniesz

Przed zaimportowanie certyfikatu osobistego w formacie PKCS #12 do programu DCM, należy najpierw zaimportować odpowiedni certyfikat ośrodka CA.

O tym zadaniu

Wykonaj poniższe kroki na komputerze, do którego ma zostać zaimportowany certyfikat.

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282.
2. Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.
3. Wybierz bazę certyfikatów, która ma być używana, i kliknij przycisk **Kontynuuj**.
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło magazynu systemowego, a następnie kliknij przycisk **Kontynuuj**.
5. Opcjonalne: Jeśli w kroku 3 wybrano opcję **Inna baza certyfikatów systemu** , w polu **Ścieżka i nazwa pliku bazy certyfikatów** wpisz ścieżkę i nazwę pliku IFS, która została ustawiona podczas tworzenia bazy certyfikatów, i wpisz hasło w polu **Hasło bazy certyfikatów** . Następnie kliknij przycisk **Kontynuuj** .
6. W kategorii zadań **Zarządzanie certyfikatami** na panelu nawigacyjnym kliknij opcję **Importuj certyfikat**.

   Strona Importowanie certyfikatu jest wyświetlana w ramce zadań.
7. Wybierz przełącznik dla typu certyfikatu i kliknij przycisk **Continue**(Kontynuuj).

   W ramce zadań zostanie wyświetlona strona Importowanie certyfikatu serwera lub certyfikatu klienta lub strona Importowanie certyfikatu ośrodka certyfikacji (CA).
8. W polu **Plik importu** wpisz nazwę pliku certyfikatu, który ma zostać zaimportowany, a następnie kliknij przycisk **Kontynuuj**.

Program DCM automatycznie określa format pliku.

9. Jeśli certyfikat jest certyfikatem **Serwer lub klient** , wpisz hasło w ramce zadania i kliknij przycisk **Kontynuuj**. Program DCM informuje, że certyfikat został zaimportowany.

Usuwanie certyfikatów w programie IBM i

Ta procedura służy do usuwania certyfikatów osobistych.

Procedura

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282.
2. Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.
3. Zaznacz pole wyboru **Inny system certyfikatów systemowych** i kliknij przycisk **Kontynuuj**.

   Zostanie wyświetlona strona Baza certyfikatów i hasło.
4. W polu **Ścieżka i nazwa pliku bazy certyfikatów** (Certificate store path and filename) wpisz ścieżkę IFS i nazwę pliku, który został ustawiony podczas tworzenia bazy certyfikatów.
5. Wpisz hasło w polu **Hasło bazy certyfikatów** . Kliknij opcję **Continue**.

   W ramce zadań zostanie wyświetlona strona Bieżąca baza certyfikatów.
6. W kategorii zadań **Zarządzanie certyfikatami** na panelu nawigacyjnym kliknij opcję **Usuń certyfikat**.

   W ramce zadań zostanie wyświetlona strona Potwierdzenie usunięcia certyfikatu.
7. Wybierz certyfikat, który chcesz usunąć. Kliknij opcję **Delete** (Usuń).
8. Kliknij przycisk **Tak** , aby potwierdzić, że certyfikat ma zostać usunięty. W przeciwnym razie kliknij opcję **Nie**.

   Program DCM informuje użytkownika, czy usunł certyfikat.

*Korzystanie ze składnicy certyfikatów *SYSTEM w celu uwierzytelniania jednokierunkowego w systemie IBM i*

Wykonaj poniższe instrukcje, aby skonfigurować uwierzytelnianie jednokierunkowe.

Zanim rozpoczniesz

- Utwórz menedżera kolejek, kanały i kolejki transmisji.
- Utwórz certyfikat serwera lub klienta w menedżerze kolejek serwera.
- Prześlij certyfikat CA do menedżera kolejek klienta i zaimportowano go do repozytorium kluczy.
- Uruchom program nasłuchujący na serwerze i w menedżerach kolejek klienta.

O tym zadaniu

Aby użyć uwierzytelniania jednokierunkowego, przy użyciu komputera IBM i , należy ustawić parametr Repozytorium kluczy SSL (SSLKEYR) na *SYSTEM. To ustawienie powoduje zarejestrowanie menedżera kolejek produktu IBM MQ jako aplikacji. Następnie można przypisać certyfikat do menedżera kolejek, aby włączyć uwierzytelnianie jednokierunkowe.

W celu zaimplementowania uwierzytelniania jednokierunkowego można również użyć prywatnych magazynów kluczy, tworząc fikcyjny certyfikat dla menedżera kolejek klienta w repozytorium kluczy.

Procedura

1. Wykonaj następujące kroki na serwerze i menedżerach kolejek klienta:

   a) Zmień menedżer kolejek, aby ustawić parametr SSLKEYR, wydając komendę `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.

b) Wprowadź hasło do domyślnego repozytorium kluczy, wydając komendę `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')`.

Hasło musi być ujęte w apostrofach.

c) Zmień kanały tak, aby w parametrze SSLCIPHER miały poprawny parametr CipherSpec .

d) Odśwież zabezpieczenia TLS, wydając komendę `RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL)`.

2. Przypisz certyfikat do menedżera kolejek serwera za pomocą programu DCM, w następujący sposób:

a) Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji "Dostęp do DCM" na stronie 282.

b) Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store).

W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.

c) Wybierz bazę certyfikatów *SYSTEM i kliknij przycisk **Continue**(Kontynuuj).

d) W panelu po lewej stronie rozwiń pozycję **Zarządzanie aplikacjami**.

e) Wybierz definicję **Wyświetl aplikację** , aby sprawdzić, czy menedżer kolejek został zarejestrowany jako aplikacja.

W tabeli znajduje się lista SSL (`WMQ`) .

f) Wybierz opcję **Aktualizacja przypisania certyfikatu**.

g) Wybierz opcję **Serwer** i kliknij przycisk **Kontynuuj**.

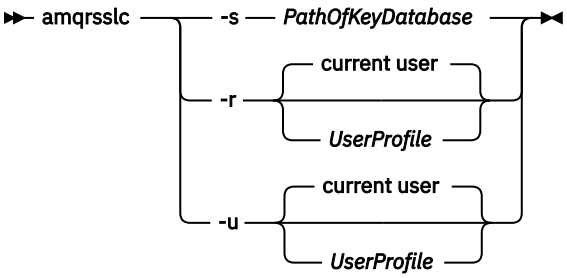
h) Wybierz opcję QMGRNAME (WMQ) i kliknij opcję **Update certificate assignment**(Aktualizuj przypisanie certyfikatu).

i) Wybierz certyfikat i kliknij opcję **Przypisz nowy certyfikat**. Zostanie otwarte okno z informacją o tym, że certyfikat został przypisany do aplikacji.

IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla IBM i

Program narzędziowy IBM MQ SSL Client (amqrsslc) for IBM i jest używany przez IBM MQ MQI client w systemach IBM i do rejestrowania lub wyrejestrowywać profilu użytkownika klienta lub ukrycia hasła do bazy certyfikatów. Program narzędziowy może być uruchamiany tylko przez użytkownika z profilem z uprawnieniem specjalnym *ALLOBJ lub z członkiem grupy QMQMADM, który ma opcje tworzenia lub usuwania rejestracji aplikacji w programie Digital Certificate Manager (DCM).

Diagram składni



Zarejestruj profil użytkownika klienta

Jeśli baza danych IBM MQ MQI client używa bazy certyfikatów *SYSTEM, należy zarejestrować profil użytkownika klienta (użytkownik logowania), który będzie używany jako aplikacja za pomocą programu Digital Certificate Manager (DCM).

Jeśli chcesz zarejestrować profil użytkownika klienta, uruchom program **amqrsslc** z opcją `-r` z opcją *UserProfile*. Profil użytkownika używany podczas wywoływania programu **amqrsslc** musi mieć uprawnienia *USE. Podanie opcji *UserProfile* przy użyciu opcji `-r` powoduje zarejestrowanie pliku *UserProfile* jako aplikacji serwera z unikalną etykietą aplikacji QIBM_WEBSPHERE_MQ_*UserProfile*

i etykietą z opisem *UserProfile* (WMQ). Następnie ta aplikacja serwera jest wyświetlana w programie DCM, a użytkownik może przypisać do tej aplikacji dowolny certyfikat serwera lub klienta w składnicy systemu.

Uwaga: Jeśli profil użytkownika nie jest określony za pomocą opcji `-r` , to zarejestrowany jest profil użytkownika uruchamiający narzędzie **amqrsslc** .

Poniższy kod używa produktu **amqrsslc** do zarejestrowania profilu użytkownika. W pierwszym przykładzie podany profil użytkownika jest zarejestrowany; w drugim jest to profil zalogowanego użytkownika:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

Wyrejestruj profil użytkownika klienta

Aby wyrejestrować profil klienta, należy uruchomić program **amqrsslc** z opcją `-u` z opcją *UserProfile*. Profil użytkownika używany podczas wywoływania programu **amqrsslc** musi mieć uprawnienia *USE. Udostępnienie partycji *UserProfile* z opcją `-u` wyrejestrowywać *UserProfile* z etykietą QIBM_WEBSPHERE_MQ_*UserProfile* z programu DCM.

Uwaga: Jeśli profil użytkownika nie jest określony za pomocą opcji `-u` , to profil użytkownika uruchamiający narzędzie **amqrsslc** jest niezarejestrowany.

Poniższy kod używa produktu **amqrsslc** do wyrejestrowania profilu użytkownika. W pierwszym przykładzie określony profil użytkownika jest niezarejestrowany; w drugim jest to profil zalogowanego użytkownika:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Ukryj hasło bazy certyfikatów

Jeśli IBM MQ MQI client nie używa bazy certyfikatów *SYSTEM i używana jest inna baza certyfikatów (to znaczy MQSSLKEYR jest ustawiona na wartość inną niż *SYSTEM), to hasło bazy danych kluczy musi być zapisane w stanie ukrytym. Użyj opcji `-s` w celu ukrytego hasła bazy danych kluczy.

W poniższym kodzie pełna nazwa pliku bazy certyfikatów jest następująca: `/Path/Of/KeyDatabase/MyKey.kdb`:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Uruchomienie tego kodu powoduje zgłoszenie hasła dla tej bazy danych kluczy. To hasło jest ukryte w pliku o tej samej nazwie, co baza danych kluczy z rozszerzeniem .sth. Ten plik jest przechowywany w tej samej ścieżce, co baza danych kluczy. Przykładowy kod generuje plik ukrytych haseł `/Path/Of/KeyDatabase/MyKey.sth`. QMQM jest właścicielem użytkownika i QMQMADM właścicielem grupy dla tego pliku. Uprawnienia do odczytu, zapisu i odczytu QMQM i QMQMADM mają tylko uprawnienia do odczytu.

Gdy zmiany w certyfikatach lub w bazie certyfikatów stają się skuteczne w systemie IBM i

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 bazie certyfikatów i w atrybucie repozytorium kluczy stają się skuteczne w następujących sytuacjach:

- Gdy nowy proces wychodzący pojedynczego kanału jest uruchamiany jako pierwszy, uruchamiany jest kanał TLS.

- Gdy nowy przychodzący proces pojedynczego kanału TCP/IP otrzyma żądanie uruchomienia kanału TLS, najpierw zostanie wysłane żądanie.
- Po wydaniu komendy MQSC REFRESH SECURITY TYPE (SSL) w celu odświeżenia środowiska TLS produktu IBM MQ .
- W przypadku procesów aplikacji klienckich, gdy ostatnie połączenie TLS w procesie jest zamknięte. Następne połączenie TLS pobiera 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 TLS. Jeśli proces zestawiania procesów już uruchomił kanał TLS 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 TLS. Jeśli proces inicjatora kanału uruchomił już kanał TLS 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 raz pierwszy odbiera żądanie uruchomienia kanału TLS. Jeśli program nasłuchujący uruchomił już kanał TLS i chcesz, aby zmiana stała się efektywna od razu, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).

Konfigurowanie sprzętu szyfrującego w systemie IBM i

Ta procedura służy do konfigurowania koprocesora szyfrującego w systemie IBM i

Zanim rozpoczniesz

Upewnij się, że profil użytkownika ma uprawnienia specjalne *ALLOBJ i *SECADM, aby można było skonfigurować sprzęt koprocesora.

Procedura

1. Przejdź do katalogu `http://`*`machine`*`.domain:2001` lub `https://`*`machine`*`.domain:2010`, gdzie *komputer* jest nazwą komputera.

   Zostanie wyświetlone okno dialogowe z prośbą o podanie nazwy użytkownika i hasła.
2. Wpisz poprawny profil użytkownika i hasło produktu IBM i .
3. Przejdź do opcji Kryptografia i postępuj zgodnie z odpowiednimi odsyłaczami, aby uzyskać więcej informacji.

Co dalej

Więcej szczegółowych informacji na temat konfigurowania koprocesora szyfrującego 4767 Cryptographic Coprocessorzawiera sekcja 4767 Cryptographic Coprocessor.

ULW Praca z protokołem SSL/TLS w systemie UNIX, Linux, and Windows

W systemach UNIX, Linux, and Windows obsługa protokołu TLS (Transport Layer Security) jest instalowana wraz z produktem IBM MQ.

Więcej szczegółowych informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja Sprawdzanie poprawności certyfikatu i projekt strategii zaufania.

ULW *Używanie produktów `runmqckm`, `runmqakm` i `strmqikm` do zarządzania certyfikatami cyfrowymi*

W systemach UNIX, Linux, and Windows zarządzanie kluczami i certyfikatami cyfrowymi za pomocą programu **`strmqikm`** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komendy **`runmqckm`** (iKeycmd) lub **`runmqakm`** (GSKCapiCmd).

V 9.1.0

Ostrzeżenie: Zarówno komendy **runmqckm** , jak i **strmqikm** opierają się na środowisku Java Runtime Environment (JRE) produktu IBM MQ . W produkcie IBM MQ 9.1, jeśli środowisko JRE nie jest zainstalowane, wyświetlany jest komunikat AMQ9183.

- W systemach **UNIX and Linux** :
  - Użyj komendy **strmqikm** (iKeyman), aby uruchomić interfejs GUI programu iKeyman .
  - Komenda **runmqckm** (iKeycmd) służy do wykonywania zadań za pomocą interfejsu wiersza komend iKeycmd .
  - Za pomocą komendy **runmqakm** (GSKCapiCmd) można wykonywać zadania za pomocą interfejsu wiersza komend runmqakm. Składnia komendy dla **runmqakm** jest taka sama, jak składnia komendy **runmqckm**.

    Jeśli wymagane jest zarządzanie certyfikatami TLS 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.

  Więcej informacji na ten temat zawiera sekcja GSKit: PKCS#11 and IBM MQ JRE addressing mode .

  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 wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend **runmqckm** lub **strmqikm** .
  - Za pomocą komendy **runmqakm -keydb** można użyć opcji *stashpw* lub *stash* .

    Podczas używania komendy **runmqakm -keydb** w ten sposób, na przykład:

    ```
    runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
    ```

    Wynikowy plik `.sth` nie ma włączonych uprawnień do odczytu dla grupy `mqm` .

    Tylko twórca może odczytać plik. Po utworzeniu pliku ukrytych haseł za pomocą komendy **runmqakm** należy sprawdzić uprawnienia do pliku i nadać uprawnienia do konta usługi, na którym działa menedżer kolejek, lub do grupy, takiej jak lokalna `mqm`.

Informacje na temat żądania śledzenia TLS w systemach UNIX, Linux lub Windows można znaleźć w sekcji strmqtrc.

Odsyłacze pokrewne

Komendy runmqckm i runmqakm
W tej sekcji opisano komendy runmqckm i runmqakm zgodnie z obiektem komendy.

ULW *Konfigurowanie repozytorium kluczy w systemie UNIX, Linux, and Windows*

Repozytorium kluczy można skonfigurować przy użyciu programu **strmqikm** (iKeyman). Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

O tym zadaniu

Połączenie TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek produktu IBM MQ i produkt IBM MQ MQI client muszą mieć dostęp do repozytorium kluczy. Więcej informacji na ten temat zawiera sekcja “Repozytorium kluczy SSL/TLS” na stronie 25.

W systemach UNIX, Linux, and Windows certyfikaty cyfrowe są przechowywane w pliku bazy danych kluczy, który jest zarządzany za pomocą interfejsu użytkownika produktu **strmqikm** , lub za pomocą komend **runmqckm** lub **runmqakm** . Te certyfikaty cyfrowe mają etykiety. Konkretna etykieta wiąże certyfikat osobisty z menedżerem kolejek lub IBM MQ MQI client. Protokół TLS używa tego certyfikatu do celów uwierzytelniania. W systemach UNIX, Linux, and Windows produkt IBM MQ używa wartości atrybutu **CERTLABL** (jeśli jest ustawiona) lub domyślnego `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem logowania użytkownika produktu IBM MQ MQI client , a wszystkie z małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

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 MQ . Na przykład: `C:\Program Files\IBM\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 IBM 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 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 systemie UNIX, Linux, and Windows” na stronie 300 . Nazwę pliku bazy danych kluczy można określić przed utworzeniem pliku bazy danych kluczy lub po jego utworzeniu.

ID użytkownika, z którego uruchamiana jest komenda **strmqikm** lub **runmqckm** , 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 **strmqikm** lub **runmqckm** , musi być członkiem grupy mqm. W przypadku partycji IBM MQ MQI client, jeśli produkt **strmqikm** lub **runmqckm** jest uruchamiany z ID użytkownika innego niż ten, w którym działa klient, należy zmienić uprawnienia dostępu do pliku, aby umożliwić IBM MQ MQI client dostęp do pliku bazy danych kluczy w czasie wykonywania. Więcej informacji na ten temat zawiera sekcja “Uzyskiwanie dostępu i zabezpieczanie plików bazy danych kluczy w systemie Windows” na stronie 298 lub “Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemach UNIX and Linux” na stronie 298.

In **strmqikm** or **runmqckm** for IBM WebSphere MQ 7.0, new key databases are automatically populated with a set of pre-defined certificate authority (CA) certificates. In **strmqikm** or **runmqckm** for IBM MQ

8.0, key databases are not automatically populated, making the initial setup more secure because you include only the CA certificates that you want, in your key database file.

Uwaga: Ze względu na tę zmianę w działaniu produktu GSKit 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. Patrz “Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy na serwerze UNIX, Linux, and Windows za pomocą programu GSKit 8.0” na stronie 299.

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:
   - Korzystanie z produktu **runmqckm**:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Korzystanie z produktu **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. (W przypadku produktu IBM MQmusi to być wartość cms.)

   -stash
   Zapisuje hasło bazy danych kluczy w pliku.

   -fips
   określa, że komenda jest uruchamiana 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, 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, 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:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (w systemach Windows).

     Ścieżka musi być zgodna z wartością atrybutu **SSLKeyRepository** menedżera kolejek.
   - W przypadku klienta IBM MQ : `/var/mqm/ssl` (w systemach UNIX and Linux) lub `C:\mqm\ssl` (w systemach Windows).
8. Kliknij przycisk **OK**.

   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 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 298 lub “Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemach UNIX and Linux” na stronie 298.

Windows *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.

Linux UNIX *Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich 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*`.crl`i *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 -----).

ULW *Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy na serwerze UNIX, Linux, and Windows za pomocą programu GSKit 8.0*

Wykonaj tę procedurę, aby dodać jeden lub więcej domyślnych certyfikatów CA do pustego repozytorium kluczy z pakietem GSKit w wersji 8.

W produkcie GSKit 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.

Użycie `strmqikm`

Na komputerze, na którym chcesz dodać certyfikat CA, wykonaj następujące kroki:

1. Uruchom interfejs GUI za pomocą komendy **`strmqikm`** (w systemie UNIX, Linux, and 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 programu **runmqckm**:

- 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 program IBM MQ ufa wszystkie certyfikaty osobiste podpisane 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.

ULW *Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie 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 komend IBM MQ Explorer lub PCF.
2. Sprawdź dane wyjściowe komendy dla ścieżki i nazwy macierzystej pliku bazy danych kluczy. Na przykład składnia
   a. w systemie 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 IBM MQ .

ULW *Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie UNIX, Linux, and 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 systemie 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\MQ\Qmgrs\QM1\ssl\Mykey')
```

Plik bazy danych kluczy zawiera pełną nazwę pliku: `C:\Program Files\IBM\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 za pomocą programu IBM 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 systemie UNIX, Linux, and Windows” na stronie 316.

ULW *Znajdowanie repozytorium kluczy dla partycji IBM MQ MQI client w systemie UNIX, Linux, and Windows*

Położenie repozytorium kluczy jest nadawane przez zmienną MQSSLKEYR lub jest określone w wywołaniu MQCONNX.

Sprawdź zmienną środowiskową MQSSLKEYR, aby znaleźć położenie pliku bazy danych kluczy dla produktu IBM MQ MQI client. 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 partycji IBM MQ MQI client w systemie UNIX, Linux, and Windows” na stronie 301. Wartość ustawiona w wywołaniu MQCONNX przesłania wartość MQSSLKEYR.

ULW *Określanie położenia repozytorium kluczy dla partycji IBM MQ MQI client w systemie UNIX, Linux, and Windows*

Dla partycji IBM MQ MQI clientnie 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 dla produktu IBM MQ MQI client można określić na dwa sposoby:

- Ustawianie zmiennej środowiskowej MQSSLKEYR. Na przykład w systemie 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\MQ\ssl\key
```

W pliku bazy danych kluczy znajduje się pełna nazwa pliku:

```
C:\Program Files\IBM\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.

ULW *Gdy zmiany w certyfikatach lub w bazie certyfikatów stają się skuteczne w systemie UNIX, Linux, and 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 TLS.
- Gdy nowy przychodzący proces pojedynczego kanału TCP/IP otrzyma żądanie uruchomienia kanału TLS, najpierw zostanie wysłane żądanie.
- Po wydaniu komendy MQSC REFRESH SECURITY TYPE (SSL) odświeżanie środowiska TLS jest wykonywane.
- W przypadku procesów aplikacji klienckich, gdy ostatnie połączenie TLS w procesie jest zamknięte. Następne połączenie TLS 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 TLS. Jeśli proces zestawiania procesów już uruchomił kanał TLS 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 TLS. Jeśli proces inicjatora kanału uruchomił już kanał TLS 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 raz pierwszy odbiera żądanie uruchomienia kanału TLS. Jeśli program nasłuchujący uruchomił już kanał TLS i chcesz, aby zmiana stała się efektywna od razu, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).

Środowisko IBM MQ TLS można również odświeżać przy użyciu programu IBM MQ Explorer lub komend PCF.

ULW *Tworzenie samopodpisanego certyfikatu osobistego w systemie UNIX, Linux, and Windows*

Certyfikat samopodpisany można utworzyć za pomocą programu **strmqikm** (iKeyman). Interfejs GUI lub z wiersza komend za pomocą komendy **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

Uwaga: Produkt IBM 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 używać certyfikatów samopodpisanych, zawiera sekcja Korzystanie z samopodpisanych certyfikatów do uwierzytelniania wzajemnego w dwóch menedżerach kolejek.

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 IBM MQ obsługuje trzy różne typy interfejsu CipherSpec. Szczegółowe informacje na ten temat zawiera sekcja “Współdziałanie krzywej eliptycznej i specyfikacji szyfrowania RSA CipherSpecs” na stronie 46 w temacie “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45 .

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.

Listę opcji dostępnych w algorytmie kodowania mieszającego **-sig_alg** można znaleźć w sekcji “Opcje runmqckm i runmqakm w systemie UNIX, Linux, and Windows” na stronie 546 .

W przypadku korzystania z:

- Interfejs GUI, patrz “Korzystanie z interfejsu użytkownika produktu strmqikm” na stronie 303
- Wiersz komend, patrz “Za pomocą wiersza komend” na stronie 304

ULW *Korzystanie z interfejsu użytkownika produktu **strmqikm***

Certyfikat osobisty można utworzyć za pomocą programu **strmqikm** (iKeyman) Interfejs GUI.

O tym zadaniu

Produkt **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny z FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Aby utworzyć certyfikat osobisty dla menedżera kolejek lub IBM MQ MQI client przy użyciu graficznego interfejsu użytkownika, wykonaj następujące kroki:

1. Uruchom interfejs GUI 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, z którego ma zostać wygenerowany żądanie, na przykład key . kdb.
6. Kliknij przycisk **OK**.

   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 **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) wprowadź etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną ibmwebspheremq z dodanym identyfikatorem menedżera kolejek lub identyfikatorem zalogowanego użytkownika IBM MQ MQI client , a wszystko to małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

10. Wpisz lub wybierz wartość w dowolnym polu w polu **Nazwa wyróżniająca** lub dowolną z pól **Nazwa alternatywna podmiotu** .
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.

Co dalej

Wyślij żądanie certyfikatu do ośrodka CA. Więcej informacji na ten temat zawiera sekcja “Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie UNIX, Linux, and Windows” na stronie 310.

ULW *Za pomocą wiersza komend*

Certyfikat osobisty można utworzyć z poziomu wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Utwórz samopodpisany certyfikat osobisty, używając komendy **runmqckm** lub **runmqakm** (GSKCapiCmd).

- Korzystanie z produktu **runmqckm** w systemie UNIX, Linux, and 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_dnsname` *DNS_names*, `-san_emailaddr` *email_addresses*lub `-san_ipaddr` *IP_addresses*.

- Korzystanie z produktu **runmqakm**:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -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. Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z nazwą menedżera kolejek lub z dodanym identyfikatorem zalogowanego użytkownika produktu IBM MQ MQI client , a wszystkie z małymi literami. Szczegółowe informacje zawiera temat “Cyfrowe etykiety certyfikatów, zrozumienie wymagań” na stronie 26.

-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.

Uwaga: Narzędzia **runmqckm** i **runmqakm** odwołują się do atrybutu kodu pocztowego jako POSTALCODE, a nie do PC. Należy zawsze podać parametr POSTALCODE w parametrze **-dn** , jeśli używane są te komendy zarządzania certyfikatami do żądania certyfikatów z kodem pocztowym.

-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.

x509version *wersja*
Wersja certyfikatu X.509 do utworzenia. Wartością może być 1, 2 lub 3. Domyślną wartością jest 3.

-file *nazwa_pliku*
Określa nazwę pliku dla żądania certyfikatu.

-expire *dni*
Czas ważności (w dniach) certyfikatu. Wartość domyślna to 365 dni dla certyfikatu.

-fips
określa, że komenda jest uruchamiana w trybie FIPS. Używany jest tylko komponent ICC FIPS, a ten komponent musi być 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, wykonanie komendy **runmqaqm** nie powiedzie się.

-sig_alg
W przypadku bazy danych **runmqckm**określa algorytm podpisu asymetrycznego używany do tworzenia pary kluczy pozycji. Może to być wartość: MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, 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_SHA384lub 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.

Co dalej

Wyślij żądanie certyfikatu do ośrodka CA. Więcej informacji na ten temat zawiera sekcja “Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie UNIX, Linux, and Windows” na stronie 310.

ULW *Żądanie certyfikatu osobistego w systemie UNIX, Linux, and Windows*

Żądanie certyfikatu osobistego można zażądać za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). 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 **strmqikm** lub z poziomu wiersza komend, z uwzględnieniem następujących czynników:

- Produkt IBM 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 IBM MQ obsługuje trzy różne typy interfejsu CipherSpec. Szczegółowe informacje na ten temat zawiera sekcja “Współdziałanie krzywej eliptycznej i specyfikacji szyfrowania RSA CipherSpecs” na stronie 46 w temacie “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45 .
- 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.

  Listę opcji dostępnych w algorytmie kodowania mieszającego **-sig_alg** można znaleźć w sekcji “Opcje runmqckm i runmqakm w systemie UNIX, Linux, and Windows” na stronie 546 .
- 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 325.

W przypadku korzystania z:

- Interfejs GUI, patrz “Korzystanie z interfejsu użytkownika produktu strmqikm” na stronie 306
- Wiersz komend, patrz “Za pomocą wiersza komend” na stronie 307

ULW *Korzystanie z interfejsu użytkownika produktu **strmqikm***

Żądanie certyfikatu osobistego można zażądać za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

O tym zadaniu

Produkt **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny z 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 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 etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem zalogowanego użytkownika IBM MQ MQI client , a wszystko to małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
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 307.
14. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując ten plik do formularza żądania na stronie internetowej ośrodka CA.

ULW *Za pomocą wiersza komend*

Za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd) można zażądać certyfikatu osobistego z wiersza komend. Jeśli wymagane jest zarządzanie certyfikatami SSL lub TLS w sposób zgodny ze standardem FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Zażądaj certyfikatu osobistego za pomocą komendy **runmqckm** lub **runmqakm** (GSKCapiCmd).

- 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`*.

- Korzystanie z produktu **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. Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z nazwą menedżera kolejek lub z dodanym identyfikatorem zalogowanego użytkownika produktu IBM MQ MQI client , a wszystkie z małymi literami. Szczegółowe informacje zawiera temat "Cyfrowe etykiety certyfikatów, zrozumienie wymagań" na stronie 26.

-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.

Uwaga: Narzędzia **runmqckm** i **runmqakm** odwołują się do atrybutu kodu pocztowego jako `POSTALCODE`, a nie do PC. Należy zawsze podać parametr `POSTALCODE` w parametrze **-dn** , jeśli używane są te komendy zarządzania certyfikatami do żądania certyfikatów z kodem pocztowym.

-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. 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. Może to być wartość: `MD2_WITH_RSA`, `MD2WithRSA`, `MD5_WITH_RSA`, `MD5WithRSA`, `SHA1WithDSA`, `SHA1WithECDSA`, `SHA1WithRSA`, `SHA2/ECDSA`, `SHA224WithECDSA`, `SHA256_WITH_RSA`, `SHA256WithECDSA`, `SHA256WithRSA`, `SHA2WithECDSA`, `SHA3/ECDSA`, `SHA384_WITH_RSA`, `SHA384WithECDSA`, `SHA384WithRSA`, `SHA3WithECDSA`, `SHA5/ECDSA`, `SHA512_WITH_RSA`, `SHA512WithECDSA`, `SHA512WithRSA`, `SHA5WithECDSA`, `SHA_WITH_DSA`, `SHA_WITH_RSA`, `SHAWithDSA`, `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.

Co dalej

Wyślij żądanie certyfikatu do ośrodka CA. Więcej informacji na ten temat zawiera sekcja "Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie UNIX, Linux, and Windows" na stronie 310.

ULW *Odnawianie istniejącego certyfikatu osobistego w systemie UNIX, Linux, and Windows*

Certyfikat osobisty można odnowić za pomocą programu **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

O tym zadaniu

Jeśli wymagane jest użycie większych wielkości kluczy dla certyfikatów osobistych, nie można odnowić istniejącego certyfikatu. Istniejący klucz należy zastąpić, wykonując kroki opisane w sekcji "Żądanie certyfikatu osobistego w systemie UNIX, Linux, and Windows" na stronie 305 , aby utworzyć nowe żądanie certyfikatu, które korzysta z wymaganych wielkości kluczy.

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 produktu **strmqikm***

O tym zadaniu

Produkt **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS. Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny z FIPS-em, należy użyć komendy **runmqakm** .

Procedura

Wykonaj następujące kroki, aby zastosować się do certyfikatu osobistego, korzystając z interfejsu użytkownika produktu **strmqikm** :

1. Uruchom interfejs użytkownika, korzystając z komendy **strmqikm** w systemie 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 **Re-create Request ...** (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 309.
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 **runmqckm** lub **runmqakm** , należy użyć następujących komend:

- Korzystanie z produktu **runmqckm** 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 systemie UNIX, Linux, and Windows" na stronie 310.

ULW *Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie UNIX, Linux, and 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.

Użycie strmqikm

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** nie udostępnia opcji zgodnej 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 IBM MQ MQI client , aby odebrać certyfikat osobisty do pliku bazy danych kluczy:

1. Uruchom interfejs GUI 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

Aby dodać certyfikat osobisty do pliku bazy danych kluczy, użyj jednej z następujących komend:

- Korzystanie z produktu **runmqckm**:

```
runmqckm -cert -receive -file filename -db filename -pw password
         -format ascii
```

- Korzystanie z produktu **runmqakm**:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

gdzie:

-file *nazwa_pliku*
Określa pełną nazwę pliku certyfikatu osobistego.

-db *nazwa_pliku*
Określa pełną nazwę pliku bazy danych kluczy CMS.

-pw *hasło*
Określa hasło do bazy danych kluczy CMS.

-format *ascii*
Określa format certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartość domyślna to `ascii`.

-fips
określa, że komenda jest uruchamiana 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.

Jeśli używany jest sprzęt szyfrujący, należy zapoznać się z “Otrzymywanie certyfikatu osobistego do sprzętu PKCS #11” na stronie 326.

ULW *Wyodrębnianie certyfikatu ośrodka CA z repozytorium kluczy w systemie UNIX, Linux, and Windows*

Aby wyodrębnić certyfikat ośrodka CA, należy wykonać następującą procedurę.

Użycie `strmqikm`

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** (iKeyman) nie udostępnia opcji zgodnej ze standardem FIPS.

Wykonaj następujące kroki na komputerze, na podstawie którego ma zostać wyodrębnienie certyfikatu ośrodka CA:

1. Uruchom interfejs GUI 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 CA za pomocą **runmqckm**, należy użyć następujących komend:

- W systemie UNIX, Linux, and 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`.
`-fips`	określa, że komenda jest uruchamiana 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.

ULW *Wyodrębnianie części publicznej certyfikatu samopodpisanego z repozytorium kluczy w systemie UNIX, Linux, and Windows*

Aby wyodrębnić część publiczną samopodpisanego certyfikatu, należy wykonać następującą procedurę.

Użycie strmqikm

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** (iKeyman) nie udostępnia opcji zgodnej ze standardem FIPS.

Wykonaj następujące kroki na maszynie, z której chcesz wyodrębnić część publiczną certyfikatu samopodpisanego:

1. Uruchom interfejs GUI za pomocą komendy **strmqikm** (w systemie UNIX, Linux, and 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 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** .
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 produktu **runmqckm** lub **runmqakm**, należy użyć następujących komend:

- W systemie UNIX, Linux, and 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`.

`-fips`	określa, że komenda jest uruchamiana 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.

ULW *Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie 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: Należy upewnić się, że certyfikat jest w kodowaniu ASCII (UTF-8) lub binarnym (DER), ponieważ produkt IBM Global Secure Toolkit (GSKit) nie obsługuje certyfikatów z innymi typami kodowania.

Użycie `strmqikm`

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS.

Na komputerze, na którym chcesz dodać certyfikat CA, wykonaj następujące kroki:

1. Uruchom interfejs GUI 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 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 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

Aby dodać certyfikat ośrodka CA do bazy danych kluczy, użyj jednej z następujących komend:

- Korzystanie z produktu **runmqckm**:

```
runmqckm -cert -add -db filename -pw password -label label
         -file filename -format ascii
```

- Korzystanie z produktu **runmqakm**:

```
runmqakm -cert -add -db filename -pw password -label label
         -file filename -format ascii -fips
```

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 dołączoną do certyfikatu.

-file *nazwa_pliku*
Określa nazwę pliku zawierającego certyfikat.

-format *ascii*
Określa format certyfikatu. Wartością może być `ascii` dla kodu ASCII w standardzie Base64 lub `binary` dla danych w formacie binarnym DER. Wartość domyślna to `ascii`.

-fips
określa, że komenda jest uruchamiana 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.

ULW *Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie UNIX, Linux, and Windows*

Aby wyeksportować certyfikat osobisty, należy wykonać następującą procedurę.

Użycie `strmqikm`

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** (iKeyman) nie udostępnia opcji zgodnej ze standardem FIPS.

Wykonaj następujące kroki na komputerze, z którego ma zostać wyeksportowany certyfikat osobisty:

1. Uruchom interfejs GUI 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 **runmqckm**, należy użyć następujących komend:

- W systemie UNIX, Linux, and 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.
`-fips`	określa, że komenda jest uruchamiana 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.
`-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.

ULW *Importowanie certyfikatu osobistego do repozytorium kluczy w systemie 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 systemie UNIX, Linux, and Windows” na stronie 314).

Pliki PKCS #12 powinny być uważane za tymczasowe i usunięte po użyciu.

Użycie strmqikm

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny z FIPS-em, należy użyć komendy **runmqakm** . Produkt **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS.

Wykonaj następujące kroki na komputerze, do którego ma zostać zaimportowany certyfikat osobisty:

1. Uruchom interfejs GUI 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. Istnieje możliwość zmiany etykiet importowanych certyfikatów, jeśli na przykład w docelowej bazie danych istnieje już certyfikat o tej samej etykiecie. Zmiana etykiet certyfikatów nie ma wpływu na sprawdzanie poprawności łańcucha certyfikatów. Aby powiązać certyfikat z konkretnym menedżerem kolejek lub IBM MQ MQI client, produkt IBM MQ używa wartości atrybutu **CERTLABL** (jeśli jest ustawiona) lub domyślnego `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem logowania użytkownika produktu IBM MQ MQI client , a wszystkie z małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
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 zarządzania kluczami produktu IBM zostanie ponownie wyświetlone razem z polami **Certyfikaty osobiste** i **Certyfikaty osób podpisującego** , które zostały zaktualizowane przy użyciu poprawnie oznaczonych certyfikatów.
19. Certyfikat jest importowany do docelowej bazy danych kluczy.

Za pomocą wiersza komend

Aby zaimportować certyfikat osobisty za pomocą programu **runmqckm**, należy użyć następującej komendy:

- W systemie UNIX, Linux, and 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` .
`-fips`	określa, że komenda jest uruchamiana 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.

Produkt **runmqckm** 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.

ULW *Importowanie certyfikatu osobistego z pliku Microsoft.pfx*

Wykonaj tę procedurę, aby zaimportować z pliku Microsoft.pfx w systemie UNIX, Linux, and Windows.

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 za pomocą komendy **strmqikm** . Zostanie wyświetlone okno zarządzania kluczami produktu IBM .
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 zarządzania kluczami produktu IBM . 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 zarządzania kluczami produktu IBM . 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 być wartością atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartością domyślną `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem logowania użytkownika produktu IBM MQ MQI client , wszystkimi małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
21. Kliknij przycisk **OK**. Okno Zmień etykiety zostanie teraz usunięte, a oryginalne okno zarządzania kluczami produktu IBM zostanie ponownie wyświetlone razem z panelami Certyfikaty osobiste i Certyfikaty osób podpisanych, zaktualizowanymi za pomocą poprawnie oznaczonego certyfikatu osobistego.
22. Certyfikat osobisty pfx jest teraz importowany do bazy danych (docelowej) bazy danych.

Zmiana etykiety certyfikatu za pomocą **runmqckm** lub **runmqakm**nie jest możliwa.

Za pomocą wiersza komend

Aby zaimportować certyfikat osobisty za pomocą programu **runmqckm** w systemie UNIX, Linux, and Windows, należy użyć następującej komendy:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -pfx
```

Aby zaimportować certyfikat osobisty za pomocą programu **runmqakm**, należy użyć następującej komendy:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

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` .
`-fips`	określa, że komenda jest uruchamiana 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.
`-pfx`	Wskazuje format pliku PFX.

Produkt **runmqckm** 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.

ULW *Importowanie certyfikatu osobistego z pliku #7 PKCS*

Narzędzia **strmqikm** (iKeyman) i **runmqckm** (iKeycmd) nie obsługują PKCS #7 (.p7b) plików. Narzędzie **runmqckm** służy do importowania certyfikatów z pliku #7 PKCS w systemie UNIX, Linux, and Windows.

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` .

ULW *Usuwanie certyfikatu z repozytorium kluczy w systemie UNIX, Linux, and Windows*

Ta procedura służy do usuwania certyfikatów osobistych lub certyfikatów CA.

Użycie `strmqikm`

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Produkt **strmqikm** (iKeyman) nie udostępnia opcji zgodnej ze standardem FIPS.

1. Uruchom interfejs GUI za pomocą komendy **strmqikm** (w systemie UNIX, Linux, and 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 “Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie UNIX, Linux, and Windows” na stronie 315).
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 **runmqckm**, należy użyć następujących komend:

- W systemie UNIX, Linux, and 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. 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.

ULW *Generowanie silnych haseł dla ochrony repozytorium kluczy w systemie UNIX, Linux, and Windows*

Za pomocą komendy **runmqakm** (GSKCapiCmd) 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 z poziomu **runmqckm**, **runmqakm** lub interfejsu GUI programu **strmqikm** nie jest konieczne wycena lub zmiana hasła. Nie jest to konieczne, ponieważ powłoki systemu operacyjnego nie mają wpływu na wprowadzanie danych w tych przypadkach.

ULW *Konfigurowanie sprzętu szyfrującego w systemie UNIX, Linux, and Windows*

Sprzęt szyfrujący dla menedżera kolejek lub klienta można skonfigurować na wiele sposobów.

Sprzęt szyfrujący dla menedżera kolejek można skonfigurować w systemie UNIX, Linux, and Windows przy użyciu jednej z następujących metod:

- Użyj komendy ALTER QMGR MQSC z parametrem SSLCRYP, zgodnie z opisem w sekcji ALTER QMGR.
- Za pomocą programu IBM MQ Explorer skonfiguruj sprzęt szyfrujący w systemie UNIX, Linux lub Windows . Więcej informacji na ten temat zawiera pomoc elektroniczna.

Sprzęt szyfrujący dla klienta IBM MQ można skonfigurować w systemie UNIX, Linux, and 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_PKCS11 parametru SSLCRYP, etykieta tokenu PKCS #11 musi być zgodna z etykietą, z którą skonfigurowano sprzęt.

- 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 323.

ULW *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 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:
   - Korzystanie z produktu **runmqckm**:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Korzystanie z produktu **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. (W przypadku produktu IBM MQmusi to być wartość cms.)

   -stash
   Zapisuje hasło bazy danych kluczy w pliku.

   -fips
   określa, że komenda jest uruchamiana 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, 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. Otwórz plik właściwości zabezpieczeń Java `java.security`.
   - W systemach UNIX and Linux plik właściwości zabezpieczeń Java znajduje się w podkatalogu `java/jre64/jre/lib/security` w katalogu instalacyjnym IBM MQ .
   - W systemach Windows plik właściwości zabezpieczeń Java znajduje się w podkatalogu `java\jre\lib\security` w katalogu instalacyjnym IBM MQ .

   Jeśli plik nie jest jeszcze obecny w pliku, dodaj dostawcę zabezpieczeń IBMPKCS11Impl . Na przykład, dodając następujący wiersz:

   ```
   security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
   ```
4. Uruchom interfejs użytkownika, uruchamiając komendę **strmqikm** .
5. Kliknij opcję **Plik bazy danych kluczy** > **Otwórz**.
6. Kliknij opcję **Key database type** (Typ bazy danych kluczy) i wybierz opcję **PKCS11Direct**.
7. 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 **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.
8. 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.
9. Wybierz etykietę tokenu urządzenia szyfrującego, która ma być używana do przechowywania certyfikatów.
10. W polu **Hasło tokenu szyfrującego** wpisz hasło, które zostało ustawione podczas konfigurowania sprzętu szyfrującego.
11. 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 “15” na stronie 325.

    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**.
12. 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` .
13. W polu **Położenie** wpisz ścieżkę, na przykład:

- Dla menedżera kolejek: `/var/mqm/qmgrs/QM1/ssl`
- W przypadku systemu IBM MQ MQI client: `/var/mqm/ssl`

Kliknij przycisk **OK**. Zostanie otwarte okno Password Prompt (Zapytanie o hasło).

14. Wprowadź hasło.

    Jeśli w kroku "11" na stronie 324wybrano opcję **Otwórz istniejący plik bazy danych kluczy drugorzędnych** , wpisz hasło w polu **Hasło** .

    Jeśli w kroku "11" na stronie 324wybrano 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 TLS 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).

15. Kliknij przycisk **OK**. Zostanie wyświetlona ramka treści bazy danych kluczy.

ULW *Żądanie certyfikatu osobistego dla sprzętu PKCS #11*

Aby zażądać certyfikatu osobistego dla sprzętu szyfrującego, należy użyć tej procedury w przypadku menedżera kolejek lub IBM MQ MQI client .

O tym zadaniu

W tym zadaniu opisano sposób, w jaki interfejs użytkownika produktu **strmqikm** jest używany do żądania certyfikatu osobistego. Jeśli korzystasz z interfejsu wiersza komend, patrz "Za pomocą wiersza komend" na stronie 307.

Uwaga: Produkt IBM 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 poziomu interfejsu użytkownika programu **strmqikm** (iKeyman), wykonaj następujące kroki:

1. Wykonaj kroki, które należy wykonać, aby pracować ze sprzętem szyfrującym. Patrz sekcja "Zarządzanie certyfikatami na sprzęcie PKCS #11" na stronie 323.
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 etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z dodanym identyfikatorem menedżera kolejek lub identyfikatorem zalogowanego użytkownika IBM MQ MQI client , a wszystko to małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
4. Wybierz **Wielkość klucza** i **Algorytm podpisu** , który jest wymagany.
5. 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. Więcej informacji na temat tych pól zawiera sekcja "Nazwy wyróżniające" na stronie 11.
6. W polu **Wprowadź nazwę pliku, w którym zostanie zapisane żądanie certyfikatu** zaakceptuj wartość domyślną `certreq.arm`lub wpisz nową wartość z pełną ścieżką.

7. Kliknij przycisk **OK**.

   Zostanie wyświetlone okno potwierdzenia.
8. 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 “6” na stronie 325.
9. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując ten plik do formularza żądania na stronie internetowej ośrodka CA.

ULW *Otrzymywanie certyfikatu osobistego do sprzętu PKCS #11*

Tej procedury należy użyć dla menedżera kolejek lub IBM MQ MQI client , aby otrzymać certyfikat osobisty dla sprzętu szyfrującego.

Zanim rozpoczniesz

Dodaj certyfikat ośrodka CA, który podpisał certyfikat osobisty. Dodaj go do sprzętu szyfrującego lub do dodatkowej bazy danych kluczy CMS. Należy to zrobić przed otrzymaniem podpisanego certyfikatu do sprzętu szyfrującego. Aby dodać certyfikat ośrodka CA do pliku kluczy, należy wykonać procedurę w produkcie “Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie UNIX, Linux, and Windows” na stronie 314.

Procedura

- Aby odebrać certyfikat osobisty za pomocą interfejsu użytkownika programu **strmqikm** (iKeyman), wykonaj następujące kroki:
  a) Wykonaj kroki, które należy wykonać, aby pracować ze sprzętem szyfrującym. Patrz sekcja “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 323.
  b) Kliknij opcję **Odbierz**. Zostanie otwarte okno Pobierz certyfikat z pliku.
  c) Wpisz nazwę i położenie pliku certyfikatu dla nowego certyfikatu osobistego lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
  d) 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.
  e) Kliknij przycisk **Tak** lub **Nie**. Zostanie otwarte okno Enter a Label (Wprowadzanie etykiety).
  f) 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.
- Aby odebrać certyfikat osobisty za pomocą komendy **runmqakm** (GSKCapiCmd), wykonaj następujące kroki:
  a) Otwórz okno komend, które jest skonfigurowane dla danego środowiska.
  b) Odebranie certyfikatu osobistego za pomocą komendy **runmqakm** (GSKCapiCmd):

```
runmqakm -cert -receive -file filename -crypto module_name
         -tokenlabel hardware_token -pw hardware_password
         -format cert_format -fips
         -secondaryDB filename -secondaryDBpw password
```

   gdzie:

   -file *nazwa_pliku*
   Określa pełną nazwę pliku zawierającego certyfikat osobisty.

   -crypto *nazwa_modułu*
   Określa pełną nazwę biblioteki PKCS #11 dostarczonej wraz ze sprzętem szyfrującym.

-tokenlabel ***znacznik_hardware_token***
Określa etykietę tokenu urządzenia szyfrującego PKCS #11 .

-pw ***hasło_magazynej_hardware_hasło***
Określa hasło dostępu do sprzętu szyfrującego.

-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. 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.

-secondaryDB ***nazwa_pliku***
Określa pełną nazwę pliku bazy danych kluczy CMS.

-secondaryDBpw ***hasło***
Określa hasło do bazy danych kluczy CMS.

MQ Appliance Praca z protokołem SSL/TLS w systemie IBM MQ Appliance

Produkt IBM MQ Appliance obsługuje protokół Transport Layer Security (TLS).

Produkt IBM MQ Appliance zawiera różne komendy służące do zarządzania certyfikatami. Szczegółowe informacje na temat zarządzania certyfikatami można znaleźć w dokumentacji produktu IBM MQ Appliance Zarządzanie certyfikatami TLS .

z/OS Praca z protokołem SSL/TLS w systemie z/OS

W tej sekcji opisano sposób konfigurowania i pracy z protokołem TLS (Transport Layer Security) w systemie z/OS.

Każdy temat zawiera przykłady wykonywania każdego zadania za pomocą programu RACF. Podobne zadania można wykonywać przy użyciu innych zewnętrznych menedżerów zabezpieczeń.

W systemie z/OSnależy również ustawić liczbę podzadań serwera, które są używane przez każdy menedżer kolejek na potrzeby przetwarzania wywołań TLS, zgodnie z opisem w sekcji “Ustawianie parametru SSLTASKS w systemie z/OS” na stronie 328.

Obsługa protokołu z/OS TLS jest integralną częścią systemu operacyjnego i jest znana jako *System SSL*(System SSL). Systemowa implementacja protokołu SSL jest częścią podstawowego elementu usług kryptograficznych produktu z/OS. Elementy podstawowe usług kryptograficznych są instalowane w katalogu *pdsname*. SIEALNKE partycjonowany zestaw danych (PDS). Instalując System SSL, należy wybrać odpowiednie opcje, aby udostępnić wymagane specyfikacje CipherSpecs .

z/OS *Dodatkowe wymagania dotyczące identyfikatora użytkownika dla protokołu TLS w systemie z/OS*

W tej sekcji opisano dodatkowe wymagania, które użytkownik musi skonfigurować w celu skonfigurowania protokołu TLS i pracy z nim w systemie z/OS.

Upewnij się, że w systemie są zainstalowane wszystkie odpowiednie aktualizacje typu High Impact lub Pervasive (HIPER).

Upewnij się, że zostały skonfigurowane następujące wymagania wstępne:

- Identyfikator użytkownika *ssidCHIN* jest zdefiniowany poprawnie w produkcie RACF, a identyfikator użytkownika *ssidCHIN* ma prawo do odczytu z następujących profili:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Te zmienne są zdefiniowane w klasie FACILITY RACF .

- Identyfikator użytkownika *ssidCHIN* jest właścicielem pliku kluczy.
- Certyfikat osobisty menedżera kolejek, jeśli został utworzony za pomocą komendy RACDCERT, jest tworzony z ID użytkownika o typie certyfikatu, który jest również taki sam, jak identyfikator użytkownika *ssidCHIN* .
- Inicjator kanału jest poddawany recyklingowi lub komenda **REFRESH SECURITY TYPE(SSL)** jest wydawana w celu pobrania wszystkich zmian wprowadzonych w pliku kluczy.
- Procedura inicjatora kanału produktu IBM MQ ma dostęp do biblioteki środowiska wykonawczego SSL systemu *nazwa-pdsname*.SIEALNKE za pomocą listy odsyłaczy, LPA lub instrukcji STEPLIB DD. Ta biblioteka musi być autoryzowana przez APF.
- Identyfikator użytkownika, pod którego uprawnieniami jest uruchomiony inicjator kanału, jest skonfigurowany pod kątem używania usług USS (UNIX System Services), zgodnie z opisem w dokumentacji z/OS UNIX System Services Planning (Planowanie usług systemowych).

  Użytkownicy, którzy nie chcą, aby inicjator kanału wywołał UNIX Usługi systemowe za pomocą segmentu guest/default UID i OMVS, muszą tylko modelować nowy segment OMVS w oparciu o segment domyślny, ponieważ inicjator kanału nie wymaga żadnych specjalnych uprawnień i nie jest uruchamiany w produkcie UNIX jako administrator.

z/OS *Ustawianie parametru SSLTASKS w systemie z/OS*

Użyj komendy ALTER QMGR, aby ustawić liczbę podzadań serwera na potrzeby przetwarzania wywołań TLS

Aby używać kanałów TLS, należy upewnić się, że istnieją co najmniej dwa podzadania serwera, ustawiając parametr SSLTASKS za pomocą komendy ALTER QMGR. Na przykład:

```
ALTER QMGR SSLTASKS(5)
```

Aby uniknąć problemów z przydzielaniem pamięci, nie należy ustawiać atrybutu SSLTASKS na wartość większą niż osiem w środowisku, w którym nie ma sprawdzania CRL (Certificate Revocation List).

Jeśli używane jest sprawdzanie list CRL, to w czasie trwania tej kontroli dany kanał jest wstrzymany przez dany kanał. Może to być znaczący czas, który upłynął podczas kontaktowania się z odpowiednim serwerem LDAP, ponieważ każde SSLTASK jest blokiem sterującym zadania z/OS .

Jeśli wartość atrybutu SSLTASKS zostanie zmieniona, należy zrestartować inicjator kanału.

z/OS *Konfigurowanie repozytorium kluczy w systemie z/OS*

Skonfiguruj repozytorium kluczy na obu końcach połączenia. Powiąż każde repozytorium kluczy z jego menedżerem kolejek.

Połączenie TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek musi mieć dostęp do repozytorium kluczy. Aby powiązać repozytorium kluczy z menedżerem kolejek, należy użyć parametru SSLKEYR w komendzie ALTER QMGR. Więcej informacji zawiera temat “Repozytorium kluczy SSL/TLS” na stronie 25.

W systemie z/OScertyfikaty cyfrowe są przechowywane w *pliku kluczy* , który jest zarządzany przez zewnętrzny menedżer zabezpieczeń (External Security Manager-ESM). Te certyfikaty cyfrowe mają etykiety, które wiążą certyfikat z menedżerem kolejek. Protokół TLS używa tych certyfikatów do celów uwierzytelniania. Wszystkie przykłady, które są następujące po użyciu komend RACF . Dla innych programów ESM istnieją równoważne komendy.

W systemie z/OSprodukt IBM MQ używa wartości atrybutu **CERTLABL** (jeśli jest ustawiona) lub domyślnego `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Nazwą repozytorium kluczy dla menedżera kolejek jest nazwa pliku kluczy w bazie danych produktu RACF . Nazwę pliku kluczy można określić przed utworzeniem pliku kluczy lub po jego utworzeniu.

Aby utworzyć nowy pierścień kluczy dla menedżera kolejek, należy użyć następującej procedury:

1. Upewnij się, że masz odpowiednie uprawnienia do wydawania komendy RACDCERT (więcej szczegółowych informacji zawiera publikacja *SecureWay Security Server RACF Command Language Reference*).
2. Wydaj następującą komendę:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   gdzie:

   - *userid1* to identyfikator użytkownika przestrzeni adresowej inicjatora kanału lub identyfikator użytkownika, który ma być właścicielem pliku kluczy (jeśli plik kluczy jest współużytkowany).
   - *nazwa-pierścienia* to nazwa, która ma zostać podana w pliku kluczy. Długość tej nazwy może mieć długość do 237 znaków. W tej nazwie rozróżniana jest wielkość liter. Aby uniknąć problemów, należy podać *nazwa-pierścienia* wielkimi literami.

z/OS *Udostępnianie certyfikatów CA dla menedżera kolejek w systemie z/OS*

Po utworzeniu pliku kluczy należy połączyć z nim wszystkie odpowiednie certyfikaty ośrodka CA.

Jeśli w zestawie danych znajduje się certyfikat ośrodka CA, należy najpierw dodać certyfikat do bazy danych RACF za pomocą następującej komendy:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Następnie, aby połączyć certyfikat CA dla My CA z Twoim pierścieniem kluczy, należy użyć następującej komendy:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

gdzie *userid1* jest albo identyfikatorem użytkownika inicjatora kanału, albo właścicielem współużytkowanego pliku kluczy.

Więcej informacji na temat certyfikatów CA można znaleźć w sekcji “certyfikaty cyfrowe” na stronie 10.

z/OS *Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie z/OS*

Ta procedura służy do uzyskiwania położenia pliku kluczy menedżera kolejek.

1. Wyświetl atrybuty menedżera kolejek przy użyciu jednej z następujących komend MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Sprawdź dane wyjściowe komendy w celu położenia położenia pliku kluczy.

z/OS *Określanie położenia repozytorium kluczy dla menedżera kolejek w systemie z/OS*

Aby określić położenie pliku kluczy menedżera kolejek, należy użyć komendy ALTER QMGR MQSC, aby ustawić atrybut repozytorium kluczy menedżera kolejek.

Na przykład:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

Jeśli właścicielem pliku kluczy jest przestrzeń adresowa inicjatora kanału, lub:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

Jeśli jest to współużytkowany pierścień kluczy, gdzie *userid1* jest identyfikatorem użytkownika, który jest właścicielem pliku kluczy.

z/OS *Nadawanie inicjatorowi kanału poprawnych praw dostępu w systemie z/OS*

Inicjator kanału (CHINIT) wymaga dostępu do repozytorium kluczy i do określonych profili zabezpieczeń.

Nadawanie dostępu CHINIT do odczytu repozytorium kluczy

Jeśli właścicielem repozytorium kluczy jest ID użytkownika CHINIT, ten ID użytkownika musi mieć prawo do odczytu IRR.DIGTCERT.LISTRING w klasie FACILITY i w przeciwnym razie zaktualizuj dostęp. Przyznaj dostęp za pomocą komendy PERMIT z parametrem ACCESS (UPDATE) lub ACCESS (READ), jeśli jest to właściwe:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

gdzie *id_użytkownika* jest identyfikatorem przestrzeni adresowej inicjatora kanału.

Nadawanie CHINIT czytaj dostęp do odpowiednich profili CSF*

Aby zapewnić obsługę sprzętu za pomocą narzędzia ICSF (Integrated Cryptographic Service Facility), należy upewnić się, że identyfikator użytkownika CHINIT ma prawo do odczytu odpowiednich profili CSF* w klasie CSFSERV za pomocą następującej komendy:

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

gdzie *zasob-csf* jest nazwą profilu CSF*, a *id_użytkownika* jest identyfikatorem przestrzeni adresowej inicjatora kanału.

Powtórz tę komendę dla każdego z następujących profili CSF*:

- CSFDSG
- CSFDSV
- CSFPKD
- CSFPKE
- CSFPKI

ID użytkownika CHINIT może również wymagać dostępu do odczytu do innych profili CSF*. Na przykład, jeśli używana jest specyfikacja szyfru ECDHE_RSA_AES_256_GCM_SHA384 , identyfikator użytkownika CHINIT wymaga również dostępu do odczytu do następujących profili CSF*:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

Więcej informacji na ten temat zawiera sekcja Wymagania dotyczące zasobów RACF CSFSERV.

Jeśli klucze certyfikatów są przechowywane w ICSF, a instalacja ma ustaloną kontrolę dostępu dla kluczy przechowywanych w ICSF, należy upewnić się, że identyfikator użytkownika CHINIT ma prawo do odczytu profilu w klasie CSFKEYS za pomocą następującej komendy:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

gdzie *id_użytkownika* jest identyfikatorem przestrzeni adresowej inicjatora kanału.

Korzystanie z narzędzia Integrated Cryptographic Service Facility (ICSF)

Inicjator kanału może użyć funkcji ICSF w celu wygenerowania liczby losowej podczas inicjowania algorytmu ochrony hasła w celu zacieślenia haseł przepływających przez kanały klienta, jeśli protokół TLS nie jest używany.

Więcej informacji na ten temat zawiera sekcja “Korzystanie z narzędzia Integrated Cryptographic Service Facility (ICSF)” na stronie 271

z/OS *Gdy zmiany w certyfikatach lub repozytorium kluczy staną się skuteczne w systemie z/OS*

Zmiany stają się skuteczne po uruchomieniu inicjatora kanału lub odświeżeniu repozytorium.

W szczególności, zmiany w certyfikatach w pliku kluczy i w atrybucie repozytorium kluczy stają się skuteczne przy jednej z następujących sytuacji:

- Gdy inicjator kanału jest uruchamiany lub restartowany.
- Gdy zostanie wywołana komenda REFRESH SECURITY TYPE (SSL), aby odświeżyć zawartość repozytorium kluczy.

z/OS *Tworzenie samopodpisanego certyfikatu osobistego w systemie z/OS*

Ta procedura służy do tworzenia samopodpisanego certyfikatu osobistego.

1. Wygeneruj certyfikat oraz parę kluczy publicznych i prywatnych za pomocą następującej komendy:

```
RACDCERT ID(userid2) GENCERT
SUBJECTSDN(CN('common-name')
           T('title')
           OU('organizational-unit')
           O('organization')
           L('locality')
           SP('state-or-province')
           C('country'))
WITHLABEL('label-name')
```

2. Połącz certyfikat z pierścieniem kluczy przy użyciu następującej komendy:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

gdzie:

- *userid1* to identyfikator użytkownika przestrzeni adresowej inicjatora kanału lub właściciela współużytkowanego pliku kluczy.
- *userid2* jest identyfikatorem użytkownika powiązanym z certyfikatem i musi być identyfikatorem przestrzeni adresowej inicjatora kanału.

  userid1 i *userid2* mogą być tym samym identyfikatorem.
- *nazwa-pierścienia* to nazwa, która została podana przez użytkownika w pliku “Konfigurowanie repozytorium kluczy w systemie z/OS” na stronie 328.
- *nazwa-etykiety* musi być wartością atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartością domyślną `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

z/OS *Żądanie certyfikatu osobistego w systemie z/OS*

Zastosuj się do certyfikatu osobistego przy użyciu produktu RACF.

Aby zastosować się do certyfikatu osobistego, należy użyć RACF w następujący sposób:

1. Utwórz samopodpisany certyfikat osobisty, jak w “Tworzenie samopodpisanego certyfikatu osobistego w systemie z/OS” na stronie 331. Ten certyfikat udostępnia żądanie z wartościami atrybutów dla nazwy wyróżniającej.
2. Utwórz żądanie certyfikatu PKCS #10 Base64-encoded zapisane w zestawie danych, używając następującej komendy:

   ```
   RACDCERT ID(userid2) GENREQ(LABEL(' label_name ')) DSN(' output_data_set_name ')
   ```

   where

   - *userid2* jest identyfikatorem użytkownika powiązanym z certyfikatem i musi być identyfikatorem przestrzeni adresowej inicjatora kanału.
   - *nazwa_etykiety* to etykieta używana podczas tworzenia certyfikatu samopodpisanego.

   Szczegółowe informacje można znaleźć w sekcji “Cyfrowe etykiety certyfikatów, zrozumienie wymagań” na stronie 26.
3. Wyślij zestaw danych do ośrodka certyfikacji (Certificate Authority-CA), aby zażądać nowego certyfikatu osobistego.
4. Po zwrócaniu się do użytkownika przez ośrodek certyfikacji podpisany certyfikat należy dodać go z powrotem do bazy danych RACF , korzystając z oryginalnej etykiety, zgodnie z opisem w sekcji “Dodawanie certyfikatów osobistych do repozytorium kluczy w systemie z/OS” na stronie 333.

z/OS *Tworzenie podpisanego certyfikatu osobistego RACF*

Produkt RACF może działać jako ośrodek certyfikacji i wystawiać własny certyfikat ośrodka CA.

W tej sekcji używany jest termin *certyfikat osoby podpisującej* w celu oznaczenia certyfikatu ośrodka CA wydanego przez produkt RACF.

Klucz prywatny dla certyfikatu osoby podpisującej musi znajdować się w bazie danych produktu RACF przed przeprowadzonym następującą procedurą:

1. Użyj następującej komendy, aby wygenerować certyfikat osobisty podpisany przez produkt RACF, korzystając z certyfikatu osoby podpisującej zawartego w bazie danych produktu RACF :

   ```
   RACDCERT ID(userid2) GENCERT
   SUBJECTSDN(CN('common-name')
              T('title')
              OU('organizational-unit')
              O('organization')
              L('locality')
              SP('state-or-province')
              C('country'))
   WITHLABEL('label-name')
   SIGNWITH(CERTAUTH LABEL('signer-label'))
   ```

2. Połącz certyfikat z pierścieniem kluczy przy użyciu następującej komendy:

   ```
   RACDCERT ID(userid1)
   CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
   ```

gdzie:

- *userid1* to identyfikator użytkownika przestrzeni adresowej inicjatora kanału lub właściciela współużytkowanego pliku kluczy.
- *userid2* jest identyfikatorem użytkownika powiązanym z certyfikatem i musi być identyfikatorem przestrzeni adresowej inicjatora kanału.

  userid1 i *userid2* mogą być tym samym identyfikatorem.
- *nazwa-pierścienia* to nazwa, która została podana przez użytkownika w pliku “Konfigurowanie repozytorium kluczy w systemie z/OS” na stronie 328.

- *nazwa-etykiety* musi być wartością atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartością domyślną `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek lub grupy współużytkowania kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
- *etykieta-osoby podpisującej* jest etykietą własnego certyfikatu osoby podpisującej.

z/OS *Dodawanie certyfikatów osobistych do repozytorium kluczy w systemie z/OS*

Ta procedura służy do dodawania lub importowania certyfikatu osobistego do pliku kluczy.

Po wysłaniu przez ośrodek certyfikacji nowego certyfikatu osobistego należy dodać go do pliku kluczy przy użyciu następującej procedury:

1. Dodaj certyfikat do bazy danych RACF za pomocą następującej komendy:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Połącz certyfikat z pierścieniem kluczy przy użyciu następującej komendy:

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ') RING( ring-name ) USAGE(PERSONAL))
```

gdzie:

- *userid1* to identyfikator użytkownika przestrzeni adresowej inicjatora kanału lub właściciela współużytkowanego pliku kluczy.
- *userid2* jest identyfikatorem użytkownika powiązanym z certyfikatem i musi być identyfikatorem przestrzeni adresowej inicjatora kanału.
- *nazwa-pierścienia* to nazwa, która została podana przez użytkownika w pliku “Konfigurowanie repozytorium kluczy w systemie z/OS” na stronie 328.
- *nazwa-zestawu-danych-wejściowego* to nazwa zestawu danych zawierającego podpisany certyfikat ośrodka CA. Zestaw danych musi być skatalogowany i nie może być zestawem PDS ani elementem zestawu PDS. Formatem rekordu (RECFM) oczekiwanym przez RACDCERT jest VB. RACDCERT dynamicznie przydziela i otwiera zestaw danych, a następnie odczytuje z niego certyfikat jako dane binarne.
- *nazwa-etykiety* jest nazwą etykiety, która była używana podczas tworzenia oryginalnego żądania. Musi to być wartość atrybutu IBM MQ **CERTLABL** , jeśli jest ustawiona, lub wartość domyślna `ibmWebSphereMQ` z dodanym nazwą menedżera kolejek lub grupy współużytkowania kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

z/OS *Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie z/OS*

Wyeksportuj certyfikat za pomocą komendy RACDCERT.

W systemie, z którego ma zostać wyeksportowany certyfikat, użyj następującej komendy:

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))
DSN(output-data-set-name) FORMAT(CERTB64)
```

gdzie:

- *userid2* to identyfikator użytkownika, pod którym certyfikat został dodany do pliku kluczy.
- *nazwa-etykiety* jest etykietą certyfikatu, który ma zostać wyodrębniony.
- *output-data-set-name* to zestaw danych, w którym znajduje się certyfikat.
- CERTB64 to certyfikat X.509 zakodowany w formacie DER, który jest w formacie Base64 . Można wybrać inny format, na przykład:

CERTDER
Zakodowany certyfikat X.509 w formacie binarnym

PKCS12B64
Certyfikat PKCS #12 w formacie Base64

PKCS12DER
Certyfikat PKCS #12 w formacie binarnym

z/OS *Usuwanie certyfikatu osobistego z repozytorium kluczy w systemie z/OS*

Usuń certyfikat osobisty za pomocą komendy RACDCERT.

Przed usunięciem certyfikatu osobistego można zapisać kopię tego certyfikatu. Aby skopiować certyfikat osobisty do zestawu danych przed jego usunięciem, należy postępować zgodnie z procedurą określoną w sekcji "Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie z/OS" na stronie 333. Następnie użyj następującej komendy, aby usunąć certyfikat osobisty:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

gdzie:

- *userid2* to identyfikator użytkownika, pod którym certyfikat został dodany do pliku kluczy.
- *nazwa-etykiety* jest nazwą certyfikatu, który ma zostać usunięty.

z/OS *Zmiana nazwy certyfikatu osobistego w repozytorium kluczy w systemie z/OS*

Zmień nazwę certyfikatu za pomocą komendy RACDCERT.

Jeśli nie chcesz, aby certyfikat z określoną etykietą był znaleziony, ale nie chcesz go usunąć, możesz zmienić jego nazwę tymczasowo za pomocą następującej komendy:

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

gdzie:

- *userid2* to identyfikator użytkownika, pod którym certyfikat został dodany do pliku kluczy.
- *nazwa-etykiety* to nazwa certyfikatu, którego nazwa ma zostać zmieniona.
- *new-label-name* jest nową nazwą certyfikatu.

Może to być przydatne podczas testowania uwierzytelniania klienta TLS.

z/OS *Tworzenie powiązania ID użytkownika z certyfikatem cyfrowym w systemie z/OS*

Produkt IBM MQ może używać identyfikatora użytkownika powiązanego z certyfikatem RACF jako identyfikatora użytkownika kanału. Powiąż identyfikator użytkownika z certyfikatem, instalując go pod tym identyfikatorem użytkownika lub korzystając z filtru nazwy certyfikatu.

Metoda opisana w tym temacie stanowi alternatywę dla metody niezależnej od platformy w celu powiązania identyfikatora użytkownika z certyfikatem cyfrowym, który korzysta z rekordów uwierzytelniania kanału. Więcej informacji na temat rekordów uwierzytelniania kanału zawiera sekcja "Rekordy uwierzytelniania kanału" na stronie 50.

Jeśli jednostka na jednym końcu kanału TLS odbierze certyfikat ze zdalnego połączenia, jednostka zwraca się z zapytaniem RACF , jeśli z tym certyfikatem jest powiązany identyfikator użytkownika. Jednostka używa tego identyfikatora użytkownika jako identyfikatora użytkownika kanału. Jeśli z certyfikatem nie jest powiązany żaden identyfikator użytkownika, jednostka korzysta z identyfikatora użytkownika, w ramach którego działa inicjator kanału.

Powiąż ID użytkownika z certyfikatem w jeden z następujących sposobów:

- Zainstaluj ten certyfikat w bazie danych RACF przy użyciu identyfikatora użytkownika, z którym ma zostać powiązany ten certyfikat, zgodnie z opisem w sekcji “Dodawanie certyfikatów osobistych do repozytorium kluczy w systemie z/OS” na stronie 333.
- Użyj filtru nazwy certyfikatu (Certificate Name Filter-CNF), aby odwzorować nazwę wyróżniającą podmiotu lub wystawcę certyfikatu na identyfikator użytkownika, zgodnie z opisem w sekcji “Konfigurowanie filtru nazwy certyfikatu w systemie z/OS” na stronie 335.

z/OS *Konfigurowanie filtru nazwy certyfikatu w systemie z/OS*

Użyj komendy RACDCERT, aby zdefiniować filtr nazw certyfikatów (CNF), który odwzorowuje nazwę wyróżniającą na identyfikator użytkownika.

Aby skonfigurować CNF, wykonaj następujące kroki.

1. Włącz funkcje CNF za pomocą następującej komendy. Aby wykonać tę procedurę, wymagane jest uprawnienie do aktualizacji w klasie DIGTNMAP.

```
SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
```

2. Zdefiniuj wartość CNF. Na przykład:

```
RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST
SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
```

   gdzie USER1 jest identyfikatorem użytkownika, który ma być używany, gdy:

   - Nazwa wyróżniająca podmiotu ma organizację `IBM` i kraj UK.
   - Nazwa wyróżniająca wystawcy ma organizację `ExampleCA` oraz Locality of `Internet`.

3. Odśwież odwzorowania CNF:

```
SETROPTS RACLIST(DIGTNMAP) REFRESH
```

Uwaga:

1. Jeśli rzeczywisty certyfikat jest zapisany w bazie danych RACF , identyfikator użytkownika, pod którym jest on zainstalowany, jest używany w preferencjach do identyfikatora użytkownika powiązanego z dowolnym CNF. Jeśli certyfikat nie jest zapisany w bazie danych RACF , używany jest identyfikator użytkownika powiązany z najbardziej konkretnym zgodnym CNF. Dopasowania nazwy wyróżniającej podmiotu są uważane za bardziej szczegółowe niż zgodne z nazwą wyróżniającą wystawcy.
2. Zmiany w CNF nie mają zastosowania, dopóki nie zostaną odświeżenie odwzorowań CNF.
3. Nazwa wyróżniająca jest zgodna z filtrem nazwy wyróżniającej (DN) w CNF tylko wtedy, gdy filtr nazwy wyróżniającej jest identyczny z *najmniej znaczącą częścią* nazwy wyróżniającej. Najmniej znacząca część nazwy wyróżniającej składa się z atrybutów, które zwykle są wyświetlane po prawej stronie nazwy wyróżniającej (DN), ale które są wyświetlane na początku certyfikatu.

   Na przykład należy wziąć pod uwagę wartość SDNFILTER `'O=IBM.C=UK'`. Nazwa wyróżniająca podmiotu `'CN=QM1.O=IBM.C=UK'` jest zgodna z tym filtrem, ale nazwa wyróżniająca podmiotu `'CN=QM1.O=IBM.L=Hursley.C=UK'` nie jest zgodna z tym filtrem.

   Najmniej znacząca część niektórych certyfikatów może zawierać pola, które nie są zgodne z filtrem nazw wyróżniających. Należy rozważyć wykluczenie tych certyfikatów przez określenie wzorca nazwy wyróżniającej w wzorcu SSLPEER w komendzie DEFINE CHANNEL.
4. Jeśli najbardziej konkretny zgodny element CNF jest zdefiniowany jako RACF jako NOTRUST, to jednostka używa ID użytkownika, pod którym działa inicjator kanału.
5. Produkt RACF używa znaku `'.'` jako separatora. Produkt IBM MQ używa przecinka lub średnika.

Można zdefiniować CNF, aby upewnić się, że jednostka nigdy nie ustawia identyfikatora użytkownika kanału na wartość domyślną, czyli ID użytkownika, pod którym działa inicjator kanału. Dla każdego certyfikatu ośrodka CA w pierścieniu kluczy powiązanym z jednostką należy zdefiniować parametr CNF

z obiektem IDNFILTER, który jest dokładnie zgodny z nazwą wyróżniającą podmiotu certyfikatu ośrodka CA. Zapewnia to, że wszystkie certyfikaty, które mogą być używane przez jednostkę, są zgodne co najmniej z jednym z tych plików CNF. Jest to spowodowane tym, że wszystkie tego typu certyfikaty muszą być połączone z pierścieniem kluczy powiązanym z jednostką lub muszą być wystawione przez ośrodek CA, dla którego certyfikat jest połączony z pierścieniem kluczy powiązanym z jednostką.

Więcej informacji na temat komend, które są używane do manipulowania CNF, zawiera publikacja *SecureWay Security Server RACF Security Administrator's Guide* .

z/OS *Definiowanie kanału nadawczego i kolejki transmisji na serwerze QMA w systemie z/OS*

Aby skonfigurować wymagane obiekty, należy użyć komend **DEFINE CHANNEL** i **DEFINE QLOCAL** .

Procedura

W systemie QMA wydaj komendy, takie jak w poniższym przykładzie:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Sender channel using TLS from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

Wyniki

Kanał nadawczy, TO.QMB, a kolejka transmisji-QMB, są tworzone.

z/OS *Definiowanie kanału odbiorczego w QMB w systemie z/OS*

Aby skonfigurować wymagany obiekt, należy użyć komendy **DEFINE CHANNEL** .

Procedura

W systemie QMB wydaj komendę, tak jak w poniższym przykładzie:

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS to QMB')
```

Wyniki

Kanał odbiorczy, TO.QMB, jest tworzony.

z/OS *Uruchamianie kanału nadawczego w systemie QMA w systemie z/OS*

Jeśli to konieczne, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom program nasłuchujący na QMB.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i uruchamia kanał odbiorczy, gdy jest on potrzebny. Więcej informacji na temat uruchamiania nasłuchiwania zawiera sekcja Uruchamianie programu nasłuchującego kanału.
2. Opcjonalne: Jeśli wszystkie kanały SSL/TLS zostały uruchomione wcześniej, wywołaj komendę `REFRESH SECURITY TYPE(SSL)`.

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
3. Uruchom kanał na QMA, korzystając z komendy `START CHANNEL(TO.QMB)`.

Wyniki

Kanał nadawczy został uruchomiony.

z/OS *Wymiana samopodpisanych certyfikatów w systemie z/OS*

Wymień certyfikaty, które wcześniej zostały wyodrębnione. Jeśli używany jest protokół FTP, należy użyć poprawnego formatu.

Procedura

Prześlij część ośrodka CA certyfikatu QM1 do systemu QM2 i odwrotnie, na przykład za pomocą protokołu FTP.

Jeśli certyfikaty są przesyłane za pomocą protokołu FTP, należy to zrobić w poprawnym formacie.

Prześlij następujące typy certyfikatów w formacie *binarnym* :

- Zakodowany plik binarny X.509
- PKCS #7 (certyfikaty CA)
- PKCS #12 (certyfikaty osobiste)

Prześlij następujące typy certyfikatów w formacie ASCII:

- PEM (prywatność-rozszerzona poczta)
- Base64 zakodowane X.509

z/OS *Definiowanie kanału nadawczego i kolejki transmisji na serwerze QM1 w systemie z/OS*

Aby skonfigurować wymagane obiekty, należy użyć komend **DEFINE CHANNEL** i **DEFINE QLOCAL** .

Procedura

W systemie QM1wprowadź komendy, takie jak w poniższym przykładzie:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) DESCR('Sender channel using TLS from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

Specyfikacje CipherSpecs na każdym końcu kanału muszą być takie same.

Tylko parametr SSLCIPH jest obowiązkowy, jeśli kanał ma używać protokołu TLS. Więcej informacji na temat dozwolonych wartości parametru SSLCIPH zawiera sekcja “CipherSpecs i CipherSuites w podręczniku IBM MQ” na stronie 40 .

Wyniki

Kanał nadawczy, QM1.TO.QM2i tworzona jest kolejka transmisji QM2.

z/OS *Definiowanie kanału odbiorczego na serwerze QM2 w systemie z/OS*

Aby skonfigurować wymagany obiekt, należy użyć komendy **DEFINE CHANNEL** .

Procedura

W systemie QM2wprowadź komendę, tak jak w następującym przykładzie:

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using TLS from QM1 to QM2')
```

Kanał musi mieć taką samą nazwę jak kanał nadawczy zdefiniowany przez użytkownika w produkcie “Definiowanie kanału nadawczego i kolejki transmisji na serwerze QM1 w systemie z/OS” na stronie 337i musi używać tej samej wartości CipherSpec.

z/OS *Uruchamianie kanału nadawczego w programie QM1 w systemie z/OS*

Jeśli to konieczne, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom program nasłuchujący na serwerze QM2.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i uruchamia kanał odbiorczy, gdy jest on potrzebny. Więcej informacji na temat uruchamiania nasłuchiwania zawiera sekcja Uruchamianie programu nasłuchującego kanału .
2. Opcjonalne: Jeśli wszystkie kanały SSL/TLS zostały uruchomione wcześniej, wywołaj komendę REFRESH SECURITY TYPE (SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
3. W systemie QM1uruchom kanał za pomocą komendy `START CHANNEL(QM1.TO.QM2)`.

Wyniki

Kanał nadawczy został uruchomiony.

z/OS *Odświeżanie środowiska SSL lub TLS w systemie z/OS*

Odśwież środowisko TLS w menedżerze kolejek QMA za pomocą komendy **REFRESH SECURITY** .

Procedura

W systemie QMA wprowadź następującą komendę:

```
REFRESH SECURITY TYPE(SSL)
```

Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.

z/OS *Zezwalanie na anonimowe połączenia na kanale odbiorczym w systemie z/OS*

Użyj komendy **ALTER CHANNEL** , aby włączyć uwierzytelnianie klienta SSL lub TLS jako opcjonalne.

Procedura

W systemie QMB wpisz następującą komendę:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Uruchamianie kanału nadawczego w programie QM1 w systemie z/OS*

Jeśli to konieczne, uruchom inicjator kanału, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom inicjator kanału.
2. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom program nasłuchujący na serwerze QM2.

Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i uruchamia kanał odbiorczy, gdy jest on potrzebny. Więcej informacji na temat uruchamiania nasłuchiwania zawiera sekcja Uruchamianie programu nasłuchującego kanału .

3. Opcjonalne: Jeśli inicjator kanału był już uruchomiony lub wszystkie kanały SSL/TLS zostały uruchomione wcześniej, wywołaj komendę REFRESH SECURITY TYPE (SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
4. W systemie QM1uruchom kanał za pomocą komendy `START CHANNEL(QM1.TO.QM2)`.

Wyniki

Kanał nadawczy został uruchomiony.

z/OS *Uruchamianie kanału nadawczego w systemie QMA w systemie z/OS*

Jeśli to konieczne, uruchom inicjator kanału, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom inicjator kanału.
2. Opcjonalne: Jeśli jeszcze tego nie zrobiono, uruchom program nasłuchujący na QMB.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i uruchamia kanał odbiorczy, gdy jest on potrzebny. Więcej informacji na temat uruchamiania nasłuchiwania zawiera sekcja Uruchamianie programu nasłuchującego kanału.
3. Opcjonalne: Jeśli inicjator kanału był już uruchomiony lub jeśli wszystkie kanały SSL/TLS zostały uruchomione wcześniej, wywołaj komendę `REFRESH SECURITY TYPE(SSL)`.

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
4. Uruchom kanał na QMA, korzystając z komendy `START CHANNEL(TO.QMB)`.

Wyniki

Kanał nadawczy został uruchomiony.

z/OS *Modyfikowanie długości klucza krzywej eliptycznej w systemie z/OS*

Sposób modyfikowania zmiennej środowiskowej GSK_CLIENT_ECURVE_LIST w celu ustawienia listy krzywych eliptycznych lub obsługiwanych grup określonych przez klienta jako łańcucha składającego się z co najmniej jednej wartości 4-znakowej w kolejności preferencji do użycia.

Ważne: You must apply the fix in z/OS APAR OA61783 to permit certain elliptic curves to be made effective by the operating system, when using TLS 1.0, TLS 1.1 and/or TLS 1.2 negotiated connections.

Tę zmienną środowiskową TLS można ustawić w kodzie JCL uruchamiania inicjatora kanału, korzystając z instrukcji CEEOPTS DD:

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

W zbiorze danych przywoływanym powyżej określ listę, która ma być używana, na przykład:

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

Ważne: Nie należy używać tej instrukcji CEEOPTS z danymi w strumieniu, ponieważ zapobiega to ustawieniu zmiennej środowiskowej dla wszystkich zadań TLS korzystających z tej instrukcji.

Upewnij się, że jest używany sekwencyjny zbiór danych lub podzbiór partycjonowanego zestawu danych, aby umożliwić to pracę, gdy wartość SSLTASKS jest większa niż jeden.

Można również użyć analogowego odpowiednika serwera GSK_CLIENT_ECURVE_LIST, który jest parametrem GSK_SERVER_ALLOWED_KEX_ECURVES. Więcej informacji na ten temat zawiera sekcja Ograniczanie krzywych eliptycznych eliptycznych .

Ponadto w tabeli 5 w sekcji Definicje zestawów algorytmów szyfrowania znajduje się lista poprawnych 4-znakowych krzywych eliptycznych i obsługiwanych specyfikacji grup.

Specyfikacja domyślna to `00210023002400250019`. Jeśli protokół TLS V1.3 jest włączony, program `0029` (`x25519`) jest dodawany na końcu listy domyślnej.

Identyfikowanie i uwierzytelnianie użytkowników

Użytkownik może zidentyfikować i uwierzytelnić użytkowników za pomocą certyfikatów X.509 , struktury MQCSP lub kilku typów programu obsługi wyjścia użytkownika.

Korzystanie z certyfikatów X.509

Użytkownicy mogą identyfikować i uwierzytelniać użytkowników za pomocą certyfikatów x.509 z komendą **CHLAUTH** i parametrem **SSLPEER** . Parametr **SSLPEER** określa filtr, który ma być używany do porównania z nazwą wyróżniającą podmiotu certyfikatu pochodzącego od menedżera kolejek węzła sieci lub klienta na drugim końcu kanału.

Więcej informacji na temat korzystania z komendy **CHLAUTH** i parametru **SSLPEER** zawiera sekcja SET CHLAUTH.

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.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP dla aplikacji klienckiej zostanie wysłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienta są odpowiednio chronione, należy zapoznać się z “Ochrona hasłem protokołu MQCSP” na stronie 30.

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 IBM MQ . W takiej sytuacji uwierzytelnianie wzajemne ma miejsce między dwoma menedżerami kolejek lub między menedżerem kolejek a użytkownikiem aplikacji IBM MQ MQI client .

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 w systemie Windows” na stronie 156.

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.

Transport Layer Security (TLS) korzysta z technik PKI, takich jak te opisane. Więcej informacji na temat sposobu uwierzytelniania przez protokół TLS zawiera sekcja “Pojęcia związane z protokołem 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 462. 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 120.

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 347.

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.

Metoda uwierzytelniania wtyczki (Pluggable Authentication Method-PAM)

Linux UNIX

PAM jest obecnie powszechnie spotykany na platformach UNIX and Linux i udostępnia ogólny mechanizm, który ukrywa szczegóły uwierzytelniania użytkowników z usług.

Różne reguły uwierzytelniania mogą być używane dla różnych usług, konfigurując reguły, bez konieczności modyfikowania samych usług.

Więcej informacji na ten temat zawiera sekcja "Korzystanie z metody PAM (Pluggable Authentication Method)" na stronie 360.

Użytkownicy uprzywilejowani

Użytkownik uprzywilejowany jest użytkownikiem, który ma pełne uprawnienia administracyjne dla produktu IBM MQ.

Oprócz użytkowników wymienionych w poniższej tabeli, istnieją pewne obiekty i autoryzacje, dla których należy zachować szczególną ostrożność przy przyznawaniu dostępu, w celu zapewnienia integralności i bezpieczeństwa menedżera kolejek. Przy przyznawaniu którejkolwiek z następujących pozwoleń należy stosować dodatkową kontrolę:

- Autoryzacje dla obiektów SYSTEM
- Uprawnienia administracyjne do tworzenia, zmieniania i usuwania obiektów.

  z/OS W systemie z/OSuprawnienie to jest zabezpieczeniem komend i uprawnieniem do zarządzania zasobami komendy w celu wydawania komend DEFINE, ALTER i DELETE.

  Multi Na wszystkich innych platformach autoryzacje te są autoryzacjami administracyjnymi, takimi jak `+crt`, `+chg` i `+dlt`.
- Autoryzacja administracyjna do czyszczenia kolejek.

  z/OS W systemie z/OSuprawnienie to jest zabezpieczeniem komend i uprawnieniem do zarządzania zasobami komendy w celu wydawania komend CLEAR.

  Multi Na wszystkich innych platformach autoryzacja ta to `+clr`.
- Autoryzacje administracyjne służące do zatrzymywania kanałów, wycofanych lub zatwierdzania komunikatów.

  z/OS W systemie z/OSuprawnienie to jest zabezpieczeniem komend i uprawnieniem do zarządzania zasobami komendy w celu wydawania komend, takich jak RESET CHANNEL, START CHANNEL i STOP CHANNEL.

  Multi Na wszystkich innych platformach autoryzacje te to `+ctrl` i `+ctrlx`.
- Alternatywna autoryzacja MQI użytkownika, która umożliwia aplikacjom eskalowanie uprawnień do sprawdzania autoryzacji.

  z/OS W systemie z/OSta autoryzacja to wszelkie uprawnienia nadane alternatywnym profilom bezpieczeństwa użytkownika.

  Multi Na wszystkich innych platformach autoryzacja ta to `+altusr`.
- Autoryzacje kontekstowe, które umożliwiają aplikacjom zmianę kontekstu zabezpieczeń komunikatów.

z/OS W systemie z/OSta autoryzacja to wszelkie uprawnienia nadane profilom zabezpieczeń kontekstu.

Multi Na wszystkich innych platformach autoryzacje te to `+setall` i `+setid`.

Jako ogólne główne aplikacje przesyłania komunikatów powinny być nadawane tylko podstawowe autoryzacje MQI do kolejek lub tematów, które są potrzebne. Kanały MCA, które są wykonywane z użyciem nieuprawnionego użytkownika MCAUSER i niektórych innych specjalnych typów aplikacji, takich jak procedury obsługi kolejek niedostarczonych komunikatów, mogą wymagać dodatkowych autoryzacji, które nie są zwykle nadawane aplikacjom w celu poprawnego działania.

Tabela 67. Użytkownicy uprzywilejowani według platformy

Platforma	Użytkownicy uprzywilejowani
Systemy Windows	• SYSTEM • Członkowie grupy mqm • Członkowie grupy Administratorzy
Systemy UNIX and Linux	• Członkowie grupy mqm
IBM i IBM i Systemy IBM i	• Profile qmqm i qmqmadm • Wszyscy członkowie grupy qmqmadm • Każdy użytkownik zdefiniowany z ustawieniem *ALLOBJ
z/OS	Identyfikator użytkownika, pod którym uruchomione są przestrzenie adresowe inicjatora kanału, menedżera kolejek i zaawansowanych zabezpieczeń komunikatów. Te identyfikatory użytkowników nie mają automatycznie pełnych uprawnień administracyjnych dla produktu IBM MQ, ale są traktowane jako uprzywilejowane ze względu na poziom dostępu, który jest zwykle nadawany tym identyfikatorom użytkowników.

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, które mogą być używane przez usługę autoryzacji do identyfikowania i uwierzytelniania użytkownika.

Istnieje możliwość zmiany protokołu MQCSP w wyjściu zabezpieczeń.

Ostrzeżenie: W niektórych przypadkach hasło w strukturze MQCSP aplikacji klienckiej będzie przesyłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienckiej są odpowiednio chronione, należy zapoznać się z sekcją “Ochrona hasłem protokołu MQCSP” na stronie 30.

Relacja między ustawieniami MQCSP i AdoptCTX

Produkt IBM MQ zawsze uwierzytelnia referencje przekazywane za pośrednictwem struktury MQCSP, chyba że funkcja uwierzytelniania połączenia nie jest włączona. Po pomyślnym uwierzytelnieniu informacji autoryzacyjnych program IBM MQ próbuje adoptować ID użytkownika na potrzeby przyszłych sprawdzeń autoryzacji, chyba że opcja adoptowania TCTX nie jest włączona.

Produkt IBM MQ ma limit długości identyfikatorów użytkowników, które mogą być sprawdzane przez użytkownika w celu autoryzacji. Te limity są szczegółowo opisane w sekcji “Identyfikatory użytkownika”

na stronie 84. Podczas adoptowania identyfikatora użytkownika przekazywanego za pośrednictwem struktury MQCSP IBM MQ zachowanie jest różne w zależności od innych opcji konfiguracyjnych:

- Jeśli używane jest uwierzytelnianie połączenia LDAP, program IBM MQ pobiera wartość pola ustawioną w programie SHORTUSR z rekordu LDAP tego użytkownika i adoptuje ten identyfikator użytkownika.

  Na przykład, jeśli parametr SHORTUSR jest ustawiony na `'CN'` i rekord LDAP zawiera użytkownika o nazwie `'CN=Test,SN=MQ,O=IBM,C=UK'`, używany jest identyfikator użytkownika `Test` .
- W przypadku używania uwierzytelniania połączenia z systemem operacyjnym lub uwierzytelniania PAM, jeśli parametr ADOPTCTX ma wartość YES, identyfikator użytkownika przekazywany przez strukturę MQCSP jest obcinany w celu spełnienia 12-znakowego limitu identyfikatora użytkownika (IBM MQ) podczas adoptowania jako kontekst połączenia.

  Jeśli opcja **ChlAuthEarlyAdopt** jest włączona, obcięcie jest wykonywane po uwierzytelnieniu informacji autoryzacyjnych użytkownika.

  Jeśli opcja **ChlAuthEarlyAdopt** nie jest włączona, obcięcie jest wykonywane przed adopcją. W systemie Windows, jeśli użytkownik jest podany w formacie `user@domain`, oznacza to, że obcięcie może spowodować, że specyfikacja domeny nie będzie poprawna, jeśli użytkownik będzie mieć mniej niż 12 znaków.

  Jeśli na przykład użytkownik `` `ibmmq@windowsdomain` `` jest udostępniany za pośrednictwem protokołu MQCSP, w tym scenariuszu jest on obcinany do wartości `` `ibmmq@window` `` . Powoduje to następujący błąd:

  ```
  AMQ8074W: Autoryzacja nie powiodła się, ponieważ identyfikator SID 'SID' nie jest zgodny z jednostką 'ibmmq@window'
  ```

  Na tej podstawie, jeśli identyfikator użytkownika jest dłuższy niż 12 znaków, na przykład identyfikator użytkownika domeny Windows w postaci `user@domain`, za pośrednictwem protokołu MQCSP należy skonfigurować parametr **ChlAuthEarlyAdopt**=*Y* w pliku qm.ini , aby uniknąć tego błędu.

  Alternatywnie można użyć parametru AdteTCTX (NO) w konfiguracji CONNAUTH AUTHINFO i zastosować alternatywne podejście, takie jak reguła CHLAUTH USERMAP, wyjście zabezpieczeń lub ustawienie MCAUSER obiektu kanału, aby ustawić identyfikator użytkownika dla kanału.

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 IBM MQ MQI client . W takiej sytuacji uwierzytelnianie wzajemne ma miejsce między dwoma menedżerami kolejek lub między menedżerem kolejek a użytkownikiem aplikacji IBM MQ MQI client .

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 w systemie Windows” na stronie 156.

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.

Transport Layer Security (TLS) korzysta z technik PKI, takich jak te opisane. Więcej informacji na temat sposobu uwierzytelniania przez protokół Secure Sockets Layer zawiera sekcja “Pojęcia związane z protokołem 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 462. 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 120.

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 347.

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 TLS 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).

Na następujących platformach obsługa SSL produktu IBM MQ sprawdza odwołane certyfikaty 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.

- 

Linux
- 

UNIX
- 

Windows

Produkty IBM MQ classes for Java i IBM MQ classes for JMS nie mogą używać informacji OCSP z pliku tabeli definicji kanału klienta. Można jednak skonfigurować protokół OCSP w sposób opisany w sekcji Korzystanie z protokołu Online Certificate Protocol.

Na następujących platformach i IBM MQ obsługa protokołu SSL sprawdza odwołane certyfikaty przy użyciu list CRL i ARL tylko na serwerach LDAP:

- 

IBM i
- 

z/OS

Więcej informacji na temat ośrodków certyfikacji zawiera sekcja “certyfikaty cyfrowe” na stronie 10.

Sprawdzanie OCSP/CRL

Sprawdzanie protokołu OCSP (Online Certificate Status Protocol) /Certificate Revocation List (CRL) jest wykonywane na zdalnych certyfikatach przychodzących. Proces sprawdza cały łańcuch związany z certyfikatem osobistym systemu zdalnego, aż do jego certyfikatu głównego.

Użycie komendy openSSL w celu sprawdzenia poprawności OCSP

Jeśli w przedsiębiorstwie używany jest protokół openSSL w celu sprawdzenia poprawności protokołu OCSP, a następnie podjęta zostanie próba użycia połączenia z pakietem GSKit TLS, zostanie wyświetlone ostrzeżenie o statusie UNKNOWN.

Dzieje się tak dlatego, że wszystkie certyfikaty w łańcuchu, oprócz katalogu głównego, są sprawdzane przez pakiet GSKit w celu uzyskania statusu odwołania. Operacja GSKit jest zgodna z dokumentem RFC 5280 i jest to opisane w strategii Trust Policy (Trust Policy) pakietu GSKit. Algorytm GSKit próbuje uzyskać wszystkie dostępne źródła informacji o cofnięciu, zgodnie z opisem w dokumencie RFC 5280 i strategii Trust Policy (Trust Policy) pakietu GSKit.

W jaki sposób sprawdzanie OCSP/CRL działa w produkcie IBM MQ?

Produkt IBM MQ obsługuje dwa mechanizmy sterowania zachowaniem podczas sprawdzania certyfikatów na podstawie nazwanych punktów końcowych OCSP lub CRL, albo w rozszerzeniu certyfikatu, albo w sposób zdefiniowany w obiektach AUTHINFO:

- Atrybuty **OCSPCheckExtensions**, **CDPCheckExtensions**i **OCSPAuthentication** w sekcji SSL sekcji pliku qm.ini, oraz
- Korzystanie z parametru SSLCRLNL menedżera kolejek oraz konfiguracji protokołu AUTHINFO OCSP i CRLLDAP. Więcej informacji na ten temat zawiera sekcja ALTER AUTHINFO i ALTER QMGR .

Ostrzeżenie:

Komenda ALTER AUTHINFO z produktem **AUTHTYPE(OCSP)** nie jest stosowana do użycia w menedżerach kolejek produktu IBM i lub z/OS . Można go jednak określić na tych platformach, które mają zostać skopiowane do tabeli definicji kanału klienta (CCDT) w celu użycia klienta.

Atrybuty sekcji SSL w produkcie **OCSPCheckExtensions** i **CDPCheckExtensions** kontrolują, czy program IBM MQ będzie weryfikował certyfikat dla serwera OCSP lub CRL w rozszerzeniu AIA certyfikatu.

Jeśli ta opcja nie jest włączona, nie zostanie nawiązany kontakt z serwerem OCSP lub CRL w rozszerzeniu certyfikatu.

Jeśli serwery OCSP lub CRL są szczegółowo opisane za pomocą obiektów AUTHINFO i odwołują się do niego za pomocą atrybutu SSLCRLNL **QMGR** , podczas przetwarzania odwołań certyfikatów program IBM MQ próbuje skontaktować się z tymi serwerami.

Ważne: Na liście nazw SSLCRLNL może być zdefiniowany tylko jeden obiekt OCSP AUTHINFO.

Jeśli:

OCSPCheckExtensions= NO i **CDPCheckExtensions**=*NO* są ustawione, a
W obiektach AUTHINFO nie zdefiniowano żadnych serwerów OCSP ani CRL

nie jest wykonywane sprawdzanie odwołań certyfikatów.

Podczas weryfikowania certyfikatu dla jego statusu odwołania produkt IBM MQ kontaktuje się z serwerami OCSP lub CRL nazwanymi w następującej kolejności, jeśli są włączone:

1. Serwer OCSP jest szczegółowo opisany w obiekcie **AUTHTYPE(OCSP)** i jest przywoływany w atrybucie SSLCRLNL **QMGR** .
2. Serwery OCSP szczegółowe w rozszerzeniu AIA certyfikatów, jeśli **OCSPCheckExtensions**=*YES*.
3. Serwery CRL szczegółowe w rozszerzeniu **CRLDistributionPoints** certyfikatów, jeśli **CDPCheckExtensions** =*YES*.
4. Wszystkie serwery CRL znajdujące się w obiektach **AUTHINFO(CRLLDAP)** i odwołują się do nich w atrybucie SSLCRLNL **QMGR** .

Podczas weryfikowania certyfikatu, jeśli wynik kroku na serwerze OCSP lub serwerze CRL zwraca ostateczną odpowiedź REVOKED lub VALID na zapytanie dla certyfikatu, nie są wykonywane żadne dodatkowe sprawdzenia, a status certyfikatu, który jest prezentowany, jest używany do określenia, czy ma on być zaufany, czy nie.

Jeśli serwer OCSP lub serwer CRL zwróci wynik działania UNKNOWN, przetwarzanie będzie kontynuowane do czasu, aż serwer OCSP lub CRL zwróci wynik ostateczny lub wszystkie opcje zostaną wyczerpane.

Zachowanie tego, czy certyfikat został uznany za odwołany, czy jego status nie może być określony, jest inny dla serwerów OCSP i CRL:

- W przypadku serwerów CRL, jeśli nie można uzyskać listy CRL, certyfikat jest uznawany za NOT_REVOKED
- W przypadku serwerów OCSP, jeśli nie można uzyskać statusu odwołania z nazwanego serwera OCSP, to zachowanie jest kontrolowane za pomocą atrybutu **OCSPAuthentication** w sekcji SSL Stanza pliku qm.ini .

  Atrybut ten można skonfigurować w taki sposób, aby blokować połączenie, zezwalać na połączenie lub zezwalać na połączenie z komunikatem ostrzegawczym.

Jeśli jest to konieczne, można użyć atrybutu **SSLHTTPProxyName**=*string* w sekcji SSL w plikach qm.ini i mqclient.ini w celu sprawdzenia OCSP. Łańcuch jest nazwą hosta lub adresem sieciowym serwera proxy HTTP, który ma być używany przez pakiet GSKit do sprawdzania protokołu OCSP.

W programie IBM MQ 9.1.5 można ustawić wartość **OCSPTimeout** w sekcji SSL plików `qm.ini` lub `mqclient.ini` , która ustawia liczbę sekund oczekiwania na odpowiedź OCSP podczas sprawdzania odwołania.

ULW Unieważnione certyfikaty i protokół OCSP

Produkt IBM 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 mają zastosowanie tylko do produktu IBM MQ w systemach UNIX, Linux, and Windows .

Aby sprawdzić status odwołania certyfikatu cyfrowego za pomocą protokołu OCSP, produkt IBM MQ może użyć dwóch metod, aby określić, który moduł odpowiadający OCSP ma 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 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 MQ nie może uzyskać dostępu do programu odpowiadającego OCSP.

- Program odpowiadający OCSP wysłał odpowiedź, lecz produkt IBM MQ nie może zweryfikować podpisu cyfrowego odpowiedzi.
- Program odpowiadający OCSP wysłał odpowiedź, która wskazuje, że nie ma danych odwołania dla certyfikatu.

Jeśli produkt IBM MQ odbierze wynik OCSP `Nieznany`, jego zachowanie zależy od ustawienia atrybutu OCSPAuthentication. W przypadku menedżerów kolejek ten atrybut jest wstrzymany w jednej z następujących lokalizacji:

- Linux UNIX W sekcji SSL pliku `qm.ini` w systemie UNIX and Linux.
- Windows W rejestrze Windows .

Ten atrybut można ustawić za pomocą IBM MQ Explorer. W przypadku klientów atrybut ten jest wstrzymany w sekcji SSL pliku konfiguracyjnego klienta.

Jeśli zostanie odebrany wynik `Nieznany` i atrybut OCSPAuthentication ma ustawioną wartość REQUIRED (domyślna), produkt IBM 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 ma ustawioną wartość OPTIONAL, produkt IBM 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 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 takim przypadku nie ma potrzeby konfigurowania dodatkowego certyfikatu. Kroki, które zostały już podjęte w celu nawiązania połączenia TLS, są wystarczające do zweryfikowania 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, który go podpisał (i że certyfikat jest podpisany przez ośrodek CA, który jest już zaufany dla połączeń TLS), 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 programu odpowiadającego OCSP do bazy danych kluczy klienta lub menedżera kolejek, który wykonuje sprawdzanie protokołu OCSP ; patrz “Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie UNIX, Linux, and Windows” na stronie 314 . Certyfikat CA jest domyślnie dodawany jako zaufany certyfikat główny, co jest ustawieniem wymaganym w tym kontekście. Jeśli ten certyfikat nie zostanie dodany, program IBM MQ nie może zweryfikować podpisu cyfrowego w odpowiedzi OCSP, a wyniki sprawdzenia OCSP są nieznane, co może spowodować zamknięcie kanału IBM MQ w zależności od wartości uwierzytelniania OCSPAuthentication.

Protokół OCSP (Online Certificate Status Protocol) w aplikacjach klienckich Java i JMS

Z powodu ograniczenia interfejsu API produktu Java produkt IBM MQ może korzystać z sprawdzania odwołań certyfikatów protokołu OCSP (Online Certificate Status Protocol) w przypadku bezpiecznych gniazd TLS tylko wtedy, gdy protokół OCSP jest włączony dla całego procesu maszyny wirtualnej Java (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.
- Użyj interfejsu java.security.Security.setProperty() Interfejs API podlega dowolnej strategii produktu Java Security Manager.

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 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

Nazwa właściwości	Opis
	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 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 skutki uboczne, gdy wirtualna maszyna języka Java jest współużytkowana z innym kodem aplikacji, który korzysta z bezpiecznych gniazd 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 zachować ostrożność podczas stosowania poprawek tymczasowych produktu Java i konserwacji produktu, aby uniknąć 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()`.
- Jeśli używany jest interfejs Interceptor AMS Java opisany w sekcji Włączanie sprawdzania OCSP w przechwytywaniach rodzimych, należy unikać używania konfiguracji protokołu OCSP java.security , która jest w konflikcie z konfiguracją protokołu OCSP AMS w pliku konfiguracyjnym magazynu kluczy.

Praca z listami odwołań certyfikatów i listami odwołań uprawnień

Obsługa IBM MQ dla list CRL i ARL jest różna w zależności od platformy.

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 IBM MQ przechowuje pamięć podręczną list CRL i ARL, do których dostęp uzyskano w ciągu ostatnich 12 godzin.

Gdy menedżer kolejek lub IBM MQ MQI client odbiera certyfikat, sprawdza ona listę CRL, aby potwierdzić, że certyfikat jest nadal ważny. IBM MQ najpierw sprawdza w pamięci podręcznej, czy jest w niej pamięć

podręczna. Jeśli lista CRL nie znajduje się w pamięci podręcznej, program IBM MQ interroguje położenia serwera CRL LDAP w kolejności, w jakiej występują na liście nazw obiektów informacji uwierzytelniających określonych za pomocą atrybutu *SSLCRLNL* , dopóki IBM MQ nie znajdzie dostępnej listy CRL. Jeśli lista nazw nie jest określona lub jest określona z pustą wartością, listy CRL nie są sprawdzane.

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 IBM MQ TLS dane binarne dla tych atrybutów muszą być zgodne z formatem DER (Definite Encoding Rules). Więcej informacji na temat plików LDIF znajduje się w dokumentacji dostarczonej wraz z serwerem LDAP.

Rysunek 20 na stronie 354 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 produkcie IBM.

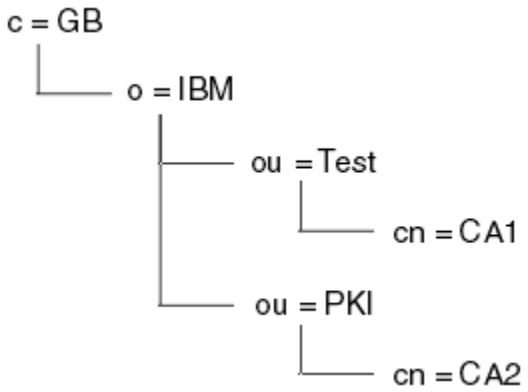
```
dn: o=IBM, c=GB
o: IBM
objectclass: top
objectclass: organization

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 20. Przykładowy plik LDIF dla ośrodka certyfikacji. Może to różnić się od implementacji do implementacji.

Rysunek 21 na stronie 355 przedstawia strukturę DIT, która jest tworzona przez serwer LDAP podczas ładowania przykładowego pliku LDIF, który jest wyświetlany w produkcie Rysunek 20 na stronie 354 razem z podobnym plikiem dla CA2, wyimaginowanym Urzędem certyfikacji, który jest skonfigurowany przez organizację PKI, również w produkcie IBM.



Rysunek 21. Przykład struktury drzewa informacji katalogu LDAP

Program 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. Program 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 z plików utworzonych w kroku “2” na stronie 355.

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. IBM i IBM MQ na IBM i zachowuje się inaczej niż inne platformy.

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 *SSLCRLNL* .

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. IBM i W systemie IBM imożna również użyć komendy CL CRTMQMAUTI.

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 zawierać identyczne informacje. Zapewnia to ciągłość usługi, jeśli jeden lub więcej serwerów LDAP nie powiedzie się.

z/OS Dodatkowo, tylko w systemie z/OS , dostęp do wszystkich serwerów LDAP musi być uzyskiwany za pomocą tego samego identyfikatora użytkownika i hasła. Identyfikator użytkownika i hasło są określone w pierwszym obiekcie AUTHINFO na liście nazw.

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. z/OS W systemie z/OSupewnij się, że atrybut NLTYPE namelist jest ustawiony na wartość AUTHINFO.
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 *SSLCRLNL*. Wartość początkowa menedżera kolejek dla tego atrybutu jest pusta.

IBM i W systemie IBM imożna określić obiekty informacji uwierzytelniających, ale menedżer kolejek nie używa ani obiektów informacji uwierzytelniających, ani listy nazw obiektów informacji uwierzytelniającej. Tylko klienty IBM MQ , które korzystają z tabeli połączeń klienta wygenerowanej przez menedżer kolejek produktu IBM i , używają informacji uwierzytelniających określonych dla tego menedżera kolejek produktu IBM i . Atrybut menedżera kolejek *SSLCRLNL* w systemie IBM i określa, jakie informacje uwierzytelniające są używane przez klientów. Informacje na temat uzyskiwania dostępu do list CRL zawiera “Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i” na stronie 356 kolejek produktu IBM i .

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.

IBM i *Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i*

Ta procedura służy do uzyskiwania dostępu do list CRL lub ARL w systemie IBM i.

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 położenie listy CRL dla konkretnego certyfikatu w systemie IBM i, wykonaj następujące kroki:

1. Uzyskaj dostęp do interfejsu programu DCM, zgodnie z opisem w sekcji “Dostęp do DCM” na stronie 282.
2. W kategorii zadań **Zarządzaj położeniami CRL** na panelu nawigacyjnym kliknij opcję **Dodaj położenie CRL**. Strona Zarządzanie położeniami CRL jest wyświetlana w ramce zadań.
3. W polu **Nazwa położenia listy CRL** wpisz nazwę położenia listy CRL, na przykład LDAP `Server #1` .
4. W polu **Serwer LDAP** wpisz nazwę serwera LDAP.
5. W polu **Use Secure Sockets Layer (SSL)** (Użyj protokołu SSL) wybierz opcję **Yes** (Tak), jeśli chcesz połączyć się z serwerem LDAP za pomocą protokołu TLS. W przeciwnym razie wybierz opcję **Nie**.
6. W polu **Port Number** (Numer portu) wpisz numer portu dla serwera LDAP, na przykład 389.
7. Jeśli serwer LDAP nie zezwala użytkownikom anonimowym na wysyłanie zapytań do katalogu, wpisz nazwę wyróżniającą logowania dla serwera w polu **Nazwa wyróżniająca logowania** .

8. Kliknij przycisk **OK**. Program DCM informuje, że utworzył położenie listy CRL.
9. Na panelu nawigacyjnym kliknij opcję **Wybierz bazę certyfikatów**(Select a Certificate Store). W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów.
10. Zaznacz pole wyboru **Inny system certyfikatów systemowych** i kliknij przycisk **Kontynuuj**. Zostanie wyświetlona strona Baza certyfikatów i hasło.
11. W polu **Ścieżka i nazwa pliku bazy certyfikatów** (Certificate store path and filename) wpisz ścieżkę i nazwę pliku IFS, który został ustawiony podczas “Tworzenie bazy certyfikatów w systemie IBM i” na stronie 283.
12. Wpisz hasło w polu **Hasło bazy certyfikatów** . Kliknij przycisk **Kontynuuj**. W ramce zadań zostanie wyświetlona strona Bieżąca baza certyfikatów.
13. W kategorii zadań **Zarządzanie certyfikatami** na panelu nawigacyjnym kliknij opcję **Aktualizuj przypisanie położenia CRL**. Strona Przypisanie położenia CRL jest wyświetlana w ramce zadania.
14. Wybierz przełącznik dla certyfikatu ośrodka CA, do którego ma zostać przypisana lokalizacja CRL. Kliknij opcję **Aktualizuj przypisanie położenia CRL**. Strona Aktualizacja przypisania położenia CRL jest wyświetlana w ramce zadania.
15. Wybierz przełącznik dla położenia CRL, które ma zostać przypisane do certyfikatu. Kliknij opcję **Aktualizuj przypisanie**. Program DCM informuje, że został on zaktualizowany.

Należy pamiętać, że program DCM umożliwia przypisanie innego serwera LDAP przez ośrodek certyfikacji.

Uzyskiwanie dostępu do list CRL i ARL za pomocą IBM MQ Explorer
Można użyć programu IBM MQ Explorer w celu poinformowania menedżera kolejek, w jaki sposób mają uzyskać 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 Lista 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 357) na listę.
   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. Wpisz nazwę listy nazw (z kroku “3.a” na stronie 357) w polu **Lista nazw CRL** .

Uzyskiwanie dostępu do list CRL i ARL z IBM MQ MQI client

Dostępne są trzy opcje określania serwerów LDAP, które przechowują listy CRL służące do sprawdzania przez IBM MQ MQI client.

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 IBM MQ MQI client działającego na serwerze Linux (platforma zSeries).

Położenie respondera OCSP i serwerów LDAP, które przechowują listy CRL
W systemie IBM MQ MQI client 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, opisywane w tym miejscu w kolejności malejącej kolejności wykonywania.

IBM i Informacje na temat produktu IBM izawiera sekcja Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i.

Gdy aplikacja IBM MQ MQI client 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, które wymaga IBM MQ MQI client w celu 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 program IBM MQ MQI client mógł uzyskać dostęp do serwera odpowiadającego OCSP lub do serwerów 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.

z/OS IBM i Obiekt informacji uwierzytelniającej o typie AUTHTYPE (OCSP) nie jest stosowany do użycia w menedżerach kolejek produktu IBM i lub z/OS , ale można go określić na tych platformach, które mają być kopiowane do tabeli definicji kanału klienta (CCDT) w celu użycia klienta.

Aby umożliwić IBM MQ MQI client 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:

Multi

Na platformach serwerowych AIX, Linux, IBM i, Solarisi Windows

Istnieje możliwość zdefiniowania listy nazw zawierającej nazwy jednego lub większej liczby obiektów informacji uwierzytelniających. Następnie można ustawić atrybut menedżera kolejek (**SSLCRLNL**) 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 jest niedostępny, jeśli jest on wymagany, IBM MQ MQI client 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, **SSLCRLNL**, 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 klienckiego jako plik współużytkowany lub jeśli w systemie klienta jest kopiowana aplikacja CCDT, IBM MQ MQI client w tym systemie może użyć położenia odwołania certyfikatu w tabeli definicji kanału klienta w celu uzyskania dostępu do serwerów odpowiadających za pomocą protokołu OCSP lub serwera LDAP, w których znajdują się 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 **SSLCRLNL**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.
4. Na komputerze klienckim można użyć komendy **runmqsc** z parametrem **-n** .

Multi

Na platformach klienckich AIX, Linux, IBM i , Solarisi Windows

Tabelę CCDT na komputerze klienta można zbudować za pomocą komendy runmqsc z parametrem **-n** i obiektami **DEFINE AUTHINFO** w pliku CCDT. Kolejność, w jakiej obiekty są zdefiniowane, jest porządkiem, w którym są one używane w pliku. Nazwy, które mogą być używane w obiekcie **DEFINE AUTHINFO** , nie są zachowywane w pliku. W przypadku **DISPLAY** obiektów **AUTHINFO** w pliku CCDT używane są tylko liczby pozycyjne.

Uwaga: Jeśli zostanie podany parametr **-n** , nie należy określać żadnego innego parametru.

Korzystanie z Active Directory w systemie Windows

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 IBM MQ classes for Java i IBM MQ classes for JMS

IBM MQ classes for Java i IBM MQ classes for JMS uzyskują dostęp do list CRL w inny sposób niż inne platformy.

Informacje na temat pracy z listami CRL i ARL przy użyciu produktu IBM MQ classes for Javazawiera sekcja Korzystanie z list odwołań certyfikatów .

Więcej informacji na temat pracy z listami CRL i ARL z produktem IBM MQ classes for JMSzawiera sekcja Właściwość obiektu SSLCERTSTORES .

Manipulowanie obiektami informacji uwierzytelniających

Obiekty informacji uwierzytelniających można manipulować za pomocą komend MQSC lub PCF, lub IBM 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 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 on dostępny, można również użyć IBM MQ Explorer.

Linux UNIX Korzystanie z metody PAM (Pluggable Authentication Method)

Aplikacji PAM można używać tylko na platformach UNIX and Linux . Typowy system UNIX posiada moduły PAM, które implementują tradycyjny mechanizm uwierzytelniania, jednak może być więcej. Podobnie jak podstawowe zadanie walidacji haseł, moduły PAM mogą być również wywoływane w celu wykonania dodatkowych reguł.

Pliki konfiguracyjne definiują metodę uwierzytelniania, która ma być używana dla każdej aplikacji. Przykładowe aplikacje to standardowe logowanie do terminalu, ftp i telnet.

Zaletą PAM jest to, że aplikacja nie musi wiedzieć, o czym dbać, w jaki sposób ID użytkownika jest rzeczywiście uwierzytelniany. Tak długo, jak aplikacja może zapewnić prawidłową formę danych uwierzytelniania do PAM, mechanizm za nim jest przezroczysty.

Format danych uwierzytelniania zależy od używanego systemu. Na przykład program IBM MQ uzyskuje hasło za pomocą parametrów, takich jak struktura MQCSP używana w wywołaniu funkcji API produktu MQCONNX .

Ważne: Nie można ustawić atrybutu **AUTHENMD** do momentu zainstalowania produktu IBM MQ 8.0.0 Fix Pack 3, a następnie zrestartowania menedżera kolejek przy użyciu*poziomu* **-e CMDLEVEL=** *802* (w komendzie strmqm), aby ustawić wymagany poziom komendy.

Konfigurowanie systemu do użycia PAM

Nazwa usługi używana przez produkt IBM MQpodczas wywoływania modułu PAM ma wartość *ibmmq*.

Należy zauważyć, że instalacja produktu IBM MQ próbuje zachować domyślną konfigurację PAM, która umożliwia nawiązanie połączeń od użytkowników systemu operacyjnego w oparciu o znane wartości domyślne dla różnych systemów operacyjnych.

Jednak administrator systemu musi sprawdzić, czy reguły zdefiniowane w plikach `/etc/pam.conf`lub `/etc/pam.d/ibmmq`nadal są odpowiednie.

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.

ULW 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.

Ta sekcja zawiera również listę kontrolną, której można użyć do określenia zadań, które należy wykonać w celu zastosowania zabezpieczeń w systemie na wszystkich platformach, a także uwagi dotyczące nadawania użytkownikom uprawnień do administrowania produktem IBM MQ oraz do pracy z obiektami produktu IBM MQ .

Jeśli dostarczone mechanizmy bezpieczeństwa nie spełniają Twoich potrzeb, można opracować własne programy obsługi wyjścia kanału.

Określanie, który użytkownik jest używany do autoryzacji

Uprawnienia dostępu do zasobów są nadawane grupom, do których użytkownik należy lub, w pewnych trybach, bezpośrednio użytkownikowi powiązanemu z połączeniem. Podczas procesu połączenia, a w szczególności w przypadku połączeń zdalnych (klienckich), tożsamość ta może zostać zmieniona przez konfigurację menedżera kolejek. Na tej stronie znajduje się lista różnych funkcji produktu IBM MQ i ich opcji konfiguracyjnych, które mogą mieć wpływ na tożsamość aplikacji nawiązującej połączenie oraz kolejność wykonywania tych funkcji.

Funkcje, które mogą modyfikować, który użytkownik jest adoptowany

Różne funkcje, które mogą określać, który użytkownik powinien być autoryzowany, są następujące:

Użytkownik sprawdzony przez aplikację
Gdy połączenie zdalne jest uruchamiane przez program IBM MQ, użytkownik systemu operacyjnego, który uruchomił proces, jest wysyłany do odbierającego menedżera kolejek. Ten użytkownik jest wysyłany, aby upewnić się, że jeśli nie istnieje dalsza konfiguracja, która modyfikuje użytkownika, istnieje użytkownik, który może być używany do sprawdzania autoryzacji.

Nie zaleca się używania tego użytkownika jako podstawy autoryzacji, ponieważ umożliwia on nawiązywanie połączeń w celu potwierdzania ich tożsamości bez sprawdzania poprawności po stronie serwera. Może to nawet obejmować użytkownika administracyjnego ('mqm ').

Ustawienie MCAUSER kanału
Aplikacje łączące się za pośrednictwem powiązań sieciowych korzystają z definicji kanału systemu IBM MQ . Definicje kanałów obsługują atrybut **MCAUSER** , którego można użyć do określenia innego użytkownika, który ma być używany do autoryzacji zamiast użytkownika sprawdzanego przez aplikacje nawiązujące połączenie.

Uwierzytelnianie połączenia-adoptowanie TCTX
Aplikacje mogą określać użytkownika i hasło, które mają zostać wysłane do menedżera kolejek w celu uwierzytelnienia. Te referencje są uwierzytelniane przy użyciu konfiguracji określonej dla opcji uwierzytelniania połączenia. Opcja **ADOPTCTX** uwierzytelniania połączenia określa, czy użytkownik powinien być używany do autoryzacji po pomyślnym sprawdzeniu jego poprawności. Jeśli ustawiona jest wartość YES, użytkownik, który jest dostarczany na potrzeby uwierzytelniania, jest adoptowany na potrzeby sprawdzania autoryzacji.

Rekord uwierzytelniania kanału MCAUSER
Podczas przetwarzania połączenia menedżer kolejek podejmie próbę znalezienia rekordu uwierzytelniania kanału, który jest zgodny z połączeniem. Jeśli rekord uwierzytelniania kanału jest zgodny, a jego wartość atrybutu **USERSRC** jest ustawiona na MAP, IBM MQ zmienia użytkownika używanego w autoryzacjach na wartość atrybutu **MCAUSER** .

Wyjścia zabezpieczeń
Wyjścia zabezpieczeń to funkcje niestandardowe, które mogą być zapisywane i wywoływane podczas przetwarzania zabezpieczeń systemu IBM MQ . Po wywołaniu funkcji jest ona dostarczana z kopią struktury MQCD, która zawiera kilka pól związanych z użytkownikiem połączeń, które będą używane do sprawdzania autoryzacji. Procedury zewnętrzne zabezpieczeń mogą modyfikować te pola w celu zmiany użytkownika, który będzie autoryzowany.

kolejność wykonywania

W poniższej tabeli przedstawiono kolejność wykonywania poszczególnych opcji bezpieczeństwa opisanych w sekcji “Funkcje, które mogą modyfikować, który użytkownik jest adoptowany” na stronie 361 , gdy program IBM MQ wybiera użytkownika do autoryzacji. Kolejność jest od najniższego do najwyższego, co oznacza, że opcja zabezpieczeń ustawiająca użytkownika w pierwszym wierszu jest nadpisywana przez dowolny inny wiersz.

Tabela 68. Kolejność wykonywania opcji zabezpieczających

Kolejność	**Funkcja**
1 (najniższy)	Identyfikator aplikacji z asercjami
2	Atrybut definicji kanału **MCAUSER**
3	Uwierzytelnianie połączenia przy użyciu produktu **ADOPTCTX(YES)**
4	Rekordy uwierzytelniania kanału z **USERSRC(MAP)**
5 (najwyższy)	Wyjście zabezpieczeń

Konsekwencje wczesnego przyjęcia

Rekordy uwierzytelniania połączenia i uwierzytelniania kanału udostępniają opcję konfiguracyjną, która steruje wykonaniem uwierzytelniania połączenia przez użytkownika. To ustawienie jest określane jako wczesne adoptowanie. Jeśli funkcja wczesnego adoptowania jest włączona, adoptowanie tożsamości uwierzytelniania połączenia ma miejsce przed przetworzeniem rekordów uwierzytelniania kanału (co oznacza, że rekordy uwierzytelniania kanału nadpisują wszystkie adopcje produktu **CONNAUTH**).

Jeśli ta opcja jest wyłączona, kolejność jest odwrotna-oznacza to, że rekordy uwierzytelniania kanału są przetwarzane przed adoptowaniem produktu **CONNAUTH** . W tej sytuacji zastosowanie uwierzytelniania połączenia ma wyższy efektywny priorytet niż rekordy uwierzytelniania kanału.

Domyślnym ustawieniem dla wczesnego adoptowania jest `włączone`.

ULW Kontrolowanie dostępu do obiektów za pomocą OAM w systemie UNIX, Linux, and Windows

Menedżer uprawnień do obiektów (Object Authority Manager-OAM) udostępnia interfejs komend do nadawania i odwoływania uprawnień do obiektów produktu IBM MQ .

Użytkownik musi mieć odpowiednie uprawnienia do korzystania z tych komend, zgodnie z opisem w sekcji “Uprawnienie do administrowania produktem IBM MQ w systemie UNIX, Linux, and Windows” na stronie 415. Identyfikatory użytkowników, którzy są uprawnieni do administrowania produktem IBM MQ , mają uprawnienia *superużytkownika* do menedżera kolejek, co oznacza, że nie ma potrzeby nadawania im dalszych uprawnień do wydawania żadnych żądań MQI lub komend.

Linux UNIX Uprawnienia oparte na użytkownikach OAM w systemie UNIX and Linux

Z poziomu produktu IBM MQ 8.0w systemach UNIX and Linux menedżer uprawnień do obiektów (OAM) może korzystać z autoryzacji opartej na użytkownikach, a także autoryzacji opartej na grupach.

Przed programem IBM MQ 8.0listy kontroli dostępu (ACL) w systemie UNIX and Linux są oparte tylko na grupach. Z poziomu produktu IBM MQ 8.0listy ACL są oparte na identyfikatorach użytkowników i grupach, a użytkownik może użyć modelu opartego na użytkownikach lub modelu opartego na grupach w celu autoryzacji, ustawiając atrybut **SecurityPolicy** na odpowiednią wartość zgodnie z opisem w sekcji Konfigurowanie usług instalowalnych i Konfigurowanie sekcji usług autoryzacji w systemie UNIX i Linux.

Zmiany w działaniu produktu IBM MQ 8.0 i nowszych

W produkcie IBM MQ 8.0podczas działania z wykorzystaniem strategii opartej na użytkowniku niektóre komendy zwracają różne informacje z wcześniejszych wersji produktu:

- Komendy **dmpmqaut** i **dmpmqcfg** prezentują rekordy oparte na użytkownikach, podobnie jak operacje równoważne z PCF.
- Wtyczka OAM dla produktu IBM MQ Explorer wyświetla rekordy oparte na użytkownikach i umożliwia modyfikacje oparte na użytkownikach.
- Funkcja OAM **Inquire** zwraca wyniki, które wskazują, że jest ona zdolna do obsługi użytkownika.

Użycie atrybutu **-p** w komendzie **setmqaut** nie daje dostępu do wszystkich użytkowników z tej samej grupy podstawowej, jeśli autoryzacje oparte na użytkownikach są włączone w pliku `qm.ini` zgodnie z opisem w sekcji Sekcja usługi pliku qm.ini.

Jeśli użytkownik uruchomi autoryzację opartą na użytkownikach i ma wielu użytkowników, prawdopodobnie będzie więcej rekordów zapisanych w kolejce AUTH niż w przypadku modelu opartego na grupach, a proces autoryzacji może zająć trochę więcej czasu niż poprzednio, ponieważ istnieje więcej rekordów do zweryfikowania. Wzrost ten nie powinien być znaczący. Jeśli jest to wymagane, można użyć kombinacji uprawnień użytkownika i grupy.

Uwagi dotyczące migracji

Jeśli model zostanie zmieniony z grupy na użytkownika dla istniejącego menedżera kolejek, nie będzie to miało bezpośredniego wpływu. Uprawnienia, które zostały już wprowadzone, nadal mają zastosowanie. Każdy użytkownik, który łączy się z menedżerem kolejek, otrzymuje te same uprawnienia, co wcześniej: kombinacja wszystkich grup, do których należy ich identyfikator. Gdy nowe komendy **setmqaut** są wydawane dla ID użytkowników, mają one natychmiastowy skutek.

Jeśli nowy menedżer kolejek zostanie utworzony przy użyciu strategii użytkownika, ten menedżer kolejek będzie miał uprawnienia tylko dla użytkownika, który go utworzył (który zwykle jest, ale nie musi, ID użytkownika `mqm`). Istnieją również uprawnienia, które są automatycznie nadawane grupie `mqm` . Jeśli jednak użytkownik nie ma grupy `mqm` jako grupy podstawowej, wówczas grupa `mqm` nie będzie uwzględniana w początkowym zestawie autoryzacji.

Jeśli użytkownik zostanie przeniesiony z strategii grupy, autoryzacje oparte na użytkownikach nie zostaną automatycznie usunięte. Jednak nie są one już używane podczas sprawdzania uprawnień. Przed przywróceniem strategii należy zapisać bieżącą konfigurację, zmienić strategię, zrestartować menedżer kolejek, a następnie odtworzyć skrypt. Ponieważ obecnie jest to menedżer kolejek oparty na grupach, to reguły identyfikatora użytkownika są zapisywane w oparciu o grupę podstawową.

Pojęcia pokrewne

menedżer uprawnień obiektu (OAM)

Nazwy użytkowników i grupy w systemach UNIX, Linux i Windows

Sekcja Service w pliku qm.ini

Odsyłacze pokrewne

crtmqm (tworzenie menedżera kolejek), komenda

ULW Nadawanie dostępu do obiektu IBM MQ w systemie UNIX, Linux, and Windows

Aby nadać użytkownikom i grupom użytkowników dostęp do obiektów produktu IBM MQ , należy użyć komendy sterującej **setmqaut** , komendy **SET AUTHREC** MQSC lub komendy PCF produktu **MQCMD_SET_AUTH_REC** . Należy pamiętać, że w systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Pełną definicję komendy sterującej **setmqaut** i jej składnię można znaleźć w sekcji setmqaut.

Pełną definicję komendy MQSC **SET AUTHREC** i jej składni można znaleźć w sekcji SET AUTHREC.

Pełną definicję 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 systemie UNIX, Linux, and Windows” na stronie 366.
- 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 można 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 również uprawnienia do umieszczania 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 setmqaut 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.

Informacje dotyczące składni komendy SET AUTHREC

Listy autoryzacji do dodania i autoryzacji do usunięcia nie mogą się nakładać. Nie można na przykład dodać uprawnienia do wyświetlania i usunąć uprawnienia do wyświetlania przy użyciu tej samej komendy. Ta reguła ma zastosowanie nawet wtedy, gdy uprawnienia są wyrażane przy użyciu różnych opcji. Na przykład następująca komenda nie powiedzie się, ponieważ uprawnienie DSP nakłada się na uprawnienie ALLADM:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

Wyjątek od tego zachowania związanego z nakładaniem się uprawnień stanowi uprawnienie ALL. Następująca komenda powoduje najpierw dodanie uprawnień ALL, a następnie usunięcie uprawnienia SETID:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

Następująca komenda powoduje najpierw usunięcie uprawnień ALL, a następnie dodanie uprawnienia DSP:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

Niezależnie od kolejności podawania uprawnień w komendzie, uprawnienia ALL są przetwarzane jako pierwsze.

ULW Korzystanie z profili ogólnych OAM w systemie UNIX, Linux, and Windows

Profile ogólne OAM służą do ustawiania w pojedynczej operacji uprawnień użytkownika do wielu obiektów, bez konieczności wydawania oddzielnych komend **setmqaut** lub **SET AUTHREC** dla każdego tworzonego obiektu. Należy zauważyć, że w urządzeniu IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Użycie profili ogólnych w komendach setmqaut lub SET AUTHREC umożliwia ustawienie uprawnień ogólnych dla wszystkich obiektów, które są zgodne z tym profilem.

Ta kolekcja tematów zawiera bardziej szczegółowy opis użycia profili ogólnych.

Używanie znaków wieloznacznych w profilach OAM

To, co sprawia, że profil jest ogólny, to użycie znaków specjalnych (znaków wieloznacznych) w nazwie profilu. Na przykład znak wieloznaczny w postaci znaku zapytania (?) odpowiada dowolnemu pojedynczemu znakowi w nazwie. Jeśli więc zostanie podana wartość ABC.?EF, uprawnienia do tego profilu będą 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 dotyczy obiektów AB.CD, AB.EDi AB.FD.

*****

Użyj gwiazdki (*) jako:

- *Kwalifikator* w nazwie profilu, który jest 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 dotyczy obiektów ABC.DEF.JKLi ABC.GHI.JKL. (Należy zauważyć, że **nie** dotyczy ABC.JKL ; Znak * używany w tym kontekście zawsze wskazuje jeden kwalifikator).
- Znak w obrębie kwalifikatora w nazwie profilu, który ma być zgodny z zerem lub większą liczbą znaków w kwalifikatorze w nazwie obiektu.

  Na przykład ABC.DE*.JKL dotyczy obiektów ABC.DE.JKL, ABC.DEF.JKLi ABC.DEGH.JKL.

******

Użyj podwójnej gwiazdki (**) **raz** w nazwie profilu jako:

- Cała nazwa profilu, która ma być zgodna ze wszystkimi nazwami obiektów. Jeśli na przykład do identyfikowania procesów używany jest system `-t prcs` , a następnie używana jest nazwa profilu **, autoryzacje dla wszystkich procesów są zmieniane.
- Jako kwalifikator początkowy, środkowy lub końcowy w nazwie profilu, aby dopasować zero lub więcej kwalifikatorów w nazwie obiektu. Na przykład **.ABC identyfikuje wszystkie obiekty z kwalifikatorem końcowym ABC.

Jako pełnego kwalifikatora można użyć tylko podwójnej gwiazdki **:

```
**.DEF
  ABC.**
  A*.**
```

ale nie jako

```
A**
```

w przeciwnym razie zostanie wyświetlony komunikat AMQ7226E: `Nazwa profilu jest niepoprawna.`

Uwaga: Jeśli w systemach UNIX i Linux używane są znaki wieloznaczne, **należy** ująć nazwę profilu w pojedynczy cudzysłów.

Priorytety profilu

Ważnym punktem, który należy zrozumieć, gdy używane są profile ogólne, jest priorytet nadawany profilom podczas podejmowania decyzji o tym, jakie uprawnienia mają być zastosowane do tworzonego obiektu. Załóżmy na przykład, że zostały wprowadzone komendy:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

Pierwszy nadaje uprawnienie do umieszczania we wszystkich kolejkach dla użytkownika fred o nazwach zgodnych z profilem AB. *; Druga nadaje uprawnienie do pobierania do tych samych typów kolejek, które są zgodne z profilem AB.C*.

Załóżmy, że została utworzona kolejka o nazwie AB.CD. Zgodnie z regułami dopasowywania znaków wieloznacznych do tej kolejki można zastosować komendę setmqaut. Więc, czy ma to jakieś autorytet?

Aby znaleźć odpowiedź, należy zastosować regułę, która za każdym razem, gdy wiele profili może mieć zastosowanie do obiektu, **ma zastosowanie tylko najbardziej szczegółowe**. Sposób stosowania tej reguły polega na porównywaniu nazw profili od lewej do prawej. Niezależnie od tego, gdzie występują różnice, znak inny niż ogólny jest bardziej specyficzny niż ogólny. W tym przykładzie jest to kolejka AB.CD ma uprawnienie **get** (AB.C* jest bardziej specyficzne niż AB. *).

Podczas porównywania znaków ogólnych kolejność *swoistości* jest następująca:

1. ?
2. *
3. **

Zrzucanie ustawień profilu

Pełną definicję komendy sterującej **dmpmqaut** i jej składnię zawiera sekcja dmpmqaut.

Pełną definicję komendy **DISPLAY AUTHREC** MQSC i jej składnię zawiera sekcja DISPLAY AUTHREC.

Pełną definicję komendy **MQCMD_INQUIRE_AUTH_RECS** PCF i jej składnię zawiera sekcja Zapytanie o rekordy uprawnień.

Poniższe przykłady przedstawiają użycie komendy sterującej **dmpmqaut** do zrzucenia rekordów uprawnień dla profili ogólnych:

1. W tym przykładzie zrzuca wszystkie rekordy uprawnień z profilem zgodnym z kolejką a.b.c dla nazwy użytkownika user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Wynikowy zrzut wygląda mniej więcej tak:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Uwaga: Użytkownicy systemów UNIX i Linux mogą używać opcji `-p` dla komendy **dmpmqaut** , ale podczas definiowania autoryzacji muszą używać opcji `-g groupname` .
2. W tym przykładzie zrzuca wszystkie rekordy uprawnień z profilem zgodnym z kolejką a.b.c.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

Wynikowy zrzut wygląda mniej więcej tak:

```
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 zrzuca wszystkie rekordy uprawnień dla profilu a.b. *, typu kolejka.

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

Wynikowy zrzut wygląda mniej więcej tak:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

4. W tym przykładzie zrzuca się wszystkie rekordy uprawnień dla menedżera kolejek qmX.

```
dmpmqaut -m qmX
```

Wynikowy zrzut wygląda mniej więcej tak:

```
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 mniej więcej tak:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Uwaga: Tylko w systemie IBM MQ for Windows wszystkie nazwy użytkowników zawierają informacje o domenie, na przykład:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW *Korzystanie ze znaków wieloznacznych w profilach OAM w systemie UNIX, Linux, and Windows*

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.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 nazwie ABC.DEF.GHI kwalifikatorami są ABC, DEF oraz GHI.

  Na przykład ABC.*.JKL ma zastosowanie do obiektów ABC.DEF.JKLi ABC.GHI.JKL. (Należy pamiętać, że program **nie** ma zastosowanie 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.

ULW *Priorytety profilu w systemie UNIX, Linux, and Windows*

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. W tym przykładzie jest to 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. **

Informacje na temat równoważnych informacji można znaleźć w sekcji SET AUTHREC , gdy używana jest ta komenda MQSC.

ULW *Zrzut ustawień profilu w systemie UNIX, Linux, and Windows*

Aby wykonać zrzut bieżących autoryzacji powiązanych z określonym profilem, należy użyć komendy sterującej **dmpmqaut** , komendy **DISPLAY AUTHREC** MQSC lub komendy PCF produktu **MQCMD_INQUIRE_AUTH_RECS** . Należy pamiętać, że w systemie IBM MQ Appliance można używać tylko komendy **DISPLAY AUTHREC** .

Pełną definicję komendy sterującej **dmpmqaut** i jej składnię można znaleźć w sekcji dmpmqaut.

Pełną definicję komendy MQSC **DISPLAY AUTHREC** i jej składni można znaleźć w sekcji DISPLAY AUTHREC.

Pełną definicję komendy **MQCMD_INQUIRE_AUTH_RECS** PCF i jej składni można znaleźć w temacie 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 systemu IBM MQ for Windows wszystkie wyświetlane nazwy użytkowników obejmują informacje o domenie, na przykład:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW Wyświetlanie ustawień dostępu w systemie UNIX, Linux, and Windows

Aby wyświetlić autoryzacje, które konkretna jednostka główna lub grupa ma dla konkretnego obiektu, należy użyć komendy sterującej **dspmqaut** , komendy **DISPLAY AUTHREC** MQSC lub komendy **MQCMD_INQUIRE_ENTITY_AUTH** PCF. Należy pamiętać, że w systemie IBM MQ Appliance można używać tylko komendy **DISPLAY AUTHREC** .

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.

Pełną definicję komendy MQSC **DISPLAY AUTHREC** i jej składni można znaleźć w sekcji DISPLAY AUTHREC.

Pełną definicję komendy **MQCMD_INQUIRE_AUTH_RECS** PCF i jej składni można znaleźć w temacie Inquire Authority Records(zapytanie o rekordy uprawnień).

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
```

ULW Zmiana i odebranie dostępu do obiektu IBM MQ w systemie UNIX, Linux, and Windows

Aby zmienić poziom dostępu użytkownika lub grupy do obiektu, należy użyć komendy sterującej **setmqaut** , komendy MQSC **DELETE AUTHREC** lub komendy PCF **MQCMD_DELETE_AUTH_REC** .

MQ Appliance Należy pamiętać, że w systemie IBM MQ Appliance można używać tylko komendy **DELETE AUTHREC** .

Proces usuwania użytkownika z grupy jest opisany w sekcji:

- Windows “Tworzenie grup i zarządzanie nimi w systemie Windows” na stronie 148
- AIX “Tworzenie grup i zarządzanie nimi w systemie AIX” na stronie 146

- Solaris “Tworzenie grup i zarządzanie nimi w systemie Solaris” na stronie 147
- Linux “Tworzenie grup i zarządzanie nimi w systemie Linux” na stronie 146

.

Identyfikator użytkownika, który tworzy obiekt IBM 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.

Pełną definicję komendy MQSC **DELETE AUTHREC** i jej składni można znaleźć w sekcji DELETE AUTHREC.

Pełną definicję komendy **MQCMD_DELETE_AUTH_REC** PCF i jej składni można znaleźć w sekcji Usuwanie rekordu uprawnień.

Windows W systemie Windowsz programu IBM MQ 8.0można w dowolnym momencie usunąć pozycje OAM odpowiadające poszczególnym kontem użytkownika Windows , używając parametru **-u** *SID* programu **setmqaut**.

Przed usunięciem profilu użytkownika przed programem IBM MQ 8.0należy usunąć pozycje OAM odpowiadające konkretnym kontem użytkownika produktu Windows . Usunięcie pozycji OAM nie było możliwe po usunięciu konta użytkownika.

ULW Zapobieganie sprawdzaniu dostępu do zabezpieczeń w systemach UNIX, Linux, and Windows

Aby wyłączyć sprawdzanie zabezpieczeń, można wyłączyć menedżera uprawnień do obiektów (OAM). Może to być odpowiednie dla środowiska testowego. Po wyłączeniu lub usunięciu menedżera OAM nie można dodać menedżera OAM do istniejącego menedżera kolejek.

Jeśli użytkownik zdecyduje, że nie chce wykonywać kontroli bezpieczeństwa (na przykład w środowisku testowym), można wyłączyć mechanizm OAM na jeden z dwóch sposobów:

- Przed utworzeniem menedżera kolejek należy ustawić zmienną środowiskową systemu operacyjnego MQSNOAUT.

  Informacje na temat wpływu ustawienia zmiennej MQSNOAUT oraz sposobu ustawienia zmiennej MQSNOAUT w systemach Windows i UNIXzawiera sekcja Opisy zmiennych środowiskowych .
- Edytuj plik konfiguracyjny menedżera kolejek, aby usunąć usługę.

Jeśli używana jest komenda **setmqaut**lub **dspmqaut** , gdy tryb OAM jest wyłączony, należy zwrócić uwagę na następujące punkty:

- OAM nie sprawdza poprawności podanej nazwy użytkownika lub grupy, co oznacza, że komenda może zaakceptować niepoprawne wartości.
- OAM nie przeprowadza sprawdzania zabezpieczeń i wskazuje, że wszystkie nazwy użytkowników i grupy mają uprawnienia do wykonywania wszystkich odpowiednich operacji na obiektach.

Ostrzeżenie: Po usunięciu menedżera OAM nie można go ponownie umieścić w istniejącym menedżerze kolejek. Dzieje się tak, ponieważ OAM musi być na miejscu w czasie tworzenia obiektu. Aby ponownie użyć funkcji OAM programu IBM MQ po jej usunięciu, należy odbudować menedżer kolejek.

Pojęcia pokrewne

Instalowalne usługi i komponenty dla systemów UNIX, Linux i Windows

Zadania pokrewne

Konfigurowanie instalowalnych usług

Odsyłacze pokrewne

Informacje uzupełniające o usługach instalowalnych

Nadawanie wymaganego dostępu do zasobów

W tym temacie opisano czynności, które należy wykonać w celu zastosowania zabezpieczeń w systemie IBM MQ w systemach UNIX, Linux, Windows, IBM ii z/OS.

O tym zadaniu

Podczas tego zadania użytkownik decyduje o tym, jakie czynności są niezbędne do zastosowania odpowiedniego poziomu zabezpieczeń do elementów instalacji produktu IBM 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 “Nadawanie częściowemu dostępowi administracyjnie do podzbioru zasobów menedżera kolejek” na stronie 374.
3. Czy ci użytkownicy potrzebują pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: Patrz “Nadawanie pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek” na stronie 384.
4. Czy ci użytkownicy muszą mieć dostęp tylko do odczytu do wszystkich zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: Patrz “Nadawanie dostępu tylko do odczytu do wszystkich zasobów w menedżerze kolejek” na stronie 392.
5. Czy ci użytkownicy potrzebują pełnego dostępu administracyjnego do wszystkich zasobów menedżera kolejek?
   a) Nie: Przejdź do następnego pytania.
   b) Tak: Patrz “Nadawanie pełnego dostępu administracyjnego do wszystkich zasobów w menedżerze kolejek” na stronie 393.
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 395
   b) Tak: Patrz “Zezwalanie aplikacjom użytkownika na łączenie się z menedżerem kolejek” na stronie 395.

Multi z/OS 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 69. 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 375
Tematy	Przyznaj częściowy dostęp administracyjny do wymaganych tematów, zgodnie z opisem w sekcji “Ograniczanie dostępu administracyjnego do niektórych tematów” na stronie 377
Kanały	Przyznaj częściowy dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji “Przyznawanie niektórych kanałów ograniczonego dostępu administracyjnego” na stronie 378
Menedżer kolejek	Przyznaj częściowy dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji “Nadawanie ograniczonego dostępu administracyjnego do menedżera kolejek” na stronie 379
Procesy	Przyznaj częściowy dostęp administracyjny do wymaganych procesów, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego niektórym procesom” na stronie 381
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 382
Usługi	Przyznaj częściowy dostęp administracyjny do wymaganych usług, zgodnie z opisem w sekcji “Ograniczanie dostępu administracyjnego do niektórych usług” na stronie 383

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i
- Linux
- UNIX

- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W przypadku systemów UNIX, Linux, and Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
  ```

- IBM i
  W systemie IBM iwykonaj następującą komendę:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS W przypadku produktu z/OSnależy wprowadzić następujące komendy w celu nadania dostępu do określonej kolejki:

  ```
  RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
  PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w kolejce, należy wprowadzić następujące komendy dla każdej komendy MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction. QType UACC(NONE)
  PERMIT QMgrName. ReqdAction. QType CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Aby zezwolić użytkownikowi na użycie komendy DISPLAY QUEUE, należy wprowadzić następujące komendy:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY. QType UACC(NONE)
  PERMIT QMgrName.DISPLAY. QType CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek.

  z/OS 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:

  – ULW W systemach UNIX, Linux, and Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + dlt, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.

  – IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.

– z/OSW systemie z/OSjedna z wartości: ALTER, CLEAR, DELETE lub MOVE.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM iIBM i
- LinuxLinux
- UNIXUNIX
- IBM iWindows

Uwaga: MQ ApplianceW systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW

  W przypadku systemów UNIX, Linux, and Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
  ```

- IBM i

  W systemie IBM iwykonaj następującą komendę:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OSW przypadku produktu z/OSnależy wprowadzić następujące komendy:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Te komendy nadają dostęp do określonego tematu. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w danym temacie, należy wprowadzić następujące komendy dla każdej komendy MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)
  PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

Aby zezwolić użytkownikowi na użycie komendy DISPLAY TOPIC, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)
PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

z/OS 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:

- ULW W systemach UNIX, Linux, and Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.
- IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.
- z/OS W systemie z/OSjedna z wartości: ALTER, CLEAR, DEFINE, DELETE lub MOVE.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS W systemie z/OS:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Te komendy nadają dostęp do określonego kanału. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w kanale, należy wprowadzić następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby zezwolić użytkownikowi na użycie komendy DISPLAY CHANNEL, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.CHANNEL UACC(NONE)
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

z/OS 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:

- ULW W systemie UNIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.
- IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLx. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.
- z/OS W systemie z/OSjedna z wartości: ALTER, CLEAR, DEFINE, DELETE lub MOVE.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
  ```

- IBM i
  W systemie IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS
  W systemie z/OS:

  Aby określić, które komendy MQSC mogą być wykonywane 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:

  – ULW W systemie UNIX, Linux, and Windowsdowolna 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.

– IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
  ```

- IBM i
  W systemie IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS W systemie z/OS:

  ```
  RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)
  PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Te komendy nadają dostęp do określonego kanału. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w kanale, należy wprowadzić następujące komendy dla każdej komendy MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.PROCESS UACC(NONE)
  PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Aby zezwolić użytkownikowi na użycie komendy DISPLAY PROCESS, należy wprowadzić następujące komendy:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.PROCESS UACC(NONE)
  PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

z/OS 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:

- ULW W systemie UNIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.
- IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.
- z/OS W systemie z/OSjedna z wartości: ALTER, CLEAR, DEFINE, DELETE lub MOVE.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS W systemie z/OS:

```
RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Te komendy nadają dostęp do określonej listy nazw. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika na liście nazw, należy wprowadzić następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.NAMELIST UACC(NONE)
PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby zezwolić użytkownikowi na użycie komendy DISPLAY NAMELIST, należy wprowadzić następujące komendy:

```
RDEFINE MQCMDS QMgrName.DISPLAY.NAMELIST UACC(NONE)
PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

z/OS 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:

- ULW W systemie UNIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.
- IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.
- z/OS W systemie z/OSjedna z wartości: ALTER, CLEAR, DEFINE, DELETE lub MOVE.

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. z/OS Należy pamiętać, że obiekty usług nie istnieją w produkcie z/OS.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
  ```

- W systemie IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS W systemie z/OS:

  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:

  - ULW W systemach UNIX, Linux, and Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoznaczna z + chg + clr + dlt + dsp.
  - IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Uprawnienie *ALLADM jest równoważne z wszystkimi tymi autoryzacjami indywidualnymi.

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 70. 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 385
Tematy	Nadaj pełny dostęp administracyjny do wymaganych tematów, zgodnie z opisem w sekcji "Nadawanie pełnego dostępu administracyjnego niektórych tematów" na stronie 386
Kanały	Nadaj pełny dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji "Nadawanie pełnego dostępu administracyjnego niektórym kanałom" na stronie 387
Menedżer kolejek	Nadaj pełny dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji "Nadawanie pełnego dostępu administracyjnego do menedżera kolejek" na stronie 388
Procesy	Nadaj pełny dostęp administracyjny do wymaganych procesów, zgodnie z opisem w sekcji "Nadawanie pełnego dostępu administracyjnego niektórym procesom" na stronie 389
Listy nazw	Nadaj pełny dostęp administracyjny do wymaganych list nazw, zgodnie z opisem w sekcji "Nadawanie pełnego dostępu administracyjnego niektórych list nazw" na stronie 390
Usługi	Należy nadać pełny dostęp administracyjny do wymaganych usług zgodnie z opisem w sekcji "Zapewnienie pełnego dostępu administracyjnego do niektórych usług" na stronie 391

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW

  W systemie UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
  ```

- IBM i

  W systemie IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName
  ')
  ```

- z/OS

  W systemie z/OS:

  ```
  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.

  z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW

  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  W systemie z/OS:

```
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.

z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  W systemie z/OS:

```
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.

z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  W systemie z/OS:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek.

z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
  ```

- IBM i
  W systemie IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS
  W systemie z/OS:

  ```
  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.

z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  W systemie z/OS:

```
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.

  z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- IBM i
  W systemie IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  W systemie z/OS:

```
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.

  z/OS 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Po zmianie wszystkich szczegółów autoryzacji należy wykonać odświeżanie zabezpieczeń za pomocą komendy REFRESH SECURITY .

Procedura

- Za pomocą kreatora:
  a) W panelu IBM MQ Explorer Navigator kliknij prawym przyciskiem myszy menedżer kolejek i kliknij opcję **Uprawnienia do obiektu** > **Dodaj uprawnienia oparte na rolach** .
  Zostanie otwarty kreator dodawania uprawnień opartych na rolach.
- Windows UNIX
  W przypadku systemów UNIX i Windows należy wprowadzić 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
+put
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 produkt IBM MQ Explorer.
- IBM i
  W przypadku produktu IBM inależy 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')
```

- z/OS

  W przypadku produktu z/OSnależy wprowadzić następujące komendy:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MXTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MXTOPIC) 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.

  z/OS 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

Można użyć kreatora dodawania uprawnień opartych na rolach lub odpowiednich komend dla używanego systemu operacyjnego.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Uwagi: ULW

1. Jeśli do administrowania menedżerem kolejek zamiast IBM MQ Explorerużywany jest produkt **runmqsc** , należy nadać uprawnienia do uzyskiwania informacji, pobierania i przeglądania SYSTEM.MQSC.REPLY.QUEUE, a użytkownik nie musi nadawać żadnych uprawnień do systemu SYSTEM.MQEXPLORER.REPLY.MODEL .
2. Jeśli użytkownik ma dostęp do wszystkich zasobów w menedżerze kolejek, istnieją pewne komendy, których użytkownik nie może uruchomić, chyba że użytkownik ma prawo do odczytu pliku `qm.ini` .

Wynika to z ograniczeń dotyczących użytkowników innych niż `mqm` , którzy mogą odczytywać plik `qm.ini` .

Użytkownik nie może wydać następujących komend, o ile użytkownik nie nadał użytkownikowi prawa do odczytu pliku qm.ini :

- Definiowanie kanału, który jest skonfigurowany pod kątem używania protokołu TLS
- Definiowanie kanału za pomocą zmiennych wstawiających do automatycznej konfiguracji zdefiniowanych w produkcie `qm.ini`

Procedura

- W przypadku korzystania z kreatora, w panelu Navigator programu IBM 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.

- Linux UNIX

  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.MODEL -t queue -g GroupName +dsp +inq +get +put
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 +connect
```

  Więcej informacji na temat `@class` zawiera sekcja **`setmqaut`** .

- Windows

  W przypadku systemów Windows należy wydać te same komendy co w przypadku systemów UNIX and Linux , ale zamiast @classnależy użyć nazwy profilu @CLASS .

- IBM i

  W systemie IBM iwykonaj następującą komendę:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- z/OS

  W przypadku produktu z/OSnależy wprowadzić następujące komendy:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek.

  z/OS 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.

W systemach UNIX, Linux, Windows i IBM imożna również użyć komendy DELETE AUTHREC .

Uwaga: W systemie IBM MQ Appliance można używać tylko komendy **DELETE AUTHREC** .

Procedura

- ULW

  W przypadku systemów UNIX, Linux, and Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName -connect
  ```

- IBM i

  W systemie IBM iwykonaj następującą komendę:

  ```
  RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
  ```

- z/OS

  W przypadku produktu z/OSnależy wprowadzić 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.

  z/OS 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 403.

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 396.

W obu przypadkach skonfiguruj zabezpieczenia połączenia zgodnie z opisem w sekcji “Konfigurowanie zabezpieczeń połączenia” na stronie 403

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 405
Dostępne są aplikacje, które korzystają z tematów	Patrz sekcja “Kontrolowanie dostępu użytkowników do tematów” na stronie 411.
Istnieją aplikacje, które zapytują się w obiekcie menedżera kolejek	Patrz sekcja “Nadawanie uprawnień do uzyskiwania informacji o menedżerze kolejek” na stronie 413.
Istnieją aplikacje, które używają obiektów procesu	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do procesów dostępu” na stronie 414
Istnieją aplikacje, które korzystają z list nazw	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do dostępu do list nazw” na stronie 414

Zabezpieczanie zdalnych połączeń z menedżerem kolejek

Istnieje możliwość zabezpieczenia połączeń zdalnych z menedżerem kolejek przy użyciu protokołu 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 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. Używanie protokołu 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 TLS, którą otrzymuje w polach SSLPeerNamePtr i SSLPeerName, które zostały przekazane do wyjścia w strukturze MQCD.
3. Używanie protokołu 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 korzystają z protokołu 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 wieloznaczny. 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 397

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 343. Więcej informacji na temat produktu *MQADMINzawiera 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 nazwa kanału połączenia z serwerem zostanie określona w następujących komendach, nie będzie to miało 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(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 klienta na identyfikator użytkownika MCAUSER
Za pomocą rekordu uwierzytelniania kanału można zmienić atrybut MCAUSER kanału połączenia z serwerem, zgodnie z ID 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 powiązany z połączeniem klienta. Wartość może zostać sprawdzona przez aplikację kliencką, zmieniona za pomocą uwierzytelniania połączenia przy użyciu wczesnego adoptowanego lub ustawionego za pośrednictwem wyjścia kanału.
użytkownik to identyfikator użytkownika, który ma być używany zamiast nazwy użytkownika klienta.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH
Atrybuty sekcji kanałów (ChlauthEarlyAdopt)

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) SSLCERTI(generic-issuer-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 MQ dla wartości SSLPEER. Więcej informacji zawiera sekcja Reguły IBM MQ dla wartości SSLPEER.
użytkownik jest identyfikatorem użytkownika, który ma być używany dla wszystkich połączeń korzystających z określonej nazwy wyróżniającej.
generic-wystawca-nazwa odnosi się do nazwy wyróżniającej wystawcy certyfikatu, który ma być zgodny. Ten parametr jest opcjonalny, ale należy go używać, aby uniknąć nadmiernej zgodności z błędnym certyfikatem, jeśli używane jest wiele ośrodków certyfikacji.

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 następującej 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 klienta
Za pomocą rekordu uwierzytelniania kanału można zapobiec nawiązaniu przez użytkownika identyfikatora użytkownika z połączenia kanału.

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 powiązany z połączeniem klienta. Wartość może zostać sprawdzona przez aplikację kliencką, zmieniona za pomocą uwierzytelniania połączenia przy użyciu wczesnego adoptowanego lub ustawionego za pośrednictwem wyjścia kanału.

Odsyłacze pokrewne
USTAW WARTOŚĆ CHLAUTH

Blokowanie dostępu dla nazwy wyróżniającej SSL lub TLS
Za pomocą rekordu uwierzytelniania kanału można zapobiec uruchamianiu nazw wyróżniających TLS (TLS Distinguished Name-DN) z kanałów wyjściowych.

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') SSLCERTI(generic-issuer-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 MQ dla wartości SSLPEER. Więcej informacji zawiera sekcja Reguły IBM MQ dla wartości SSLPEER.

generic-wystawca-nazwa odnosi się do nazwy wyróżniającej wystawcy certyfikatu, który ma być zgodny. Ten parametr jest opcjonalny, ale należy go używać, aby uniknąć nadmiernej zgodności z błędnym certyfikatem, jeśli używane jest wiele ośrodków certyfikacji.

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W systemie UNIX, Linux, and Windows:

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

- IBM i
  W systemie IBM i:

  ```
  GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
  ```

- z/OS
  W systemie z/OS:

  ```
  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 zadania wsadowego, 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.

Pojęcia pokrewne

“Profile zabezpieczeń połączenia dla inicjatora kanału” na stronie 203
Profile służące do sprawdzania połączeń z inicjatora kanału składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejki, po której następuje słowo *CHIN*. Podaj identyfikator użytkownika używany przez inicjator kanału, który uruchomił dostęp do przestrzeni adresowej zadania READ do profilu połączenia.

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 405
Kontekst zbiorów aplikacji	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do ustawiania kontekstu” na stronie 406
Kontekst przekazuje kontekst	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do przekazywania kontekstu” na stronie 407
Aplikacja umieszcza komunikaty w kolejce klastrowej	Więcej informacji znajduje się w sekcji “Autoryzowanie umieszczania komunikatów w kolejkach klastra zdalnego” na stronie 474
Aplikacja umieszcza komunikaty w kolejce lokalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 408
Aplikacja umieszcza komunikaty w kolejce modelowej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce modelowej” na stronie 409
Aplikacja umieszcza komunikaty w kolejce zdalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra” na stronie 410

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i
- Linux
- UNIX
- Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić następujące komendy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and Windows wydaj 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
    ```

  Uwaga: Aby można było używać uprawnień `setid` lub `setall` , autoryzacje muszą być nadawane zarówno dla odpowiedniego obiektu kolejki, jak i dla obiektu menedżera kolejek.
- 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 przypadku produktu 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- ULW
  W przypadku systemów UNIX, Linux, and Windows wydaj 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
```

- IBM i
  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 ')
```

- z/OS
  W przypadku produktu 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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 “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 408. 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić następujące komendy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
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 71. 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 411
Aplikacja subskrybuje temat	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do subskrybowania tematów” na stronie 412

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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i
- Linux
- UNIX
- IBM i

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i
- Linux
- UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

Na następujących platformach można również użyć komendy SET AUTHREC :

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Uwaga: MQ Appliance W systemie IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Procedura

- W przypadku systemów UNIX, Linux, and 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 przypadku produktu z/OSnależy wprowadzić 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.

ULW Uprawnienie do administrowania produktem IBM MQ w systemie UNIX, Linux, and Windows

Administratorzy produktu IBM MQ mogą używać wszystkich komend produktu IBM 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 MQ mają uprawnienia do używania wszystkich komend produktu IBM MQ (w tym komend do nadawania uprawnień IBM MQ dla innych użytkowników).

Aby być administratorem produktu IBM MQ , użytkownik musi być członkiem specjalnej grupy, która jest nazywana grupą **mqm** .

Windows Alternatywnie, na kontach lokalnych w systemie Windows , konta lokalne mogą administrować produktem IBM MQ , jeśli są członkami grupy Administratorzy w systemach Windows .

Ostrzeżenie: Użytkownik AD Azure może zostać dodany do grupy mqm za pomocą komendy administratora. Na przykład użyj komendy `net localgroup mqm AzureAD\<your userID> /add`. Następnie uruchom komendy administracyjne produktu IBM MQ lub użyj komendy IBM MQ Explorer.

Grupa **mqm** jest tworzona automatycznie po zainstalowaniu produktu IBM MQ . Można dodać kolejnych użytkowników do grupy, 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 IBM MQ. Jedną z tych komend sterujących jest **setmqaut**, która jest używana do nadawania uprawnień innym użytkownikom w celu umożliwienia im dostępu do zasobów IBM MQ lub ich sterowania. Komendy PCF służące do zarządzania rekordami uprawnień są dostępne dla administratorów innych niż administratorzy, którym nadano 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 muszą mieć wymagane uprawnienia dla komend MQSC, które mają być przetwarzane przez zdalny menedżer kolejek. IBM MQ Explorer wydaje komendy PCF służące do wykonywania zadań administracyjnych. Administratorzy nie muszą mieć dodatkowych uprawnień do używania produktu IBM MQ Explorer do administrowania menedżerem kolejek w systemie lokalnym. Gdy produkt IBM 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.

Ostrzeżenie: Z poziomu produktu IBM MQ 8.0nie trzeba być administratorem, aby używać komendy sterującej **runmqsc**, która wydaje komendy IBM 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.

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 IBM 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 .
- z/OS Informacje na temat komend MQSC, które są przetwarzane przez serwer komend w systemie IBM MQ for z/OS, zawiera sekcja Zabezpieczenia komend i zabezpieczenia zasobów komend w systemie z/OS .

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

Na platformach UNIX and Linux tworzony jest również specjalny identyfikator użytkownika produktu **mqm** , który jest używany tylko przez produkt. Nigdy nie może być ona dostępna dla użytkowników nieuprzywilejowanych. Wszystkie obiekty IBM 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 domenę **mqm** domeny na kontrolerze domeny, która zawiera wszystkie identyfikatory użytkowników uprzywilejowanych aktywnych w domenie, a następnie dodać ją do lokalnej grupy **mqm** . Niektóre komendy, na przykład **crtmqm**, manipulują uprawnieniami do obiektów IBM 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 użytkownik odmawia uprawnienia, jeśli użytkownik ma użytkownika lokalnego i użytkownika uwierzytelnianego domenowo o tej samej nazwie. Jest to opisane w sekcji “Nazwy użytkowników i grupy w systemie UNIX, Linux, and Windows” na stronie 420.

Wersje produktu 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 IBM 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**.

Aby wykonać następujące działania, użytkownik nie musi należeć do grupy **mqm** :

- 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 114).
- Wywołaj wywołania MQI z programu aplikacji (chyba że wymagane jest użycie powiązań krótkiej ścieżki w wywołaniu `MQCONNX`).
- Komenda `crtmqcvx` służy do tworzenia fragmentu kodu, który wykonuje konwersję danych w strukturach typu danych.
- Aby wyświetlić menedżery kolejek, należy użyć komendy `dspmq` .
- Użyj komendy `dspmqtrc` , aby wyświetlić dane wyjściowe śledzenia w formacie IBM MQ .

Ograniczenie o 12 znaków dotyczy zarówno identyfikatorów grup, jak i użytkowników.

Platformy UNIX and Linux zwykle ograniczają długość identyfikatora użytkownika do 12 znaków. Program AIX 5.3 podniósł ten limit, ale program IBM MQ nadal obserwuje ograniczenie 12 znaków na wszystkich platformach UNIX and Linux . Jeśli używany jest identyfikator użytkownika o długości większej niż 12 znaków, program IBM MQ zastąpi go wartością `UNKNOWN` . Nie należy definiować ID użytkownika o wartości `UNKNOWN` .

ULW Zarządzanie grupą mqm w systemie UNIX, Linux, and Windows

Użytkownicy należący do grupy mqm mają nadane pełne uprawnienia administracyjne w produkcie IBM MQ. Z tego powodu nie należy rejestrowywać aplikacji ani zwykłych użytkowników w grupie mqm. Grupa mqm powinna zawierać wyłącznie konta administratorów produktu IBM MQ .

Zadania te są opisane w:

- Windows Tworzenie grup i zarządzanie nimi w systemie Windows
- AIX Tworzenie grup i zarządzanie nimi w systemie AIX
- Solaris Tworzenie grup i zarządzanie nimi w systemie Solaris
- Linux Tworzenie grup i zarządzanie nimi w systemie Linux

Windows Jeśli kontroler domeny działa w systemie Windows 2000 lub Windows 2003 lub nowszym, administrator domeny może skonfigurować specjalne konto dla produktu IBM MQ , które ma być używane. Więcej informacji na ten temat zawiera sekcja Konfigurowanie produktu IBM MQ przy użyciu konsoli Prepare IBM MQ Wizard oraz Tworzenie i konfigurowanie kont domeny Windows dla produktu IBM MQ.

ULW Uprawnienia do pracy z obiektami IBM MQ w systemie UNIX, Linux, and Windows

Wszystkie obiekty są chronione przez produkt IBM MQ, a nazwy użytkowników muszą mieć odpowiednie uprawnienia, aby uzyskać do nich dostęp. 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. Zasoby te są chronione przez produkt IBM 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 w przypadku określonej kolejki może być dozwolone wykonywanie operacji umieszczania i pobierania przez jedną grupę. W przypadku innej grupy może być dozwolona tylko przeglądanie 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 MQ w systemie UNIX, Linux, and Windows” na stronie 415

Administratorzy produktu IBM MQ mogą używać wszystkich komend produktu IBM 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 .

ULW Podczas sprawdzania zabezpieczeń w systemie 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. Następnie program IBM MQ sprawdza, czy ID użytkownika jest uprawniony do łączenia się z menedżerem kolejek i zachowuje ID użytkownika w celu przeprowadzenia przyszłych operacji sprawdzania.

Użytkownicy nie muszą logować się do produktu IBM MQ; IBM MQ zakłada, że użytkownicy wpisali się do bazowego systemu operacyjnego i zostali uwierzytelnieni przez ten system.

Otwieranie obiektu (wywołania MQOPEN lub MQPUT1)
Do obiektów produktu IBM MQ można uzyskać dostęp poprzez otwarcie obiektu i wydanie komend dla niego. 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).

Program IBM MQ sprawdza zasób o nazwie podanej 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 134.

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 w drzewie tematów, w którym aplikacja zasubskrybowano, lub powyżej. 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.

ULW Sposób implementowania kontroli dostępu przez produkt IBM MQ w systemie UNIX, Linux, and Windows

Produkt IBM MQ korzysta z usług zabezpieczeń udostępnianych przez bazowy system operacyjny, korzystając z menedżera uprawnień do obiektów. Produkt IBM MQ udostępnia komendy służące do tworzenia i obsługi list kontroli dostępu.

Interfejs kontroli dostępu o nazwie Interfejs usługi autoryzacji (Authorization Service Interface) jest częścią produktu IBM MQ. Produkt IBM 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 sprawdzaniu dostępu do zabezpieczeń w systemach UNIX, Linux, and Windows” na stronie 373). 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 IBM MQ tylko wtedy, gdy mają odpowiednie uprawnienia. “Kontrolowanie dostępu do obiektów za pomocą OAM w systemie UNIX, Linux, and Windows” na stronie 363 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 IBM MQ udostępnia komendy służące do tworzenia i obsługi list kontroli dostępu. Więcej informacji na temat tych komend zawiera sekcja “Kontrolowanie dostępu do obiektów za pomocą OAM w systemie UNIX, Linux, and Windows” na stronie 363.

Program IBM MQ przekazuje żądanie OAM zawierające nazwę użytkownika, nazwę zasobu i typ dostępu. OAM nadaje lub odrzuca dostęp na podstawie listy ACL, którą utrzymuje. Produkt IBM MQ jest zgodny z decyzją OAM; jeśli OAM nie może podjąć decyzji, program IBM MQ nie zezwala na dostęp.

ULW Identyfikowanie identyfikatora użytkownika w systemie 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 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 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 “Uprawnienie kontekstowe w systemie UNIX, Linux, and Windows” na stronie 423. Aplikacje nie mogą zmieniać tych informacji, jeśli nie zostały autoryzowane do zmiany informacji o kontekście.

ULW *Nazwy użytkowników i grupy w systemie UNIX, Linux, and Windows*

Jednostki główne mogą należeć do grup. Przydzielaniu dostępu do zasobów grupom, a nie osobom fizycznym, można zmniejszyć ilość wymaganych czynności administracyjnych. Listy kontroli dostępu (ACL) są oparte na obu grupach i identyfikatorach 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.

Ten proces definiowania grup i zarządzania nimi jest opisany dla poszczególnych platform:

- Windows Tworzenie grup i zarządzanie nimi w systemie Windows
- AIX Tworzenie grup i zarządzanie nimi w systemie AIX
- Solaris Tworzenie grup i zarządzanie nimi w systemie Solaris

- Linux 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 wprowadzone w przynależności do grupy nazwy użytkownika nie są rozpoznawane do momentu zrestartowania menedżera kolejek, chyba że zostanie wydana komenda MQSC **REFRESH SECURITY** (lub jej odpowiednik PCF).

Linux UNIX **Systemy UNIX and Linux**

Z poziomu produktu IBM MQ 8.0listy kontroli dostępu (ACL) są oparte zarówno na identyfikatorach użytkowników, jak i na grupach, a użytkownik może skorzystać z autoryzacji, ustawiając atrybut **SecurityPolicy** na odpowiednią wartość zgodnie z opisem w sekcji Konfigurowanie usług instalowalnych i Konfigurowanie sekcji usług autoryzacji w systemie UNIX i Linux.

W produkcie IBM MQ 8.0można używać *modelu opartego na użytkownikach* do autoryzacji, a to pozwala na korzystanie zarówno z użytkowników, jak i grup. Jeśli jednak użytkownik określi użytkownika w komendzie setmqaut , nowe uprawnienia mają zastosowanie tylko do tego użytkownika, a nie do grup, do których należy ten użytkownik. Więcej informacji na ten temat zawiera sekcja Uprawnienia oparte na użytkownikach OAM w systemach UNIX i Linux.

Jeśli do autoryzacji używany jest *model oparty na grupie* , do listy ACL dołączona jest grupa podstawowa, do której należy dany identyfikator użytkownika. 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. Użytkownik może zmienić autoryzację w grupie `nobody` , aby nadać dostęp do zasobów produktu IBM MQ użytkownikom 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 `NIEZNANY`.

Identyfikatory użytkowników mogą zawierać do 12 znaków i nazw grup do 12 znaków.

Windows **Systemy Windows**

Listy ACL są oparte na identyfikatorach użytkowników i grupach. Kontrole są takie same, jak w przypadku produktu UNIX. Z tym samym identyfikatorem użytkownika można mieć różnych użytkowników w różnych domenach. Produkt IBM 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_name\group_name
```

Grupy globalne są sprawdzane przez OAM tylko w dwóch przypadkach:

1. Sekcja zabezpieczeń menedżera kolejek zawiera następujące ustawienie: `GroupModel=GlobalGroups`. Patrz sekcja Zabezpieczanie.
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 IBM MQ przy użyciu 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.

Więcej informacji na temat ustawiania atrybutu **SecurityPolicy** w systemie Windowszawiera sekcja Usługi instalowalne oraz sekcja Konfigurowanie sekcji usług autoryzacji w systemie Windows.

Windows *Identyfikatory zabezpieczeń Windows (identyfikatory SID)*

Produkt IBM MQ w systemie Windows korzysta z identyfikatora SID, w którym jest dostępny. Jeśli identyfikator SID produktu Windows nie jest dostarczony z żądaniem autoryzacji, produkt IBM 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, które identyfikują pełne szczegóły konta użytkownika w bazie danych SAM (Security account manager) produktu Windows , w której zdefiniowany jest użytkownik. Gdy komunikat jest tworzony w systemie IBM MQ for Windows, program IBM MQ zapisuje identyfikator SID w deskryptorze komunikatu. Gdy program IBM MQ na serwerze Windows przeprowadza 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 produktu Windows nie jest dostarczony wraz z żądaniem autoryzacji, produkt IBM 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 IBM MQ . Aby zapobiec temu problemowi, należy dołączyć identyfikator SID w każdym żądaniu autoryzacji. Identyfikator SID jest używany przez produkt IBM MQ do ustanawiania referencji użytkownika.

Aby określić, że wszystkie żądania autoryzacji muszą zawierać identyfikator SID, należy użyć **regedit**. Ustaw parametr SecurityPolicy na wartość NTSIDsRequired.

ULW Uprawnienia użytkownika alternatywnego w systemie UNIX, Linux, and Windows

Użytkownik może określić, że ID użytkownika może korzystać z uprawnień innego użytkownika podczas uzyskiwania dostępu do obiektu IBM MQ . Jest to nazywane *uprawnieniami użytkownika alternatywnego*i można go używać w dowolnym obiekcie IBM 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.

ULW Uprawnienie kontekstowe w systemie UNIX, Linux, and Windows

Kontekst jest informacją, która ma zastosowanie do konkretnego komunikatu i jest zawarty w deskryptorze komunikatu MQMD, który jest częścią komunikatu. Aplikacje mogą określać dane kontekstu podczas wykonywania wywołania MQOPEN lub MQPUT .

Informacje o kontekście znajdują się w dwóch sekcjach:

Sekcja Tożsamość
Od kogo pochodzi wiadomość. Składa się z pól UserIdentifier, AccountingTokeni ApplIdentityData .

Sekcja pochodzenia
Skąd pochodzi komunikat i kiedy został umieszczony w kolejce. Składa się z pól PutApplType, PutApplName, PutDate, PutTimei ApplOriginData .

Aplikacje mogą określać dane kontekstu podczas wykonywania wywołania MQOPEN lub MQPUT . Te dane mogą być generowane przez aplikację, przekazywane z innego komunikatu lub domyślnie generowane przez menedżer kolejek. Na przykład dane kontekstowe mogą być używane przez programy serwera do sprawdzania tożsamości requestera, sprawdzając, czy komunikat pochodzi z aplikacji działającej z autoryzowanym ID użytkownika.

Program serwera może użyć UserIdentifier do określenia identyfikatora użytkownika alternatywnego. Autoryzacja kontekstu służy do określania, czy użytkownik może określić dowolne opcje kontekstu dla dowolnego wywołania MQOPEN lub MQPUT1 .

Sekcja Kontrolowanie informacji o kontekście zawiera informacje o opcjach kontekstu, a sekcja Przegląd deskryptora MQMD zawiera opisy pól deskryptora komunikatu związanych z kontekstem.

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 IBM 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.

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.

Multi W systemie Wiele platform, o ile wartość *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 połączeniu się 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.

z/OS 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 aplikacją kliencką IBM MQ przepływa z połączenia klienckiego MCA do połączenia z serwerem 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 IBM MQ MQI client . 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 w kanale używany jest protokół TLS, nazwa wyróżniająca partnera (DN) 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 IBM WebSphere MQ 7.1 mogą wymagać aktualizacji. Więcej informacji na ten temat zawiera sekcja Programy obsługi wyjścia zabezpieczeń kanału.

Uwierzytelnianie użytkownika menedżera uprawnień do obiektów produktu IBM MQ

W przypadku połączeń produktu IBM MQ MQI client można użyć wyjścia zabezpieczeń w celu zmodyfikowania lub utworzenia 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, gdy uzyskuje dostęp do zasobów IBM 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 346.

Implementowanie kontroli dostępu w wyjściu API i interfejsie wyjścia funkcji API

Wyjście funkcji API lub wyjście funkcji API może zapewnić dostęp do elementów sterujących w celu uzupełnienia tych udostępnionych przez produkt IBM 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.

Autoryzacja LDAP

Za pomocą autoryzacji LDAP można usunąć potrzebę użycia lokalnego identyfikatora użytkownika.

Dostępność autoryzacji LDAP na obsługiwanych platformach

Autoryzacja LDAP jest dostępna na następujących platformach:

- UNIX
- IBM i
- Windows

Ostrzeżenie:

Z ogólnej dostępności produktu IBM MQ 9.0 ta funkcja jest dostępna we wszystkich menedżerach kolejek, niezależnie od tego, czy są to nowe, czy migrowane z wcześniejszej wersji.

Przegląd autoryzacji LDAP

Za pomocą autoryzacji LDAP komendy, które obsługują konfigurację autoryzacji, takie jak **setmqaut** i **DISPLAY AUTHREC**, mogą przetwarzać nazwy wyróżniające. Wcześniej użytkownicy zostali uwierzytelnieni poprzez porównanie ich referencji z maksymalnymi dostępnymi znakami, które istnieją dla użytkowników i grup w lokalnym systemie operacyjnym.

Ostrzeżenie: Jeśli została uruchomiona komenda **DEFINE AUTHINFO** , należy zrestartować menedżer kolejek. Jeśli menedżer kolejek nie zostanie zrestartowany, komenda setmqaut nie zwróci poprawnego wyniku.

Jeśli użytkownik udostępnia ID użytkownika, a nie nazwę wyróżniającą, ID użytkownika jest przetwarzany. Na przykład, gdy w kanale z PUTAUT (CTX) pojawia się komunikat przychodzący, znaki w ID użytkownika są odwzorowywane na nazwę wyróżniającą LDAP, a odpowiednie sprawdzenia autoryzacji są wykonywane.

Inne komendy, takie jak **DISPLAY CONN**, kontynuują pracę i przedstawiają rzeczywistą wartość dla identyfikatora użytkownika, nawet jeśli ten ID użytkownika może nie istnieć w lokalnym systemie operacyjnym.

UNIX Gdy autoryzacja LDAP jest w miejscu, menedżer kolejek zawsze używa modelu zabezpieczeń użytkownika na platformach UNIX , niezależnie od atrybutu **SecurityPolicy** w pliku `qm.ini` . Więc ustawianie uprawnień dla pojedynczego użytkownika wpływa tylko na tego użytkownika, a nie na nikogo innego, kto należy do żadnej z tych grup.

Podobnie jak w przypadku modelu systemu operacyjnego, użytkownik nadal ma połączone uprawnienie, które zostało przypisane zarówno do jednostki, jak i do wszystkich grup (jeśli istnieją), do których należy użytkownik.

Załóżmy na przykład, że następujące rekordy zostały zdefiniowane w repozytorium LDAP.

- W klasie **inetOrgPerson** :

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
        email=JohnDoe1@yourcompany.com [longer than 12 characters]
        shortu=jodoe
        Phone=1234567
```

- W klasie **groupOfNames** :

```
dn="cn=Application Group A, ou=groups, o=yourcompany, c=yourcountry"
        longname=ApplicationGroupA [longer than 12 characters]
        members="cn=JaneDoe, ou=users, o=yourcompany, c=yourcountry",
                "cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
```

Na potrzeby uwierzytelniania menedżer kolejek używający tego serwera LDAP musi być zdefiniowany w taki sposób, aby jego wartość **CONNAUTH** wskazywała na obiekt **AUTHINFO** o typie IDPWLDAPi którego odpowiednie atrybuty rozdzielczość nazw są prawdopodobnie ustawione w następujący sposób:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Biorąc pod uwagę tę konfigurację do uwierzytelniania, aplikacja może wypełnić pole CSPUserID używane w wywołaniu MQCNO, przy użyciu jednego z następujących zestawów wartości:

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

lub wersji

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

W obu przypadkach system może użyć podanych wartości do uwierzytelnienia kontekstu systemu operacyjnego. " jodoe".

Ustawianie autoryzacji

Sposób użycia nazwy skróconej lub **USRFIELD** w celu ustawienia autoryzacji.

Podejście do pracy z wieloma formatami, opisanymi w “Autoryzacja LDAP” na stronie 425, jest kontynuowane w komendach autoryzacji, z dalszym rozszerzeniem, które może być używane przez produkt shortname lub USRFIELD w sposób nieprzystosowany do pracy.

Łańcuch znaków określa określony atrybut w rekordzie LDAP podczas nadawania nazw użytkownikom (principals) do autoryzacji.

Ważne: Łańcuch znaków nie może zawierać znaku = , ponieważ znak ten nie może być używany w ID użytkownika systemu operacyjnego.

Jeśli użytkownik przekaże nazwę użytkownika OAM do autoryzacji, która jest potencjalnie shortname, łańcuch znaków musi zmieścić się na 12 znaków. Algorytm odwzorowania najpierw próbuje go rozstrzygnąć na nazwę wyróżniającą przy użyciu atrybutu SHORTUSR w jego zapytaniu LDAP.

Jeśli błąd ten zakończy się niepowodzeniem z błędem UNKNOWN_ENTITY lub jeśli podany łańcuch nie może być shortname, to w celu skonstruowania zapytania LDAP zostanie podjęta kolejna próba użycia atrybutu USRFIELD.

Ostrzeżenie: Jeśli użytkownik uruchomił komendę DEFINE AUTHINFO, należy zrestartować menedżer kolejek. Jeśli menedżer kolejek nie zostanie zrestartowany, komenda setmqaut nie zwróci poprawnego wyniku.

Aby można było przetwarzać autoryzacje użytkowników, następujące ustawienia komendy setmqaut są równoważne.

Tabela 72. Ustawienia autoryzacji użytkownika

Komenda	**Uwaga**
setmqaut -m QM -t qmgr -p jodoe +connect	Jest to płaska, niekwalifikowana nazwa, rozwiązana przez SHORTUSR.
setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect	Również płaska, niekwalifikowana nazwa, tłumaczana przez USRFIELD na ten sam podmiot.
setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect	Korzystanie z nazwanego atrybutu.

Tabela 72. Ustawienia autoryzacji użytkownika (kontynuacja)	
Komenda	**Uwaga**
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	Za pomocą innego nazwanego atrybutu, który nie musi być żaden z tych skonfigurowanych w obiekcie AUTHINFO.

Komendy MQSC SET AUTHREC można użyć jako alternatywy dla komendy **setmqaut** :

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

lub za pomocą komendy PCF Set Authority Record (MQCMD_SET_AUTH_REC) z elementem MQCACF_PRINCIPAL_ENTITY_NAMES zawierającym łańcuch:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Podczas przetwarzania grup nie ma dwuznaczności na temat przetwarzania produktu `shortname` , ponieważ nie ma wymogu dopasowania dowolnej nazwy grupy do 12-znaków. Oznacza to, że dla grup nie ma odpowiednika atrybutu SHORTUSR.

Oznacza to, że przykłady składni opisane w podręczniku Tabela 73 na stronie 428 są poprawne, zakładając, że został skonfigurowany obiekt AUTHINFO z atrybutami rozszerzanymi i ustawiony na:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabela 73. Ustawienia autoryzacji grupy	
Komenda	**Uwaga**
`setmqaut -m QM -t qmgr -g ApplicationGroupA +connect`	Używanie GRPFIELD do rozstrzygnięcia
`setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect`	Nazywanie pojedynczego atrybutu
`setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect`	Korzystanie z pełnej nazwy wyróżniającej

Komendy MQSC SET AUTHREC można użyć jako alternatywy dla poprzedniej komendy **setmqaut** :

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

lub za pomocą komendy PCF Ustaw rekord uprawnień (Set Authority Record-MQCMD_SET_AUTH_REC) z elementem MQCACF_GROUP_ENTITY_NAMES zawierającym łańcuch:

```
 "ApplicationGroupA"
```

Ważne:

W zależności od formatu, który będzie używany do odwołania się do nazwy użytkownika lub grupy, musi istnieć możliwość uzyskania unikalnej nazwy wyróżniającej.

Tak więc na przykład nie można mieć dwóch odrębnych rekordów, które mają "`shortu=jodoe`".

Jeśli nie można określić pojedynczej unikalnej nazwy wyróżniającej, OAM zwraca wartość MQRC_UNKNOWN_ENTITY.

Wyświetlanie autoryzacji

Różne metody wyświetlania autoryzacji użytkowników lub grup.

dspmqaut, komenda

Najprostszą metodą wyświetlania autoryzacji dostępnych dla użytkownika lub grupy jest użycie komendy dspmqaut .

W celu zidentyfikowania użytkownika lub grupy można użyć zapytania dotyczącego dowolnej z wariantów składni. Należy zauważyć, że dane wyjściowe komendy powtarzają tożsamość w formacie podanym w wierszu komend. Dane wyjściowe nie są raportowane w pełnej rozstrzygniętej nazwie wyróżniającej.

Na przykład:

```
dspmqaut -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
    connect
```

lub wersji

```
dspmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
    connect
```

Komendy dmpmqaut i dmpmqcfg

Komenda dmpmqaut oraz jej odpowiedniki MQSC lub PCF mogą określać nazwę użytkownika lub grupę w dowolnym z obsługiwanych formatów, na przykład w tabelach produktu **setmqaut** opisanych w sekcji “Ustawianie autoryzacji” na stronie 427. Jednak w odróżnieniu od **dspmqaut**, komenda **dmpmqaut** zawsze raportuje pełną nazwę wyróżniającą.

```
dmpmqaut -m QM -t qmgr -p jodoe
------------------------------------
profile: self
object type:qmgr
entity:cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry
entity type: principal
authority: connect
```

Podobnie komenda dmpmqcfg , która nie ma żadnego filtrowania w wybranych rekordach, zawsze wyświetla pełną nazwę wyróżniającą w formacie, który może zostać później powtórzony.

```
dmpmqcfg -m QM -x authrec
------------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

Inne uwagi dotyczące korzystania z autoryzacji LDAP

Krótki opis zmian w interfejsie kolejek komunikatów (MQI) oraz innych komend MQSC i PCF, które należy znać podczas korzystania z autoryzacji LDAP z produktu IBM MQ 9.0.0.

ADOPTCTX

Nie ma wymagania, aby aplikacje udostępniły informacje uwierzytelniające, lub aby atrybut ADOPTCTX został ustawiony na wartość YES.

Jeśli aplikacja nie uwierzytelnia się jawnie lub jeśli parametr **ADOPTCTX** ma wartość NO dla aktywnego obiektu CONNAUTH, to kontekst tożsamości powiązany z aplikacją jest przyjmowany z identyfikatora użytkownika systemu operacyjnego.

Jeśli wymagane jest zastosowanie autoryzacji, kontekst ten jest odwzorowywany na tożsamość LDAP przy użyciu tych samych reguł, co w przypadku komend setmqaut .

Parametry wejściowe do wywołań MQI

MQOPEN, MQPUT1i MQSUB mają struktury, które umożliwiają określenie alternatywnego identyfikatora użytkownika.

Jeśli używane są te pola, 12-znakowy ID użytkownika jest odwzorowywany na nazwę wyróżniającą przy użyciu tych samych reguł, co w komendach **setmqaut**, **dmpmqaut**i **dspmqaut** .

Komendy MQPUT i MQPUT1 umożliwiają również ustawianie odpowiednio autoryzowanych programów w celu ustawienia pola MQMD UserIdentifier . Wartość tego pola nie jest policowana podczas procesu PUT i może być ustawiona na dowolną wartość.

Jednak jak zwykle, wartość **UserIdentifier** może być używana do autoryzacji na późniejszych etapach przetwarzania komunikatów, na przykład wtedy, gdy parametr PUTAUT (CTX) jest zdefiniowany w kanale odbierającym.

W tym momencie identyfikator zostanie sprawdzony pod kątem autoryzacji przy użyciu konfiguracji tego menedżera kolejek odbiorczego-może to być protokół LDAP lub oparty na systemie OS-ów.

Parametry wyjściowe do wywołań MQI

Wszędzie tam, gdzie identyfikator użytkownika jest udostępniany programowi w strukturze MQI, jest to 12-znakowa skrócona wersja nazwy powiązana z połączeniem.

Na przykład wartością **MQAXC.UserId** Exits interfejsu API jest skrócona nazwa zwrócona przez odwzorowanie LDAP.

Inne administracyjne komendy MQSC i PCF

Komendy, które przedstawiają informacje o użytkowniku w statusie obiektu, takie jak DISPLAY CONN USERID zwracają 12-znakową nazwę skróconą powiązaną z kontekstem. Pełna nazwa wyróżniająca nie jest wyświetlana.

Komendy pozwalające na asercję tożsamości, takie jak reguły odwzorowania CHLAUTH lub wartości MCAUSER dla kanałów, mogą przyjmować wartości do maksymalnej długości zdefiniowanej dla tych atrybutów (obecnie 64 znaki).

Nie ma żadnej zmiany składni. Jeśli dla tej tożsamości wymagana jest autoryzacja, jest ona wewnętrznie odwzorowywana na nazwę wyróżniającą, używając tych samych reguł, co w komendach **setmqaut**, **dmpmqaut**i **dspmqaut** .

Oznacza to, że wartość parametru MCAUSER w definicji kanału może nie być wyświetlana jako ten sam łańcuch co DISPLAY CHSTATUS , ale odnoszą się one do tej samej tożsamości.

Na przykład:

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

Następnie DISPLAY CHSTATUS (*) ALL wyświetla wartość SHORTUSR, *MCAUSER (jodoe)* dla wszystkich połączeń.

Przełączanie między modelami autoryzacji systemu operacyjnego i LDAP

W jaki sposób przełącza się między różnymi metodami autoryzacji na różnych platformach.

Atrybut CONNAUTH punktów menedżera kolejek w obiekcie AUTHINFO. Jeśli obiekt jest typu IDPWLDAP, do uwierzytelniania używany jest repozytorium LDAP.

Teraz można zastosować metodę autoryzacji do tego samego obiektu, co pozwala na kontynuowanie autoryzacji opartej na systemie operacyjnym lub pracę z autoryzacją LDAP.

Platformy UNIX i IBM i

IBM i UNIX

Menedżer kolejek może być przełączany w dowolnym momencie między modelami systemu operacyjnego i LDAP. Konfigurację i konfigurację tej konfiguracji można zmienić za pomocą komendy REFRESH SECURITY TYPE (CONNAUTH) .

Na przykład, jeśli ten obiekt został już skonfigurowany z informacjami o połączeniu na potrzeby uwierzytelniania:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
        AUTHORMD(SEARCHGRP) +
        BASEDNG('ou=groups,o=ibm,c=uk') +
        <other attributes>
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

Windows

Windows

Jeśli zmiana konfiguracji uprawnień obejmuje przełączanie między modelami systemu operacyjnego i LDAP, menedżer kolejek musi zostać zrestartowany, aby zmiany zostały uwzględnione. W przeciwnym razie można wprowadzić zmiany za pomocą komendy REFRESH SECURITY TYPE (CONNAUTH) .

Reguły przetwarzania

Podczas przełączania się z systemu operacyjnego na autoryzację LDAP wszystkie istniejące reguły uprawnień systemu operacyjnego, które zostały ustawione, stają się nieaktywne i niewidoczne.

Komendy, takie jak **dmpmqaut** , nie wyświetlają tych reguł systemu operacyjnego. Podobnie, podczas przełączania się z katalogu LDAP do systemu operacyjnego wszystkie zdefiniowane autoryzacje LDAP stają się nieaktywne i niewidoczne, przywracając oryginalne reguły systemu operacyjnego.

Aby z dowolnej przyczyny utworzyć kopię zapasową definicji menedżera kolejek za pomocą komendy **dmpmqcfg** , ta kopia zapasowa będzie zawierać tylko te reguły, które są zdefiniowane dla danej metody autoryzacji w momencie tworzenia kopii zapasowej.

Administrowanie LDAP

Przegląd informacji o tym, w jaki sposób każda platforma administruje LDAP.

Jeśli używana jest autoryzacja LDAP, przypisanie do grupy `mqm` (lub jej odpowiedników) w systemie operacyjnym nie jest takie ważne. Bycie członkiem tej grupy kontroluje tylko, czy niektóre komendy wiersza komend mogą być przetwarzane.

W szczególności należy być w tej grupie, aby wydać komendy strmqm i endmqm .

Gdy menedżer kolejek jest uruchomiony, istnieją ograniczenia dotyczące konta w pełni uprzywilejowanego. Oprócz identyfikatora użytkownika, który wydaje komendę **strmqm** , inni użytkownicy należący do grupy systemu operacyjnego `mqm` (lub równoważnej) nie mają specjalnych uprawnień.

Autoryzacje innych użytkowników są oparte na grupach LDAP, do których należą. Niekwalifikowane użycie nazwy grupy `mqm` w komendach, takich jak **setmqaut** , nie jest dozwolone, aby można było odwzorować na dowolną grupę LDAP.

UNIX platformy

Gdy menedżer kolejek jest uruchomiony, jedynym automatycznie w pełni uprzywilejowanym kontem jest rzeczywisty użytkownik, który uruchomił menedżer kolejek.

Identyfikator `mqm` nadal istnieje i jest używany jako właściciel zasobów systemu operacyjnego, takich jak pliki, ponieważ `mqm` jest efektywnym identyfikatorem, pod którym działa menedżer kolejek. Jednak użytkownik `mqm` nie będzie mógł automatycznie wykonywać czynności administracyjnych kontrolowanych przez OAM.

IBM i

W systemie IBM ikonta automatycznie uprzywilejowane są to konta, które uruchamiają menedżera kolejek i identyfikator QMQM.

Wymagane są oba identyfikatory, ponieważ identyfikator użytkownika, który uruchamia menedżer kolejek, jest wymagany tylko do uruchomienia systemu. Po uruchomieniu procesy menedżera kolejek mają tylko uprawnienie QMQM.

Windows platformy

W systemie Windowskonta automatycznie w pełni uprzywilejowane to użytkownik systemu operacyjnego, który uruchomił menedżer kolejek, a także użytkownik uruchamiający podstawowe procesy menedżera kolejek, takie jak MUSR_MQADMIN, jeśli menedżer kolejek został uruchomiony jako usługa Windows .

Podczas pracy w trybie autoryzacji LDAP produkt Windows działa podobnie jak platformy UNIX . Zajmuje się 12-znakowymi nazwami skróconą, a pełną nazwą DN.

Przykładowy skrypt

W związku z tym, że grupa może wykonywać pełną administrację w menedżerze kolejek, przykładowy skrypt jest dostarczany na platformach UNIX jako:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

Ten przykład przyjmuje dwa parametry:

- Nazwa menedżera kolejek
- Nazwa grupy LDAP

Przykładowe procesy komendy setmqaut , nadając pełne uprawnienia dla wszystkich obiektów. Jest to ten sam skrypt, który jest generowany przez kreator OAM produktu IBM MQ Explorer dla ról administracyjnych. Na przykład kod rozpoczyna się od:

```
setmqaut -t q -m qmgr -n "**" +alladm +allmqi -g
      groupname
```

Poufność komunikatów

Aby zachować poufność, należy zaszyfrować komunikaty. W zależności od potrzeb dostępne są różne metody szyfrowania komunikatów w produkcie IBM 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 programu Advanced Message Security do zaszyfrowania komunikatów, lub napisać własne wyjście funkcji API lub wyjście funkcji API.

Jeśli wymagane jest szyfrowanie wiadomości tylko wtedy, gdy są one transportowane za pośrednictwem kanału, ponieważ w menedżerach kolejek są odpowiednie zabezpieczenia, można użyć protokołu TLS lub można napisać własne wyjście zabezpieczeń, wyjście komunikatów lub programy obsługi wyjścia wysyłania i odbierania.

z/OS V 9.1.4 Jeśli konieczne jest szyfrowanie komunikatów w stanie spoczynku w menedżerze kolejek, można użyć funkcji szyfrowania zestawu danych z/OS w tym menedżerze kolejek.

Więcej informacji na temat produktu Advanced Message Securityzawiera sekcja “Planowanie dla produktu Advanced Message Security” na stronie 107. Korzystanie z protokołu TLS z produktem IBM MQ jest opisane w sekcji “Protokoły zabezpieczeń TLS w produkcie IBM 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 462.

Patrz sekcja poufność danych w produkcie IBM MQ for z/OS przy użyciu szyfrowania zestawu danych. Aby uzyskać więcej informacji na temat szyfrowania zestawu danych z/OS .

Zadania pokrewne

Łączenie dwóch menedżerów kolejek za pomocą protokołu TLS

Bezpieczne podłączanie klienta do menedżera kolejek

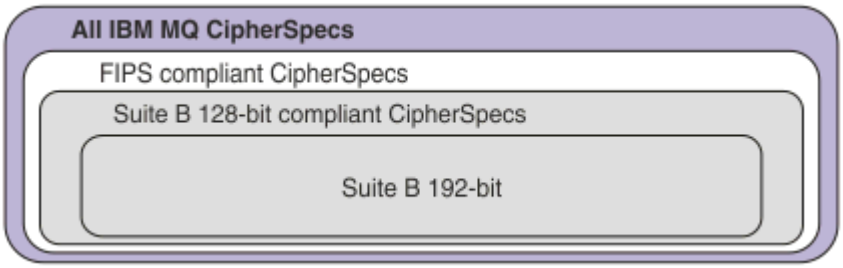
Włączanie opcji CipherSpecs

Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

Niektóre ze specyfikacji CipherSpecs , których można używać z produktem IBM MQ , są zgodne ze standardem FIPS. Niektóre atrybuty zgodne ze standardem FIPS (CipherSpecs) są zgodne ze standardem Suite B, ale inne, na przykład TLS_RSA_WITH_AES_256_CBC_SHA, nie są zgodne.

Wszystkie specyfikacje CipherSpecs zgodne ze standardem Suite B są również zgodne ze standardem FIPS. Wszystkie zgodne elementy CipherSpecs Suite B należą do dwóch grup: 128 bitów (na przykład ECDHE_ECDSA_AES_128_GCM_SHA256) i 192 bit (na przykład ECDHE_ECDSA_AES_256_GCM_SHA384),

Na poniższym diagramie przedstawiono relacje między tymi podzbiorami:



Liczba obsługiwanych specyfikacji CipherSpecs została zmniejszona z IBM MQ 8.0.0 Fix Pack 3 .

V 9.1.1 Więcej informacji na temat konfigurowania domyślnej specyfikacji CipherSpecszawiera sekcja “Domyślne wartości atrybutu CipherSpec włączone w produkcie IBM MQ” na stronie 437. Istnieje również możliwość udostępnienia alternatywnego zestawu specyfikacji CipherSpecs , które są włączone w celu użycia z kanałami MQ . Patrz “Udostępnianie niestandardowej listy włączonych specyfikacji CipherSpecs na wielu platformach” na stronie 438.

Więcej informacji na temat włączania nieaktualnych specyfikacji CipherSpecsmożna znaleźć w sekcji “Włączanie nieaktualnych specyfikacji CipherSpecs na wielu platformach” na stronie 439 lub “Włączanie nieaktualnych specyfikacji CipherSpecs w systemie z/OS” na stronie 439. Listę obiektów CipherSpecs ,

które można ponownie włączyć w celu użycia z produktem IBM MQ, można znaleźć w sekcji “Nieaktualne CipherSpecs” na stronie 442.

ULW V 9.1.4 W produkcie IBM MQ 9.1.4produkt IBM MQ obsługuje protokół zabezpieczeń TLS 1.3 w systemie UNIX, Linux, and Windows. Informacje na temat używania tych specyfikacji CipherSpecszawierają “Korzystanie z protokołu TLS 1.3 w produkcie IBM MQ” na stronie 437 i “IBM MQ MQI client i TLS 1.3” na stronie 437.

CipherSpecs , których można używać z obsługą protokołu IBM MQ TLS

Specyfikacje szyfru, które mogą być używane z menedżerem kolejek produktu IBM MQ , są automatycznie wymienione w poniższej tabeli. Jeśli żądasz certyfikatu osobistego, należy podać wielkość klucza dla pary kluczy publicznego i prywatnego. Wielkość klucza używana podczas uzgadniania TLS jest wielkością zapisaną w certyfikacie, o ile nie jest ona określona przez atrybut CipherSpec, co zostało określone w tabeli.

Tabela 74. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ

Obsługa platformy “1” na stronie 436	**Nazwa specyfikacji szyfrowania**	**Kod szesnastkowy**	**Używany protokół**	**Integralność danych**	**Algorytm szyfrowania (bity szyfrowania)**	**FIPS** “2” na stronie 436	**Suite B**
V 9.1.4 V 9.1.4 **Specyfikacje szyfrowania aliasów**							
Wszystkie	ANY_TLS13_OR_HIGHER “3” na stronie 436 “4” na stronie 436 “5” na stronie 436	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY_TLS13 “4” na stronie 436 “5” na stronie 436 “6” na stronie 436	N/D	TLS 1.3	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY_TLS12_OR_HIGHER “4” na stronie 436 “5” na stronie 436 “7” na stronie 436	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY_TLS12 “8” na stronie 436	N/D	TLS 1.2	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY “9” na stronie 436	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane
V 9.1.4 V 9.1.4 **Specyfikacje szyfrowania dla protokołu TLS 1.3**							
Wszystkie	TLS_AES_128_GCM_SHA256 “4” na stronie 436	1301	TLS 1.3	GCM	AES-128 z GCM (128)	Tak	Nie
Wszystkie	TLS_AES_256_GCM_SHA384 “4” na stronie 436	1302	TLS 1.3	GCM	AES-256 z GCM (256)	Tak	Nie
Wszystkie	TLS_CHACHA20_POLY1305_SHA256 “4” na stronie 436	1303	TLS 1.3	POLY1305	CHACHA20 (256)	Nie	Nie

Tabela 74. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 436	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 436	Suite B
ULW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	AES-128 z funkcją CTR (128)	Tak	Nie
ULW	TLS_AES_128_CCM_8_SHA256 "11" na stronie 436	1305	TLS 1.3	CBC-MAC	AES-128 z funkcją CTR (128)	Tak	Nie
Specyfikacje szyfrowania dla protokołu TLS 1.2							
Wszystkie	TLS_RSA_WITH_AES_128_CBC_SHA256 "10" na stronie 436	003C	TLS 1.2	SHA-256	AES (128)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_256_CBC_SHA256 "10" na stronie 436 "12" na stronie 436	003D	TLS 1.2	SHA-256	Algorytm AES (256)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_128_GCM_SHA256 "10" na stronie 436 "13" na stronie 436	009C	TLS 1.2	SHA-256 i AEAD GCM	AES (128)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_256_GCM_SHA384 "10" na stronie 436 "12" na stronie 436 "13" na stronie 436	009D	TLS 1.2	SHA-384 i AEAD GCM	Algorytm AES (256)	Tak	Nie
Wszystkie	ECDHE_ECDSA_AES_128_CBC_SHA256 "10" na stronie 436	C023	TLS 1.2	SHA-256	AES (128)	Tak	Nie
Wszystkie	ECDHE_ECDSA_AES_256_CBC_SHA384 "10" na stronie 436 "12" na stronie 436	C024	TLS 1.2	SHA-384	Algorytm AES (256)	Tak	Nie
Wszystkie	ECDHE_RSA_AES_128_CBC_SHA256 "10" na stronie 436	C027	TLS 1.2	SHA-256	AES (128)	Tak	Nie
Wszystkie	ECDHE_RSA_AES_256_CBC_SHA384 "10" na stronie 436 "12" na stronie 436	C028	TLS 1.2	SHA-384	Algorytm AES (256)	Tak	Nie
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 "12" na stronie 436 "13" na stronie 436	C02B	TLS 1.2	SHA-256 i AEAD GCM	Algorytm AES (SHA384)	Tak	128 bitów
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 "12" na stronie 436 "13" na stronie 436	C02C	TLS 1.2	SHA-384 i AEAD GCM	Algorytm AES (SHA384)	Tak	192 bity
Wszystkie	ECDHE_RSA_AES_128_GCM_SHA256 "13" na stronie 436	C02F	TLS 1.2	SHA-256 i AEAD GCM	AES (128)	Tak	Nie
Wszystkie	ECDHE_RSA_AES_256_GCM_SHA384 "12" na stronie 436 "13" na stronie 436	C030	TLS 1.2	AEAD AES-128 GCM	Algorytm AES (SHA384)	Tak	Nie

Tabela 74. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 436	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 436	Suite B

Uwagi:

1. Listę platform obsługiwanych przez każdą z ikon platformy można znaleźć w sekcji Ikony platform i wersji w dokumentacji produktu.
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. ULW Specyfikacja szyfrowania aliasów ANY_TLS13_OR_HIGHER negocjuje najwyższy poziom zabezpieczeń, który umożliwia zdalny element końcowy połączenia. Połączenie jest nawiązywane tylko za pośrednictwem protokołu TLS 1.3 lub nowszego.
4. z/OS Aby można było używać protokołu TLS 1.3 lub JAKIEJKOLWIEK specyfikacji szyfrów w systemie IBM MQ for z/OS, wymagany jest system operacyjny z/OS 2.4 lub nowszy.
5. IBM i Aby można było używać protokołu TLS 1.3 lub JAKIEJKOLWIEK specyfikacji szyfrów w systemie IBM i, wersja systemu operacyjnego musi obsługiwać protokół TLS 1.3. Więcej informacji na ten temat można znaleźć na stronie Obsługa systemowa protokołu TLS 1.3.
6. ULW Specyfikacja szyfrowania aliasów ANY_TLS13 reprezentuje podzbiór akceptowalnych specyfikacji szyfrowania korzystających z protokołu TLS 1.3. Te specyfikacje szyfrowania wymieniono w poniższej tabeli z uwzględnieniem platform.
7. ULW Specyfikacja szyfrowania aliasów ANY_TLS12_OR_HIGHER negocjuje najwyższy poziom zabezpieczeń, który umożliwia zdalny element końcowy połączenia. Połączenie jest nawiązywane tylko za pośrednictwem protokołu TLS 1.2 lub nowszego.
8. Specyfikacja szyfrowania ANY_TLS12 reprezentuje podzbiór akceptowalnych specyfikacji szyfrowania korzystających z protokołu TLS 1.2. Te specyfikacje szyfrowania wymieniono w poniższej tabeli z uwzględnieniem platform.
9. ULW Specyfikacja szyfrowania aliasów ANY negocjuje najwyższy poziom zabezpieczeń, który umożliwia zdalny element końcowy połączenia.
10. IBM i Następujące specyfikacje szyfrowania nie są włączone w systemach IBM i 7.4 i mają wartość systemową QSSLCSLCTL ustawioną na *OPSSYS.
11. ULW Te specyfikacje szyfrowania korzystają z wartości sprawdzania integralności (Integrity Check Value – ICV) złożonej z 8 oktetów, a nie z 16.
12. Ta specyfikacja szyfrowania nie może być używana do zabezpieczania połączenia programu IBM MQ Explorer z menedżerem kolejek, chyba że do środowiska JRE używanego przez program Explorer zastosowano odpowiednie nieograniczone pliki strategii.
13. Windows Linux Zgodnie z zaleceniem GSKitprotokół TLS 1.2 GCM CipherSpecs ma ograniczenie, które oznacza, że po wysłaniu rekordów TLS o treści 2o324.5 przy użyciu tego samego klucza sesji połączenie zostanie przerwane i zostanie wyświetlony komunikat AMQ9288E. To ograniczenie GCM jest aktywne, niezależnie od używanego trybu FIPS.

    Aby zapobiec występowaniu tego błędu, należy unikać używania szyfrów TLS 1.2 GCM , włączyć resetowanie klucza tajnego lub uruchomić menedżera kolejek lub klienta IBM MQ z ustawioną zmienną środowiskową GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE . W przypadku bibliotek produktu GSKit należy ustawić tę zmienną środowiskową po obu stronach połączenia i zastosować ją zarówno do połączeń klienta z menedżerem kolejek, jak i połączeń menedżera kolejek z menedżerem kolejek. Należy zauważyć, że to ustawienie ma wpływ na niezarządzane klienty .NET , ale nie na klienty Java ani zarządzane klienty .NET . Więcej informacji na ten temat zawiera sekcja Ograniczenie szyfrowania AES-GCM.

Korzystanie z protokołu TLS 1.3 w produkcie IBM MQ

ULW V 9.1.4

Z poziomu produktu IBM MQ 9.1.4produkt IBM MQ obsługuje protokół TLS 1.3 w systemie UNIX, Linux, and Windows. W każdej obsługiwanej instalacji nowe menedżery kolejek są tworzone z wpisem w sekcji SSL sekcji pliku `qm.ini` , która zawiera następujące elementy:

```
SSL:
  AllowTLSV13=TRUE
```

Uwaga: Plik `qm.ini` można znaleźć w katalogu *<data directory>*`/qmgrs/`*<qmgr name>*.

Jeśli menedżer kolejek został utworzony przy użyciu produktu IBM MQ w wersji wcześniejszej niż IBM MQ 9.1.4, ale później został uruchomiony przy użyciu produktu IBM MQ 9.1.4 lub nowszej, nie będzie miał ustawionego zestawu właściwości **AllowTLSV13** . Aby włączyć protokół TLS 1.3, należy dokonać edycji `qm.ini file` i dodać do niej właściwość w sposób przedstawiony w przykładzie (w tym sekcję "SSL:", jeśli jeszcze nie istnieje).

Ta właściwość pliku .ini umożliwia obsługę protokołu TLS 1.3, co umożliwia korzystanie z protokołu TLS 1.3 CipherSpecs. Zgodnie ze specyfikacją TLS 1.3wszelkie próby komunikacji ze słabą wartością CipherSpec, niezależnie od tego, czy są włączone w produkcie IBM MQ , czy nie, zostaną odrzucone. Specyfikacja CipherSpecs , którą TLS 1.3 uważa za słabe, to CipherSpecs , które spełniają jeden lub kilka z następujących kryteriów:

- Korzysta z protokołu SSL 3.0 .
- Używa algorytmu szyfrowania RC4 lub RC2 jako algorytmu szyfrowania.
- Ma wielkość klucza szyfrowania (bit) równa lub mniejsza niż 112.

Te ograniczenia są oznaczone jako adnotacja [10] w Tabeli 1 nieaktualnych specyfikacji CipherSpecs.

Jeśli konieczne jest kontynuowanie korzystania z takich specyfikacji CipherSpecs, należy wyłączyć tryb TLS 1.3 . W tym celu należy zmodyfikować plik `qm.ini` menedżera kolejek i zmienić ustawienie właściwości **AllowTLSV13** na:

```
SSL:
  AllowTLSV13=FALSE
```

Uwaga: W tym miejscu nie można używać protokołu TLS 1.3 CipherSpecs.

IBM MQ MQI client i TLS 1.3

ULW V 9.1.4

Jeśli używany jest klient IBM MQ MQI client , wartość **AllowTLSV13** jest wnioskowana, chyba że zostanie ona jawnie określona w sekcji SSL pliku `mqclient.ini` używanego przez aplikację.

- Jeśli włączona jest opcja CipherSpecs słabych stron, parametr **AllowTLSV13** ma wartość FALSE , a nie można użyć protokołu TLS 1.3 CipherSpecs .
- W przeciwnym razie parametr **AllowTLSV13** ma wartość TRUE , a nowy protokół TLS 1.3 CipherSpecs i alias CipherSpecs mogą być używane.

Domyślne wartości atrybutu CipherSpec włączone w produkcie IBM MQ

Multi V 9.1.1

W domyślnej konfiguracji produkt IBM MQ zapewnia obsługę protokołu TLS 1.2 oraz różnych algorytmów szyfrowania przy użyciu specyfikacji CipherSpecs. Ze względu na kompatybilność produkt IBM MQ można również skonfigurować w taki sposób, aby używały protokołów SSL 3.0 i TLS 1.0 oraz algorytmów szyfrujących, które są słabe lub podatne na zagrożenia związane z bezpieczeństwem. Lista obiektów CipherSpecs , które są włączone w konfiguracji domyślnej, może zostać zmieniona przez zastosowanie konserwacji.

Produkt IBM MQ można skonfigurować w taki sposób, aby ograniczał lub zezwalał na używanie specyfikacji CipherSpecs przy użyciu następujących elementów sterujących:

- Zezwala się na stosowanie specyfikacji CipherSpecs zgodnych ze standardem FIPS 140-2 przy użyciu protokołu SSLFIPS.
- ULW Zezwala się tylko na zgodne ze standardem NSA Suite B CipherSpecs przy użyciu SUITEB.
- ULW Zezwól na niestandardową listę CipherSpecs przy użyciu zmiennej środowiskowej **AllowedCipherSpecs** lub **AMQ_ALLOWED_CIPHERS** .
- ULW Zezwalaj na użycie nieaktualnych specyfikacji CipherSpecs przy użyciu zmiennej środowiskowej **AllowWeakCipher** lub **AMQ_SSL_WEAK_CIPHER_ENABLE** .
- z/OS Zezwalaj na użycie nieaktualnych specyfikacji CipherSpecs przy użyciu instrukcji DD w JCL CHINIT.

Uwaga: Jeśli zostanie określona niestandardowa lista opcji CipherSpecs przy użyciu produktu **AllowedCipherSpecs** lub **AMQ_ALLOWED_CIPHERS** , ta opcja nadpisuje włączenie wszystkich nieaktualnych specyfikacji CipherSpecs. Należy pamiętać, że w przypadku używania ograniczeń standardu NSA Suite B lub FIPS 140-2 w połączeniu z niestandardową listą CipherSpec należy upewnić się, że lista niestandardowa zawiera tylko CipherSpecs dozwolone przez ustawienia Suite B lub FIPS 140-2.

Udostępnianie niestandardowej listy włączonych specyfikacji CipherSpecs na wielu platformach

Multi V 9.1.1

Istnieje możliwość udostępnienia alternatywnego zestawu specyfikacji CipherSpecs , które mogą być używane z kanałami produktu IBM MQ , przy użyciu zmiennej środowiskowej **AMQ_ALLOWED_CIPHERS** lub atrybutu sekcji SSL **AllowedCipherSpecs** pliku `.ini` . Można użyć tego ustawienia, aby ograniczyć obiekty nasłuchiwania produktu IBM MQ do akceptowania przychodzących żądań uruchomienia kanału, chyba że używają jednego z nazwanych specyfikacji CipherSpecs. Ta funkcja może być używana do sterowania specyfiką CipherSpecs , które są zawarte w pliku ANY* CipherSpecs.

W zmiennej środowiskowej **AMQ_ALLOWED_CIPHERS** lub w atrybucie sekcji SSL produktu **AllowedCipherSpecs** akceptowane są następujące wartości:

- Pojedyncza nazwa CipherSpec , lub
- Lista oddzielonych przecinkami nazw IBM MQ CipherSpec , które mają zostać ponownie włączone, lub
- Wartość specjalna ALL, reprezentująca wszystkie specyfikacje CipherSpecs (niezalecane).

Uwaga: Włączenie opcji **ALL** CipherSpecs nie jest zalecane, ponieważ spowoduje to włączenie protokołów SSL 3.0 i TLS 1.0 oraz dużej liczby słabych algorytmów szyfrujących.

Jeśli to ustawienie jest skonfigurowane, nadpisuje domyślną listę CipherSpec i powoduje, że IBM MQ zignoruje słabe ustawienia dezaktualizacji szyfru (patrz poniżej):

- Programy nasłuchujące produktu IBM MQ akceptują tylko propozycje SSL/TLS, które korzystają z jednej z nazwanych specyfikacji CipherSpecs.
- Kanały produktu IBM MQ zezwalają tylko na pustą wartość SSLCIPH lub jedną z nazwanych specyfikacji CipherSpecs.
- Uzupełnianie wartości opcji SSLCIPH na karcie **runmqsc** powoduje ograniczenie wartości zakończenia do jednej z nazw CipherSpecs.

Na przykład, aby umożliwić zdefiniowanie/zmianę definicji kanałów i nasłuchiwanie akceptowania ECDHE_RSA_AES_128_GCM_SHA256 lub ECDHE_ECDSA_AES_256_GCM_SHA384 , można ustawić następujące wartości w pliku `qm.ini` :

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

Należy pamiętać, że szyfry używane przez kanały AMQP lub MQTT mogą być ograniczone za pomocą ustawień pliku java.security .

Włączanie nieaktualnych specyfikacji CipherSpecs na wielu platformach

Multi

Domyślnie nie jest dozwolone określanie nieaktualnego atrybutu CipherSpec w definicji kanału. Jeśli zostanie podjęta próba określenia nieaktualnego atrybutu CipherSpec w systemie Wiele platform, zostanie wyświetlony komunikat AMQ8242: niepoprawna definicja SSLCIPH, a program PCF zwraca wartość MQRCCF_SSL_CIPHER_SPEC_ERROR.

Nie można uruchomić kanału z nieaktualnym obiektem CipherSpec. Jeśli zostanie podjęta próba użycia nieaktualnej specyfikacji CipherSpec, system zwróci wartość MQCC_FAILED (2) wraz z **Reason** z MQRC_SSL_INITIALIZATION_ERROR (2393) .

Można ponownie włączyć jeden lub więcej nieaktualnych specyfikacji CipherSpecs w celu definiowania kanałów, w czasie wykonywania na serwerze, ustawiając zmienną środowiskową **AMQ_SSL_WEAK_CIPHER_ENABLE**.

Zmienna środowiskowa **AMQ_SSL_WEAK_CIPHER_ENABLE** akceptuje:

- Pojedyncza nazwa CipherSpec , lub
- Lista oddzielonych przecinkami nazw IBM MQ CipherSpec , które mają zostać ponownie włączone, lub
- Wartość specjalna ALL, reprezentująca wszystkie specyfikacje CipherSpecs (niezalecane).

Uwaga: Ponowne włączenie opcji ALL CipherSpecs nie jest zalecane, ponieważ spowoduje to włączenie protokołów SSL 3.0 i TLS 1.0 oraz dużej liczby słabych algorytmów szyfrujących.

Na przykład, aby ponownie włączyć ECDHE_RSA_RC4_128_SHA256, należy ustawić następującą zmienną środowiskową:

```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

lub, alternatywnie zmień sekcję SSL w pliku qm.ini , ustawiając:

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

Włączanie nieaktualnych specyfikacji CipherSpecs w systemie z/OS

z/OS

Domyślnie nie jest dozwolone określanie nieaktualnego atrybutu CipherSpec w definicji kanału.
W przypadku próby określenia nieaktualnego atrybutu CipherSpec w systemie z/OSwyświetlany jest komunikat CSQM102E lub komunikat CSQX674E.

Aby włączyć słabe (nieaktualne) specyfikacje cipherspec, należy zdefiniować następującą instrukcję DD w pliku JCL CHINIT:

```
JCL: //CSQXWEAK DD DUMMY
```

Uwaga: Nie wszystkie nieaktualne CipherSpecs wymagają użycia tej instrukcji DD, patrz uwaga 11 w tabeli w produkcie “Nieaktualne CipherSpecs” na stronie 442.

Aby włączyć nieaktualny protokół SSL 3.0 , należy również zdefiniować następującą instrukcję DD w pliku JCL CHINIT:

```
JCL: //CSQXSSL3 DD DUMMY
```

V 9.1.0 Aby włączyć nieaktualny protokół TLS 1.0 , należy również zdefiniować następującą instrukcję DD w pliku JCL CHINIT:

```
JCL: //TLS10ON DD DUMMY
```

Należy pamiętać, że nazwą karty DD jest TLS10ON, co oznacza, że protokół TLS 1.0 jest włączony, a nie TLS100N.

Aby włączyć obsługę protokołu TLS 1.0 , należy użyć następującej instrukcji:

```
JCL: //TLS10OFF DD DUMMY
```

Jeśli użytkownik nie chce negocjować z programem nasłuchującym przy użyciu słabych lub niepoprawnych specyfikacji szyfrów, należy zdefiniować następującą instrukcję DD w pliku JCL CHINIT:

```
JCL: //WCIPSOFF DD DUMMY
```

Aby negocjować tylko z programem nasłuchującym przy użyciu specyfikacji szyfrów wymienionych na domyślnej liście specyfikacji szyfrów w produkcie **System SSL** , należy zdefiniować następującą instrukcję DD w pliku JCL CHINIT:

```
JCL: //GSKDCIPS DD DUMMY
```

Minimalny poziom w porównaniu ze stałym poziomem CipherSpecs

ULW V 9.1.4

Produkt IBM MQ obsługuje dwa różne typy specyfikacji CipherSpecs:

- **Minimalny poziom** CipherSpecs to te, które nie ustawiają górnej granicy, na przykład ANY, ANY_TLS12_OR_HIGHER lub ANY_TLS13_OR_HIGHER.
- **Poziom stały** CipherSpecs to te, które identyfikują konkretny protokół, na przykład ANY_TLS12 i ANY_TLS13, lub konkretny algorytm, taki jak ECDHE_ECDSA_3DES_EDE_CBC_SHA256 .

Aby zmaksymalizować prostotę konfiguracji przy zachowaniu bezpieczeństwa, po obu stronach kanału zalecane jest użycie **minimalnego poziomu** CipherSpecs . Dzięki temu komunikacja jest automatycznie obsługiwana i używana jest wyższa wersja protokołu TLS, gdy obie strony obsługują nową wersję bez konieczności zmiany konfiguracji po obu stronach.

Użycie **minimalnego poziomu** CipherSpec po stronie inicjującej, ale **fixed level** CipherSpec po stronie odbierającej może spowodować odrzucenie połączenia i wydanie komunikatów AMQ9631 i AMQ9641 .

Tabela “Relacja między ustawieniami aliasu CipherSpec” na stronie 446 zawiera tabele zawierające różne wyniki dla ustawień CipherSpec aliasów.

Pojęcia pokrewne

“Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45
Ten temat zawiera informacje dotyczące wybierania odpowiednich CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa. W tym celu należy zapoznać się z relacją między CipherSpecs i certyfikatami cyfrowymi w produkcie IBM MQ.

“CipherSpecs i CipherSuites” na stronie 19
Protokoły zabezpieczeń szyfrujących muszą być zgodne z algorytmami używannymi przez bezpieczne połączenie. Atrybuty CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

“Konfigurowanie produktu IBM MQ dla pakietu B” na stronie 43
Produkt IBM MQ można skonfigurować do działania zgodnie ze standardem NSA Suite B na platformach Windowsi UNIX and Linux .

“Standardy FIPS (Federal Information Processing Standards)” na stronie 33

Niniejszy temat zawiera wprowadzenie do standardu FIPS (Federal Information Processing Standards) Cryptomodule Validation Program of the US National Institute of Standards and Technology oraz funkcji kryptograficznych, które mogą być używane na kanałach TLS.

Zadania pokrewne

Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia opcji ANY_TLS12_OR_HIGHER CipherSpec

Odsyłacze pokrewne

Zdefiniowanie kanału

ZMIEŃ KANAŁ

Zmiana, kopiowanie i tworzenie kanału

ULW AES-ograniczenie szyfruGCM

Przewodnik po ograniczeniach, które są nakładane na szyfry AES-GCM używane na potrzeby szyfrowania TLS. Ograniczenia te są narzucane przez organizacje IETF i NIST i wymagają, aby ten sam klucz sesji nie był używany do bezpiecznego przesyłania więcej niż 2 rekordów[24.5] TLS podczas korzystania z szyfrów AES-GCM .

Więcej informacji na temat tych ograniczeń zawiera dokument RFC 9325 Section 4.4 Limits on Key Usage i RFC 8446 section 5.5.

IBM MQ nie implementuje bezpośrednio funkcji kryptograficznych. Zamiast tego w celu zapewnienia funkcjonalności protokołów TLS i Advanced Message Security używanych jest kilka różnych bibliotek szyfrujących. W systemach operacyjnych Windows, Linuxi AIX biblioteką kryptograficzną używaną przez IBM MQ jest GSKit. W przypadku aplikacji, biblioteki C i niezarządzane .NET używają GSKit do obsługi funkcji kryptograficznych. Implementacja algorytmów szyfrowania AES-GCM firmy GSKit obejmuje ograniczenia określone przez grupę standardów. Ograniczenia te są również domyślnie włączone. W związku z tym komunikacja TLS produktu IBM MQ przy użyciu szyfrów AES-GCM kończy się, jeśli więcej niż 2 rekordy TLS produktu[24.5] zostaną przesłane przy użyciu tego samego klucza sesji.

Uwaga: To ograniczenie nie występuje w przypadku platform IBM i, IBM Z , IBM MQ for HPE NonStop lub Java/JMSzarządzanych aplikacji .NET , ponieważ używane są różne biblioteki kryptograficzne, a te biblioteki nie zaimplementowały tego samego ograniczenia.

Jeśli kanał IBM MQ działa wystarczająco długo, aby więcej niż 2 rekordy TLS[24.5] zostały przesłane przy użyciu tego samego klucza sesji, bazowa biblioteka szyfrująca przerywa połączenie. Spowoduje to zakończenie działania kanału i wygenerowanie komunikatu o błędzie AMQ9288E . Aplikacje, których komunikacja została przerwana w ten sposób, otrzymują kod powrotu `MQRC_CONNECTION_BROKEN` od wykonywanej operacji IBM MQ .

Połączenie można zakończyć po obu stronach komunikacji, ale tylko na końcach, które korzystają z funkcji kryptograficznych systemu GSKit .

Porady dotyczące łagodzenia ograniczenia

Niektóre opcje zapobiegania lub obsługi komunikacji, która została zakończona z powodu tego ograniczenia, są następujące:

Użyj klientów z możliwością ponownego połączenia

Aplikacje można skonfigurować w taki sposób, aby podejmowały automatyczne próby ponownego nawiązania połączenia w przypadku niepowodzenia połączenia. Obejmuje to połączenia, które zostały zakończone z powodu ograniczenia GCM . Po skonfigurowaniu do ponownego połączenia aplikacja kliencka jest odtwarzana automatycznie w każdym punkcie awarii i odtwarzane są wszystkie uchwyty do otwartych obiektów. Odbywa się to bez powrotu do kodu aplikacji.

Więcej informacji na ten temat zawiera sekcja Automatyczne ponowne łączenie klienta.

Ustaw wartość resetowania klucza tajnego

Produkt IBM MQ można skonfigurować w taki sposób, aby żądał resetowania klucza sesji po przesłaniu konfigurowalnej liczby bajtów przez kanał. Po osiągnięciu tego limitu program IBM MQ

żąda, aby warstwa szyfrująca wykonująca reset klucza sesji, co spowoduje utworzenie nowego klucza sesji.

Należy zauważyć, że podana wartość jest liczbą przesłanych bajtów, która odnosi się do wielkości komunikatów wysyłanych przez program IBM MQ. Ograniczenie dotyczy liczby wysyłanych rekordów TLS. Nie ma bezpośredniego odwzorowania między bajtami komunikatu a rekordami TLS, ponieważ rekord TLS może wysłać maksymalną liczbę bajtów w zależności od wartości MTU (Maximum Transmission Unit) sieci. Wszystkie wysyłane komunikaty, które są większe niż ta wartość, są przesyłane jako wiele rekordów TLS. Wartość MTU różni się w zależności od sieci. Istnieją również inne powody, dla których może być konieczne wysłanie rekordu TLS poza przekazaniem danych komunikatu IBM MQ , na przykład IBM MQ Heartbeat checks, TLS alerts, other IBM MQ protocol messages. Te dodatkowe rekordy TLS są uwzględniane w maksymalnej liczbie rekordów TLS, ale nie są uwzględniane w wartości resetowania klucza tajnego IBM MQ .

Regularne resetowanie klucza sesji za pomocą resetowania klucza tajnego może uniemożliwić zakończenie kanału z powodu ograniczenia AES-GCM .

Więcej informacji na ten temat zawiera sekcja Resetowanie kluczy tajnych SSL i TLS.

V 9.1.4 **Użyj specyfikacji szyfrowania TLS 1.3**

Podczas korzystania z protokołu TLS 1.3 nadal występuje ograniczenie AES-GCM , ale protokół TLS 1.3 obsługuje automatyczne resetowanie klucza sesji bez konieczności przerywania komunikacji TLS. Umożliwia to programowi GSKit zarządzanie resetowaniem klucza sesji, gdy jest to konieczne, bez konieczności żądania przez program IBM MQ resetowania klucza tajnego.

Więcej informacji na ten temat zawiera sekcja Korzystanie z protokołu TLS 1.3 w podręczniku IBM MQ w podręczniku “Włączanie opcji CipherSpecs” na stronie 433.

Wyłącz ograniczenie AES-GCM

W razie potrzeby ograniczenie można wyłączyć, ustawiając zmienną środowiskową **GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE** w celu wyłączenia ograniczenia AES-GCM . Pozwala to na wysłanie dowolnej liczby rekordów TLS przy użyciu tego samego klucza sesji. Jeśli zostanie wybrana ta mitygacja, należy ustawić zmienną środowiskową na każdym końcu komunikacji, która używa GSKit do bezpiecznej komunikacji.

Ostrzeżenie: Ta opcja nie jest zalecana, ponieważ po wysłaniu więcej niż 2 rekordów TLS[24.5] możliwe jest wykonanie przez atakujących analizy wysłanych rekordów w celu określenia używanego klucza sesji. Po określeniu klucza sesji cała istniejąca i przyszła komunikacja używająca tego klucza sesji zostanie naruszona.

Nieaktualne CipherSpecs

Lista nieaktualnych specyfikacji CipherSpecs , które są w stanie używać z produktem IBM MQ , jeśli jest to konieczne.

Więcej informacji na temat włączania nieaktualnych specyfikacji CipherSpecsmożna znaleźć w sekcji “Włączanie nieaktualnych specyfikacji CipherSpecs na wielu platformach” na stronie 439 lub “Włączanie nieaktualnych specyfikacji CipherSpecs w systemie z/OS” na stronie 439.

W poniższej tabeli wymieniono nieaktualne specyfikacje CipherSpecs , których można używać z obsługą protokołu IBM MQ TLS.

Tabela 75. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ

Obsługa platformy "1" na stronie 445	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 445	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Specyfikacje szyfrowania dla protokołu SSL 3.0								
IBM i	AES_SHA_US "3" na stronie 445	002F	SSL 3.0	SHA-1	AES (128)	Nie	Nie	9.0.0.0
Wszystkie	DES_SHA_EXPORT "3" na stronie 445 "4" na stronie 445 "5" na stronie 445	0009	SSL 3.0	SHA-1	DES (56)	Nie	Nie	9.0.0.0
ULW	DES_SHA_EXPORT1024 "3" na stronie 445 "6" na stronie 445	0062	SSL 3.0	SHA-1	DES (56)	Nie	Nie	9.0.0.0
ULW	FIPS_WITH_DES_CBC_SHA "3" na stronie 445	FEFE	SSL 3.0	SHA-1	DES (56)	Nie "7" na stronie 445	Nie	9.0.0.0
ULW	FIPS_WITH_3DES_EDE_CBC_SHA "3" na stronie 445	FEFF	SSL 3.0	SHA-1	3DES (168)	Nie "8" na stronie 445	Nie	9.0.0.1 i 9.0.1
Wszystkie	NULL_MD5 "3" na stronie 445	0001	SSL 3.0	MD5	Brak	Nie	Nie	9.0.0.1
Wszystkie	NULL_SHA "3" na stronie 445	0002	SSL 3.0	SHA-1	Brak	Nie	Nie	9.0.0.1
Wszystkie	RC2_MD5_EXPORT "3" na stronie 445 "4" na stronie 445 "5" na stronie 445	0006	SSL 3.0	MD5	RC2 (40)	Nie	Nie	9.0.0.0
Wszystkie	RC4_MD5_EXPORT "4" na stronie 445 "3" na stronie 445	0003	SSL 3.0	MD5	RC4 (40)	Nie	Nie	9.0.0.0
Wszystkie	RC4_MD5_US "3" na stronie 445	0004	SSL 3.0	MD5	RC4 (128)	Nie	Nie	9.0.0.0
Wszystkie	RC4_SHA_US "3" na stronie 445 "5" na stronie 445	0005	SSL 3.0	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ULW	RC4_56_SHA_EXPORT1024 "3" na stronie 445 "6" na stronie 445	0064	SSL 3.0	SHA-1	RC4 (56)	Nie	Nie	9.0.0.0
Wszystkie	TRIPLE_DES_SHA_US "3" na stronie 445 "5" na stronie 445	000A	SSL 3.0	SHA-1	3DES (168)	Nie	Nie	9.0.0.1 i 9.0.1
Specyfikacje szyfrowania dla protokołu TLS 1.0								
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5 "3" na stronie 445	0006	TLS 1.0	MD5	RC2 (40)	Nie	Nie	9.0.0.0
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5 "3" na stronie 445 "4" na stronie 445	0003	TLS 1.0	MD5	RC4 (40)	Nie	Nie	9.0.0.0

Tabela 75. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 445	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 445	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Wszystkie	TLS_RSA_WITH_DES_CBC_SHA "3" na stronie 445	0009	TLS 1.0	SHA-1	DES (56)	Nie "9" na stronie 445	Nie	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" na stronie 445	0001	TLS 1.0	MD5	Brak	Nie	Nie	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" na stronie 445	0002	TLS 1.0	SHA-1	Brak	Nie	Nie	9.0.0.1
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" na stronie 445	0004	TLS 1.0	MD5	RC4 (128)	Nie	Nie	9.0.0.0
z/OS ULW	TLS_RSA_WITH_AES_128_CBC_SHA "10" na stronie 445	002F	TLS 1.0	SHA-1	AES (128)	Tak	Nie	9.0.5
z/OS ULW	TLS_RSA_WITH_AES_256_CBC_SHA "6" na stronie 445 "10" na stronie 445	0035	TLS 1.0	SHA-1	Algorytm AES (256)	Tak	Nie	9.0.5
Wszystkie	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000A	TLS 1.0	SHA-1	3DES (168)	Tak	Nie	9.0.0.1 i 9.0.1
Specyfikacje szyfrowania dla protokołu TLS 1.2								
ULW	ECDHE_ECDSA_NULL_SHA256 "3" na stronie 445	C006	TLS 1.2	SHA-1	Brak	Nie	Nie	9.0.0.1
ULW	ECDHE_ECDSA_RC4_128_SHA256 "3" na stronie 445	C007	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
IBM i ULW	ECDHE_RSA_NULL_SHA256 "3" na stronie 445	C010	TLS 1.2	SHA-1	Brak	Nie	Nie	9.0.0.1
IBM i ULW	ECDHE_RSA_RC4_128_SHA256 "3" na stronie 445	C011	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ULW	TLS_RSA_WITH_NULL_NULL "3" na stronie 445	0000	TLS 1.2	Brak	Brak	Nie	Nie	9.0.0.1
Wszystkie	TLS_RSA_WITH_NULL_SHA256 "3" na stronie 445	003B	TLS 1.2	SHA-256	Brak	Nie	Nie	9.0.0.1
ULW	TLS_RSA_WITH_RC4_128_SHA256 "3" na stronie 445	0005	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ULW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	C0008	TLS 1.2	SHA-1	3DES (168)	Tak	Nie	9.0.0.1 i 9.0.1

Tabela 75. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 445	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 445	Suite B	Aktualizacja, w której uznano ją za nieaktualną
IBM i ULW	ECDHE_RSA_3DES_EDE_CBC_SHA256	C012	TLS 1.2	SHA-1	3DES (168)	Tak	Nie	9.0.0.1 i 9.0.1

Uwagi:

1. Listę platform obsługiwanych przez każdą z ikon platformy można znaleźć w sekcji Ikony platform i wersji w dokumentacji produktu.
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. ULW Te specyfikacje szyfrowania są wyłączone, gdy jest włączona obsługa protokołu TLS 1.3 (za pomocą właściwości AllowTLSV13 w `qm.ini`).

   z/OS Menedżery kolejek utworzone w wersji IBM MQ for z/OS 9.2.0 lub nowszej domyślnie włączają protokół TLS 1.3 , co powoduje wyłączenie tych CipherSpecs. W razie potrzeby można włączyć te specyfikacje szyfrów, wyłączając protokół TLS 1.3. W tym celu należy dodać **AllowTLSV13**=*FALSE* do sekcji TransportSecurity zestawu danych QMINI ustawionego w menedżerze kolejek JCL. Menedżery kolejek zmigrowane do wersji IBM MQ for z/OS 9.2.0 z wcześniejszej wersji nie mają domyślnie włączonego protokołu TLS 1.3 i dlatego mają włączone CipherSpecs .
4. 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.
5. Te specyfikacje szyfrowania nie są już obsługiwane przez produkty IBM MQ classes for Java ani IBM MQ classes for JMS. Więcej informacji na ten temat zawiera sekcja Specyfikacje szyfrowania i zestawy algorytmów szyfrowania SSL/TLS w programie IBM MQ classes for Java lub sekcja Specyfikacje szyfrowania i zestawy algorytmów szyfrowania SSL/TLS w programie IBM MQ classes for JMS.
6. Wielkość klucza uzgadniania to 1024 bity.
7. 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.
8. Nazwa `FIPS_WITH_3DES_EDE_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.
9. Ta specyfikacja szyfrowania uzyskała certyfikat FIPS 140-2 przed 19 maja 2007.
10. z/OS Ponowne włączenie tylko tych specyfikacji CipherSpec nie wymaga użycia instrukcji CSQXWEAK DD.

Pojęcia pokrewne

"Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ" na stronie 45

Ten temat zawiera informacje dotyczące wybierania odpowiednich CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa. W tym celu należy zapoznać się z relacją między CipherSpecs i certyfikatami cyfrowymi w produkcie IBM MQ.

Odsyłacze pokrewne
Zdefiniowanie kanału
ZMIEŃ KANAŁ

Relacja między ustawieniami aliasu CipherSpec

W poniższych tabelach przedstawiono oczekiwane zachowanie, gdy TLS1.3 nie jest włączony ani na kliencie, menedżerze kolejek, ani w obu tych systemach, a TLS1.3 jest włączony zarówno na kliencie, jak i w menedżerze kolejek.

W poniższych tabelach przedstawiono relacje między różnymi ustawieniami aliasu CipherSpec a oczekiwanym rezultatem. Tabela 76 na stronie 446 pokazuje oczekiwane zachowanie, gdy protokół TLS 1.3 nie jest włączony na kliencie, serwerze lub w obu tych systemach. Tabela 77 na stronie 446 pokazuje oczekiwane zachowanie, gdy protokół TLS 1.3 jest włączony zarówno na kliencie, jak i na serwerze. W obu przypadkach CipherSpecs dla klienta są wyświetlane na osi Y tabeli, a wartość CipherSpecs dla serwera jest wyświetlana na osi X tabeli.

Uwaga: Jeśli w pozycji *Prawdopodobne jest niepowodzenie* jest to spowodowane tym, że jeśli używany jest określony protokół TLS 1.3 lub TLS 1.2 CipherSpec jako wartość CipherSpec , która jest najsilniejsza dla klienta i menedżera kolejek, uzgadnianie TLS rozwiąże ten problem, a więc dopasuje wartość SSCIPH kanału.

Tabela 76. Oczekiwane zachowanie w przypadku, gdy protokół TLS 1.3 nie jest włączony na kliencie, serwerze lub w obu tych systemach

	Serwer			
Klient	**Specyficzny protokół TLS 1.2 CipherSpec**	**ANY**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
Określony protokół TLS 1.2 CipherSpec	Połączenia	Połączenia	Połączenia	Połączenia
any	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia
ANY_ TLS12	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia
ANY_TLS12_ OR_HIGHER	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia

Tabela 77. Oczekiwane zachowanie przy włączonej opcji TLS 1.3 zarówno na kliencie, jak i na serwerze

	Serwer						
Klient	**Specyficzny protokół TLS 1.2 CipherSpec**	**Specyficzny protokół TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_HIGHER**	**ANY_TLS13_ OR_HIGHER**
Określony protokół TLS 1.2 CipherSpec	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	**Nie powiodło się**	Połączenia	**Nie powiodło się**

Tabela 77. Oczekiwane zachowanie przy włączonej opcji TLS 1.3 zarówno na kliencie, jak i na serwerze (kontynuacja)

	Serwer						
Klient	**Specyficzny protokół TLS 1.2 CipherSpec**	**Specyficzny protokół TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_HIGHER**	**ANY_TLS13_ OR_HIGHER**
Określony protokół TLS 1.3 CipherSpec	**Nie powiodło się**	Połączenia	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	Połączenia
any	**Nie powiodło się**	*Prawdopodobna awaria*	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	Połączenia
ANY_TLS12	*Prawdopodobna awaria*	**Nie powiodło się**	Połączenia	Połączenia	**Nie powiodło się**	Połączenia	**Nie powiodło się**
ANY_TLS13	**Nie powiodło się**	*Prawdopodobna awaria*	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	Połączenia
ANY_TLS12_ OR_HIGHER	**Nie powiodło się**	*Prawdopodobna awaria*	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	Połączenia
ANY_TLS13_ OR_HIGHER	**Nie powiodło się**	*Prawdopodobna awaria*	Połączenia	**Nie powiodło się**	Połączenia	Połączenia	Połączenia

Pojęcia pokrewne

"Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ" na stronie 45

Ten temat zawiera informacje dotyczące wybierania odpowiednich CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa. W tym celu należy zapoznać się z relacją między CipherSpecs i certyfikatami cyfrowymi w produkcie IBM MQ.

"CipherSpecs i CipherSuites" na stronie 19

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

"Włączanie opcji CipherSpecs" na stronie 433

Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

Zadania pokrewne

Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia opcji ANY_TLS12_OR_HIGHER CipherSpec

Uzyskiwanie informacji o specyfikacji CipherSpecs przy użyciu produktu IBM MQ Explorer

Za pomocą programu IBM MQ Explorer można wyświetlać opisy specyfikacji CipherSpecs.

Aby uzyskać informacje na temat specyfikacji CipherSpecs w produkcie "Włączanie opcji CipherSpecs" na stronie 433, należy wykonać następującą procedurę:

1. Otwórz program IBM 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 TLS, 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 ma zastosowania do systemów UNIX, Linux lub Windows , ponieważ CipherSpecs są dostarczane z produktem IBM MQ , dlatego nowe CipherSpecs nie stają się dostępne po wysyłce.

W przypadku platform, w których system operacyjny udostępnia obsługę protokołu TLS, system może obsługiwać nowe specyfikacje CipherSpecs , które nie są dołączone do produktu “Włączanie opcji CipherSpecs” na stronie 433. Nową specyfikację CipherSpec można określić za pomocą parametru SSLCIPH, ale wartość, którą należy podać, zależy od używanej platformy. We wszystkich przypadkach specyfikacja musi być zgodna z protokołem TLS CipherSpec , który jest poprawny i obsługiwany przez wersję protokołu TLS, w którym działa system.

IBM i

Dwuznakowy łańcuch reprezentujący wartość szesnastkową.

Więcej informacji na temat dozwolonych wartości można znaleźć w punkcie trzecim w sekcji Uwagi dotyczące użycia w sekcji Ustawianie informacji o znaku dla sesji chronionej.

Ostrzeżenie: Nie należy podawać szesnastkowych wartości szyfrów w parametrze SSLCIPH, ponieważ na podstawie wartości nie będzie można jednoznacznie określić używanego szyfru, a używany protokół nie zostanie określony. Użycie szesnastkowych wartości szyfrów może prowadzić do wystąpienia błędów niezgodności specyfikacji CipherSpec .

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

Czteroznakowy łańcuch reprezentujący wartość szesnastkową. Kody szesnastkowe odpowiadają wartościom zdefiniowanym w protokole TLS.

Więcej informacji można znaleźć w sekcji Definicje zestawów algorytmów szyfrowania , gdzie znajduje się lista wszystkich obsługiwanych specyfikacji szyfrów TLS 1.0, TLS 1.2i TLS 1.3 w postaci 4-cyfrowych kodów szesnastkowych.

Uwagi dotyczące klastrów produktu IBM MQ

W przypadku klastrów IBM MQ najbezpieczniej jest używać nazw CipherSpec w produkcie “Włączanie opcji CipherSpecs” na stronie 433. Jeśli używana jest specyfikacja alternatywna, należy pamiętać, że specyfikacja może nie być poprawna na innych platformach. Więcej informacji zawiera sekcja “SSL/TLS i klastry” na stronie 477.

Określanie specyfikacji CipherSpec dla partycji IBM MQ MQI client

Dostępne są trzy opcje określania wartości CipherSpec dla IBM MQ MQI client.

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 za pomocą produktów IBM MQ classes for Java i IBM MQ classes for JMS

Produkty IBM MQ classes for Java i IBM MQ classes for JMS określają parametr CipherSuites w inny sposób niż w przypadku innych platform.

Informacje na temat określania pakietu CipherSuite z produktem IBM MQ classes for Javazawiera sekcja Obsługa protokołu TLS (Transport Layer Security) dla produktu Java .

Informacje na temat określania partycji CipherSuite z produktem IBM MQ classes for JMSzawiera sekcja Korzystanie z protokołu TLS (Transport Layer Security) z produktem IBM MQ classes for JMS

Określanie specyfikacji CipherSpec dla IBM MQ.NET

W przypadku produktu IBM MQ.NET można określić wartość CipherSpec przy użyciu klasy MQEnvironment lub MQC.SSL_CIPHER_SPEC_PROPERTY w tabeli mieszającej właściwości połączenia.

Więcej informacji na temat określania specyfikacji CipherSpec dla niezarządzanego klienta .NET zawiera sekcja Włączanie protokołu TLS dla niezarządzanego klienta .NET .

Informacje na temat określania CipherSpec dla klienta zarządzanego .NET można znaleźć w sekcji Obsługa CipherSpec dla zarządzanego klienta .NET .

z/OS Używanie protokołu AT-TLS z produktem IBM MQ for z/OS

Aplikacja Transparent Transport Layer Security (AT-TLS) zapewnia obsługę protokołu TLS dla aplikacji produktu z/OS bez konieczności implementowania obsługi protokołu TLS przez te aplikacje lub nawet należy pamiętać o tym, że używany jest protokół TLS. AT-TLS jest dostępny tylko w systemie z/OS.

AT-TLS może być używany ze wszystkimi wersjami produktu IBM MQ for z/OS.

Przed użyciem protokołu AT-TLS z produktem IBM MQ for z/OSnależy zapoznać się z “Ograniczenia” na stronie 451 zaangażowanym w to działanie.

Aby użyć opcji Przezroczyste zabezpieczenia warstwy transportowej aplikacji , należy zdefiniować instrukcje strategii zawierające zestaw reguł używanych przez produkt z/OS Communications Server w celu określenia, które połączenia TCP/IP mają włączoną obsługę protokołu TLS w sposób przezroczysty.

Produkt IBM MQ for z/OS ma własną implementację protokołu TLS, która wymaga, aby kanały miały parametr SSLCIPH skonfigurowany przy użyciu obsługiwanego obiektu CipherSpec.

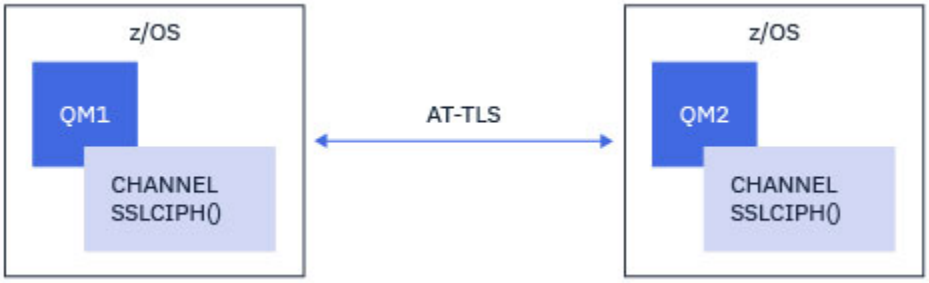
Decydując się na włączenie protokołu TLS w kanale, administrator produktu IBM MQ może zdecydować się na używanie protokołu AT-TLS lub IBM MQ TLS. Decyzja jest często podejmowana na podstawie tego, czy protokół AT-TLS jest używany dla innego oprogramowania pośredniego, czy też ze względu na wpływ na wydajność. Podstawowe porównanie wydajności protokołów AT-TLS i IBM MQ TLS znajduje się w sekcji MP16: Planowanie mocy obliczeniowej i strojenie dla IBM MQ for z/OS.

Scenariusze

Korzystanie z protokołu AT-TLS z produktem IBM MQ jest obsługiwane w następujących scenariuszach:

Scenariusz 1

Między dwoma menedżerami kolejek produktu IBM MQ for z/OS , w których obie strony kanału korzystają z protokołu AT-TLS. Oznacza to, że żaden kanał nie określa atrybutu SSLCIPH. To podejście może być używane z dowolnym kanałem komunikatów.

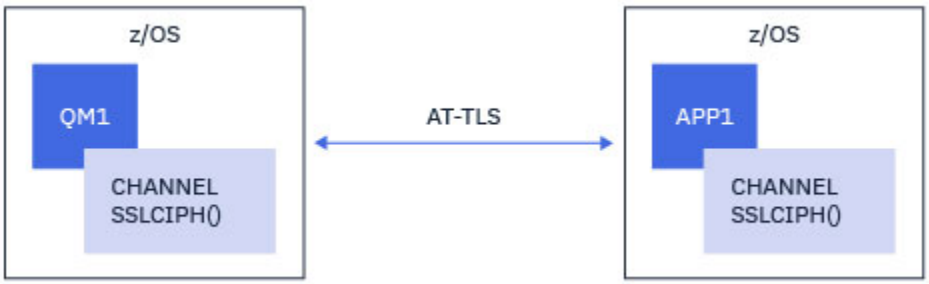


Wdrożenie tego scenariusza polega na zdefiniowaniu dwóch strategii AT-TLS, po jednym dla każdej strony kanału. Strategie te są takie same, jak te używane w scenariuszu Scenariusz 3.

Jeśli na przykład kanał został zmieniony z użyciem jednego, o nazwie CipherSpec do korzystania z protokołu AT-TLS, kanał danych wychodzących będzie używać strategii z produktu “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek produktu IBM MQ for Multiplatforms przy użyciu pojedynczej, nazwanej CipherSpec” na stronie 452 , a kanał danych przychodzących będzie używać strategii z produktu “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec” na stronie 456.

Scenariusz2

Między menedżerem kolejek produktu IBM MQ for z/OS i aplikacją kliencką IBM MQ Java działającą w systemie z/OS , w którym obie strony kanału korzystają z protokołu AT-TLS. Oznacza to, że ani kanał połączenia z serwerem, ani kanał połączenia klienckiego nie określają atrybutu SSLCIPH.

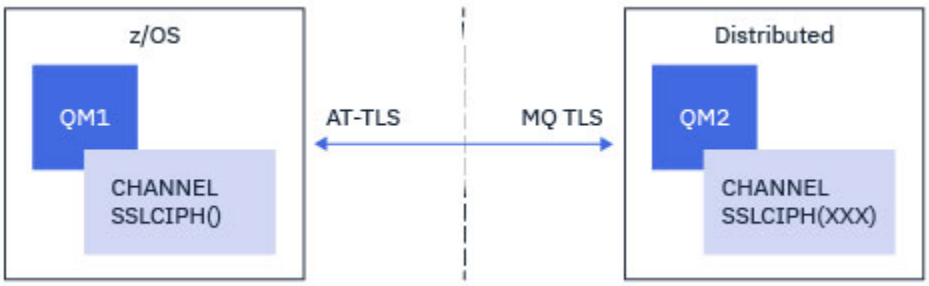


Wdrożenie tego scenariusza polega na zdefiniowaniu dwóch strategii AT-TLS, po jednym dla każdej strony kanału. Strategie te są takie same, jak te używane w scenariuszu Scenariusz 3.

Jeśli na przykład kanał został zmieniony z użyciem pojedynczego, o nazwie CipherSpec do korzystania z protokołu AT-TLS, kanał połączenia klienckiego będzie używać strategii z produktu “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek produktu IBM MQ for Multiplatforms przy użyciu pojedynczej, nazwanej CipherSpec” na stronie 452 , a kanał połączenia z serwerem będzie używać strategii z produktu “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec” na stronie 456.

Scenariusz 3

Między menedżerem kolejek produktu IBM MQ for z/OS a menedżerem kolejek działającym w systemie IBM MQ for Multiplatforms, w którym menedżer kolejek produktu IBM MQ for z/OS korzysta z protokołu AT-TLS, a menedżer kolejek produktu IBM MQ for Multiplatforms używa protokołu IBM MQ TLS. Dotyczy to wszystkich typów kanałów komunikatów innych niż kanał wysyłający klastry i odbiornik klastra.

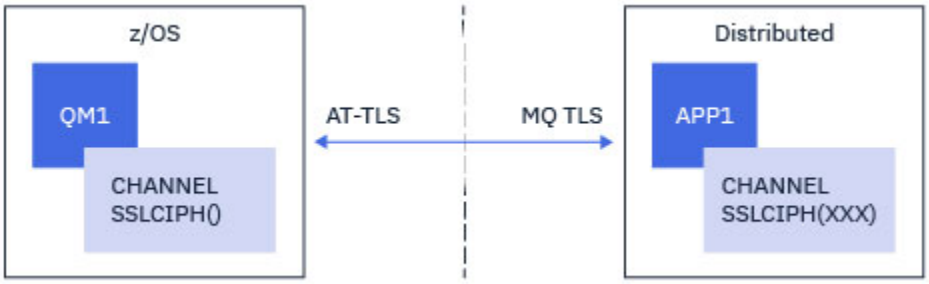


Przykład konfiguracji AT-TLS dla kanałów wychodzących z menedżera kolejek produktu IBM MQ for z/OS do menedżera kolejek produktu IBM MQ for Multiplatforms oraz “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec” na stronie 456 dla przykładowej konfiguracji AT-TLS dla kanałów danych przychodzących z menedżera kolejek produktu IBM MQ for Multiplatforms do menedżera kolejek produktu IBM MQ for z/OS zawiera sekcja “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek produktu IBM MQ for Multiplatforms przy użyciu pojedynczej, nazwanej CipherSpec” na stronie 452 .

Ta sama konfiguracja protokołu AT-TLS może być używana, gdy oba menedżery kolejek znajdują się w systemie z/OS, ale menedżer kolejek po prawej stronie nie został skonfigurowany pod kątem używania protokołu AT-TLS.

Scenariusz 4

Między menedżerem kolejek produktu IBM MQ for z/OS i aplikacją kliencką działającą w systemie IBM MQ for Multiplatforms, gdzie menedżer kolejek produktu IBM MQ for z/OS używa protokołu AT-TLS, a aplikacja kliencka używa protokołu IBM MQ TLS przez określenie atrybutu SSLCIPH z pojedynczym obiektem o nazwie CipherSpec.



W tym scenariuszu wymagana jest pojedyncza strategia AT-TLS, która spełnia te same wymagania, jak te używane przez kanał komunikatów przychodzących. Patrz sekcja “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec” na stronie 456.

Ta sama konfiguracja protokołu AT-TLS może być używana, gdy aplikacja kliencka jest aplikacją Java i działa również w systemie z/OS, ale nie została skonfigurowana pod kątem używania protokołu AT-TLS.

Ograniczenia

Produkt IBM MQ for z/OS nie jest świadomy AT-TLS, dlatego istnieje kilka ograniczeń, które mają zastosowanie w przypadku poprzednich scenariuszy:

- AT-TLS w połączeniu z protokołem IBM MQ TLS nie działa z kanałami wysyłającego klastry i kanały odbierające klastry.
- Menedżery kolejek produktu IBM MQ for z/OS nie mają informacji o tym, że korzystają z protokołu AT-TLS i nie otrzymują żadnych informacji o certyfikacie z ich partnerskiego menedżera kolejek lub klienta.

Oznacza to, że następujące atrybuty nie mają wpływu na stronę z/OS kanału z użyciem protokołu AT-TLS:

- Atrybuty kanału SSLCAUTH i SSLPEER
- Atrybut menedżera kolejek SSLRKEYC
- Atrybuty SSLPEERMAP dla reguł CHLAUTH

- Korzystanie z renegocjacji klucza tajnego TLS wymaga, aby obie strony kanału korzystały z protokołu IBM MQ TLS. Dlatego menedżer kolejek produktu IBM MQ for Multiplatforms lub klient nie powinien mieć włączonej procedury renegocjacji klucza tajnego TLS, jeśli nawiąże połączenie z menedżerem kolejek produktu IBM MQ for z/OS przy użyciu protokołu AT-TLS.

  Aby wyłączyć renegocjację klucza tajnego TLS dla menedżera kolejek, należy ustawić parametr SSLRKEYC menedżera kolejek na wartość `0`. W przypadku klienta należy ustawić odpowiedni parametr na wartość `0` w zależności od typu klienta. Szczegółowe informacje o tym, jak to zrobić, zawiera sekcja “Resetowanie kluczy tajnych SSL i TLS” na stronie 460.

Instrukcje konfiguracji AT-TLS

Protokół AT-TLS został skonfigurowany przy użyciu zestawu instrukcji. W scenariuszach opisanych w tym temacie znajdują się następujące scenariusze:

TTLSRule
Określa zestaw kryteriów dopasowywania połączenia TCP/IP do konfiguracji TLS. To z kolei odnosi się do innych typów instrukcji.

TTLSGroupAction
Określa, czy odwołanie `TTLSRule` jest włączone, czy nie.

TTLSEnvironmentAction
Określa szczegółową konfigurację dla przywołującego `TTLSRule` i odwołuje się do wielu innych instrukcji.

TTLSKeyringParms
Odwołuje się do klucza-ring, który ma być używany przez AT-TLS.

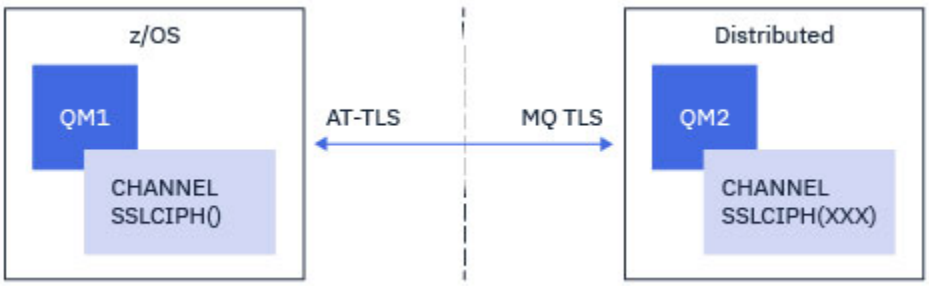
TTLSCipherParms
Definiuje zestawy algorytmów szyfrowania, które mają być używane.

TTLSEnvironmentAdvancedParms
Definiuje, które protokoły TLS lub SSL są włączone.

Ostrzeżenie: Istnieją inne instrukcje strategii AT-TLS z protokołem AT-TLS, które nie zostały tutaj udokumentowane, i mogą być używane z produktem IBM MQ w zależności od potrzeby. Jednak produkt IBM MQ został przetestowany tylko z strategiami opisanymi w tym temacie.

Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek produktu IBM MQ for Multiplatforms przy użyciu pojedynczej, nazwanej CipherSpec

Sposób konfigurowania mechanizmu AT-TLS w kanale wychodzącym z menedżera kolejek systemu IBM MQ for z/OS do menedżera kolejek systemu IBM MQ for Multiplatforms . W tym przypadku kanał w menedżerze kolejek systemu z/OS jest kanałem nadawczym, który nie ma ustawionego atrybutu SSLCIPH, a kanał w menedżerze kolejek systemu innego niżz/OS jest kanałem odbiorczym, którego atrybut SSLCIPH jest ustawiony na wartość pojedynczą o nazwie CipherSpec.



W tym przykładzie istniejąca para kanałów nadawca-odbiorca, która używa protokołu TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec , zostanie dopasowana w taki sposób, aby kanał nadawczy używał protokołu AT-TLS zamiast protokołu IBM MQ TLS.

Innych protokołów TLS i CipherSpecs można użyć, dostosowując konfigurację w niewielkim stopniu. Inne typy kanałów komunikatów, oprócz kanałów wysyłających i odbierających klastry, mogą być używane bez zmian w konfiguracji AT-TLS.

Procedura

Krok 1: zatrzymanie kanału

Krok 2: tworzenie i stosowanie strategii AT-TLS

W tym scenariuszu należy utworzyć następujące instrukcje AT-TLS:

1. Instrukcja TTLSRule dopasowująca połączenia wychodzące z przestrzeni adresowej inicjatora kanału do adresu IP i numeru portu docelowego kanału odbiorczego. Te wartości powinny być zgodne z informacjami użytymi w polu CONNAME kanału nadawczego. W tym miejscu włączono dodatkowe filtrowanie w celu dopasowania do konkretnej nazwy zadania inicjatora kanału.

```
TTLSRule                        CSQ1-TO-REMOTE
{
  LocalAddr                     ALL
  RemoteAddr                    123.456.78.9
  RemotePortRange               1414
  Jobname                       CSQ1CHIN
  Direction                     OUTBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}
```

   Poprzednia reguła dopasowuje połączenia z adresem IP 123.456.78.9 na porcie 1414 z zadania CSQ1CHIN .

   Bardziej zaawansowane opcje filtrowania opisano w sekcji TTLSRule.

2. Instrukcja TTLSGroupAction włączającą regułę. TTLSRule odwołuje się do TTLSGroupAction za pomocą właściwości **TTLSGroupActionRef** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Instrukcja TTLSEnvironmentAction powiązana z TTLSRule przez właściwość **TTLSEnvironmentActionRef** . Program TTLSEnvironmentAction konfiguruje środowisko TLS i określa, który plik kluczy ma być używany.

```
TTLSEnvironmentAction               CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                     CLIENT
  TTLSKeyringParmsRef               CSQ1-KEYRING
  TTLSCipherParmsRef                CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef   CSQ1-ENVIRONMENT-ADVANCED
}
```

4. Instrukcja TTLSKeyringParms powiązana z wartością TTLSEnvironmentAction przez właściwość **TTLSKeyringParmsRef** i definiująca plik kluczy używany przez AT-TLS.

   Plik kluczy powinien zawierać certyfikaty zaufane w zdalnym menedżerze kolejek innym niżz/OS . Ten plik kluczy można zdefiniować w taki sam sposób, jak plik kluczy używany przez inicjator kanału; patrz sekcja “Konfigurowanie systemu z/OS do używania protokołu TLS” na stronie 263.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Instrukcja TTLSCipherParms powiązana z TTLSEnvironmentAction przez właściwość **TTLSCipherParmsRef** .

   Ta instrukcja musi zawierać pojedynczą nazwę zestawu algorytmów szyfrowania, która musi być odpowiednikiem nazwy CipherSpec produktu IBM MQ użytej w docelowym kanale odbiorczym.

   Uwaga: Nazwy zestawów algorytmów szyfrowania AT-TLS nie muszą być zgodne z nazwami CipherSpec produktu IBM MQ . Można jednak znaleźć nazwę zestawu algorytmów szyfrowania AT-TLS zgodną z nazwą IBM MQ CipherSpec , wyszukując nazwę IBM MQ CipherSpec w poniższej tabeli i odwołując się do czteroznakowej kolumny kodu z rozszerzoną kolumną znaków z tabeli 2 w temacie TTLSCipherParms .

Tabela 78. Konwersja z kodów czteroznakowych na nazwy specyfikacji szyfrowania CipherSpec

Czteroznakowy kod	Protokół	Domyślnie włączone	Nazwa specyfikacji szyfrowania
0001	SSL 3.0	Nie	NULL_MD5
0002	SSL 3.0	Nie	NULL_SHA
0003	SSL 3.0	Nie	RC4_MD5_EXPORT
0004	SSL 3.0	Nie	RC4_MD5_US
0005	SSL 3.0	Nie	RC4_SHA_US
0006	SSL 3.0	Nie	RC2_MD5_EXPORT
0008	SSL 3.0	Nie	DES_SHA_EXPORT
0009	TLS 1.0	Tak	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	Nie	TRIPLE_DES_SHA_US
000A	TLS 1.0	Tak	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Tak	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Tak	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	Tak	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	Tak	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	Tak	TLS_RSA_WITH_AES_256_CBC_SHA256

Tabela 78. Konwersja z kodów czteroznakowych na nazwy specyfikacji szyfrowania CipherSpec (kontynuacja)

Czteroznakowy kod	Protokół	Domyślnie włączone	Nazwa specyfikacji szyfrowania
C023	TLS 1.2	Tak	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Tak	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Tak	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Tak	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. Instrukcja TTLSEnvironmentAdvancedParms jest powiązana z TTLSEnvironmentAction przez właściwość **TTLSEnvironmentAdvancedParmsRef** .

   Za pomocą tej instrukcji można określić, które protokoły SSL i TLS są włączone. W przypadku IBM MQ należy włączyć tylko jeden protokół zgodny z nazwą zestawu algorytmów szyfrowania użytą w instrukcji TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         ON
  TLSv1.3         OFF
}
```

Pełny zestaw instrukcji jest następujący i powinien zostać zastosowany do agenta strategii:

```
TTLSRule                      CSQ1-TO-REMOTE
{
  LocalAddr                   ALL
  RemoteAddr                  123.456.78.9
  RemotePortRange             1414
  Jobname                     CSQ1CHIN
  Direction                   OUTBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

Krok 3: usuwanie parametru SSLCIPH z kanału z/OS

Usuń specyfikację szyfrowania CipherSpec z kanału z/OS za pomocą następującej komendy:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

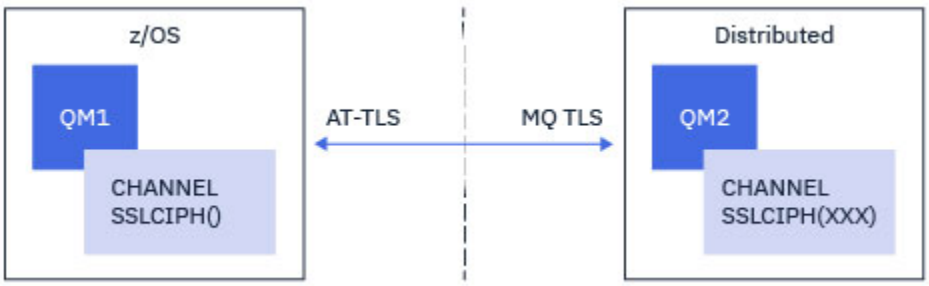
Krok 4: Uruchamianie kanału

Po uruchomieniu kanału zostanie użyta kombinacja protokołów AT-TLS i IBM MQ TLS.

Ostrzeżenie: Wcześniejsze instrukcje AT-TLS są tylko minimalną konfiguracją. Istnieją inne instrukcje strategii AT-TLS z AT-TLS, które nie zostały opisane w tej sekcji i mogą być używane z produktem IBM MQ w zależności od potrzeb. Jednak produkt IBM MQ został przetestowany tylko z opisanymi strategiami.

Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec

Sposób konfigurowania mechanizmu AT-TLS w kanale danych przychodzących z menedżera kolejek systemu IBM MQ for Multiplatforms do menedżera kolejek systemu IBM MQ for z/OS . W tym przypadku kanał w menedżerze kolejek systemu z/OS jest kanałem odbiorczym, który nie ma ustawionego atrybutu SSLCIPH, a kanał w menedżerze kolejek systemu innego niżz/OS jest kanałem nadawczym z atrybutem SSLCIPH ustawionym na wartość pojedynczą o nazwie CipherSpec.



W tym przykładzie istniejąca para kanałów nadawca-odbiorca, która używa protokołu TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec , zostanie dopasowana w taki sposób, aby kanał odbiorczy używał protokołu AT-TLS zamiast protokołu IBM MQ TLS.

Innych protokołów TLS i CipherSpecs można użyć, dostosowując konfigurację w niewielkim stopniu. Inne typy kanałów komunikatów, oprócz kanałów wysyłających i odbierających klastry, mogą być używane bez zmian w konfiguracji AT-TLS.

Procedura

Krok 1: zatrzymanie kanału

Krok 2: tworzenie i stosowanie strategii AT-TLS

W tym scenariuszu należy utworzyć następujące instrukcje AT-TLS:

1. Instrukcja TTLSRule dopasowująca połączenia przychodzące do przestrzeni adresowej inicjatora kanału z adresu IP kanału nadawczego. W tym miejscu włączono dodatkowe filtrowanie w celu dopasowania do konkretnej nazwy zadania inicjatora kanału.

```
TTLSRule                        REMOTE-TO-CSQ1
{
  LocalAddr                     ALL
  LocalPortRange                1414
  RemoteAddr                    123.456.78.9
  Jobname                       CSQ1CHIN
  Direction                     INBOUND
  TTLSGroupActionRef            CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef      CSQ1-INBOUND-ENVIRONMENT-ACTION
}
```

   Powyższa reguła jest zgodna z połączeniami przychodzącymi do zadania CSQ1CHIN na lokalnym porcie 1414 ze zdalnego adresu IP 123.456.78.9.

   Bardziej zaawansowane opcje filtrowania opisano w sekcji TTLSRule.

2. Instrukcja TTLSGroupAction włączającą regułę. TTLSRule odwołuje się do TTLSGroupAction za pomocą właściwości **TTLSGroupActionRef** .

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Instrukcja TTLSEnvironmentAction jest powiązana z TTLSRule przez właściwość **TTLSEnvironmentActionRef** . Program TTLSEnvironmentAction konfiguruje środowisko TLS i określa, który plik kluczy ma być używany.

```
TTLSEnvironmentAction                 CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                       SERVER
  TTLSKeyringParmsRef                 CSQ1-KEYRING
  TTLSCipherParmsRef                  CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef     CSQ1-ENVIRONMENT-ADVANCED
}
```

Protokół AT-TLS umożliwia uwierzytelnianie wzajemne, co jest równoważne z użyciem atrybutu kanału SSLCAUTH. W tym celu należy mieć instrukcję `TTLSEnvironmentAction` z wartością **HandshakeRole** równą *ServerWithClientAuth* dla przychodzącej instrukcji `TTLSEnvironmentAction` .

4. Instrukcja TTLSKeyringParms jest powiązana z właściwością `TTLSEnvironmentAction` przez właściwość **TTLSKeyringParmsRef** i definiuje plik kluczy używany przez AT-TLS.

   Plik kluczy powinien zawierać certyfikaty zaufane w zdalnym menedżerze kolejek innym niż/OS . Ten plik kluczy można zdefiniować w taki sam sposób, jak plik kluczy używany przez inicjator kanału; patrz sekcja “Konfigurowanie systemu z/OS do używania protokołu TLS” na stronie 263.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Instrukcja TTLSCipherParms powiązana z `TTLSEnvironmentAction` przez właściwość **TTLSCipherParmsRef** .

   Ta instrukcja musi zawierać pojedynczą nazwę zestawu algorytmów szyfrowania, która musi być odpowiednikiem nazwy CipherSpec produktu IBM MQ używanej w zdalnym kanale nadawczym.

   Uwaga: Nazwy zestawów algorytmów szyfrowania AT-TLS nie muszą być zgodne z nazwami CipherSpec produktu IBM MQ . Można jednak znaleźć nazwę zestawu algorytmów szyfrowania AT-TLS zgodną z nazwą IBM MQ CipherSpec , wyszukując nazwę IBM MQ CipherSpec w poniższej tabeli i odwołując się do czteroznakowej kolumny kodu z rozszerzoną kolumną znaków z tabeli 2 w temacie TTLSCipherParms .

Tabela 79. Konwersja z kodów czteroznakowych na nazwy specyfikacji szyfrowania CipherSpec

Czteroznakowy kod	Protokół	Domyślnie włączone	Nazwa specyfikacji szyfrowania
0001	SSL 3.0	Nie	NULL_MD5
0002	SSL 3.0	Nie	NULL_SHA
0003	SSL 3.0	Nie	RC4_MD5_EXPORT
0004	SSL 3.0	Nie	RC4_MD5_US
0005	SSL 3.0	Nie	RC4_SHA_US
0006	SSL 3.0	Nie	RC2_MD5_EXPORT
0008	SSL 3.0	Nie	DES_SHA_EXPORT
0009	TLS 1.0	Tak	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	Nie	TRIPLE_DES_SHA_US
000A	TLS 1.0	Tak	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Tak	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Tak	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	Tak	TLS_RSA_WITH_NULL_SHA256

Tabela 79. Konwersja z kodów czteroznakowych na nazwy specyfikacji szyfrowania CipherSpec (kontynuacja)

Czteroznakowy kod	Protokół	Domyślnie włączone	Nazwa specyfikacji szyfrowania
003C	TLS 1.2	Tak	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	Tak	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	Tak	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Tak	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Tak	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Tak	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. Instrukcja TTLSEnvironmentAdvancedParms jest powiązana z TTLSEnvironmentAction przez właściwość **TTLSEnvironmentAdvancedParmsRef** .

   Za pomocą tej instrukcji można określić, które protokoły SSL i TLS są włączone. W przypadku IBM MQ należy włączyć tylko jeden protokół zgodny z nazwą zestawu algorytmów szyfrowania użytą w instrukcji TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

Pełny zestaw instrukcji jest następujący i powinien zostać zastosowany do agenta strategii:

```
TTLSRule                      REMOTE-TO-CSQ1
{
  LocalAddr                   ALL
  LocalPortRange              1414
  RemoteAddr                  123.456.78.9
  Jobname                     CSQ1CHIN
  Direction                   INBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Krok 3: usuwanie parametru SSLCIPH z kanału z/OS

Usuń specyfikację szyfrowania CipherSpec z kanału z/OS za pomocą następującej komendy:

```
ALTER CHANNEL(channel-name) CHLTYPE(RCVR) SSLCIPH(' ')
```

Krok 4: Uruchamianie kanału

Po uruchomieniu kanału zostanie użyta kombinacja protokołów AT-TLS i IBM MQ TLS.

Ostrzeżenie: Wcześniejsze instrukcje AT-TLS są tylko minimalną konfiguracją. Istnieją inne instrukcje strategii AT-TLS z AT-TLS, które nie zostały opisane w tej sekcji i mogą być używane z produktem IBM MQ w zależności od potrzeb. Jednak produkt IBM MQ został przetestowany tylko z opisanymi strategiami.

Resetowanie kluczy tajnych SSL i TLS

Program IBM MQ obsługuje resetowanie kluczy tajnych w menedżerach kolejek i klientach.

Klucze tajne są resetowane, gdy określona liczba zaszyfrowanych bajtów danych przepłynie przez kanał. Jeśli puls kanału jest włączony, klucz tajny jest resetowany przed wysłaniem lub odebraniem danych zgodnie z pulsem kanału.

Wartość resetowania klucza jest zawsze ustawiana przez stronę inicjującą kanału IBM MQ .

Menedżer kolejek

W przypadku menedżera kolejek należy użyć komendy **ALTER QMGR** z parametrem **SSLRKEYC** , aby ustawić wartości używane podczas renegocjacji klucza.

W systemie IBM inależy użyć parametru **CHGMQM** z parametrem **SSLRSTCNT** .

MQI client

Domyślnie klienty MQI nie renegocjują klucza tajnego. Klient MQI może renegocjować klucz na jeden z trzech sposobów. Na poniższej liście metody są wyświetlane w kolejności priorytetów. W przypadku określenia wielu wartości używana jest wartość najwyższego priorytetu.

1. Używając pola Licznik KeyResetw strukturze MQSCO w wywołaniu MQCONNX.
2. Za pomocą zmiennej środowiskowej MQSSLRESET.
3. Przez ustawienie atrybutu liczby SSLKeyResetw pliku konfiguracyjnym klienta MQI.

Te zmienne mogą być ustawione na liczbę całkowitą z zakresu od 0 do 999 999 999, reprezentującą liczbę niezaszyfrowanych bajtów wysłanych i odebranych w konwersacji TLS przed renegocjacją tajnego klucza TLS. Podanie wartości 0 oznacza, że klucze tajne TLS nigdy nie są renegocjowane. Jeśli zostanie podana liczba operacji resetowania tajnego klucza TLS z zakresu od 1 bajtu do 32 kB, kanały TLS będą używać liczby operacji resetowania tajnego klucza o wielkości 32 kB. Ma to na celu uniknięcie nadmiernej liczby operacji resetowania klucza, które miałyby miejsce w przypadku małych wartości resetowania tajnego klucza TLS.

Jeśli dla kanału zostanie podana wartość większa niż zero i zostaną włączone pulsy kanału, klucz tajny również zostanie renegocjowany przed wysłaniem lub odebraniem danych komunikatu zgodnie z pulsem kanału.

Liczba bajtów do następnej ponownej renegocjacji klucza tajnego jest resetowana po każdej pomyślnej renegocjacji.

Szczegółowe informacje na temat struktury MQSCO zawiera sekcja KeyResetCount (MQLONG). Szczegółowe informacje na temat komendy MQSSLRESET zawiera sekcja MQSSLRESET. Więcej informacji na temat używania protokołu TLS w pliku konfiguracyjnym klienta zawiera sekcja SSL w pliku konfiguracyjnym klienta.

Java

W systemie IBM MQ classes for Javaaplikacja może zresetować klucz tajny w jeden z następujących sposobów:

- Przez ustawienie pola liczby sslResetw klasie MQEnvironment.
- Przez ustawienie właściwości środowiska MQC.SSL_RESET_COUNT_PROPERTY w obiekcie Hashtable. Następnie aplikacja przypisuje tabelę mieszającą do pola `properties` w klasie MQEnvironment lub przekazuje ją do obiektu MQQueueManager w jej konstruktorze.

Jeśli aplikacja używa więcej niż jednej z tych metod, mają zastosowanie zwykłe reguły pierwszeństwa. Reguły dotyczące kolejności wykonywania operacji zawiera sekcja Klasa com.ibm.mq.MQEnvironment .

Wartość pola sslResetlub właściwości środowiska MQC.SSL_RESET_COUNT_PROPERTY reprezentuje łączną liczbę bajtów wysłanych i odebranych przez kod klienta IBM MQ classes for Java przed ponownym negocjowaniem klucza tajnego. Liczba wysłanych bajtów jest liczbą przed szyfrowaniem, a liczba odebranych bajtów jest liczbą po deszyfrowaniu. Liczba bajtów obejmuje również informacje sterujące wysyłane i odbierane przez klienta IBM MQ classes for Java .

Jeśli licznik resetowania ma wartość zero, co jest wartością domyślną, klucz tajny nigdy nie jest renegocjowany. Licznik resetowania jest ignorowany, jeśli nie określono opcji CipherSuite .

JMS

W przypadku systemu IBM MQ classes for JMSwłaściwość SSLRESETCOUNT reprezentuje łączną liczbę bajtów wysłanych i odebranych przez połączenie przed renegocjacją klucza tajnego używanego do szyfrowania. Liczba wysłanych bajtów jest liczbą przed szyfrowaniem, a liczba odebranych bajtów jest liczbą po deszyfrowaniu. Liczba bajtów obejmuje również informacje sterujące wysyłane i odbierane przez IBM MQ classes for JMS. Aby na przykład skonfigurować obiekt ConnectionFactory , który może być używany do tworzenia połączenia przez kanał MQI z włączoną obsługą protokołu TLS z kluczem tajnym, który jest renegocjowany po przekazaniu 4 MB danych, należy wydać następującą komendę w narzędziu JMSAdmin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Jeśli wartość parametru SSLRESETCOUNT wynosi zero, co jest wartością domyślną, klucz tajny nigdy nie jest renegocjowany. Właściwość SSLRESETCOUNT jest ignorowana, jeśli nie ustawiono właściwości SSLCIPHERSUITE.

.NET

W przypadku niezarządzanych klientów .NET liczba całkowita podana we właściwości SSLKeyResetwskazuje liczbę niezaszyfrowanych bajtów wysłanych i odebranych w ramach konwersacji TLS przed ponownym wynegocjowaniem klucza tajnego.

Więcej informacji na temat używania właściwości obiektu w programie IBM MQ classes for .NETzawiera sekcja Pobieranie i ustawianie wartości atrybutów.

W przypadku klientów zarządzanych przez .NET klasa SSLStream nie obsługuje resetowania/renegocjacji klucza tajnego. Jednak, aby zachować spójność z innymi klientami IBM MQ , IBM MQ zarządzany .NET klient umożliwia aplikacjom ustawianie liczby SSLKeyReset. Więcej informacji na ten temat zawiera sekcja Resetowanie lub renegocjowanie klucza tajnego.

XMS .NET

W przypadku niezarządzanych klientów XMS .NET należy zapoznać się z sekcją Zabezpieczanie połączeń z menedżerem kolejek produktu IBM MQ.

Odsyłacze pokrewne

ALTER QMGR (Zmiana menedżera kolejek)

WYŚWIETLENIE QMGR

Zmiana menedżera kolejek komunikatów (Change Message Queue Manager-CHGMQM)

Wyświetlenie menedżera kolejek komunikatów (Display Message Queue Manager-DSPMQM)

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 462.

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.

z/OS V 9.1.4 Poufność danych w stanie spoczynku w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych

Produkt IBM MQ for z/OS może wykorzystać dane klienta i dane konfiguracyjne, zapisując dane do aktywnych zestawów danych dziennika, zestawów danych dziennika archiwalnego, zestawów stron, zestawy danych paska startowego (BSDS) i V 9.1.5 współużytkowane zestawy danych komunikatów (SMDS).

Produkt z/OS udostępnia wydajne, oparte na strategiach szyfrowanie zestawów danych. Produkt IBM MQ for z/OS obsługuje szyfrowanie zestawu danych z/OS dla:

- Aktywne zestawy danych dziennika; patrz uwaga “1” na stronie 464
- Archiwalne zestawy danych dziennika; patrz uwaga “2” na stronie 464
- Zestawy stron; patrz uwaga “1” na stronie 464
- BSDS; patrz uwaga “2” na stronie 464
- Zestawy danych CSQINP*; patrz uwaga “2” na stronie 464
- V 9.1.5 SMDS; patrz uwaga “3” na stronie 464

Zapewnia to poufność danych w pozostałej części menedżera kolejek systemu z/OS .

Uwagi:

1. From IBM MQ 9.1.4, IBM MQ for z/OS supports z/OS data set encryption for active logs and page sets.
2. Szyfrowanie zestawu danych dla dzienników archiwalnych, zestawów danych BSDS i CSQINP* jest obsługiwane we wszystkich wersjach produktu IBM MQ for z/OS.
3. V 9.1.5 From IBM MQ 9.1.5, IBM MQ for z/OS supports z/OS data set encryption for SMDS.
4. Produkt IBM MQ Advanced Message Security udostępnia alternatywny mechanizm ochrony danych w stanie spoczynku. Ponadto produkt AMS zabezpiecza również dane w pamięci i w locie

Więcej informacji na temat szyfrowania zestawu danych z/OS zawiera sekcja Korzystanie z rozszerzeń szyfrowania zestawu danych w systemie z/OS .

Konfiguracja szyfrowania zestawu danych z/OS znajduje się poza kontrolą systemu IBM MQ for z/OS. Ustawienia szyfrowania są aktywne, gdy zestaw danych jest tworzony.

Oznacza to, że wszystkie istniejące zestawy danych muszą zostać ponownie utworzone, aby można było użyć nowej strategii szyfrowania zestawu danych.

Produkt IBM MQ for z/OS może być uruchamiany z mieszaniną zaszyfrowanych i niezaszyfrowanych zestawów danych, ale standardowa konfiguracja szyfruje wszystkie używane zestawy danych lub nie są one używane.

z/OS V 9.1.4 Przegląd kroków w celu zaszyfrowania zestawu danych IBM MQ for z/OS

Sposób szyfrowania zestawu danych IBM MQ for z/OS .

Zanim rozpoczniesz

Należy upewnić się, że poprawnie skonfigurowano szyfrowanie zestawu danych z/OS w przedsiębiorstwie. Jeśli konfigurowane jest szyfrowanie zestawu danych w grupie współużytkowania kolejek, należy skonfigurować szyfrowanie zestawu danych produktu z/OS na potrzeby współużytkowania danych.

Uwaga: Szyfrowany zestaw danych z/OS musi być zestawem danych w formacie rozszerzalnym.

Procedura

1. Skonfiguruj klucz szyfrowania i produkt `key-label` w programie RACF, który ma być używany do szyfrowania zestawu danych.
2. Utwórz profil dla produktu `key-label` w klasie RACF CSFKEYS.
3. Nadaj prawo do odczytu identyfikatorem użytkownika menedżera kolejek oraz wszystkim innym użytkownikom, którzy muszą mieć dostęp do zaszyfrowanych danych.

   Może to obejmować identyfikatory użytkowników, które są używane do uruchamiania programów narzędziowych do drukowania w zestawie danych. Na przykład użytkownik, który uruchomił program CSQUTIL SCOPY, musiałby zdeszyfrować odpowiedni zestaw stron.
4. Powiąż szyfrowanie `key-label` z nazwą zestawu danych.

   Można to zrobić za pomocą klasy danych SMS lub segmentu RACF DFP, dla nazwy zestawu danych lub kwalifikatora wysokiego poziomu.

   You can also associate the `key-label` with the data set when the data set is allocated.
5. Zmień nazwę dowolnego istniejącego zestawu danych za pomocą komendy IDCAMS ALTER.
6. Ponownie przydziel zestaw danych odpowiednimi atrybutami.
7. Skopiuj zawartość zestawu danych o zmienionej nazwie do nowego zestawu danych za pomocą programu IDCAMS REPRO.

   Dane są szyfrowane przez działanie kopiowania danych do zestawu danych.
8. Powtórz kroki od “4” na stronie 465 do “6” na stronie 465 dla wszystkich innych zestawów danych, które muszą być szyfrowane.

z/OS V 9.1.4 Przykład szyfrowania aktywnych dzienników menedżera kolejek

Poniższe tematy prowadzą użytkownika przez proces włączania szyfrowania zestawu danych w istniejących aktywnych dziennikach.

Uwaga: Proces dla innych zestawów danych jest podobny do procesu w przypadku aktywnych dzienników.

W tym przykładzie:

- Menedżer kolejek CSQ1 jest uruchamiany dla użytkownika QMCSQ1i ma aktywne zestawy danych dziennika CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002, itd.
- Środowisko sprzętowe i programowe jest w stanie używać szyfrowania zestawu danych z/OS
- Narzędzie RACF jest używane jako narzędzie SAF
- Menedżer kolejek został zatrzymany

Wykonaj procedurę w następującej kolejności:

1. “Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek” na stronie 465
2. “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 466

z/OS V 9.1.4 Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek

W jaki sposób można skonfigurować klucz szyfrowania zestawu danych dla menedżera kolejek.

O tym zadaniu

To zadanie jest wymagane wstępnie dla produktu “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 466.

Procedura

1. Skonfiguruj klucz szyfrowania bitowego AES-256 z etykietą, na przykład CSQ1DSKY, za pomocą programu narzędziowego generatora kluczy (KGUP) z/OS .
2. Zdefiniuj profil RACF CSFKEYS dla klucza szyfrowania CSQ1DSKY , wydając następującą komendę:

   ```
   RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
   ```

3. Skonfiguruj segment ICSF profilu, aby zezwolić na użycie klucza jako klucza zabezpieczonego, wydając następującą komendę:

   ```
   RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
   ```

4. Zezwól menedżerowi kolejek na korzystanie z klucza szyfrowania przez nadanie dostępu QMCSQ1 READ do profilu, wydając następującą komendę:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Przyznaj ten sam dostęp do wszystkich użytkowników administracyjnych, którzy muszą odczytywać lub zapisywać szyfrowany zestaw danych.
5. Odśwież klasę CSFKEYS, wydając następującą komendę.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Co dalej

Skonfiguruj szyfrowanie zestawu danych dla zestawów danych w sposób opisany w sekcji “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 466

z/OS V 9.1.4 Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika

Sposób konfigurowania szyfrowania w zestawach danych dziennika.

Zanim rozpoczniesz

Upewnij się, że przeczytałeś:

Przegląd kroków w celu zaszyfrowania zestawu danych IBM MQ for z/OSi wykonanie procedury w “Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek” na stronie 465

O tym zadaniu

Ta metoda korzysta z segmentu DFP profilu ogólnego RACF , dzięki czemu można użyć klucza szyfrowania dla wszystkich nowych zestawów danych zgodnych z profilem.

Alternatywnie można skonfigurować i użyć klasy danych SMS albo etykiety klucza można określić bezpośrednio przy przydzielaniu zestawu danych.

Jak opisano powyżej, w tym przykładzie menedżer kolejek CSQ1 jest uruchamiany dla użytkownika QMCSQ1i ma aktywne zestawy danych dziennika CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002i tak dalej.

Procedura

1. Utwórz profil ogólny, jeśli nie istnieje, wydając następującą komendę:

   ```
   ADDSD 'CSQ1.LOGS.*' UACC(NONE)
   ```

2. Aby zezwolić użytkownikowi menedżera kolejek na zmianę dostępu do profilu, należy wydać następującą komendę:

```
PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
```

Należy również zezwolić na odpowiedni dostęp wymagany dla dowolnego użytkownika administracyjnego.

3. Dodaj segment DFP z etykietą klucza szyfrowania, wydając następującą komendę:

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

Uwaga: Należy użyć tego samego klucza szyfrowania, który został użyty w sekcji Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek.

4. Odśwież ogólne profile zestawu danych, wydając następującą komendę:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Zmień nazwę każdego zestawu danych dziennika na kopię zapasową, a następnie ponownie utwórz i odtwórz dane, używając programu IDCAMS. Poniższy fragment kodu JCL przekształca CSQ1.LOGS.LOGCOPY1.DS001:

   a) Zmień nazwę zestawu danych na kopii zapasowej

```
//RENAME   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RENAME DATASET TO BACKUP                                    */
  /*-------------------------------------------------------------*/
  ALTER 'CSQ1.LOGS.LOGCOPY1.DS001'                  -
        NEWNAME('CSQ1.BAK.LOGS.LOGCOPY1.DS001')
```

   b) Zdefiniuj ponownie zestaw danych.

   Nowy zestaw danych zostanie zaszyfrowany ze względu na profil RACF.

   Uwaga: Zastąp + + EXTDCLASS + + nazwą klasy danych rozszerzonych formatu, która ma być używana dla zestawu danych.

```
//REDEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* REDEFINE THE DATASET                                        */
  /*-------------------------------------------------------------*/
  DEFINE CLUSTER                                    -
         (NAME(CSQ1.LOGS.LOGCOPY1.DS001)            -
         LINEAR                                     -
         SHAREOPTIONS(2 3)                          -
         MODEL(CSQ1.BAK.LOGS.LOGCOPY1.DS001)        -
         DATACLAS(++EXTDCLASS++))
```

   c) Skopiuj dane z kopii zapasowej do ponownie ustawionego zestawu danych.

   Ten krok szyfruje dane:

```
//RESTORE  EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RESTORE DATA INTO ENCRYPTED LOG                             */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)     -
        OUTDATASET(CSQ1.LOGS.LOGCOPY1.DS001)
```

Co dalej

Powtórz krok “5” na stronie 467 dla wszystkich aktywnych zestawów danych dziennika.

Wymagany jest tylko jeden klucz szyfrowania, a wszystkie zestawy danych mogą być powiązane z tą samą etykietą klucza.

Zrestartuj menedżer kolejek CSQ1. Aby sprawdzić, czy zestawy danych dziennika zostały zaszyfrowane, należy użyć danych wyjściowych komendy DISPLAY LOG .

z/OS V 9.1.4 Uwagi dotyczące szyfrowania zestawu danych produktu z/OS w grupie współużytkowania kolejek

Każdy menedżer kolejek w grupie współużytkowania kolejek (QSG) musi być w stanie odczytać dzienniki, BSDS V 9.1.5 oraz współużytkowane zestawy danych komunikatów (SMDS) każdego innego menedżera kolejek w QSG.

Oznacza to, że każdy system, na którym może działać członek QSG, musi spełniać wymagania dotyczące szyfrowania zestawu danych z/OS , a wszystkie etykiety kluczy i klucze szyfrowania używane do zabezpieczania zestawów danych dla każdego menedżera kolejek w QSG muszą być dostępne w każdym systemie.

Menedżer kolejek wcześniejszy niż IBM MQ for z/OS 9.1.3 nie może uzyskać dostępu do zaszyfrowanego aktywnego zestawu danych dziennika.

V 9.1.5 Menedżer kolejek wcześniejszy niż IBM MQ for z/OS 9.1.3 nie może uzyskać dostępu do zaszyfrowanego SMDS.

V 9.1.5 Przed rozpoczęciem korzystania z szyfrowania zestawu danych z/OS należy przeprowadzić migrację wszystkich menedżerów kolejek w QSG do co najmniej IBM MQ for z/OS 9.1.3.

Jeśli menedżer kolejek w QSG jest uruchamiany z dowolnym szyfrowanym zestawem danych dziennika, a każdy inny menedżer kolejek w QSG został uruchomiony, ale nie został ostatnio uruchomiony z wersją programu IBM MQ for z/OS obsługując szyfrowane aktywne dzienniki, menedżer kolejek z zaszyfrowanym aktywnym dziennikiem kończy się nieprawidłowo z kodem nieprawidłowego zakończenia 5C6-00F50033.

V 9.1.5 Można przekształcić QSG w taki sposób, aby używały szyfrowanych dzienników aktywnych i SMDS bez pełnego wyłączenia, poprzez:

1. Migrowanie każdego menedżera kolejek do co najmniej IBM MQ 9.1.5 z kolei.
2. Przekształcanie aktywnych dzienników w szyfrowane zestawy danych dla każdego menedżera kolejek z kolei. Wymaga to wyłączenia menedżera kolejek, a następnie zrestartowania.

   Jednocześnie jest prawdopodobne, że zestawy stron i dzienniki archiwalne będą mogły być włączone dla szyfrowanych zestawów danych, ale nie ma to wpływu na migrację QSG.

   Procedura przekształcania każdego zestawu danych jest opisana w podręczniku “Przykład szyfrowania aktywnych dzienników menedżera kolejek” na stronie 465 .
3. Konwertowanie SMDS do szyfrowanych zestawów danych dla każdej indywidualnej struktury CF z kolei przez:
   a. Wydanie komendy RESET SMDS (*) ACCESS (DISABLED) CFSTRUCT (structure-name) umożliwia zawieszenie dostępu menedżera kolejek do SMDS.

      Należy pamiętać, że w tym czasie dane w kolejkach współużytkowanych powiązanych z SMDS są tymczasowo niedostępne.
   b. Przekształcanie każdego zestawu danych, który tworzy SMDS w szyfrowanych zestawach danych, przy użyciu procedury opisanej w sekcji “Przykład szyfrowania aktywnych dzienników menedżera kolejek” na stronie 465.
   c. Wydanie komendy RESET SMDS (*) ACCESS (ENABLED) CFSTRUCT (structure-name) w celu wznowienia dostępu menedżera kolejek do SMDS.

Ostrzeżenie: Należy zamknąć menedżer kolejek w sposób czysty przed przekształceniem dzienników, a odtwarzanie struktury narzędzia CF może nie być możliwe podczas konwersji, ponieważ aktywne zestawy danych dziennika będą tymczasowo niedostępne.

z/OS V 9.1.4 Uwagi dotyczące migracji wstecznej przy korzystaniu z szyfrowania zestawu danych z/OS

Podczas migracji wstecznej menedżera kolejek, który zawiera co najmniej jeden zaszyfrowany zestaw danych, należy wziąć pod uwagę następujące kwestie.

Szyfrowanie zestawu danych z/OS jest obsługiwane w następujących zestawach danych IBM MQ for z/OS :

- Zestawy danych aktywnego dziennika
- Archiwalne zestawy danych dziennika
- Zestawy stron
- BSDS
- V 9.1.5 SMDS
- Zestawy danych CSQINP*

Nie ma uwag dotyczących migracji wstecznej dla zestawów danych BSDS, dziennika archiwalnego lub CSINP*.

Należy jednak wziąć pod uwagę następujące kwestie:

- V 9.1.5 SMDS
- Zestaw stron i
- Aktywny dziennik

Zestawy danych, które są używane z szyfrowaniem zestawu danych systemu z/OS , nie są obsługiwane w produkcie IBM MQ for z/OS 9.1.0i wcześniejszych wersjach obsługi długoterminowej.

Przed migracją wsteczną należy usunąć wszystkie strategie szyfrowania dla zestawów V 9.1.5 SMDS, zestawów stron i zestawów danych aktywnego dziennika, a następnie zdeszyfrować dane. Ten proces jest opisany w sekcji “Usuwanie szyfrowania zestawu danych z zestawu danych” na stronie 469.

Ostrzeżenie: Jeśli menedżer kolejek, który ma być migrowany wstecz, jest częścią grupy współużytkowania kolejek (QSG), należy najpierw przeczytać sekcję “Uwagi dotyczące grupy współużytkowania kolejek” na stronie 470 .

Usuwanie szyfrowania zestawu danych z zestawu danych

W tym przykładzie przedstawiono sposób usunięcia szyfrowania zestawu danych z zestawu danych dziennika CSQ1.LOGS.LOGCOPY1.DS001DS001. Można użyć równoważnego procesu dla zestawów stron V 9.1.5 SMDS i .

W przykładzie założono, że:

- RACF to narzędzie SAF
- Menedżer kolejek używający zestawu danych został zatrzymany
- Etykieta klucza szyfrowania została powiązana z ogólnym profilem RACF CSQ1.LOGS.*

Wykonaj następującą procedurę:

1. Skopiuj dane z zestawu danych do zestawu danych kopii zapasowej.
   a. Zdefiniuj zapasowy zestaw danych, który nie jest powiązany z etykietą klucza szyfrowania.

      Uwaga: Zastąp + + EXTDCLASS + + nazwą klasy danych w formacie rozszerzonym, która ma być używana dla zestawu danych.

```
//DEFINE EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
```

```
  /* DEFINE UNENCRYPTED DATA SET                                  */
  /*-------------------------------------------------------------*/
  DEFINE CLUSTER                                 -
         (NAME(CSQ1.BAK.LOGS.LOGCOPY1.DS001)     -
         LINEAR                                  -
         SHAREOPTIONS(2 3)                       -
         MODEL(CSQ1.LOGS.LOGCOPY1.DS001)         -
         DATACLAS(++EXTDCLASS++))
/*
```

b. Skopiuj dane z oryginalnego zestawu danych do kopii zapasowej. Ten krok deszyfruje dane.

```
//COPY     EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* COPY DATA INTO UNENCRYPTED DATA SET                         */
  /*-------------------------------------------------------------*/
  REPRO INDATASET(CSQ1.LOGS.LOGCOPY1.DS001)          -
        OUTDATASET(CSQ1.BAK.LOGS.LOGCOPY1.DS001)
/*
```

c. Usuń oryginalny zestaw danych

```
//DELETE   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DELETE ORIGINAL                                             */
  /*-------------------------------------------------------------*/
  DELETE ('CSQ1.LOGS.LOGCOPY1.DS001')
/*
```

d. Zmień nazwę kopii zapasowej na nazwę oryginalnego zestawu danych. Dane pozostają niezaszyfrowane

```
//RENAME   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* RENAME UNENCRYPTED DATA SET                                 */
  /*-------------------------------------------------------------*/
  ALTER CSQ1.BAK.LOGS.LOGCOPY1.DS001'                -
         NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001)
  ALTER 'CSQ1.BAK.LOGS.LOGCOPY1.DS001.*'              -
         NEWNAME('CSQ1.LOGS.LOGCOPY1.DS001.*')
/*
```

2. Opcjonalnie powtórz ten proces dla innych zestawów danych, z którymi powiązana jest etykieta klucza szyfrowania za pośrednictwem CSQ1.LOGS.* profil ogólny.
3. Opcjonalnie, jeśli wszystkie zestawy danych są powiązane z CSQ1.LOGS.* profil ogólny został zdeszyfrowany, usuń klucz DATAKEY powiązany z profilem ogólnym, wydając następującą komendę

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

4. Odśwież ogólne profile zestawu danych, wydając następującą komendę:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Zrestartuj menedżer kolejek.
6. Jeśli klucz szyfrowania nie jest już potrzebny, usuń go i usuń powiązany z nim profil RACF z klasy CSFKEYS.

Uwagi dotyczące grupy współużytkowania kolejek

Jeśli menedżer kolejek, który jest częścią grupy współużytkowania kolejek, ma zostać zmigrowany wstecz do wersji produktu IBM MQ for z/OS , która nie obsługuje szyfrowania zestawu danych, wszystkie aktywne

zestawy danych dziennika V 9.1.5 i SMDS wszystkich menedżerów kolejek w grupie QSG muszą mieć usunięte strategie szyfrowania zestawu danych, a ich dane zostały zdeszyfrowane.

Ma to zastosowanie niezależnie od tego, czy pojedynczy element grupy QSG jest migrowany wstecz, czy też wszystkie elementy grupy QSG.

Można usunąć strategie szyfrowania i deszyfrować dane bez konieczności pełnego wyłączenia QSG przez:

1. Zamykanie każdego menedżera kolejek w grupie QSG po kolei, usuwanie strategii szyfrowania i deszyfrowanie danych z aktywnych protokołów przy użyciu procesu opisanego w sekcji “Usuwanie szyfrowania zestawu danych z zestawu danych” na stronie 469.

   Jeśli menedżer kolejek ma być migrowany wstecz, jego zestaw stron również powinien zostać zdeszyfrowany w tym momencie. Następnie zrestartuj menedżer kolejek.

2. V 9.1.5 Usuwanie strategii szyfrowania i deszyfrowanie danych dla SMDS każdej struktury CF po kolei przez:

   a. Wykonywanie komendy

   ```
   RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)
   ```

   w celu zawieszenia dostępu menedżera kolejek do SMDS. W tym czasie dane w kolejkach współużytkowanych powiązanych z SMDS będą tymczasowo niedostępne.

   b. Wykonaj proces opisany w sekcji “Usuwanie szyfrowania zestawu danych z zestawu danych” na stronie 469 dla każdego zestawu danych, który składa się na zestaw SMDS.

   c. Wykonywanie komendy

   ```
   RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name)
   ```

   w celu wznowienia dostępu menedżera kolejek do SMDS.

Używanie szyfrowania zestawu danych programu z/OS z menedżerem kolejek, który go nie obsługuje

W przypadku przypadkowej migracji wstecznej menedżera kolejek do wersji produktu IBM MQ for z/OS , która nie obsługuje szyfrowania zestawu danych, należy zapomnieć o usunięciu strategii szyfrowania i deszyfrowaniu danych, gdy menedżer kolejek próbuje uzyskać dostęp do zestawu danych, gdy wystąpi błąd.

Błąd zależy od typu zestawu danych i jest wyświetlany w poniższej tabeli.

Uwaga: Jeśli wystąpi co najmniej jeden z tych błędów, należy postępować zgodnie z procesami opisanymi w sekcji “Usuwanie szyfrowania zestawu danych z zestawu danych” na stronie 469 dla danego zestawu danych. Można je wykonać bez zmiany wersji produktu IBM MQ for z/OS.

Zestaw danych	**Błąd, jeśli menedżer kolejek nie obsługuje szyfrowania zestawu danych systemu z/OS**
Zestaw stron 0	Nieprawidłowe zakończenie 5C6-00C91400 podczas uruchamiania menedżera kolejek
Zestawy stron 1-99	MQRC 2193 "Błąd zestawu stron" podczas uzyskiwania dostępu do zestawu stron, na przykład w MQPUT
Aktywny dziennik	Nieprawidłowe zakończenie 5C6-00E80084 podczas uruchamiania menedżera kolejek
V 9.1.5 SMDS	Komunikat IEC161I-122 został zarejestrowany w dzienniku "Zestaw danych ma etykietę KEYLABEL, ale użytkownik nie określił, że aplikacja może obsługiwać szyfrowanie".

Zestaw danych	Błąd, jeśli menedżer kolejek nie obsługuje szyfrowania zestawu danych systemu z/OS
	SMDS oznaczył AVAIL (BŁĄD).

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 TLS, wybór opcji CipherSpec określa poziom integralności danych w przedsiębiorstwie. Jeśli używany jest produkt IBM 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,

Więcej informacji

Więcej informacji na temat zapewnienia integralności danych można znaleźć w sekcji dotyczącej produktu “Włączanie opcji CipherSpecs” na stronie 433 .

Zadania pokrewne

Łączenie dwóch menedżerów kolejek za pomocą protokołu TLS

Bezpieczne podłączanie klienta do menedżera kolejek

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 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 TLS 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 za pomocą RACF w systemie z/OSlub OAM na innych platformach.

O tym zadaniu

Aby kontrolować dostęp do kolejek, należy użyć zabezpieczeń platformy oraz mechanizmu kontroli dostępu w produkcie IBM 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 systemie IBM 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 sprawdzenie może dotyczyć zarówno identyfikatora użytkownika otrzymanego z sieci, jak i pochodzącego z MCAUSERlub obu tych elementów. Tej opcji należy użyć, jeśli odsyłacz jest zaufany i uwierzytelniony.

   ONLYMCA (tylko z/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 (tylko z/OS)
   Tak jak w przypadku CTX, ale każdy ID użytkownika otrzymany z sieci nie jest używany.

Autoryzowanie umieszczania komunikatów w kolejkach klastra zdalnego

W systemie z/OS skonfiguruj uprawnienia do umieszczania w kolejce klastra za pomocą programu RACF. Na innych platformach autoryzuj dostęp do połączeń z menedżerami kolejek i umieszczaj je w kolejkach dla tych menedżerów 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 produktu z/OSnależy wprowadzić następujące komendy:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- W przypadku systemów UNIX, Linux, and Windows należy wprowadzić następujące komendy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- W przypadku produktu IBM inależy wprowadzić następujące komendy:

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

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. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.

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 410.

Pojęcia 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 TLS udostępnionej 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.

   z/OS z/OS

   Moduł ładujący wyjścia zabezpieczeń musi znajdować się w zestawie danych określonym w instrukcji `CSQXLIB DD` w procedurze adres-przestrzeń inicjatora kanału.

   ULW 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.

Uwaga: Chociaż użycie komendy RESET CLUSTER w sposób wymuszający usuwa menedżer kolejek z klastra, użycie komendy RESET CLUSTER przez siebie samego nie uniemożliwia późniejszego ponownego uruchomienia klastra przez menedżer kolejek. Aby upewnić się, że menedżer kolejek nie zostanie ponownie przyłączony do klastra, należy wykonać kroki opisane w sekcji "Zapobieganie łączeniu menedżerów kolejek z klastrem" na stronie 475.

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)
```

   Uwaga: QMID to łańcuch, więc wartość qmid powinna być ujęta w pojedynczy cudzysłów, na przykład QMID('FR01_2019-07-15_14.42.42').

Wyniki

Wymuszone usunięcie menedżera kolejek nie jest zmieniane; jego lokalne definicje klastrów pokazują, że ma on znajdować się 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/TLS i klastry

Podczas konfigurowania protokołu TLS 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 TLS, należy skonfigurować protokół TLS we wszystkich menedżerach kolejek, które komunikują się z użyciem kanału.

Więcej informacji na temat protokołu TLS można znaleźć w sekcji “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24. Porady są zwykle stosowane do kanałów klastra, ale warto zwrócić szczególną uwagę na następujące informacje:

W klastrze IBM 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 TLS, należy wziąć pod uwagę następujące kwestie:

- Wszystkie menedżery kolejek, które mają komunikować się z tym serwerem CLUSRCVR , muszą mieć dostęp do obsługi TLS. Ten zapis TLS 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 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=IBM 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 bazująca obsługa protokołu TLS implementuje ten parametr 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 TLS_RSA_WITH_AES_128_CBC_SHA).

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/TLS

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 IBM 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.

Ostrzeżenie: Nie jest możliwe użycie kombinacji certyfikatów podpisanych z krzywą eliptyczną i certyfikatów podpisanych przez RSA w menedżerach kolejek, które mają być połączone w ramach klastra.

Menedżery kolejek w klastrze muszą używać podpisanych certyfikatów RSA lub wszystkich certyfikatów podpisanych przez EC, a nie mieszanych obu tych certyfikatów.

Więcej informacji zawiera sekcja "Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ" na stronie 45.

Zaktualizuj wszystkie menedżery kolejek w klastrze do wersji IBM MQ V8 lub nowszej, jeśli nie znajdują się jeszcze na tych poziomach. Rozdziel certyfikaty i klucze tak, aby TLS działa z każdego z nich.

Aby zaktualizować tom lub użyć specyfikacji ANY_TLS12 CipherSpecs, należy zaktualizować wszystkie menedżery kolejek w klastrze do wersji IBM MQ 9.1.2 lub nowszej.

Aby zaktualizować lub użyć dowolnego innego aliasu CipherSpecs (ANY_TLS13, ANY_TLS12, ANY_TLS12_OR_HIGHERitd.), należy zaktualizować wszystkie menedżery kolejek w klastrze do wersji IBM MQ 9.1.4 lub wyższej.

O tym zadaniu

Zmień kanały CLUSRCVR przed kanałami CLUSSDR .

Procedura

1. Przełącz kanały CLUSRCVR na protokół TLS w dowolnej kolejności, zmieniając jednocześnie jeden CLUSRCVR i zezwalaj na przepływ zmian przez klaster przed zmianą następnego.

   Ważne: Upewnij się, że nie została zmieniona odwrotna ścieżka, dopóki zmiany dla bieżącego kanału nie zostaną rozdystrybuowane w całym klastrze.
2. Opcjonalne: Przełącz wszystkie ręczne kanały CLUSSDR na TLS.

   Nie ma to żadnego wpływu na działanie klastra, o ile nie zostanie użyta komenda REFRESH CLUSTER z opcją REPOS(YES) .

   Uwaga: W przypadku dużych klastrów użycie komendy **REFRESH CLUSTER** może być zakłócające dla klastra, gdy jest ono w toku, a następnie co 27 dni po tym, kiedy obiekty klastra automatycznie wysyłają aktualizacje statusu do wszystkich zainteresowanych menedżerów kolejek. Informacje na ten temat zawiera sekcja Odświeżanie dużego klastra może mieć wpływ na jego wydajność i dostępność.
3. Użyj komendy DISPLAY CLUSQMGR , aby upewnić się, że nowa konfiguracja zabezpieczeń została propagowana w całym klastrze.
4. Zrestartuj kanały, aby używały protokołu TLS, a następnie uruchom komendę REFRESH SECURITY (SSL).

Pojęcia pokrewne

"Włączanie opcji CipherSpecs" na stronie 433
Enable a CipherSpec by using the **SSLCIPH** parameter in either the **DEFINE CHANNEL** MQSC command or the **ALTER CHANNEL** MQSC command.

"Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ" na stronie 45
Ten temat zawiera informacje dotyczące wybierania odpowiednich CipherSpecs i certyfikatów cyfrowych dla strategii bezpieczeństwa. W tym celu należy zapoznać się z relacją między CipherSpecs i certyfikatami cyfrowymi w produkcie IBM MQ.

Informacje pokrewne

Technologia klastrowa: sprawdzone procedury użycia komendy REFRESH CLUSTER

Wyłączanie protokołu SSL/TLS w przypadku klastrowych menedżerów kolejek i kanałów

Aby wyłączyć protokół 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 IBM i, lub *NONE w IBM i .

   Protokół TLS można wyłączyć w kanałach odbiorników klastra w dowolnej kolejności, w jakiej się znajduje.

   Należy pamiętać, że zmiany są wprowadzane w odwrotnym kierunku w kanałach, w których aktywny jest protokół TLS.
2. Sprawdź, czy nowa wartość została odzwierciedlona we wszystkich innych menedżerach kolejek, używając komendy **DISPLAY CLUSQMGR(*)** ALL.
3. Wyłącz TLS we wszystkich kanałach nadawczych klastra ręcznego.

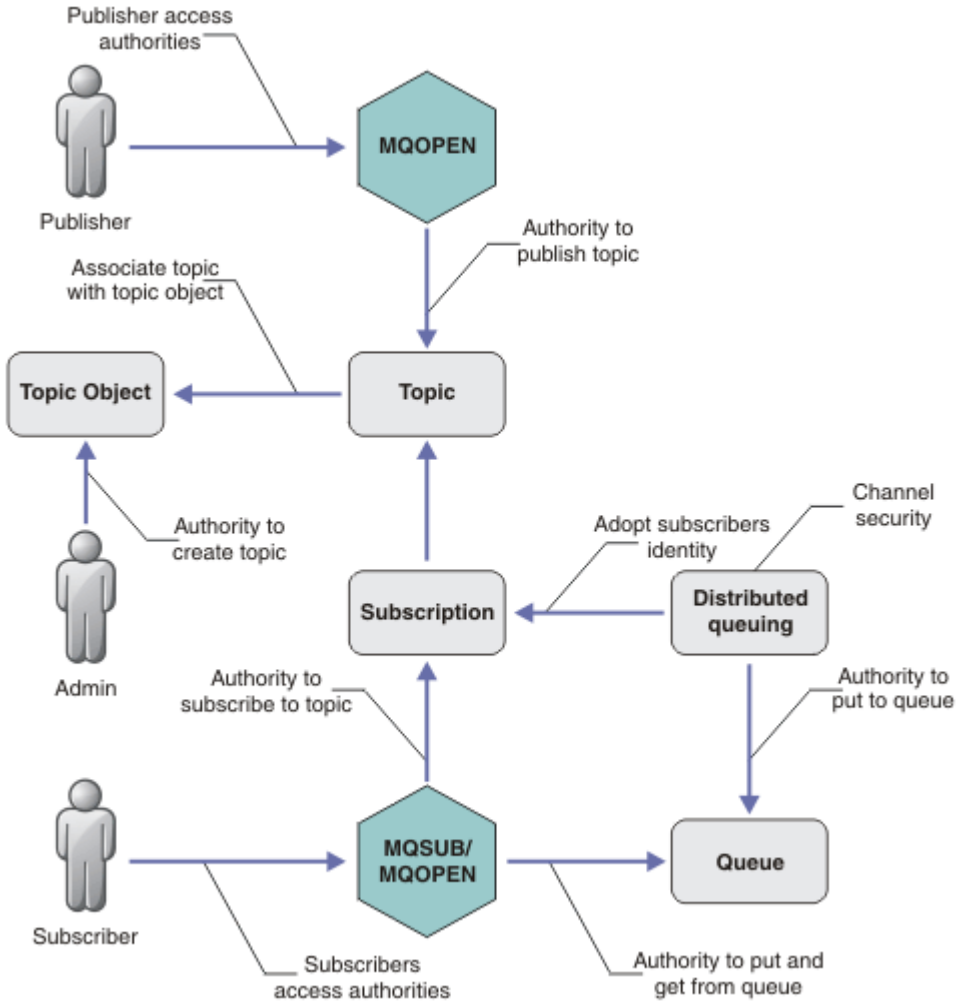
   Nie ma to żadnego wpływu na działanie klastra, o ile nie zostanie użyta komenda **REFRESH CLUSTER** z opcją REPOS (YES).

   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 22 na stronie 481 i opisane w poniższym przykładzie.



Rysunek 22. Relacje bezpieczeństwa publikowania/subskrypcji między różnymi komponentami

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. Sekcja “Model zabezpieczeń tematu” na stronie 483 wyjaśnia sposób zabezpieczania tematów 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 488 i “Przyznaj użytkownikowi prawa dostępu do publikowania w temacie” na stronie 495. z/OS Aby kontrolować dostęp do obiektów tematów w systemie z/OS, należy zapoznać się z sekcją Profile dla zabezpieczeń tematów.

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 484

Subskrybowanie tematu

“Subskrybuj przy użyciu łańcucha tematu, w którym węzeł tematu nie istnieje” na stronie 485

Subskrybuj przy użyciu tematu z użyciem znaków wieloznacznych
"Subskrybuj przy użyciu łańcucha tematu zawierającego znaki wieloznaczne" na stronie 486

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 "Zabezpieczenia subskrypcji" na stronie 501.

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 "Uprawnienia do kolejek docelowych" na stronie 486.

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" na stronie 503

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 IBM MQ kanały są konfigurowane za pomocą programu PUTAUT=DEF w celu umieszczania komunikatów w kolejkach docelowych przy użyciu uprawnień procesu kanału. Konfigurację kanału można zmodyfikować w taki sposób, aby korzystała z produktu PUTAUT=CTX w celu wymagania, aby użytkownik subskrybujący miał uprawnienia do propagowania subskrypcji do innego menedżera kolejek w klastrze.

W sekcji "Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek" na stronie 503 opisano sposób zmiany definicji kanałów w celu kontrolowania użytkowników, którzy mogą 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. IBM 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.

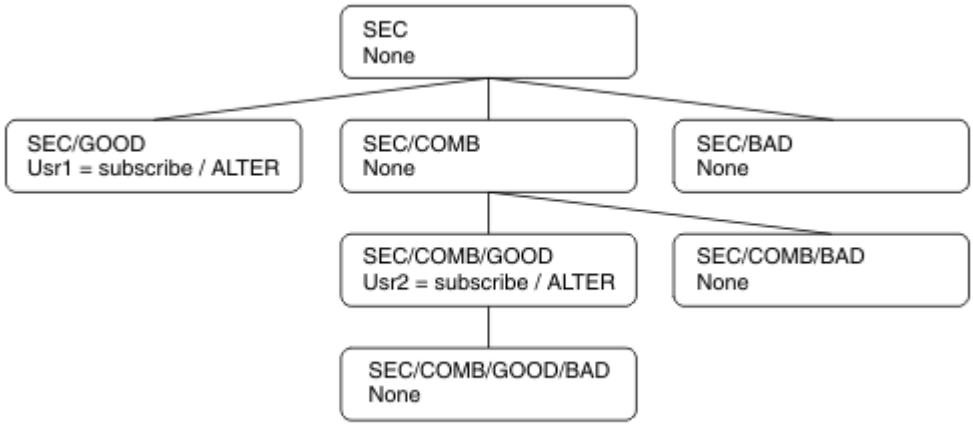
Rozważmy następujący przykład, w którym obiekty tematów zostały zdefiniowane z atrybutami zabezpieczeń lub wyświetlane są uprawnienia:

Tabela 80. Przykładowe uprawnienia do obiektu tematu

Nazwa tematu	Łańcuch tematu	Uprawnienia-nie z/OS	z/OS uprawnienia
SECROOT	SEC	Brak	Brak
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Brak	Brak HLQ.SUBSCRIBE.SECBAD

Tabela 80. Przykładowe uprawnienia do obiektu tematu (kontynuacja)			
Nazwa tematu	**Łańcuch tematu**	**Uprawnienia-nie z/OS**	**z/OS uprawnienia**
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.

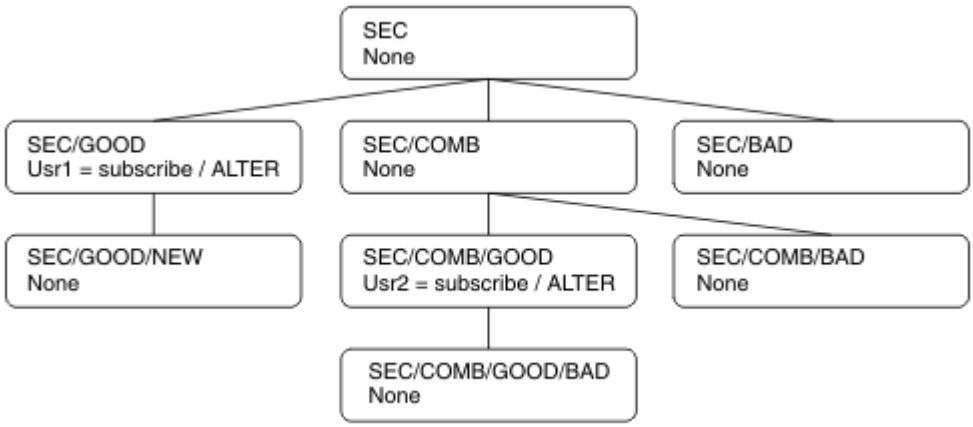
Subskrypcja za pomocą łańcucha tematu, w którym znajduje się węzeł tematu

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, nie są wykonywane operacje sprawdzania 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 w sekcji Tabela 81 na stronie 488:

Tabela 81. Identyfikatory użytkowników używane do sprawdzania zabezpieczeń komend			
Komenda	**Określono SUBUSER i puste**	**Podano i zakończono SUBUSER**	**Nie określono SUBUSER**
	Użyj identyfikatora administratora		Użyj ID użytkownika z subskrypcji LIKE
	Użyj identyfikatora administratora		Użyj ID.DEFAULT.SUużytkownikB -jeśli pole a z SYSTEMjest puste, należy użyć 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 ustawioną kontrolę dostępu do tematów w taki sposób, aby w razie potrzeby można było zastosować kontrolę zabezpieczeń.

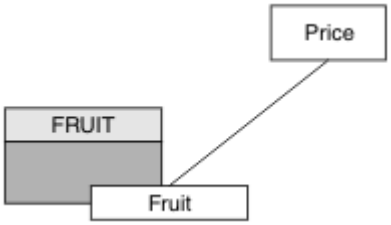
Nadawanie użytkownikowi dostępu do subskrybowania tematu

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 23. Przykład dostępu do obiektu tematu

Tabela 82. 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:

   - z/OS **z/OS** :

     Przyznaj dostęp do produktu USER1 , aby zasubskrybować temat `"Price/Fruit"` , nadając użytkownikowi dostęp do profilu produktu `hlq.SUBSCRIBE.FRUIT` . W tym celu należy użyć następujących komend produktu RACF :

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
     PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - 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:

     ULW **Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*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:

- z/OS W systemie z/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Na innych platformach następujące zdarzenie autoryzacji:

  ```
  MQRC_NOT_AUTHORIZED
  ```

```
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- IBM i W systemie IBMi, 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

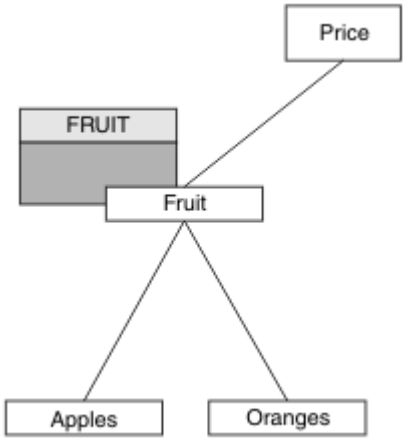
Ten temat jest drugim z listy zadań, które informują o tym, jak nadać dostęp do tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Nadawanie użytkownikowi dostępu do subskrybowania tematu” na stronie 488.

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 24. Przykład nadawania dostępu do tematu w drzewie tematów

Tabela 83. Wymagania dotyczące dostępu dla przykładowych tematów i obiektów tematów

Temat	Wymagany dostęp do subskrypcji	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Owoce	USER1	fruit

Tabela 83. Wymagania dotyczące dostępu dla przykładowych tematów i obiektów tematów (kontynuacja)		
Temat	**Wymagany dostęp do subskrypcji**	**Obiekt tematu**
Cena/Owoce/Jabłka	USER1	
Cena/Owoce/Pomarańcze	USER1	

W poprzednim zadaniu USER1 uzyskano dostęp do subskrypcji tematu `"Price/Fruit"` , nadając mu dostęp do profilu `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/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają 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 takie same jak te, które zostały odebrane w poprzednim zadaniu, ponieważ te same obiekty tematów i profile mają kontrolę nad dostępem.
- 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.

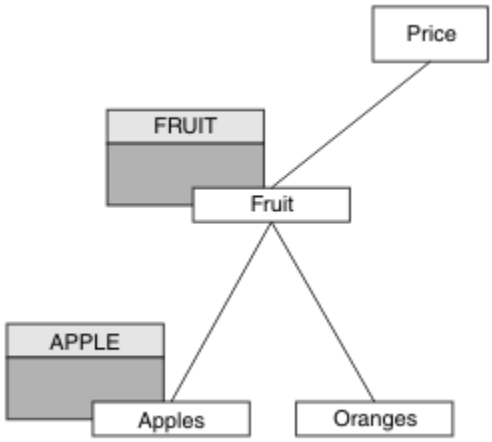
Ten temat jest trzecim na liście zadań, które informują użytkownika o tym, jak przyznać dostęp do subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Nadawanie użytkownikowi dostępu do subskrybowania tematu w obrębie drzewa” na stronie 490.

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 25. Nadawanie dostępu do konkretnych tematów w drzewie tematów

Tabela 84. 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:

   - z/OS **z/OS** :

     W poprzednim zadaniu USER1 został przyznany dostęp do subskrypcji tematu `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do profilu `hlq.SUBSCRIBE.FRUIT` .

     Ten pojedynczy profil również nadał USER1 dostęp do subskrybowania produktu `"Price/Fruit/Oranges"` `"Price/Fruit/#"` , a ten dostęp pozostaje nawet z dodaniem nowego obiektu tematu i powiązanych z nim profili.

     Przyznaj dostęp do produktu USER2 , aby zasubskrybować temat `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do profilu produktu `hlq.SUBSCRIBE.APPLE` . W tym celu należy użyć następujących komend produktu RACF :

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
     PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
     ```

   - 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:

ULW **Windows, UNIX and Linux**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

IBM i **IBM i**

```
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*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:

- z/OS W systemie z/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Na platformach Windows, platformy UNIX and Linux , następujące zdarzenie autoryzacji:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

- IBM i W systemie IBMi, 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

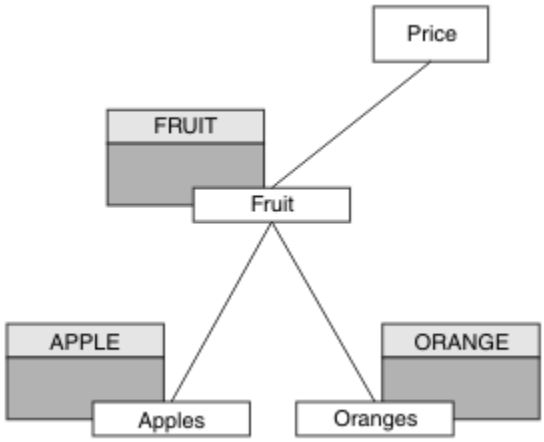
Ten temat jest czwartym z listy zadań, które informują użytkownika o sposobach nadawania dostępu do subskrybowania tematów przez więcej niż jednego użytkownika oraz w celu uniknięcia dodatkowych komunikatów programu RACF ICH408I w systemie z/OS.

Zanim rozpoczniesz

W tym temacie rozszerzono konfigurację opisaną w sekcji “Nadaj innemu użytkownikowi dostęp, aby zasubskrybować tylko temat głębiej w obrębie drzewa.” na stronie 491 , tak aby 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 26. 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:
   - z/OS **z/OS** :

     Zdefiniuj nowy profil i dodaj dostęp do tego profilu, a także istniejące profile. W tym celu należy użyć następujących komend produktu RACF :

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.ORANGE UACC(NONE)
     PERMIT hlq.SUBSCRIBE.ORANGE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     PERMIT hlq.SUBSCRIBE.APPLE CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - Inne platformy:

     Skonfiguruj równorzędny dostęp za pomocą komend autoryzacji dla platformy:

ULW **Windows, UNIX and Linux**

```
setmqaut -t topic -n ORANGE -p USER1 +sub
setmqaut -t topic -n APPLE -p USER1 +sub
```

IBM i **IBM i**

```
GRTMQAUT OBJ(ORANGE) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER1) AUT(*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:

- z/OS W systemie z/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ULW 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"
```

- IBM i W systemie IBMi, następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

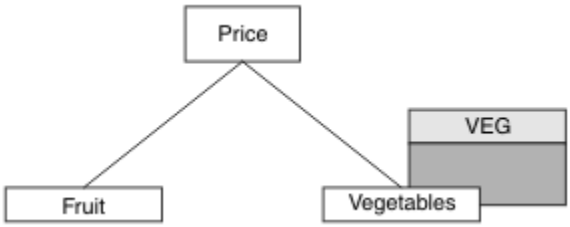
Przyznaj użytkownikowi prawa dostępu do publikowania w temacie

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 27. Nadawanie dostępu publikowania do tematu

Tabela 85. 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:

   - z/OS **z/OS** :

     Nadaj dostęp do produktu USER1 , aby opublikować go w temacie `"Price/Vegetables"` , nadając użytkownikowi dostęp do profilu produktu `hlq.PUBLISH.VEG` . W tym celu należy użyć następujących komend produktu RACF :

     ```
     RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
     PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
     ```

   - 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:

     ULW **Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n VEG -p USER1 +pub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*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:

- z/OS W systemie z/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ULW Na innych platformach następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

- IBM i W systemie IBMi, 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

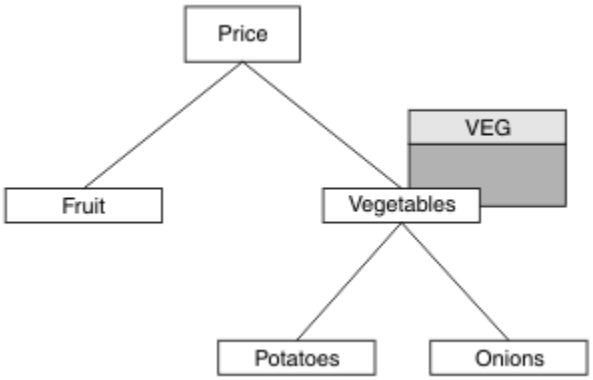
Ten temat jest drugi na liście zadań, które informują o sposobach nadawania dostępu do publikowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Przyznaj użytkownikowi prawa dostępu do publikowania w temacie” na stronie 495.

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 28. Nadawanie dostępu publikowania do tematu w drzewie tematów

Tabela 86. 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 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/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają 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 takie same jak te, które zostały odebrane w poprzednim zadaniu, ponieważ te same obiekty tematów i profile mają kontrolę nad dostępem.
- 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

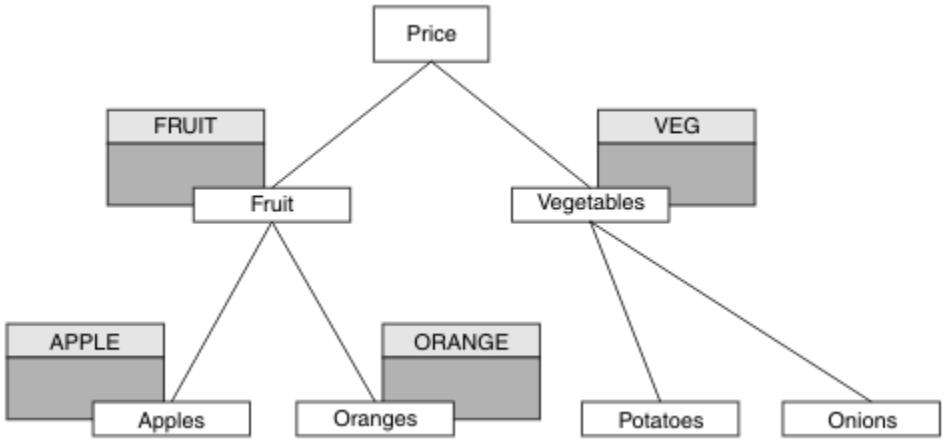
Ten temat jest ostatnim z listy zadań, które informują użytkownika o sposobach nadawania dostępu do publikowania i subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie opisano konfigurację opisaną w sekcji “Przyznaj użytkownikowi dostęp do tematu w celu głębszego publikowania tematu w drzewie” na stronie 497.

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 29. Nadawanie dostępu do publikowania i subskrybowania

Tabela 87. 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:

- z/OS **z/OS** :

  We wcześniejszym zadaniu USER1 uzyskano dostęp do subskrypcji tematu `"Price/Fruit"` , nadając użytkownikowi dostęp do profilu `hlq.SUBSCRIBE.FRUIT` .

  Aby opublikować temat w `"Price/Fruit"` , należy nadać uprawnienia dostępu do produktu USER1 do profilu produktu `hlq.PUBLISH.FRUIT` . W tym celu należy użyć następujących komend produktu RACF :

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
  PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- 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:

  ULW **Windows, UNIX and Linux**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
  ```

Wyniki

W systemie z/OS, gdy program USER1 próbuje publikować w temacie `"Price/Fruit"` , sprawdzanie 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:

- z/OS W systemie z/OSwyświetlane są następujące komunikaty wyświetlane na konsoli, które zawierają pełną ścieżkę zabezpieczeń przy użyciu drzewa tematów, które próbowano wykonać:

  ```
  ICH408I USER(USER2   ) ...
    hlq.PUBLISH.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
  ```

- ULW Na platformach Windows, UNIXi Linux następujące zdarzenie autoryzacji:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit"
  ```

- IBM i W systemie IBMi, 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 88. 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 w dzienniku konsoli produktu z/OS nie są wyświetlane żadne dodatkowe ostrzeżenia dotyczące zabezpieczeń. 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 89. 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.

Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek

Komunikaty wewnętrzne publikowania/subskrybowania, takie jak subskrypcje proxy i publikacje, są umieszczane w kolejkach systemowych publikowania/subskrypcji przy użyciu normalnych reguł zabezpieczeń kanału. Informacje i diagramy w tym temacie wyróżniają różne procesy i identyfikatory użytkowników związane z dostarczaniem tych komunikatów.

Lokalna kontrola dostępu

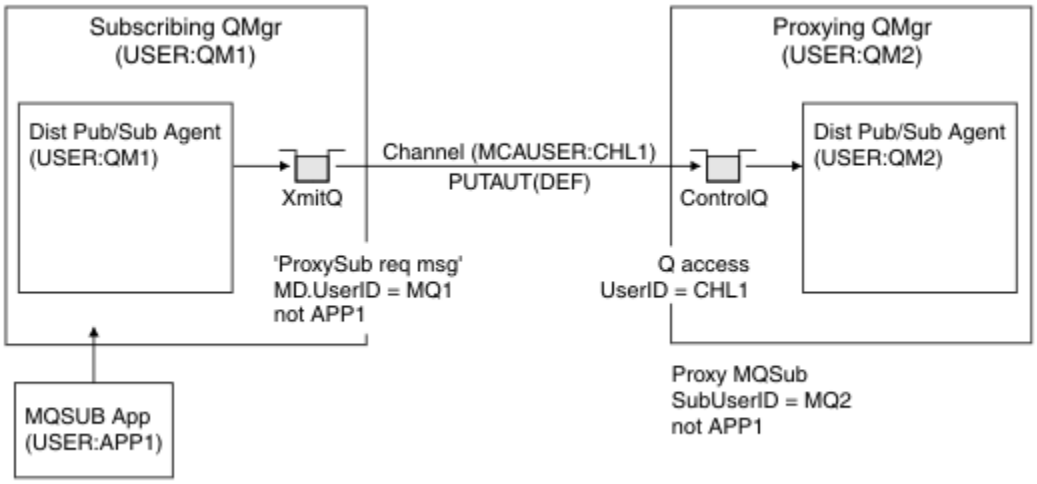
Dostęp do tematów dotyczących publikacji i subskrypcji jest określany przez lokalne definicje zabezpieczeń i reguły, które są opisane w sekcji Zabezpieczenia publikowania/subskrypcji. W systemie z/OSdo ustanowienia kontroli dostępu nie jest wymagany żaden lokalny obiekt tematu. Do kontroli dostępu na innych platformach nie jest wymagany żaden temat lokalny. Administratorzy mogą zdecydować się na zastosowanie kontroli dostępu do obiektów tematu w klastrze, niezależnie od tego, czy istnieją jeszcze w klastrze.

Administratorzy systemu są odpowiedzialni za kontrolę dostępu w ich systemie lokalnym. Muszą oni ufać administratorom innych członków hierarchii lub kolektywów klastra, aby byli odpowiedzialni za ich strategię kontroli dostępu. Ponieważ kontrola dostępu jest zdefiniowana dla każdej odrębnej maszyny, może być ona uciążana, jeśli wymagana jest kontrola poziomu precyzyjnego. Może nie być konieczne narzucenie kontroli dostępu lub dostęp do kontroli dostępu w obiektach wysokiego poziomu w drzewie tematów. Kontrola dostępu na poziomie fine może być zdefiniowana dla każdego podobszaru przestrzeni nazw tematów.

Tworzenie subskrypcji proxy

Zaufanie do organizacji w celu połączenia jego menedżera kolejek z menedżerem kolejek jest potwierdzane za pomocą zwykłych metod uwierzytelniania kanału. Jeśli ta zaufana organizacja jest również dopuszczona do rozproszonego publikowania/subskrybowania, sprawdzanie uprawnień jest wykonywane. Sprawdzenie jest wykonywane, gdy kanał umieszcza komunikat w rozproszonej kolejce publikowania/subskrypcji. Na przykład, jeśli komunikat jest umieszczany w kolejce `SYSTEM.INTER.QMGR.CONTROL` . Identyfikator użytkownika dla sprawdzania uprawnień do kolejki zależy od wartości PUTAUT kanału odbierającego. Na przykład: ID użytkownika kanału, `MCAUSER`, kontekst komunikatu, w zależności od wartości i platformy. Więcej informacji na temat bezpieczeństwa kanału znajduje się w sekcji Zabezpieczenia kanału.

Subskrypcje proxy są wykonywane przy użyciu identyfikatora użytkownika rozproszonego agenta publikowania/subskrypcji w zdalnym menedżerze kolejek. Na przykład: `QM2` w Rysunek 30 na stronie 504. Użytkownik może wówczas łatwo uzyskać dostęp do lokalnych profili obiektów tematu, ponieważ ten identyfikator użytkownika jest zdefiniowany w systemie i dlatego nie ma konfliktów domen.



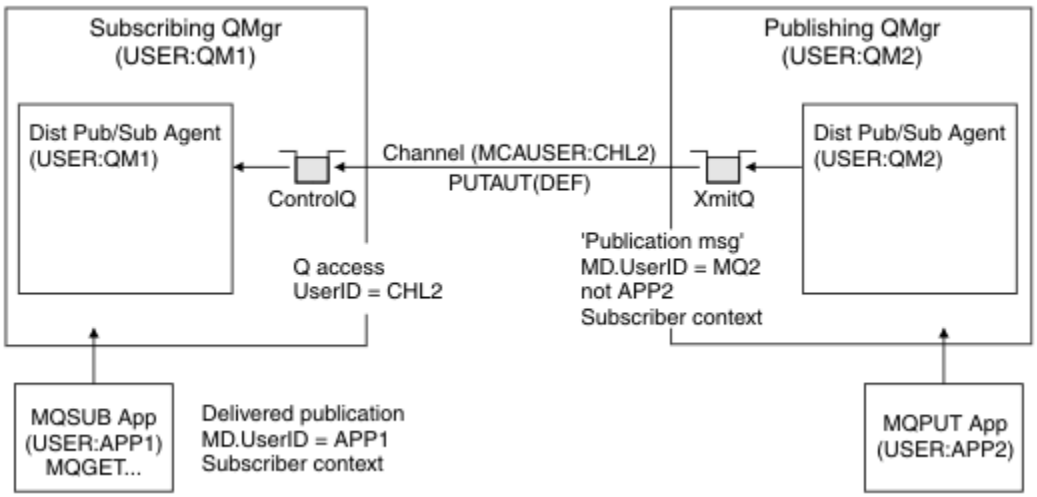
Rysunek 30. Zabezpieczenia subskrypcji proxy, subskrypcja

Wysyłanie zdalnych publikacji

Po utworzeniu publikacji w menedżerze kolejek publikowania tworzona jest kopia publikacji dla dowolnej subskrypcji proxy. Kontekst skopiowanej publikacji zawiera kontekst identyfikatora użytkownika, który dokonał subskrypcji; QM2 w produkcie Rysunek 31 na stronie 504. Subskrypcja proxy jest tworzona z kolejką docelową, która jest kolejką zdalną, a więc komunikat publikacji jest rozstrzygany w kolejce transmisji.

Zaufanie do organizacji w celu połączenia jego menedżera kolejek QM2z innym menedżerem kolejek, QM1, jest potwierdzane za pomocą zwykłych metod uwierzytelniania kanału. Jeśli ta zaufana organizacja jest wtedy dozwolona dla rozproszonego publikowania/subskrybowania, to sprawdzanie uprawnień jest wykonywane, gdy kanał umieszcza komunikat publikacji w rozproszonej kolejce publikowania/subskrypcji SYSTEM.INTER.QMGR.PUBS. ID użytkownika dla sprawdzania uprawnień do kolejki zależy od wartości PUTAUT kanału odbierającego (na przykład identyfikator użytkownika kanału, MCAUSER, kontekst komunikatu i inne, w zależności od wartości i platformy). Więcej informacji na temat bezpieczeństwa kanału znajduje się w sekcji Zabezpieczenia kanału.

Gdy komunikat publikacji dociera do menedżera kolejek subskrybujących, inna operacja MQPUT dla tego tematu jest wykonywana z uprawnieniami tego menedżera kolejek, a kontekst z komunikatem jest zastępowany przez kontekst każdego subskrybentów lokalnych, ponieważ każdy z nich otrzymuje ten komunikat.



Rysunek 31. Zabezpieczenia subskrypcji proxy, przekazywanie publikacji

W systemie, w którym niewiele zostało rozważone na temat bezpieczeństwa, procesy rozproszonego publikowania/subskrypcji mogą działać pod identyfikatorem użytkownika w grupie `mqm` , parametr `MCAUSER` w kanale jest pusty (domyślnie), a komunikaty są dostarczane do różnych kolejek systemowych zgodnie z wymaganiami. Niezabezpieczony system ułatwia ustawienie dowodu na to, aby zademonstrować rozproszoną publikacji/subskrybowanie.

W systemie, w którym zabezpieczenia są bardziej poważnie brane pod uwagę, te komunikaty wewnętrzne podlegają tym samym kontrolom zabezpieczeń, co każdy komunikat przechodnie przez kanał.

Jeśli kanał jest skonfigurowany z niepustym parametrem `MCAUSER` i wartością parametru `PUTAUT` , która określa, że parametr `MCAUSER` musi zostać sprawdzony, to należy nadać użytkownikowi `MCAUSER` dostęp do kolejek produktu `SYSTEM.INTER.QMGR.*` . Jeśli istnieje wiele różnych zdalnych menedżerów kolejek, z kanałami działaniającymi pod różnymi identyfikatorami `MCAUSER` , wszystkie te identyfikatory użytkowników muszą mieć dostęp do kolejek produktu `SYSTEM.INTER.QMGR.*` . Kanały działające pod różnymi identyfikatorami `MCAUSER` mogą wystąpić na przykład wtedy, gdy wiele połączeń hierarchicznych jest skonfigurowanych w jednym menedżerze kolejek.

Jeśli kanał jest skonfigurowany z wartością `PUTAUT` , która określa, że używany jest kontekst komunikatu, to dostęp do kolejek produktu `SYSTEM.INTER.QMGR.*` jest sprawdzany na podstawie identyfikatora użytkownika wewnątrz komunikatu wewnętrznego. Ponieważ wszystkie te komunikaty są umieszczane za pomocą ID użytkownika agenta rozproszonego publikowania/subskrypcji z menedżera kolejek, który wysyła komunikat wewnętrzny, lub komunikat publikacji (patrz Rysunek 31 na stronie 504), nie jest zbyt duży zestaw identyfikatorów użytkowników, aby nadać dostęp do różnych kolejek systemowych (jeden dla każdego menedżera kolejek zdalnych), jeśli w ten sposób mają zostać skonfigurowane rozproszone zabezpieczenia publikowania/subskrypcji. Nadal ma on wszystkie te same problemy, które zawsze mają zabezpieczenia kontekstu kanału, a także różne domeny identyfikatorów użytkowników oraz fakt, że identyfikator użytkownika w komunikacie nie został zdefiniowany w systemie odbierającym. Jest to jednak w pełni akceptowalny sposób uruchomienia, jeśli jest to wymagane.

z/OS Opcja Zabezpieczenia kolejki systemowej udostępnia listę kolejek oraz dostęp, który jest wymagany do bezpiecznego skonfigurowania rozproszonego środowiska publikowania/subskrybowania. Jeśli komunikaty wewnętrzne lub publikacje nie powiodą się z powodu naruszeń bezpieczeństwa, kanał zapisuje komunikat w dzienniku w normalny sposób, a komunikaty mogą być wysyłane do kolejki niedostarczonych komunikatów zgodnie z normalnym przetwarzaniem błędów kanału.

Wszystkie komunikaty menedżera kolejek między kolejkami w celu rozproszonego działania publikowania/subskrypcji korzystają z normalnego bezpieczeństwa kanału.

Więcej informacji na temat ograniczania publikacji i subskrypcji proxy na poziomie tematu zawiera sekcja Zabezpieczenia publikowania/subskrypcji.

Korzystanie z domyślnych identyfikatorów użytkowników z hierarchią menedżera kolejek

Jeśli hierarchia menedżerów kolejek jest uruchomiona na różnych platformach i korzysta z domyślnych identyfikatorów użytkowników, należy pamiętać, że te domyślne identyfikatory użytkowników różnią się między platformami i mogą nie być znane na platformie docelowej. W wyniku tego menedżer kolejek działający na jednej platformie odrzuca komunikaty odebrane z menedżerów kolejek na innych platformach z kodem przyczyny `MQRC_NOT_AUTHORIZED`.

Aby uniknąć odrzucenia komunikatów, należy dodać przynajmniej następujące uprawnienia do domyślnych identyfikatorów użytkowników, które są używane na innych platformach:

- *PUT uprawnienia *GET w systemie SYSTEM.BROKER. kolejki
- *PUB *SUB (uprawnienia SUB) w systemie SYSTEM.BROKER. tematy
- *ADMCRT Uprawnienie *ADMDLT *ADMCHG w systemie SYSTEM.BROKER.CONTROL.QUEUE .

Domyślne identyfikatory użytkowników z hierarchią menedżera kolejek są następujące:

Platforma	Domyślny identyfikator użytkownika
Windows	MUSR_MQADMIN
Systemy UNIX and Linux	mqm
IBM i	QMQM
z/OS	Identyfikator użytkownika przestrzeni adresowej inicjatora kanału

Utwórz i przyznaj dostęp do identyfikatora użytkownika 'qmqm', jeśli jest on hierarchicznie przyłączony do menedżera kolejek w produkcie IBM i dla menedżerów kolejek na platformach Windows, UNIX, Linuxi z/OS .

Utwórz i przyznaj dostęp do identyfikatora użytkownika 'mqm', jeśli jest on hierarchicznie przyłączony do menedżera kolejek w systemach Windows, UNIXlub Linux dla menedżerów kolejek na platformach IBM i i z/OS .

Utwórz i przyznaj dostęp użytkownika do identyfikatora użytkownika przestrzeni adresowej inicjatora kanału produktu z/OS , jeśli jest on hierarchicznie przyłączony do menedżera kolejek w produkcie z/OS dla menedżerów kolejek na platformach Windows, UNIX, Linuxi IBM i .

W identyfikatorach użytkowników może być rozróżniana wielkość liter. Inicjujący menedżer kolejek (w przypadku systemów IBM i, Windows, UNIXlub Linux) wymusza, aby ID użytkownika był zapisany wielkimi literami. Odbierający menedżer kolejek (w przypadku systemów Windows, UNIX lub Linux) wymusza na ID użytkownika wszystkie małe litery. Z tego powodu wszystkie identyfikatory użytkowników utworzone w systemach UNIX and Linux muszą być utworzone w postaci małych liter. Jeśli został zainstalowany program obsługi wyjścia komunikatów, wymuszenie nazwy ID użytkownika na wielkie lub małe litery nie jest możliwe. Należy zwrócić uwagę na sposób, w jaki program obsługi wyjścia komunikatów przetwarza identyfikator użytkownika.

Aby uniknąć potencjalnych problemów z konwersją identyfikatorów użytkowników:

- W systemach UNIX, Linux, and Windows należy się upewnić, że identyfikatory użytkowników są określone małymi literami.
- W systemach IBM i i z/OSnależy się upewnić, że identyfikatory użytkowników są określone wielkimi literami.

V 9.1.0 Zabezpieczenia IBM MQ Console i REST API

Zabezpieczenia dla partycji IBM MQ Console i REST API są konfigurowane przez edycję konfiguracji serwera mqweb w pliku `mqwebuser.xml` .

O tym zadaniu

Użytkownik może śledzić działania użytkowników i kontrolować użycie IBM MQ Console i REST API , sprawdzając pliki dziennika serwera mqweb.

Użytkownicy partycji IBM MQ Console i REST API mogą być uwierzytelniani za pomocą następujących elementów:

- Rejestr podstawowy
- Rejestr LDAP
- Rejestr lokalnego systemu operacyjnego
- SAF w systemie z/OS
- Dowolny inny typ rejestru obsługiwany przez produkt WebSphere Liberty

Role mogą być przypisywane do użytkowników programu IBM MQ Console oraz do użytkowników produktu REST API w celu określenia poziomu dostępu, którym nadano dostęp do obiektów produktu IBM MQ . Aby na przykład wykonać przesyłanie komunikatów, użytkownicy muszą mieć przypisaną rolę

`MQWebUser` . Więcej informacji na temat dostępnych ról zawiera sekcja "Role w serwerach IBM MQ Console i REST API" na stronie 518.

Po przypisaniu użytkownika do roli, istnieje pewna liczba metod, których można użyć do uwierzytelnienia użytkownika. Za pomocą programu IBM MQ Consoleużytkownicy mogą logować się przy użyciu nazwy użytkownika i hasła lub mogą korzystać z uwierzytelniania za pomocą certyfikatu klienta. W przypadku produktu REST APIużytkownicy mogą korzystać z podstawowego uwierzytelniania HTTP, uwierzytelniania opartego na tokenie lub uwierzytelniania certyfikatu klienta.

Procedura

1. Zdefiniuj rejestr użytkowników w celu uwierzytelniania użytkowników i przypisz każdemu użytkownikowi lub grupie rolę, aby autoryzować użytkowników i grupy do korzystania z produktu IBM MQ Console lub REST API. Więcej informacji: "Konfigurowanie użytkowników i ról" na stronie 508
2. Wybierz sposób uwierzytelniania użytkowników produktu IBM MQ Console na serwerze mqweb. Nie ma potrzeby używania tej samej metody dla wszystkich użytkowników:
   - Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować czas utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
   - Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja "Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console" na stronie 520.
3. Wybierz sposób uwierzytelniania użytkowników produktu REST API na serwerze mqweb. Nie ma potrzeby używania tej samej metody dla wszystkich użytkowników:
   - Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja "Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API" na stronie 524.
   - Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja "Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API" na stronie 525.

     Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Jeśli jednak włączono połączenia HTTP, można zezwolić na użycie znacznika LTPA dla połączenia HTTPS, który ma być używany dla połączenia HTTP. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
   - Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja "Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console" na stronie 520.
4. Opcjonalne: Skonfiguruj opcję Cross Origin Resource Sharing dla REST API.

   Domyślnie przeglądarka WWW nie zezwala na wywoływanie REST API , takich jak JavaScript, w przypadku, gdy skrypt nie pochodzi z tego samego miejsca, co REST API. Oznacza to, że żądania o różnych pochodzeniu nie są włączone. Istnieje możliwość skonfigurowania funkcji CORS (Cross

Origin Resource Sharing) w taki sposób, aby zezwalać na żądania między pochodzeniem z określonych adresów URL. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie architektury CORS dla REST API” na stronie 528.

5. Opcjonalne: Skonfiguruj sprawdzanie poprawności nagłówka hosta dla produktów IBM MQ Console i REST API.

   Można skonfigurować sprawdzanie poprawności nagłówka hosta i utworzyć listę dozwolonych nazw hostów i portów, aby upewnić się, że tylko żądania zawierające konkretne nagłówki hosta są przetwarzane przez produkty IBM MQ Console i REST API. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie sprawdzania poprawności nagłówka hosta dla produktów IBM MQ Console i REST API” na stronie 529.

V 9.1.0 Konfigurowanie użytkowników i ról

Aby korzystać z produktu IBM MQ Console lub REST API, użytkownicy muszą uwierzytelniać się w rejestrze użytkowników zdefiniowanym na serwerze mqweb.

O tym zadaniu

Uwierzytelnieni użytkownicy muszą należeć do jednej z grup, która autoryzuje dostęp do możliwości produktów IBM MQ Console i REST API. Domyślnie rejestr użytkowników nie zawiera żadnych użytkowników. Te potrzeby należy dodać, edytując plik `mqwebuser.xml` .

Konfigurując użytkowników i grupy, należy najpierw skonfigurować rejestr użytkowników w celu uwierzytelnienia użytkowników i grup. Ten rejestr użytkowników jest współużytkowany przez IBM MQ Console i REST API. Podczas konfigurowania ról dla użytkowników i grup można określić, czy użytkownicy i grupy mają dostęp do serwera IBM MQ Console, REST APIlub obu tych grup.

Po skonfigurowaniu rejestru użytkowników należy skonfigurować role dla użytkowników i grup w celu nadania im autoryzacji. Dostępnych jest kilka ról, w tym role specyficzne dla korzystania z REST API dla Managed File Transfer. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

Wraz z serwerem mqweb udostępniono wiele przykładowych plików XML, aby ułatwić konfigurację użytkowników i grup. Użytkownicy, którzy są zaznajomiani ze skonfigurowaniem zabezpieczeń w produkcie WebSphere Liberty (WLP), mogą preferować nie używanie przykładów. Program WLP udostępnia inne możliwości autoryzacji oprócz tych, które zostały tutaj udokumentowane.

Procedura

- Skonfiguruj użytkowników i grupy z podstawowym rejestrem przy użyciu pliku `basic_registry.xml` .

  Nazwy użytkowników i hasła w rejestrze są używane do uwierzytelniania i autoryzowania użytkowników IBM MQ Console i REST API.

  Aby skonfigurować rejestr podstawowy za pomocą przykładowego pliku `basic_registry.xml` , należy zapoznać się z “Konfigurowanie rejestru podstawowego dla produktów IBM MQ Console i REST API” na stronie 510.

- Skonfiguruj użytkowników i grupy z rejestrem LDAP przy użyciu pliku `ldap_registry.xml` .

  Nazwy użytkowników i hasła w rejestrze LDAP są używane do uwierzytelniania i autoryzacji korzystania z IBM MQ Console i REST API.

  Informacje na temat konfigurowania rejestru LDAP za pomocą przykładowego pliku `ldap_registry.xml` zawiera sekcja “Konfigurowanie rejestru LDAP dla serwerów IBM MQ Console i REST API” na stronie 514.

- ULW

  Skonfiguruj użytkowników i grupy z lokalnym rejestrem systemu operacyjnego za pomocą pliku `local_os_registry.xml` .

Nazwy użytkowników i hasła w rejestrze systemu operacyjnego są używane do uwierzytelniania i autoryzacji użytkowników produktów IBM MQ Console i REST API.

Informacje na temat konfigurowania lokalnego rejestru systemu operacyjnego za pomocą przykładowego pliku `local_os_registry.xml` zawiera sekcja "Konfigurowanie lokalnego rejestru systemu operacyjnego dla serwerów IBM MQ Console i REST API" na stronie 512.

- z/OS

  Skonfiguruj użytkowników i grupy za pomocą interfejsu SAF (System authorization facility) w systemie z/OS , korzystając z pliku `zos_saf_registry.xml` .

  Produkt RACF lub inny produkt zabezpieczeń, profile są używane do nadawania użytkownikom i grupom dostępu do ról. Nazwy użytkowników i hasła w bazie danych RACF są używane do uwierzytelniania i autoryzowania użytkowników produktów IBM MQ Console i REST API.

  Informacje na temat konfigurowania interfejsu SAF przy użyciu przykładowego pliku `zos_saf_registry.xml` zawiera sekcja "Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API" na stronie 516.
- Wyłącz zabezpieczenia, w tym możliwość uzyskiwania dostępu do produktu IBM MQ Console, lub REST APIprzy użyciu protokołu HTTPS, za pomocą pliku `no_security.xml` .

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować przedział czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja "Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console" na stronie 520.

REST API Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja "Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API" na stronie 524.
- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja "Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API" na stronie 525. Istnieje możliwość skonfigurowania przedziału czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja "Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console" na stronie 520.

V 9.1.0 Konfigurowanie rejestru podstawowego dla produktów IBM MQ Console i REST API

Istnieje możliwość skonfigurowania podstawowego rejestru w pliku `mqwebuser.xml` . Nazwy użytkowników, hasła i role w pliku XML są używane do uwierzytelniania i autoryzowania użytkowników produktów IBM MQ Console i REST API.

Zanim rozpoczniesz

- Podczas konfigurowania użytkowników w podstawowym rejestrze konieczne jest przypisanie każdego użytkownika roli. Każda rola udostępnia różne poziomy uprawnień dostępu do produktów IBM MQ Console i REST APIoraz określa kontekst zabezpieczeń, który jest używany w przypadku próby wykonania dozwolonej operacji. Przed skonfiguroniem podstawowego rejestru należy zapoznać się z tymi rolami. Więcej informacji na temat każdej z ról zawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.
- Aby wykonać tę czynność, należy być użytkownikiem z odpowiednimi uprawnieniami do edycji pliku `mqwebuser.xml` :
  - z/OS W systemie z/OSużytkownik musi mieć prawo do zapisu w pliku `mqwebuser.xml` .
  - Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.

Procedura

1. Skopiuj przykładowy plik XML `basic_registry.xml` z jednej z następujących ścieżek:
   - ULW W systemie UNIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS W systemie z/OS: `PathPrefix /web/mq/samp/configuration`

   gdzie `PathPrefix` jest ścieżką instalacyjną IBM MQ Unix System Services Components.
2. Umieść przykładowy plik w odpowiednim katalogu:
   - ULW

     W systemie UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     W systemie z/OS: *WLP_user_directory*`/servers/mqweb`

     gdzie *katalog_użytkownika_WLP_użytkownika* to katalog, który został określony podczas tworzenia skryptu produktu **crtmqweb** w celu utworzenia definicji serwera WWW mqweb.
3. Opcjonalne: Jeśli zmieniono jakiekolwiek ustawienia konfiguracyjne w programie `mqwebuser.xml`, skopiuj je do przykładowego pliku.
4. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę pliku przykładowego na `mqwebuser.xml`.
5. Edytuj nowy plik `mqwebuser.xml` , aby dodać użytkowników i grupy w obrębie znaczników produktu **basicRegistry** .

   Należy pamiętać, że każdy użytkownik pełniący rolę `MQWebUser` może wykonywać tylko operacje, które użytkownik ma nadane w celu wykonania na menedżerze kolejek. Oznacza to, że identyfikator użytkownika zdefiniowany w rejestrze musi mieć identyczny identyfikator użytkownika w systemie, w którym zainstalowano produkt IBM MQ . Te identyfikatory użytkowników muszą być w tym samym przypadku lub odwzorowania między identyfikatorami użytkowników mogą się nie powieść.

Więcej informacji na temat konfigurowania podstawowych rejestrów użytkowników znajduje się w sekcji Konfigurowanie podstawowego rejestru użytkowników dla serwera Liberty w dokumentacji produktu WebSphere Liberty .

6. Przypisz role do użytkowników i grup, edytując plik `mqwebuser.xml` :

   Dostępnych jest kilka ról, które autoryzują użytkowników i grupy do korzystania z produktu IBM MQ Consoleoraz produktu REST API. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

   - Aby przypisać role i nadać uprawnienia dostępu do produktu IBM MQ Console, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach produktu **<enterpriseApplication id="com.ibm.mq.console">** .
   - Aby przypisać role i nadać uprawnienia dostępu do produktu REST API, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach produktu **<enterpriseApplication id="com.ibm.mq.rest">** .

   Informacje na temat formatu informacji o użytkownikach i grupach w znacznikach **security-role** można znaleźć w przykładach.

7. Jeśli w produkcie `mqwebuser.xml`zostały podane hasła dla użytkowników, należy zakodować te hasła, aby były bardziej bezpieczne, za pomocą komendy **securityUtility encoding** udostępnianej przez produkt WebSphere Liberty. Więcej informacji na ten temat zawiera sekcja Komenda Liberty:securityUtility w dokumentacji produktu WebSphere Liberty .

Przykład

W poniższym przykładzie grupa `MQWebAdminGroup` ma nadany dostęp do IBM MQ Console z rolą `MQWebAdmin`. Użytkownik, `reader`, ma nadany dostęp z rolą `MQWebAdminRO`, a użytkownikowi `guest` nadano mu dostęp z rolą `MQWebUser`:

```
<enterpriseApplication id="com.ibm.mq.console">
        <application-bnd>
            <security-role name="MQWebAdmin">
                <group name="MQWebAdminGroup" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebAdminRO">
                <user name="reader" realm="defaultRealm"/>
            </security-role>
            <security-role name="MQWebUser">
                <user name="guest" realm="defaultRealm"/>
            </security-role>
        </application-bnd>
    </enterpriseApplication>
```

W poniższym przykładzie użytkownicy `reader` i `guest` uzyskują dostęp do IBM MQ Console. Użytkownikowi `user` jest nadawany dostęp do REST API, a wszyscy użytkownicy z grupy `MQAdmin` uzyskują dostęp do IBM MQ Console i REST API. Użytkownik produktu `mftadmin` ma nadany dostęp do REST API dla MFT :

```
<enterpriseApplication id="com.ibm.mq.console">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebAdminRO">
            <user name="reader" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="guest" realm="defaultRealm"/>
        </security-role>
    </application-bnd>
</enterpriseApplication>

<enterpriseApplication id="com.ibm.mq.rest">
    <application-bnd>
        <security-role name="MQWebAdmin">
            <group name="MQAdmin" realm="defaultRealm"/>
        </security-role>
        <security-role name="MQWebUser">
            <user name="user" realm="defaultRealm"/>
```

```
        </security-role>
        <security-role name="MFTWebAdmin">
            <user name="mftadmin" realm="defaultRealm"/>
        </security-role>
    </application-bnd>
</enterpriseApplication>
```

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować przedział czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

REST API Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API” na stronie 524.
- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API” na stronie 525. Istnieje możliwość skonfigurowania przedziału czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

ULW V 9.1.0 Konfigurowanie lokalnego rejestru systemu operacyjnego dla serwerów IBM MQ Console i REST API

Rejestr lokalnego systemu operacyjnego można skonfigurować w pliku `mqwebuser.xml` . Nazwy użytkowników i hasła w lokalnym systemie operacyjnym są używane do uwierzytelniania i autoryzacji użytkowników produktów IBM MQ Console i REST API.

Zanim rozpoczniesz

- W przypadku uwierzytelniania przy użyciu certyfikatu klienta z funkcją uwierzytelniania lokalnego systemu operacyjnego tożsamość użytkownika jest nazwą zwykłą (CN) z nazwy wyróżniającej (DN) certyfikatu klienta. Jeśli tożsamość użytkownika nie istnieje jako użytkownik systemu operacyjnego,

logowanie do certyfikatu klienta nie powiedzie się i zostanie ponownie uwierzytelnienie w oparciu o hasło.

- Aby wykonać tę czynność, użytkownik musi być użytkownikiem uprzywilejowanym.

O tym zadaniu

W rejestrze lokalnego systemu operacyjnego użytkownicy i grupy są automatycznie przypisani do roli:

- Każdy użytkownik należący do grupy mqm lub grupa 'QMQMADM' w systemie IBM ima nadane role MQWebAdmin i MFTWebAdmin .
- Wszystkim innym użytkownikom nadawana jest rola MQWebUser .

Więcej informacji na temat tych ról zawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

Rejestr lokalnego systemu operacyjnego może być używany tylko w systemie UNIX, Linux, and Windows. Równoważną funkcję można uzyskać w produkcie z/OS , konfigurując rejestr SAF. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API” na stronie 516.

Procedura

1. Skopiuj przykładowy plik XML `local_os_registry.xml` z następującej ścieżki:
   MQ_INSTALLATION_PATH`/web/mq/samp/configuration`
2. Umieść przykładowy plik w następującym katalogu:
   MQ_DATA_PATH`/web/installations/`*installationName*`/servers/mqweb`
3. Opcjonalne: Jeśli zmieniono jakiekolwiek ustawienia konfiguracyjne w programie `mqwebuser.xml`, skopiuj je do przykładowego pliku.
4. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę pliku przykładowego na `mqwebuser.xml`.

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować przedział czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

REST API Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API” na stronie 524.
- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą

metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API” na stronie 525. Istnieje możliwość skonfigurowania przedziału czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.

- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

V 9.1.0 Konfigurowanie rejestru LDAP dla serwerów IBM MQ Console i REST API

Rejestr LDAP można skonfigurować w pliku `mqwebuser.xml` . Nazwy użytkowników i hasła w rejestrze LDAP są używane do uwierzytelniania i autoryzowania użytkowników produktów IBM MQ Console i REST API.

Zanim rozpoczniesz

- Podczas konfigurowania rejestru LDAP należy przypisać każdemu użytkownikowi rolę. Każda rola udostępnia różne poziomy uprawnień dostępu do produktów IBM MQ Console i REST APIoraz określa kontekst zabezpieczeń, który jest używany w przypadku próby wykonania dozwolonej operacji. Przed skonfiguroniem rejestru należy zapoznać się z tymi rolami. Więcej informacji na temat każdej z ról zawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

  Należy pamiętać, że każdy użytkownik pełniący rolę `MQWebUser` może wykonywać tylko operacje, które użytkownik ma nadane w celu wykonania na menedżerze kolejek. Oznacza to, że identyfikator użytkownika zdefiniowany na serwerze LDAP musi mieć identyczny identyfikator użytkownika w systemie, w którym jest zainstalowany produkt IBM MQ . Te identyfikatory użytkowników muszą być w tym samym przypadku lub odwzorowania między identyfikatorami użytkowników mogą się nie powieść.
- Aby wykonać tę czynność, należy być użytkownikiem z odpowiednimi uprawnieniami do edycji pliku `mqwebuser.xml` :
  - z/OS W systemie z/OSużytkownik musi mieć prawo do zapisu w pliku `mqwebuser.xml` .
  - Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.

Procedura

1. Skopiuj przykładowy plik XML `ldap_registry.xml` z jednej z następujących ścieżek:
   - ULW W systemie UNIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS W systemie z/OS: `PathPrefix /web/mq/samp/configuration`

     gdzie `PathPrefix` jest ścieżką instalacyjną IBM MQ Unix System Services Components.
2. Umieść przykładowy plik w odpowiednim katalogu:
   - ULW

     W systemie UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

W systemie z/OS: *WLP_user_directory*/servers/mqweb

gdzie *katalog_użytkownika_WLP_użytkownika* to katalog, który został określony podczas tworzenia skryptu produktu **crtmqweb** w celu utworzenia definicji serwera WWW mqweb.

3. Opcjonalne: Jeśli zmieniono jakiekolwiek ustawienia konfiguracyjne w programie `mqwebuser.xml`, skopiuj je do przykładowego pliku.
4. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę pliku przykładowego na `mqwebuser.xml`.
5. Edytuj nowy plik `mqwebuser.xml` , aby zmienić ustawienia rejestru LDAP w znacznikach **ldapRegistry** i **idsLdapFilterProperties** .

   Więcej informacji na temat konfigurowania rejestrów LDAP zawiera sekcja Konfigurowanie rejestrów użytkowników LDAP w profilu Liberty w dokumentacji produktu WebSphere Liberty .
6. Przypisz role do użytkowników i grup, edytując plik `mqwebuser.xml` :

   Dostępnych jest kilka ról, które autoryzują użytkowników i grupy do korzystania z produktu IBM MQ Consoleoraz produktu REST API. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

   - Aby przypisać role i nadać uprawnienia dostępu do produktu IBM MQ Console, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach produktu **<enterpriseApplication id="com.ibm.mq.console">** .
   - Aby przypisać role i nadać uprawnienia dostępu do produktu REST API, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach produktu **<enterpriseApplication id="com.ibm.mq.rest">** .

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować przedział czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

REST API Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API” na stronie 524.
- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API” na stronie 525. Istnieje możliwość skonfigurowania przedziału czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.

- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

z/OS V 9.1.0 Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API

Interfejs SAF (System Authorization Facility) umożliwia serwerowi mqweb wywoływanie zewnętrznego menedżera zabezpieczeń w celu uwierzytelniania i sprawdzania autoryzacji. Następnie użytkownik może zalogować się do IBM MQ Console i REST API przy użyciu identyfikatora i hasła użytkownika z/OS .

Zanim rozpoczniesz

- Podczas konfigurowania rejestru SAF należy przypisać użytkownikom rolę. Każda rola udostępnia różne poziomy uprawnień dostępu do IBM MQ Console i REST APIoraz określa kontekst zabezpieczeń, który jest używany podczas próby wykonania dozwolonej operacji. Przed skonfigurowaniem rejestru należy zapoznać się z tymi rolami. Więcej informacji na temat każdej z ról zawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.
- Aby można było używać autoryzowanego interfejsu SAF, musi być uruchomiony proces Angel systemu WebSphere Liberty . Więcej informacji na ten temat zawiera sekcja Włączanie autoryzowanych usług systemu z/OS na serwerze Liberty for z/OS .
- Aby wykonać to zadanie, użytkownik musi mieć uprawnienia do zapisu w pliku `mqwebuser.xml` oraz uprawnienia do definiowania profili menedżera zabezpieczeń.

Uwaga: V 9.1.0.20 W produkcie IBM MQ 9.1.0 Fix Pack 20przykładowy plik konfiguracyjny `zos_saf_registry.xml` został zaktualizowany w celu usunięcia zduplikowanego wpisu safAuthorization .

Ta aktualizacja rozwiązuje problem polegający na tym, że może wystąpić błąd ICH408I , gdy produkt MQ Console w systemie z/OS jest aktualizowany do wersji WebSphere Liberty Profile 22.0.0.12 lub nowszej: czyli z wersji IBM MQ 9.1.0 Fix Pack 15. Posiadanie więcej niż jednej instrukcji safAuthorization nie jest obsługiwane i może spowodować błąd ICH408I , gdy użytkownicy, którzy nie mają ról MQWebAdmin lub MQWebAdminRO w klasie EBJROLE, próbują uzyskać dostęp do menedżera kolejek z/OS za pośrednictwem MQ Console.

Wartością domyślną dla **racRouteLog**, która określa typy prób dostępu do dziennika, jest NONE(BRAK). Jeśli wymagany jest dodatkowy raport lub rekord na potrzeby kontroli zabezpieczeń, więcej informacji na ten temat zawiera sekcja Autoryzacja SAF (safAuthorization) .

O tym zadaniu

Interfejs SAF umożliwia serwerowi mqweb wywoływanie zewnętrznego menedżera zabezpieczeń w celu uwierzytelniania i sprawdzania autoryzacji zarówno w przypadku serwera IBM MQ Console , jak i serwera REST API.

Procedura

1. Wykonaj kroki opisane w sekcji Włączanie autoryzowanych usług systemu z/OS na serwerze Liberty for z/OS , aby umożliwić serwerowi mqweb dostęp do używania autoryzowanych usług systemu z/OS .

   Przykładowy kod JCL służący do uruchamiania procesu Angel znajduje się w katalogu USS_ROOT/`web/templates/zos/procs/bbgzangl.jcl`, gdzie USS_ROOT to ścieżka w usługach systemu Unix, w której zainstalowano komponenty USS IBM MQ for z/OS .

   W pliku `bbgzangl.jcl`zmień instrukcję SET ROOT, aby wskazywała na USS_ROOT/`web`, na przykład `/usr/lpp/mqm/V9R1M0/web`.

Więcej informacji na temat zatrzymywania i uruchamiania procesu Angel zawiera sekcja Administrowanie serwerem Liberty w systemie z/OS .

2. Wykonaj kroki opisane w sekcji Liberty: konfigurowanie nieuwierzytelnionego użytkownika SAF (System Authorization Facility) , aby utworzyć nieuwierzytelnionego użytkownika wymaganego przez produkt Liberty.
3. Skopiuj plik `zos_saf_registry.xml` z następującej ścieżki: `PathPrefix /web/mq/samp/configuration` , gdzie `PathPrefix` jest ścieżką instalacyjną komponentów usług systemu IBM MQ Unix.
4. Umieść plik przykładowy w katalogu *`WLP_user_directory`*`/servers/mqweb` , gdzie *katalog_użytkownika_WLP* to katalog, który został określony podczas wykonywania skryptu **crtmqweb** w celu utworzenia definicji serwera mqweb.
5. Opcjonalne: Jeśli wcześniej zmieniono jakiekolwiek ustawienia konfiguracyjne w pliku `mqwebuser.xml`, skopiuj je do pliku przykładowego.
6. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę przykładowego pliku na `mqwebuser.xml`.
7. Dostosuj element **safCredentials** w pliku `mqwebuser.xml`.
   a. Jako wartość parametru **profilePrefix** ustaw nazwę unikalną dla serwera Liberty. Jeśli w jednym systemie działa więcej niż jeden serwer mqweb, należy wybrać inną nazwę dla każdego serwera, na przykład MQWEB910 i MQWEB905.
   b. Ustaw wartość **unauthenticatedUser** na nazwę nieuwierzytelnionego użytkownika utworzonego w kroku “2” na stronie 517.
8. Zdefiniuj identyfikator APPLID serwera mqweb w pliku RACF.

   Nazwa zasobu APPLID jest wartością podaną w atrybucie **profilePrefix** w kroku “7” na stronie 517. W poniższym przykładzie zdefiniowano identyfikator APPLID serwera mqweb w pliku RACF:

   ```
   RDEFINE APPL profilePrefix UACC(NONE)
   ```

9. Nadaj wszystkim użytkownikom lub grupom uprawnienia do uwierzytelniania na poziomie dostępu MQ Console lub REST API READ do identyfikatora APPLID serwera mqweb w klasie APPL.

   Należy to zrobić również dla nieuwierzytelnionego użytkownika zdefiniowanego w kroku “2” na stronie 517. W poniższym przykładzie nadawany jest użytkownikowi dostęp do odczytu (READ) do identyfikatora APPLID serwera mqweb w pliku RACF:

   ```
   PERMIT profilePrefix CLASS(APPL) ACCESS(READ) ID(userID)
   ```

10. Zdefiniuj profile w klasie EJBROLE potrzebne do nadania użytkownikom dostępu do ról w systemach MQ Console i REST API.

    W poniższym przykładzie zdefiniowano profile w pliku RACF, gdzie **profilePrefix** jest wartością określoną dla atrybutu **profilePrefix** w kroku “7” na stronie 517.

```
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdminRO UACC(NONE)
```

11. Nadaj użytkownikom dostęp do ról w MQ Console i REST API.

    W tym celu nadaj użytkownikom lub grupom prawo do odczytu jednego lub większej liczby profili w klasie EBJROLE utworzonej w kroku “10” na stronie 517. Więcej informacji na temat ról zawiera sekcja “Role w serwerach IBM MQ Console i REST API” na stronie 518.

    Poniższy przykład nadaje użytkownikowi dostęp do roli MQWebAdmin dla REST API w RACF, gdzie **profilePrefix** jest wartością określoną dla atrybutu **profilePrefix** w kroku “7” na stronie 517.

```
PERMIT profilePrefix.com.ibm.mq.rest.MQWebAdmin CLASS(EJBROLE) ACCESS(READ) ID(userID)
```

Wyniki

Skonfigurowano uwierzytelnianie SAF dla systemów IBM MQ Console i REST API.

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik wprowadza ID użytkownika i hasło w dzienniku IBM MQ Console na ekranie. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Do korzystania z tej opcji uwierzytelniania nie jest wymagana dalsza konfiguracja, ale opcjonalnie można skonfigurować przedział czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do IBM MQ Console, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

REST API Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą podstawowego uwierzytelniania HTTP. W takim przypadku nazwa użytkownika i hasło są kodowane, ale nie są szyfrowane i wysyłane wraz z każdym żądaniem REST API do uwierzytelniania i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy używać protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API” na stronie 524.
- Pozwól użytkownikom na uwierzytelnianie za pomocą uwierzytelniania za pomocą tokenu. W tym przypadku użytkownik udostępnia ID użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi pozostaw zalogowanie się i autoryzowanie przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API” na stronie 525. Istnieje możliwość skonfigurowania przedziału czasu utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Umożliwia użytkownikom uwierzytelnianie za pomocą certyfikatów klienta. W takim przypadku użytkownik nie korzysta z identyfikatora użytkownika ani hasła w celu zalogowania się do REST API, ale zamiast niego korzysta z certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console” na stronie 520.

V 9.1.0 Role w serwerach IBM MQ Console i REST API

Autoryzując użytkowników i grupy do korzystania z IBM MQ Console lub REST API, należy przypisać użytkowników i grupy jedną z dostępnych ról: **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin**i **MFTWebAdminRO**. Każda rola udostępnia różne poziomy uprawnień dostępu do produktów IBM MQ Console i REST APIoraz określa kontekst zabezpieczeń, który jest używany w przypadku próby wykonania dozwolonej operacji.

Uwaga: Z wyjątkiem roli **MQWebUser** , w identyfikatorze użytkownika nie jest rozróżniana wielkość liter. Konkretne wymagania dla tej roli można znaleźć w sekcji “MQWebUser” na stronie 519 .

MQWebAdmin

Użytkownik lub grupa, która jest przypisana do tej roli, może wykonywać wszystkie operacje administracyjne i działać w kontekście zabezpieczeń identyfikatora użytkownika systemu operacyjnego używanego do uruchamiania serwera mqweb.

Użytkownik lub grupa z tą rolą nie ma dostępu do następujących usług REST:

- REST API dla MFT. Aby można było korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MFTWebAdmin** lub **MFTWebAdminRO** .
- messaging REST API. Aby można było używać messaging REST API, użytkownik musi mieć przypisaną rolę **MQWebUser** .

MQWebAdminRO
Ta rola umożliwia dostęp tylko do odczytu do produktu IBM MQ Console lub REST API. Użytkownik lub grupa, która ma przypisaną tę rolę, może wykonywać następujące operacje:

- Wyświetlaj i zapytaj o operacje na obiektach IBM MQ , takich jak kolejki i kanały.
- Przeglądanie komunikatów w kolejkach.

Użytkownik lub grupa, do której przypisano tę rolę, działa w kontekście zabezpieczeń identyfikatora użytkownika systemu operacyjnego, który jest używany do uruchamiania serwera mqweb.

Użytkownik lub grupa z tą rolą nie ma dostępu do następujących usług REST:

- REST API dla MFT. Aby można było korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MFTWebAdmin** lub **MFTWebAdminRO** .
- messaging REST API. Aby można było używać messaging REST API, użytkownik musi mieć przypisaną rolę **MQWebUser** .

MQWebUser
Użytkownik lub grupa, do której przypisano tę rolę, może wykonać dowolną operację, która zostanie nadana temu identyfikatorowi użytkownika w menedżerze kolejek. Na przykład:

- Uruchamianie i zatrzymywanie operacji na obiektach IBM MQ , takich jak kanały.
- Definiowanie i ustawianie operacji na obiektach IBM MQ , takich jak kolejki i kanały.
- Wyświetlaj i zapytaj o operacje na obiektach IBM MQ , takich jak kolejki i kanały.
- Służy do umieszczania i pobierania komunikatów za pomocą messaging REST API.

Użytkownik lub grupa, która jest przypisana do tej roli, działa w kontekście zabezpieczeń nazwy użytkownika i może wykonywać tylko operacje, które dany ID użytkownika jest nadawany do wykonania w menedżerze kolejek.

Oznacza to, że użytkownik lub grupa zdefiniowana w rejestrze użytkowników produktu mqweb musi mieć uprawnienia w produkcie IBM MQ , zanim użytkownik ten będzie mógł wykonywać jakiekolwiek operacje. By using this role, you can finely control which users have which type of access to specific IBM MQ resources when they use the IBM MQ Console and REST API.

Uwaga:

- Maksymalna długość identyfikatora użytkownika, któremu przypisano tę rolę, wynosi 12 znaków.
- Wielkość liter w identyfikatorze użytkownika musi być taka sama w rejestrze użytkowników mqweb i w systemie IBM MQ . Jeśli przypadek identyfikatora użytkownika jest inny, użytkownik może być uwierzytelniany przez IBM MQ Console i REST API , ale nie ma uprawnień do korzystania z zasobów IBM MQ .

Użytkownik lub grupa z tą rolą nie ma dostępu do żadnej z usług produktu REST API for MFT .
Aby można było korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MFTWebAdmin** lub **MFTWebAdminRO** .

MFTWebAdmin
Użytkownik lub grupa przypisana do tej roli może wykonywać wszystkie operacje REST produktu MFT i działa w kontekście zabezpieczeń identyfikatora użytkownika systemu operacyjnego, który jest używany do uruchamiania serwera `mqweb` .

Użytkownik lub grupa z tą rolą nie ma dostępu do żadnej z usług IBM MQ REST API . Aby można było korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MQWebAdmin**, **MQWebAdminRO**lub **MQWebUser** .

MFTWebAdminRO
Ta rola zapewnia dostęp tylko do odczytu do REST API dla MFT . Użytkownik lub grupa, która jest przypisana do tej roli, może wykonywać operacje tylko do odczytu (żądania GET), takie jak lista operacji przesyłania list i lista agentów.

Użytkownik lub grupa, do której przypisano tę rolę, działa w kontekście zabezpieczeń identyfikatora użytkownika systemu operacyjnego, który jest używany do uruchamiania serwera mqweb.

Użytkownik lub grupa z tą rolą nie ma dostępu do żadnej z usług IBM MQ REST API . Aby można było korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MQWebAdmin**, **MQWebAdminRO**lub **MQWebUser** .

Więcej informacji na temat konfigurowania użytkowników i grup do korzystania z tych ról zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 508.

Nakładające się role

Użytkownik lub grupa może mieć przypisaną więcej niż jedną rolę. Gdy użytkownik wykonuje operację w tej sytuacji, używana jest najwyższa rola uprawnień, która ma zastosowanie do tej operacji. Na przykład, jeśli użytkownik o rolach **MQWebAdminRO** i **MQWebUser** wykonuje operację kolejki zapytań, używana jest rola **MQWebAdminRO** , a operacja jest podejmowana w kontekście identyfikatora użytkownika systemu, który uruchomił serwer WWW. Jeśli ten sam użytkownik wykona operację define, używana jest rola **MQWebUser** , a operacja jest wykonywana w kontekście nazwy użytkownika.

ULW V 9.1.0 Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta przy użyciu opcji REST API i IBM MQ Console

Certyfikaty klienta można odwzorowywać na nazwy użytkowników w celu uwierzytelniania użytkowników IBM MQ Console i REST API .

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do korzystania z produktów IBM MQ Console i REST API. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 508.
- Jeśli używany jest produkt REST API, można wysłać zapytanie do informacji autoryzacyjnych bieżącego użytkownika za pomocą metody HTTP GET w zasobie `login` , udostępniając certyfikat klienta w celu uwierzytelnienia żądania. To żądanie zwraca informacje o nazwie użytkownika i rolach, do których przypisany jest użytkownik. Więcej informacji na ten temat zawiera sekcja GET `/login`.
- Podczas odwzorowywania certyfikatów klienta na jednostki główne w celu uwierzytelniania użytkowników, nazwa wyróżniająca certyfikatu klienta jest używana do dopasowania się do użytkowników w skonfigurowanym rejestrze użytkowników:
  - W przypadku rejestru podstawowego nazwa zwykła (CN) jest zgodna z nazwą użytkownika. Na przykład `CN=Fred, O=IBM, C=GB` jest porównywany z nazwą użytkownika `Fred`.
  - W przypadku rejestru LDAP domyślnie pełna nazwa wyróżniająca jest dopasowana do katalogu LDAP. Istnieje możliwość skonfigurowania filtrów i odwzorowania w celu dostosowania dopasowania. Więcej informacji na ten temat zawiera sekcja Tryb odwzorowywania certyfikatów Liberty :LDAP w dokumentacji produktu WebSphere Liberty .

O tym zadaniu

Gdy użytkownik uwierzytelnia się przy użyciu certyfikatu klienta, certyfikat jest używany w miejsce nazwy użytkownika i hasła. W przypadku bazy danych REST APIcertyfikat klienta jest udostępniany z każdym żądaniem REST w celu uwierzytelnienia użytkownika. W przypadku IBM MQ Console, gdy użytkownik loguje się z certyfikatem, użytkownik nie może zostać wylogowany.

W procedurze przyjęto następujące informacje:

- Ten plik `mqwebuser.xml` jest oparty na jednej z następujących przykładów:

  - `basic_registry.xml`
  - `local_os_registry.xml`
  - `ldap_registry.xml`
- Używany jest system UNIX, Linuxlub Windows .
- Użytkownik jest użytkownikiem uprzywilejowanym.

Aby skonfigurować uwierzytelnianie za pomocą certyfikatu klienta za pomocą pliku kluczy RACF w systemie z/OS, należy wykonać procedurę w produkcie “Konfigurowanie protokołu TLS dla serwerów REST API i IBM MQ Console w systemie z/OS” na stronie 533.

Uwaga: W poniższej procedurze przedstawiono kroki niezbędne do korzystania z certyfikatów klienta w serwerach IBM MQ Console i REST API. Aby uzyskać wygodę dla programistów, należy szczegółowo określić sposób tworzenia i używania certyfikatów samopodpisanych. Jednak w przypadku produkcji należy używać certyfikatów, które są uzyskiwane z ośrodka certyfikacji.

Procedura

1. Uruchom serwer mqweb, wprowadzając komendę **strmqweb** w wierszu komend.
2. Utwórz certyfikat klienta:
   a) Utwórz magazyn kluczy PKCS#12 :
      i) Otwórz narzędzie IBM Key Management, wprowadzając komendę **strmqikm** w wierszu komend.
      ii) W menu **Key Database File** (Plik bazy danych kluczy) w narzędziu IBM Key Management kliknij opcję **New**(Nowy).
      iii) Wybierz opcję **PKCS12** z listy **Typ bazy danych kluczy** .
      iv) Wybierz miejsce, w którym ma zostać zapisany magazyn kluczy, a następnie wprowadź odpowiednią nazwę w polu **Nazwa pliku** . Na przykład: `user.p12`
      v) Po wyświetleniu zachęty ustaw hasło.
   b) Utwórz certyfikat, tworząc samopodpisany certyfikat, albo uzyskując certyfikat z ośrodka certyfikacji:
      - Utwórz certyfikat samopodpisany:
        i) Kliknij opcję **Nowy samopodpisany**.
        ii) Wpisz `user` w polu **Etykieta klucza** .
        iii) Jeśli używany jest podstawowy rejestr użytkowników, wprowadź nazwę użytkownika z rejestru użytkowników w polu **Nazwa zwykła** . Na przykład: `mqadmin`. W przypadku rejestru użytkowników LDAP należy upewnić się, że nazwa wyróżniająca certyfikatu jest zgodna z nazwą wyróżniającą w rejestrze LDAP.
        iv) Kliknij przycisk **OK**.
      - Uzyskaj certyfikat z ośrodka certyfikacji. Certyfikat ośrodka CA musi zawierać odpowiednią nazwę użytkownika w obrębie nazwy zwykłej (CN) pola nazwy wyróżniającej (DN):
        i) Zażądaj nowego certyfikatu. W menu **Utwórz** kliknij opcję **Nowe żądanie certyfikatu**.
        ii) W polu **Key Label** (Etykieta klucza) wprowadź etykietę certyfikatu.
        iii) Jeśli używany jest podstawowy rejestr użytkowników, w polu **Nazwa zwykła** wprowadź nazwę użytkownika, dla którego ma być używany certyfikat.

        Jeśli używany jest lokalny rejestr systemu operacyjnego, pole **Nazwa zwykła** musi być zgodne z identyfikatorem użytkownika lokalnego systemu operacyjnego.

        W przypadku rejestru użytkowników LDAP należy upewnić się, że nazwa wyróżniająca certyfikatu jest zgodna z nazwą wyróżniającą w rejestrze LDAP.
        iv) Wpisz lub wybierz wartości dla pozostałych pól, odpowiednio.

v) Wybierz miejsce, w którym ma zostać zapisane żądanie certyfikatu, oraz nazwę pliku dla żądania certyfikatu, a następnie kliknij przycisk **OK**.

vi) Wyślij plik żądania certyfikatu do ośrodka certyfikacji (CA).

vii) Jeśli certyfikat jest używany przez ośrodek CA, należy otworzyć narzędzie IBM Key Management, wprowadzając komendę **strmqikm** w wierszu komend.

viii) W menu **Key Database File** (Plik bazy danych kluczy) w narzędziu IBM Key Management kliknij opcję **Open**(Otwórz).

ix) Wybierz magazyn kluczy PKCS#12 , w którym znajduje się certyfikat klienta. Na przykład `user.p12`

x) Kliknij opcję **Odbierz**, wybierz odpowiedni certyfikat, a następnie kliknij przycisk **OK**.

3. Wyodrębnij część publiczną certyfikatu klienta:
   a) Otwórz narzędzie IBM Key Management, wprowadzając komendę **strmqikm** w wierszu komend.
   b) W menu **Key Database File** (Plik bazy danych kluczy) w narzędziu IBM Key Management kliknij opcję **Open**(Otwórz).
   c) Wybierz magazyn kluczy PKCS#12 , w którym znajduje się certyfikat klienta. Na przykład `user.p12`
   d) Wybierz certyfikat klienta z listy certyfikatów w narzędziu IBM Key Management.
   e) Kliknij opcję **Wyodrębnij certyfikat**.
   f) Wybierz miejsce, w którym ma zostać zapisany certyfikat, a następnie wprowadź odpowiednią nazwę pliku w polu **Nazwa pliku certyfikatu** . Na przykład: `user.arm`.
4. Zaimportuj publiczną część certyfikatu klienta do magazynu kluczy zaufanych certyfikatów serwera mqweb jako certyfikat osoby podpisującej, dzięki czemu serwer może sprawdzić poprawność certyfikatu klienta:
   a) Utwórz magazyn kluczy produktu `trust.jks` do użycia przez serwer mqweb, jeśli jeszcze nie istnieje:
      i) W menu **Key Database File** (Plik bazy danych kluczy) w narzędziu IBM Key Management kliknij opcję **New**(Nowy).
      ii) Z listy **Key database type** (Typ bazy danych kluczy) wybierz pozycję **JKS** .
      iii) Kliknij przycisk **Przeglądaj** i przejdź do: `MQ_DATA_DIRECTORY/web/installations/installationName/servers/mqweb/resources/security`.

      Ten katalog powinien już zawierać plik `key.jks` . Jeśli plik `trust.jks` już istnieje, otwórz istniejący plik, a nie nadpisz go.
      iv) W polu **File Name** (Nazwa pliku) wpisz `trust.jks` .
      v) Po wyświetleniu zachęty ustaw hasło.
   b) Z menu rozwijanego wybierz opcję **Signer Certificates**(Certyfikaty osoby podpisującej).
   c) Kliknij przycisk **Add** (Dodaj).
   d) Wybierz odpowiedni plik arm, a następnie kliknij przycisk **OK**. Na przykład wybierz `user.arm`.
   e) Wprowadź etykietę dla certyfikatu.
5. Zmień hasło magazynu kluczy serwera mqweb:
   a) W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz).
   b) Z listy **Key database type** (Typ bazy danych kluczy) wybierz pozycję **JKS** .
   c) Kliknij przycisk **Przeglądaj** i przejdź do opcji *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/resources/security` .
   d) Wybierz magazyn kluczy `key.jks` , a następnie kliknij przycisk **Otwórz**.
   e) Po wyświetleniu zapytania wprowadź hasło. Domyślnym hasłem jest `password`.
   f) W menu **Plik bazy danych kluczy** kliknij opcję **Zmień hasło**.
   g) Wprowadź nowe hasło do magazynu kluczy.
6. Włącz uwierzytelnianie certyfikatu klienta w pliku `mqwebuser.xml` :

Plik mqwebuser.xml można znaleźć w następującej ścieżce: *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb

a) Usuń znak komentarza z sekcji w pliku mqwebuser.xml , który umożliwia uwierzytelnianie certyfikatu klienta. Sekcja zawiera następujący tekst:

```
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
    <keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
    <ssl id="thisSSLConfig" clientAuthenticationSupported="true"
keyStoreRef="defaultKeyStore"
          trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"
serverKeyAlias="default"/>
    <sslDefault sslRef="thisSSLConfig"/>
```

b) Upewnij się, że wartość **serverKeyAlias** jest zgodna z nazwą certyfikatu serwera. Jeśli używany jest domyślny certyfikat serwera, wartość jest poprawna.

c) Zmień wartość parametru **password** dla defaultKeyStore na zakodowaną wersję hasła dla magazynu kluczy key.jks :

i) Z poziomu katalogu *MQ_INSTALLATION_PATH*/web/bin wprowadź następującą komendę w wierszu komend:

```
securityUtility encode password
```

ii) Umieść dane wyjściowe tej komendy w polu **Hasło** dla defaultKeyStore.

d) Zmień wartość parametru **password** dla defaultTrustStore , aby była zgodna z hasłem dla magazynu kluczy trust.jks :

i) Z poziomu katalogu *MQ_INSTALLATION_PATH*/web/bin wprowadź następującą komendę w wierszu komend:

```
securityUtility encode password
```

ii) Umieść dane wyjściowe tej komendy w polu **Hasło** dla defaultTrustStore.

e) Usuń lub skomentuj następujący wiersz z pliku mqwebuser.xml :

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

7. Zatrzymaj serwer mqweb, wprowadzając komendę **endmqweb** w wierszu komend.
8. Uruchom serwer mqweb, wprowadzając komendę **strmqweb** w wierszu komend.
9. Użyj certyfikatu klienta do uwierzytelnienia:

- Aby użyć certyfikatu klienta z produktem IBM MQ Console, należy zainstalować certyfikat klienta w przeglądarce WWW, która jest używana do uzyskiwania dostępu do produktu IBM MQ Console. Na przykład, zainstaluj certyfikat klienta user.p12 jako certyfikat osobisty.
- Aby użyć certyfikatu klienta z produktem REST API, należy udostępnić certyfikat klienta dla każdego żądania REST. Jeśli używane są metody HTTP POST, PATCH lub DELETE, należy zapewnić dodatkowe uwierzytelnianie przy użyciu certyfikatu klienta, aby zapobiec atakom typu cross-site request forgery. Oznacza to, że dodatkowe uwierzytelnianie jest używane w celu potwierdzenia, że informacje autoryzacyjne używane do uwierzytelniania żądania są używane przez właściciela referencji.

  To dodatkowe uwierzytelnianie jest udostępniane przez nagłówek HTTP produktu ibm-mq-rest-csrf-token . Ustaw wartość nagłówka ibm-mq-csrf-token na dowolną wartość, w tym pustą, a następnie wyślij żądanie.

Przykład

Ważne: W tym przykładzie nie wszystkie implementacje cURL obsługują samopodpisane certyfikaty, dlatego należy użyć implementacji cURL , która ma być używana.

Poniższy przykład cURL przedstawia sposób tworzenia nowej kolejki Q1, w menedżerze kolejek QM1, z uwierzytelnianiem za pomocą certyfikatu klienta. Dokładna konfiguracja tej komendy cURL zależy od

bibliotek, dla których została zbudowana wartość cURL . Ten przykład jest oparty na systemie Windows z cURL zbudowanym w oparciu o OpenSSL.

- Użyj metody HTTP POST z zasobem kolejki, uwierzytelniając przy użyciu certyfikatu klienta i dołączając nagłówek HTTP `ibm-mq-rest-csrf-token` z dowolną wartością. Ta wartość może być dowolna, w tym wartość pusta. Opcja `--cert-type` określa, że certyfikat jest certyfikatem PKCS#12 . Opcja `--cert` określa położenie certyfikatu, po którym następuje dwukropek (:), a następnie hasło dla certyfikatu:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -
-cert-type P12 --cert c:\user.p12:password
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 Korzystanie z podstawowego uwierzytelniania HTTP przy użyciu produktu REST API

Użytkownicy produktu REST API mogą uwierzytelniać się, podając swój identyfikator użytkownika i hasło w obrębie nagłówka HTTP. Aby użyć tej metody uwierzytelniania przy użyciu metod HTTP, takich jak POST, PATCH i DELETE, należy również podać nagłówek HTTP produktu `ibm-mq-rest-csrf-token` , a także identyfikator użytkownika i hasło.

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do korzystania z produktu REST API. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 508.
- Upewnij się, że podstawowe uwierzytelnianie HTTP jest włączone. Sprawdź, czy w pliku `mqwebuser.xml` znajduje się następujący kod XML i nie jest on przekształtony w komentarz. Ten kod XML musi znajdować się w znacznikach produktu `<featureManager>` :

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS W systemie z/OSużytkownik musi mieć uprawnienia do zapisu w programie `mqwebuser.xml` , aby móc edytować ten plik.

Multi We wszystkich innych systemach operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym , aby edytować plik `mqwebuser.xml` .

- Upewnij się, że podczas wysyłania żądań REST używane jest bezpieczne połączenie. Ponieważ kombinacja nazwy użytkownika i hasła jest kodowana, ale nie jest szyfrowana, należy użyć bezpiecznego połączenia (HTTPS), gdy używane jest podstawowe uwierzytelnianie HTTP przy użyciu produktu REST API.
- Użytkownik może wysłać zapytanie do referencji bieżącego użytkownika za pomocą metody HTTP GET w zasobie `login` , udostępniając podstawowe informacje uwierzytelniające w celu uwierzytelnienia żądania. To żądanie zwraca informacje o nazwie użytkownika i rolach, do których przypisany jest użytkownik. Więcej informacji na ten temat zawiera sekcja GET `/login`.

Procedura

1. Konkatenuj nazwę użytkownika z dwukropkiem i hasłem. Należy pamiętać, że w nazwie użytkownika rozróżniana jest wielkość liter.

   Na przykład nazwa użytkownika admin i hasło administratora stają się następującym łańcuchem:

   ```
   admin:admin
   ```

2. Zakoduj ten łańcuch nazwy użytkownika i hasła w kodowaniu base64 .
3. Dołącz tę zakodowaną nazwę użytkownika i hasło do nagłówka HTTP `Authorization: Basic` .

Na przykład przy użyciu zakodowanej nazwy użytkownika admin i hasła administratora, tworzony jest następujący nagłówek:

```
Authorization: Basic YWRtaW46YWRtaW4=
```

4. Jeśli używane są metody HTTP POST, PATCH lub DELETE, należy podać dodatkowe uwierzytelnianie, a także nazwę użytkownika i hasło.

   To dodatkowe uwierzytelnianie jest udostępniane przez nagłówek HTTP produktu `ibm-mq-rest-csrf-token` . Nagłówek HTTP `ibm-mq-rest-csrf-token` musi być obecny w żądaniu, ale jego wartość może być dowolna, w tym wartość pusta.
5. Wyślij żądanie REST do produktu IBM MQ z odpowiednimi nagłówkami.

Przykład

Poniższy przykład przedstawia sposób tworzenia nowej kolejki Q1, w menedżerze kolejek QM1, z uwierzytelnianiem podstawowym, w systemach Windows . W przykładzie użyto komendy cURL:

- Użyj metody HTTP POST z zasobem kolejki, uwierzytelniając przy użyciu podstawowego uwierzytelniania, włącznie z nagłówkiem `ibm-mq-rest-csrf-token` HTTP o dowolnej wartości. Ta wartość może być dowolna, w tym wartość pusta:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST
-u mqadmin:mqadmin
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 Korzystanie z uwierzytelniania opartego na tokenach przy użyciu interfejsu REST API

Użytkownicy produktu REST API mogą uwierzytelniać się, podając identyfikator użytkownika i hasło do zasobu REST API `login` przy użyciu metody HTTP POST. Generowany jest token LTPA, który umożliwia użytkownikowi uwierzytelnienie przyszłych żądań. Ten znacznik LTPA ma przedrostek `LtpaToken2`. Użytkownik może wylogować się za pomocą metody HTTP DELETE i może wysłać zapytanie do dziennika w informacjach o bieżącym użytkowniku przy użyciu metody HTTP GET.

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do korzystania z produktu REST API. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 508.
- Domyślnie nazwa informacji cookie, która zawiera znacznik LTPA, rozpoczyna się od `LtpaToken2`i zawiera przyrostek, który może ulec zmianie po zrestartowaniu serwera mqweb. Ta zrandomizowana nazwa informacji cookie pozwala na uruchamianie więcej niż jednego serwera mqweb w tym samym systemie. Jeśli jednak nazwa informacji cookie ma pozostać spójną, można określić nazwę, którą ma informacje cookie za pomocą komendy **setmqweb** . Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Domyślnie informacja cookie znacznika LTPA traci ważność po 120 minutach. Za pomocą komendy **setmqweb** można skonfigurować czas utraty ważności informacji cookie znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Upewnij się, że podczas wysyłania żądań REST używane jest bezpieczne połączenie. Jeśli w zasobie `login` używana jest metoda HTTP POST, kombinacja nazwy użytkownika i hasła, która jest wysyłana z żądaniem, nie jest szyfrowana. Dlatego należy używać bezpiecznego połączenia (HTTPS), gdy używane jest uwierzytelnianie oparte na tokenie za pomocą REST API. Domyślnie nie można używać protokołu HTTP z uwierzytelnianiem tokenu LTPA. Istnieje możliwość włączenia znacznika LTPA, który ma być używany przez niezabezpieczone połączenia HTTP, ustawiając wartość **secureLTPA** na `False`. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Użytkownik może wysłać zapytanie do referencji bieżącego użytkownika za pomocą metody HTTP GET w zasobie `login` , udostępniając znacznik LTPA do uwierzytelnienia żądania. To żądanie zwraca

informacje o nazwie użytkownika i rolach, do których przypisany jest użytkownik. Więcej informacji na ten temat zawiera sekcja GET /login.

Procedura

1. Zaloguj się do użytkownika:
   a) Użyj metody HTTP POST dla zasobu `login` :

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   Podaj nazwę użytkownika i hasło w treści żądania JSON, w następującym formacie:

   ```
   {
       "username" : name,
       "password" : password
   }
   ```

   b) Zapisz znacznik LTPA, który jest zwracany z żądania w lokalnej składnicy informacji cookie. Domyślnie ten znacznik LTPA ma przedrostek `LtpaToken2`.
2. Uwierzytelnij żądania REST przy użyciu zapisanego znacznika LTPA jako informacji cookie z każdym żądaniem.

   W przypadku żądań, które korzystają z metod HTTP PUT, PATCH lub DELETE, należy dołączyć nagłówek `ibm-mq-rest-csrf-token` . Wartość tego nagłówka może być dowolna, w tym wartość pusta.
3. Wyloguj użytkownika:
   a) Użyj metody HTTP DELETE dla zasobu `login` :

   ```
   https://host:9443/ibmmq/rest/v1/login
   ```

   Aby uwierzytelnić żądanie, należy udostępnić znacznik LTPA jako plik cookie i dołączyć nagłówek `ibm-mq-rest-csrf-token` . Wartość tego nagłówka może być dowolna, w tym wartość pusta

   b) Przetwórz instrukcję, aby usunąć znacznik LTPA z lokalnej składnicy informacji cookie.

   Uwaga: Jeśli instrukcja nie jest przetwarzana, a token LTPA pozostaje w lokalnej składnicy informacji cookie, to znacznik LTPA może być używany do uwierzytelniania przyszłych żądań REST. Oznacza to, że gdy użytkownik podejmie próbę uwierzytelnienia przy użyciu znacznika LTPA po zakończeniu sesji, tworzona jest nowa sesja, która używa istniejącego tokenu.

Przykład

Poniższy przykład cURL przedstawia sposób tworzenia nowej kolejki Q1, w menedżerze kolejek QM1, z uwierzytelnianiem opartym na tokenach, w systemach Windows :

- Zaloguj się i dodaj znacznik LTPA z przedrostkiem `LtpaToken2`do lokalnej składnicy informacji cookie. Informacje o nazwie użytkownika i haśle są zawarte w treści JSON. Opcja `-c` określa położenie pliku, w którym ma zostać zapisany znacznik:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/login -X POST
  -H "Content-Type: application/json" --data
  "{\"username\":\"mqadmin\",\"password\":\"mqadmin\"}"
  -c c:\cookiejar.txt
  ```

- Utwórz kolejkę. Użyj metody HTTP POST z zasobem kolejki, uwierzytelniając za pomocą znacznika LTPA. Znacznik LTPA z przedrostkiem `LtpaToken2` jest pobierany z pliku `cookiejar.txt` za pomocą opcji `-b` . Ochrona CSRF jest zapewniana przez obecność nagłówka HTTP `ibm-mq-rest-csrf-token` :

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -b
  c:\cookiejar.txt -H "ibm-mq-rest-csrf-token: value" -H "Content-Type: application/json"
  --data "{\"name\":\"Q1\"}"
  ```

- Wyloguj się i usuń znacznik LTPA z lokalnej składnicy informacji cookie. Znacznik LTPA jest pobierany z pliku `cookiejar.txt` za pomocą opcji `-b` . Ochrona CSRF jest zapewniana przez obecność nagłówka

HTTP `ibm-mq-rest-csrf-token` . Położenie pliku `cookiejar.txt` jest określane za pomocą opcji `-c` , dzięki czemu znacznik LTPA jest usuwany z pliku:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X DELETE
-H "ibm-mq-rest-csrf-token: value" -b c:\cookiejar.txt
-c c:\cookiejar.txt
```

Odsyłacze pokrewne

POST /login

GET /login

USUŃ /login

V 9.1.3 Osadzanie partycji IBM MQ Console w ramce IFrame

Element HTML < iframe> może być używany do osadzania jednej strony WWW w inny sposób przy użyciu ramki Inline (IFrame). Ze względów bezpieczeństwa produkt IBM MQ Console nie może być domyślnie osadzony w ramce IFrame. Można jednak włączyć i-ramkę, korzystając z właściwości konfiguracyjnej **mqConsoleFrameAncestors** na serwerze mqweb.

O tym zadaniu

Serwer mqweb przechowuje listę identyfikatorów pochodzenia stron WWW, które mogą osadzać IBM MQ Console za pomocą ramki IFrame. Początek jest kombinacją schematu URL, domeny i portu, na przykład `https://example.com:1234`.

Aby określić pozycje na liście, można użyć właściwości konfiguracyjnej produktu **mqConsoleFrameAncestors** na serwerze mqweb.

Domyślnie pole **mqConsoleFrameAncestors** jest puste, co oznacza, że IBM MQ Console nie może być osadzony w ramce IFrame.

Procedura

Podaj listę początków stron WWW, które mogą osadzać IBM MQ Console w ramce IFrame, wprowadzając następującą komendę:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

gdzie *allowedOrigins* jest rozdzielaną przecinkami listą źródeł. Każde pochodzenie powinno składać się z:

- Nazwa hosta lub adres IP
- Opcjonalny schemat adresu URL
- Opcjonalny numer portu

Należy zauważyć, że nazwa hosta może rozpoczynać się znakiem wieloznacznym (*), a numer portu może również używać znaku wieloznacznego (*).

Przykładowe pochodzenie to:

```
https://example.com:1234
```

który umożliwia dostęp do dowolnej strony WWW z programu `https://example.com:1234` w celu osaenia IBM MQ Console w ramce IFrame.

```
https://*.example.com:*
```

który umożliwia dowolną stronę WWW HTTPS z nazwą hosta kończącą się na serwerze `example.com`i używaniem dowolnego portu w celu osaczenia partycji IBM MQ Console w ramce IFrame.

Przykład

Poniższy przykład umożliwia osadzanie produktu IBM MQ Console w ramce IFrame ze stron WWW obsługiwanych przez produkt `https://site2.example.com:1234` lub `https://site2.example.com:1235`:

```
setmqweb properties -k mqConsoleFrameAncestors -v
https://site2.example.com:1234,https://site2.example.com:1235
```

V 9.1.0 Konfigurowanie architektury CORS dla REST API

Domyślnie przeglądarka WWW nie zezwala na wywoływanie REST API , takich jak JavaScript, w przypadku, gdy skrypt nie pochodzi z tego samego miejsca, co REST API. Oznacza to, że żądania o różnych pochodzeniu nie są włączone. Istnieje możliwość skonfigurowania funkcji CORS (Cross Origin Resource Sharing) w celu zezwolenia na żądania krzyżowe z określonych źródeł pochodzenia.

O tym zadaniu

Dostęp do produktu REST API można uzyskać za pomocą przeglądarki WWW, na przykład za pomocą skryptu. Ponieważ te żądania pochodzą z innego źródła do składnika REST API, przeglądarka WWW odmawia żądania, ponieważ jest to żądanie o charakterze krzyżowym. Pochodzenie jest inne, jeśli domena, port lub schemat nie są takie same.

Jeśli na przykład istnieje skrypt, który jest udostępniany w produkcie `http://localhost:1999/` , należy utworzyć żądanie dotyczące wielu źródeł, jeśli zostanie wysłane żądanie HTTP GET na stronie WWW, która jest udostępniana w produkcie `https://localhost:9443/`. To żądanie jest żądaniem międzypochodnym, ponieważ numery portów i schematu (HTTP) są różne.

Żądania dotyczące wielu źródeł można włączyć, konfigurując system CORS i określając źródła, które mogą uzyskiwać dostęp do produktu REST API.

Więcej informacji na temat architektury CORS można znaleźć w sekcji https://www.w3.org/TR/cors/ i https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS.

Procedura

1. Wyświetl bieżącą konfigurację, wprowadzając następującą komendę:

   `dspmqweb properties -a`

   Pozycja `mqRestCorsAllowedOrigins` określa dozwolone pochodzenie. Pozycja `mqRestCorsMaxAgeInSeconds` określa czas (w sekundach), przez który przeglądarka WWW może buforować wyniki wszystkich sprawdzeń przed lotem CORS.
2. Określ źródła, które mogą uzyskiwać dostęp do produktu REST API , wprowadzając następującą komendę:

   `setmqweb properties -k mqRestCorsAllowedOrigins -v` *`allowedOrigins`*

   gdzie *allowedOrigins* określa źródło, z którego mają być dozwolone żądania dotyczące krzyżowego pochodzenia. Można użyć znaku gwiazdki otoczonego podwójnymi cudzysłowami, "*", aby zezwolić na wszystkie żądania związane z krzyżem. Istnieje możliwość wprowadzenia więcej niż jednego źródła w postaci listy rozdzielanej przecinkami, otoczonej znakami podwójnego cudzysłowu. Aby nie zezwalać na żądania krzyżowe, należy wprowadzić puste znaki cudzysłowu jako wartość parametru *allowedOrigins*.
3. Określ czas (w sekundach), przez jaki przeglądarka WWW ma buforować wyniki sprawdzania przed lotem CORS, wprowadzając następującą komendę:

   `setmqweb properties -k mqRestCorsMaxAgeInSeconds -v` *`time`*

Przykład

W poniższym przykładzie przedstawiono żądania krzyżowe włączone dla produktów `http://localhost:9883`, `https://localhost:1999`i `https://localhost:9663`. Maksymalny wiek buforowanych wyników wszystkich kontroli przed lotem CORS wynosi 90 sekund:

```
setmqweb properties -k mqRestCorsAllowedOrigins -v "http://localhost:9883,https://
localhost:1999,https://localhost:9663"
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v 90
```

Konfigurowanie sprawdzania poprawności nagłówka hosta dla produktów IBM MQ Console i REST API

Serwer mqweb można skonfigurować w taki sposób, aby ograniczał dostęp do serwerów IBM MQ Console i REST API w taki sposób, aby przetwarzane były tylko żądania wysyłane z nagłówkiem hosta, który jest zgodny z określoną listą allowlist. Jeśli wartość nagłówka hosta, która nie znajduje się na liście allowlist, jest używana, zwracany jest błąd.

O tym zadaniu

Serwer mqweb korzysta z hostów wirtualnych w celu zdefiniowania listy dozwolonych nagłówków hosta. Więcej informacji na temat hostów wirtualnych można znaleźć w dokumentacji produktu WebSphere Liberty : https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html

Aby wykonać tę czynność, należy być użytkownikiem z odpowiednimi uprawnieniami do edycji pliku `mqwebuser.xml` :

- z/OS W systemie z/OSużytkownik musi mieć prawo do zapisu w pliku `mqwebuser.xml` .
- Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.

Procedura

1. Otwórz plik `mqwebuser.xml`. Ten plik znajduje się w jednym z następujących miejsc:
   - ULW

     W systemie UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     W systemie z/OS: *WLP_user_directory*`/servers/mqweb`

     gdzie *katalog_użytkownika_WLP_użytkownika* to katalog, który został określony podczas tworzenia skryptu produktu **crtmqweb** w celu utworzenia definicji serwera WWW mqweb.
2. Dodaj lub usuń komentarz z następującego kodu w pliku `mqwebuser.xml` :

   ```
   <virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
           <hostAlias>localhost:9080</hostAlias>
   </virtualHost>
   ```
3. Edytuj pole **<hostAlias>** , wstawiając nazwę hosta i kombinację portów, które mają być dozwolone.

   Może to być nazwa hosta i nazwa portu, które zostały użyte w konfiguracji serwera mqweb. Na przykład, jeśli używana jest domyślna konfiguracja produktu `localhost:9443`, w polu **<hostAlias>** może być konieczne użycie produktu `localhost:9443` .

   W razie potrzeby można dodać wiele pól **<hostAlias>** w znacznikach **<virtualHost>** , aby zezwolić na większą liczbę kombinacji nazwy hosta i portu. Na przykład, aby zezwolić nagłówkom hosta, które korzystają z portu HTTP, a także nagłówkom hosta korzystającym z portu HTTPS.

V 9.1.0 Kontrola

Rekordy kontroli operacji wykonywanych w IBM MQ Console i REST API mogą być generowane przez włączenie komend i zdarzeń konfiguracyjnych menedżera kolejek, a w przypadku UNIX, Linux, and Windows istotne zmiany stanu są zapisywane w plikach dziennika serwera mqweb.

Istotne zmiany stanu

ULW

W systemie UNIX, Linux, and Windowsrekordy programu IBM MQ Console zmieniają stan znaczący jako komunikaty w dziennikach serwera mqweb. Każdy komunikat wskazuje nazwę uwierzytelnionego użytkownika, który zażądał tej operacji.

Istotne zmiany stanu, takie jak podczas tworzenia, uruchamiania, końkowania lub usuwania menedżerów kolejek, są rejestrowane w plikach `messages.log` serwera WWW mqweb i plikach `console.log` na poziomie rejestrowania [AUDIT]. Każda pozycja dziennika wskazuje nazwę uwierzytelnionego użytkownika, który zażądał tej operacji.

Pliki `messages.log` i `console.log` znajdują się w następującym miejscu:

- ULW W systemie UNIX, Linux, and Windows:
  MQ_DATA_PATH`\web\installations\`*installationName*`\servers\mqweb\logs`

Więcej informacji na temat konfigurowania poziomów rejestrowania serwera mqweb znajduje się w sekcji Konfigurowanie rejestrowania.

Zdarzenia dotyczące komend i konfiguracji

Opcjonalnie można włączyć zdarzenia dotyczące komend i konfiguracji w menedżerze kolejek, aby udostępnić informacje o większości działań IBM MQ Console i REST API . Na przykład tworzenie kanałów i uzyskiwanie informacji o kolejkach generują zdarzenia komendy i konfiguracji. Więcej informacji na temat włączania zdarzeń dotyczących komend i konfiguracji zawiera sekcja Kontrolowanie konfiguracji, komend i zdarzeń programu rejestrującego.

W przypadku tych komunikatów komend i zdarzeń konfiguracji pole MQIACF_EVENT_ORIGIN jest ustawione na wartość MQEVO_REST, a pole MQCACF_EVENT_APPL_IDENTITY zgłasza pierwsze 32 znaki uwierzytelnionej nazwy użytkownika. Jeśli użytkownik ma rolę **MQWebAdmin** lub **MQWebAdminRO** , pole MQCACF_EVENT_USER_ID zgłasza identyfikator użytkownika serwera WWW mqweb, a nie nazwę użytkownika nazwy użytkownika, który wydał komendę. Jeśli jednak użytkownik ma rolę **MQWebUser** , atrybut MQCACF_EVENT_USER_ID raportuje nazwę użytkownika nazwy użytkownika, która wydała komendę.

Pojęcia pokrewne

“Kontrola” na stronie 473
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 MQ Explorer.

Uwagi dotyczące zabezpieczeń dla produktów IBM MQ Console i REST API w systemie z/OS

Funkcje zabezpieczeń IBM MQ Console i REST API kontrolują, czy użytkownik może wydawać, wyświetlać lub zmieniać komendy. Komendy są następnie przekazywane do menedżera kolejek, a zabezpieczenia menedżera kolejek są następnie używane do sterowania, czy użytkownik może wydać komendę do tego konkretnego menedżera kolejek.

Procedura

1. Upewnij się, że identyfikator użytkownika uruchomionego zadania serwera WWW mqweb ma odpowiednie uprawnienia do wydawania określonych komend PCF i uzyskiwania dostępu do określonych kolejek. Więcej informacji na ten temat zawiera "Uprawnienia wymagane przez identyfikator użytkownika uruchomionego zadania serwera mqweb" na stronie 531.
2. Upewnij się, że wszyscy użytkownicy, którzy mają przypisaną rolę `MQWebUser` , mają odpowiednie uprawnienia.

   Użytkownicy IBM MQ Console i REST API , którzy są przypisani do roli `MQWebUser` , działają w kontekście zabezpieczeń użytkownika. Te identyfikatory użytkowników mogą wykonywać operacje, które mają być wykonywane przez użytkownika w menedżerze kolejek i muszą mieć nadane prawa dostępu do tych samych kolejek systemowych, co przestrzeń adresowa serwera mqweb.

   Identyfikator użytkownika uruchomionego zadania serwera mqweb musi mieć nadany alternatywny dostęp użytkownika do wszystkich użytkowników przypisanych do roli `MQWebUser` .

   Więcej informacji na temat nadawania odpowiednich uprawnień użytkownikom z rolą `MQWebUser` można znaleźć w sekcji "Dostęp do zasobów IBM MQ wymaganych do korzystania z MQ Console lub REST API" na stronie 532.
3. Opcjonalne: Skonfiguruj protokół TLS dla serwerów IBM MQ Console i REST API. Więcej informacji na ten tematzawiera sekcja "Konfigurowanie protokołu TLS dla serwerów REST API i IBM MQ Console w systemie z/OS" na stronie 533.

z/OS Uprawnienia wymagane przez identyfikator użytkownika uruchomionego zadania serwera mqweb

W systemie z/OSidentyfikator użytkownika uruchomionego zadania serwera mqweb wymaga od niektórych uprawnień do wydawania komend PCF i uzyskiwania dostępu do zasobów systemu.

Identyfikator użytkownika uruchomionego zadania serwera mqweb wymaga:

- Identyfikator użytkownika (UID) systemu z/OS w systemie UNIX, który może używać usług systemu UNIX z/OS .
- Dostęp do zestawów danych `hlq.SCSQAUTH` i `hlq.SCSQANL*` w instalacji produktu IBM MQ .
- Prawo do odczytu plików instalacyjnych produktu IBM MQ w systemie z/OS UNIX System Services.
- Dostęp do odczytu i zapisu do katalogu użytkownika produktu Liberty utworzonego przez skrypt **`crtmqweb`** .
- Uprawnienie do nawiązywania połączenia z menedżerem kolejek. Przyznaj, że serwer mqweb uruchomił ID użytkownika zadania *READ* dla profilu `hlq.BATCH` w klasie MQCONN.
- Uprawnienia do wydawania komend IBM MQ i uzyskiwania dostępu do określonych kolejek. Te szczegóły zostały opisane w produktach "IBM MQ Console -wymagane profile zabezpieczeń komend" na stronie 234, "Bezpieczeństwo kolejki systemowej" na stronie 210i "Profile zabezpieczeń kontekstu" na stronie 221.
- Uprawnienie do subskrybowania tematu `SYSTEM.FTE` w celu użycia produktu REST API dla produktu MFT. Przyznaj, że serwer mqweb uruchomił ID użytkownika zadania *ALTER* w profilu `hlq.SUBSCRIBE.SYSTEM.FTE` w klasie MXTOPIC.
- Jeśli konfigurowany jest rejestr SAF, dostęp do różnych profili zabezpieczeń. Więcej informacji zawiera sekcja "Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API" na stronie 516.

Uwierzytelnianie połączenia

Jeśli menedżer kolejek został skonfigurowany tak, aby wymagał, aby wszystkie aplikacje wsadowe udostępniły poprawny identyfikator użytkownika i hasło, ustawiając wartość CHKLOCL (REQUIRED), należy nadać serwerowi mqweb uruchomionego zadania ID użytkownika zadania *UPDATE* dostęp do profilu `hlq.BATCH` w klasie MQCONN.

To uprawnienie powoduje, że uwierzytelnianie połączenia działa w trybie CHKLOCL (OPTIONAL) dla identyfikatora użytkownika uruchomionego zadania serwera mqweb.

Jeśli menedżer kolejek nie został skonfigurowany w taki sposób, aby wymagał, aby wszystkie aplikacje wsadowe udostępniały poprawny identyfikator użytkownika i hasło, wystarczy podać ID użytkownika, który uruchamia zadanie serwera mqweb *READ* dostępu do profilu `hlq.BATCH` w klasie MQCONN.

Więcej informacji na temat komendy CHCKLOCL zawiera sekcja "Korzystanie z produktu CHCKLOCL w lokalnie powiązanych aplikacjach" na stronie 200.

Dostęp do zasobów IBM MQ wymaganych do korzystania z MQ Console lub REST API

Operacje wykonywane w MQ Consolelub REST APIprzez użytkownika w roli `MQWebUser` mają miejsce w kontekście zabezpieczeń użytkownika.

O tym zadaniu

Więcej informacji na temat ról w serwerach MQ Console i REST APIzawiera sekcja "Role w serwerach IBM MQ Console i REST API" na stronie 518 .

Aby nadać użytkownikowi rolę w roli `MQWebUser` , należy skorzystać z następującej procedury: dostęp do zasobów menedżera kolejek wymaganych do używania produktu MQ Console lub REST API.

Procedura

1. Nadaj użytkownikowi `mqweb server started task` alternatywny dostęp użytkownika do każdego identyfikatora użytkownika w roli `MQWebUser` .

   Należy to zrobić w każdym menedżerze kolejek, który będzie administrować przez użytkowników za pomocą produktu MQ Console lub REST API.

   Można użyć następujących przykładowych komend RACF , aby nadać użytkownikowi `mqweb server started task` alternatywny dostęp użytkownika do roli w roli `MQWebUser` :

   ```
   RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
   PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
   SETROPTS RACLIST(MQADMIN) REFRESH
   ```

   gdzie:

   `hlq`
   Jest to przedrostek profilu, który może być nazwą menedżera kolejek lub nazwą grupy współużytkowania kolejki.

   `userId`
   Jest to użytkownik w roli `MQWebUser` .

   `mqwebUserId`
   Jest to identyfikator użytkownika produktu `mqweb server started task` .

   Uwaga: Jeśli używane są zabezpieczenia mieszanego elementu pracy, należy użyć klasy MXADMIN zamiast klasy MQADMIN.

2. Nadaj każdemu użytkownikowi w roli `MQWebUser` dostęp do kolejek systemowych, które są niezbędne do korzystania z produktów MQ Console i REST API.

   W tym celu w przypadku obu systemów SYSTEM.ADMIN.COMMAND.QUEUE i SYSTEM.REST.REPLY.QUEUE, należy nadać każdemu użytkownikowi dostęp UPDATE do klas MQQUEUE lub MXQUEUE, w zależności od tego, czy używane są zabezpieczenia mieszanego elementu pracy.

   Należy to zrobić w każdym menedżerze kolejek, który będzie administrowany przez użytkownika za pomocą REST API, w tym zdalnych menedżerów kolejek administrowanych za pomocą bramyadministrative REST API.

3. Aby umożliwić użytkownikowi w roli `MQWebUser` administrowanie zdalnymi menedżerami kolejek, należy nadać użytkownikowi dostęp UPDATE do profilu w klasie MQQUEUE lub MXQUEUE, chroniąc kolejkę transmisji używaną do wysyłania komend do zdalnego menedżera kolejek. Należy pamiętać, że należy nadać użytkownikowi uprawnienie UPDATE do menedżera kolejek bramy.

   W zdalnym menedżerze kolejek należy nadać temu samemu użytkownikowi dostęp do kolejki transmisji używanej do wysyłania komunikatów odpowiedzi komendy z powrotem do menedżera kolejek gatewaya.
4. Nadaj użytkownikom w roli `MQWebUser` dostęp do wszelkich innych zasobów wymaganych do wykonania operacji obsługiwanych przez produkty MQ Console i REST API.

   Dostęp wymagany do:

   - Operacje wykonywane w REST APIsą opisane w sekcjach *Wymagania dotyczące zabezpieczeń* poszczególnych zasobów REST API .
   - Komendy wydawania przez MQ Console są opisane w sekcji “IBM MQ Console -wymagane profile zabezpieczeń komend” na stronie 234

V 9.1.0 Konfigurowanie protokołu TLS dla serwerów REST API i IBM MQ Console w systemie z/OS

W systemie z/OSmożna skonfigurować serwer mqweb, tak aby używany był pierścień kluczy produktu RACF do przechowywania certyfikatów dla bezpiecznych połączeń z protokołem TLS, a także uwierzytelnianie certyfikatów klienta.

Zanim rozpoczniesz

Aby wykonać tę procedurę, należy być użytkownikiem, który ma uprawnienia do zapisu w pliku `mqwebuser.xml` oraz uprawnienia do pracy z pierścieniami kluczy SAF.

O tym zadaniu

Domyślna konfiguracja serwera WWW mqweb korzysta z magazynów kluczy Java dla serwera i zaufanych certyfikatów. W systemie z/OSmożna skonfigurować serwer mqweb w taki sposób, aby używany był pierścień kluczy produktu RACF , a nie magazyny kluczy produktu Java . Serwer można również skonfigurować w taki sposób, aby zezwalał użytkownikom na uwierzytelnianie za pomocą certyfikatu klienta.

Informacje na temat używania pierścieni kluczy RACF w programie Libertyzawiera sekcja Liberty: Keystores .

Wykonaj tę procedurę, aby skonfigurować serwer mqweb w taki sposób, aby używany był pierścień kluczy produktu RACF i opcjonalnie skonfigurować uwierzytelnianie certyfikatu klienta.

Procedura

1. Utwórz certyfikat ośrodka certyfikacji (CA), który będzie używany do podpisywania certyfikatu serwera. Na przykład wprowadź następującą komendę RACF :

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb Certification Authority')
    O('IBM')
    OU('MQ'))
  SIZE(2048)
  WITHLABEL('mqwebCertauth')
```

2. Utwórz certyfikat serwera podpisany z certyfikatem ośrodka CA utworzonym w kroku 1, wprowadzając następującą komendę:

```
RACDCERT ID(mqwebUserId) GENCERT
  SUBJECTSDN(CN('hostname')
```

```
   O('IBM')
   OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebCertauth'))
  WITHLABEL('mqwebServerCert')
```

gdzie *mqwebUserId* to identyfikator użytkownika uruchomionego zadania serwera WWW mqweb, a *nazwa_hosta* to nazwa hosta serwera mqweb.

3. Połącz certyfikat ośrodka CA i certyfikat serwera z pierścieniem kluczy SAF, wprowadzając następujące komendy:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
```

gdzie *mqwebUserId* to identyfikator użytkownika uruchomionego zadania serwera WWW mqweb, a *keyring* to nazwa pliku kluczy, który ma zostać użyty.

4. Wyeksportuj certyfikat CA do pliku CER, wprowadzając następującą komendę:

```
RACDCERT CERTAUTH EXPORT(LABEL('mqwebCertauth'))
        DSN('hlq.CERT.MQWEBCA')
        FORMAT(CERTDER)
        PASSWORD('password')
```

5. Prześlij wyeksportowany certyfikat CA do stacji roboczej za pomocą protokołu FTP, a następnie zaimportuj go do przeglądarki jako certyfikat ośrodka certyfikacji.
6. Opcjonalne: Jeśli chcesz skonfigurować uwierzytelnianie certyfikatów klienta, utwórz i wyeksportuj certyfikat klienta.
   a) Utwórz certyfikat ośrodka certyfikacji (CA), który będzie używany do podpisywania certyfikatu klienta. Na przykład wprowadź następującą komendę RACF :

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb User CA')
   O('IBM')
   OU('MQ'))
   SIZE(2048)
  WITHLABEL('mqwebUserCertauth')
```

   b) Połącz certyfikat CA z pierścieniem kluczy SAF, wprowadzając następującą komendę:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

   gdzie *mqwebUserId* to identyfikator użytkownika uruchomionego zadania serwera WWW mqweb, a *keyring* to nazwa pliku kluczy, który ma zostać użyty.

   c) Utworzenie certyfikatu klienta podpisanego z certyfikatem ośrodka CA. Na przykład:

```
RACDCERT ID(clientUserId) GENCERT
  SUBJECTSDN(CN('clientUserId')
     O('IBM')
     OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebUserCertauth'))
  WITHLABEL('userCertLabel')
```

   gdzie *clientUserId* jest nazwą użytkownika.

   Metoda używana do odwzorowania certyfikatu na nazwę użytkownika zależy od typu skonfigurowanego rejestru użytkowników:

   - Jeśli używany jest rejestr podstawowy, pole Nazwa zwykła w certyfikacie jest dopasowywane do użytkownika w rejestrze.

- Jeśli używany jest rejestr SAF, a certyfikat znajduje się w bazie danych RACF , używany jest właściciel certyfikatu, określony za pomocą parametru **ID** podczas tworzenia certyfikatu.
- Jeśli używany jest rejestr LDAP, pełna nazwa wyróżniająca w certyfikacie jest zgodna z rejestrem LDAP.

d) Wyeksportuj certyfikat klienta do pliku #12 PKCS, wprowadzając następującą komendę:

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) PASSWORD('password')
DSN('hlq.USER.CERT')
```

e) Prześlij wyeksportowany certyfikat za pomocą protokołu FTP do stacji roboczej. Aby użyć certyfikatu klienta z produktem IBM MQ Console, należy zaimportować go do przeglądarki WWW używanej w celu uzyskania dostępu do bazy danych IBM MQ Console jako certyfikatu osobistego.

7. Zmodyfikuj plik *WLP_user_directory*/servers/mqweb/mqwebuser.xml, gdzie *katalog_użytkownika_WLP_użytkownika* to katalog, który został określony podczas tworzenia skryptu produktu **crtmqweb** w celu utworzenia definicji serwera WWW mqweb.

   Wprowadź następujące zmiany, aby skonfigurować serwer mqweb w taki sposób, aby używany był pierścień kluczy produktu RACF :

   a) Usuń lub skomentuj następujący wiersz:

   ```
   <sslDefault sslRef="mqDefaultSSLConfig"/>
   ```

   b) Dodaj następujące instrukcje:

   ```
   <keyStore id="defaultKeyStore" filebased="false" location="safkeyring://mqwebUserId/
   keyring"
             password="password" readOnly="true" type="JCERACFKS" />
   <ssl id="thisSSLConfig" keyStoreRef="defaultKeyStore" sslProtocol="TLSv1.2"
             serverKeyAlias="mqwebServerCert" clientAuthenticationSupported="true" />
   <sslDefault sslRef="thisSSLConfig"/>
   ```

   gdzie:

   - *Identyfikator użytkownikamqwebUser* to identyfikator użytkownika uruchomionego zadania serwera WWW mqweb.
   - *keyring* to nazwa pliku kluczy RACF .
   - *mqwebServerCert* jest etykietą certyfikatu serwera WWW mqweb.

   Uwagi: Wartość **keyStore password** jest ignorowana.

8. Zrestartuj serwer mqweb, zatrzymując i restartując uruchomione zadanie serwera mqweb.
9. Opcjonalne: Użyj certyfikatu klienta do uwierzytelnienia:

   - Aby użyć certyfikatu klienta z produktem IBM MQ Console, należy wprowadzić adres URL dla MQ Console w przeglądarce WWW, w której zainstalowano certyfikat klienta.
   - Aby użyć certyfikatu klienta za pomocą interfejsu REST API, należy udostępnić certyfikat klienta dla każdego żądania REST.

   Uwagi:

   a. Jeśli do uwierzytelniania na serwerze IBM MQ Consoleużywane są tylko certyfikaty, przeglądarka może wyświetlić listę certyfikatów, z których można wybrać opcję.

   b. Aby użyć innego certyfikatu, konieczne może być zamknięcie i zrestartowanie przeglądarki.

   c. Jeśli używane są certyfikaty klienta, które nie znajdują się w bazie danych RACF , można użyć filtrowania nazwy certyfikatu produktu RACF , aby odwzorować atrybuty certyfikatu na identyfikator użytkownika. Na przykład:

   ```
   RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
   ```

   odwzorowuje certyfikaty z nazwą wyróżniającą podmiotu zawierającą OU=DEPT1 i C=US na ID użytkownika DEPT3USR.

Wyniki

Został skonfigurowany interfejs TLS dla serwerów IBM MQ Console i REST API.

ULW Zarządzanie kluczami i certyfikatami w systemie UNIX, Linux, and Windows

Za pomocą komend `runmqckm` (UNIX i Windows) oraz komendy `runmqakm` (UNIX, Linux, and Windows) można zarządzać kluczami, certyfikatami i żądaniami certyfikatów.

Komenda runmqckm

Komenda **runmqckm** jest dostępna w systemach UNIX i Windows.

Komenda **runmqckm** udostępnia funkcje podobne do funkcji programu iKeyman, które zostały opisane w sekcji “zabezpieczanieIBM MQ” na stronie 5.

Aby użyć komendy **runmqckm** , należy upewnić się, że zmienne środowiskowe systemów są poprawnie skonfigurowane, uruchamiając komendę **setmqenv** .

V 9.1.0 Komenda **runmqckm** wymaga zainstalowania komponentu IBM MQ JRE. Jeśli ten komponent nie jest zainstalowany, można zamiast niego użyć komendy **runmqackm** .

Komenda runmqakm

Komenda **runmqakm** jest dostępna w systemach UNIX, Linuxi Windows.

Aby użyć komendy **runmqaqm** , należy upewnić się, że zmienne środowiskowe systemów są poprawnie skonfigurowane, uruchamiając komendę **setmqenv** .

Jeśli wymagane jest zarządzanie certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend produktu **runmqckm** . Jest to spowodowane tym, że komenda **runmqakm** obsługuje silniejsze szyfrowanie.

Użyj komend `runmqckm` i `runmqakm` , aby wykonać następujące czynności:

- Utwórz typ plików bazy danych kluczy CMS wymaganych przez produkt IBM MQ .
- Tworzenie żądań certyfikatów
- Importuj certyfikaty osobiste
- Importowanie certyfikatów CA
- Zarządzanie certyfikatami samopodpisanymi

Informacje pokrewne

Keytool

ULW Komendy runmqckm i runmqakm w systemie UNIX, Linux, and Windows

W tej sekcji opisano komendy runmqckm i runmqakm zgodnie z obiektem komendy.

Główne różnice między tymi dwiema komendami są następujące:

- ULW **runmqakm**
  - Jest dostępna w systemach UNIX, Linuxi Windows.
  - Obsługuje tworzenie certyfikatów i żądań certyfikatów z kluczami publicznymi Elliptic Curve, podczas gdy komenda **runmqckm** nie.
  - Obsługuje silniejsze szyfrowanie pliku repozytorium kluczy niż komenda **runmqckm** z parametrem **-strong** .
  - Został certyfikowany jako zgodny ze standardem FIPS 140-2 i można go skonfigurować do działania w sposób zgodny ze standardem FIPS przy użyciu parametru **-fips** (w przeciwieństwie do komendy **runmqckm**).

- Windows UNIX **runmqckm**
  - Jest dostępna w systemach UNIX i Windows.
  - Obsługuje formaty plików repozytorium kluczy JKS i JCEKS, natomiast komenda **runmqakm** nie obsługuje tych formatów.

Ostrzeżenie: V 9.1.0 Komenda **runmqckm** wymaga zainstalowania składnika IBM MQ Java runtime environment (JRE).

Każda komenda określa co najmniej jeden *obiekt*. Komendy dla operacji na urządzeniach PKCS #11 mogą określać dodatkowe obiekty. Komendy dla obiektów bazy danych kluczy, certyfikatu i żądania certyfikatu również określają *działanie*. Obiekt może być jednym z następujących obiektów:

-keydb
Działania mają zastosowanie do bazy danych kluczy

-cert
Działania mają zastosowanie do certyfikatu

-certreq
Działania mają zastosowanie do żądania certyfikatu

-help
wyświetla pomoc

-version
Wyświetla informacje o wersji

W poniższych podtematach opisano działania, które można wykonać na obiektach bazy danych kluczy, certyfikatów i żądań certyfikatów. Opis opcji tych komend zawiera sekcja “Opcje runmqckm i runmqakm w systemie UNIX, Linux, and Windows” na stronie 546 .

ULW Komendy dla bazy danych kluczy CMS tylko w systemie UNIX, Linux, and Windows

Do zarządzania kluczami i certyfikatami dla bazy danych kluczy CMS można użyć komend **runmqckm**i **runmqakm** .

-keydb -changepw
Zmień hasło dla bazy danych kluczy CMS:

```
-keydb -changepw -db filename -pw password -new_pw new_password


-stash
```

-keydb -create
Utwórz bazę danych kluczy CMS:

```
-keydb -create -db filename
-pw password -type cms -expire days -stash
```

-keydb -stashpw
Zapisz hasło bazy danych kluczy CMS w pliku:

```
-keydb -stashpw -db filename
-pw password
```

-cert -getdefault

Uwaga: Certyfikat domyślny nie jest obsługiwany przez program IBM MQ 8.0. Należy użyć konfiguracji etykiety certyfikatu zgodnie z opisem w sekcji "Cyfrowe etykiety certyfikatów, zrozumienie wymagań" na stronie 26.

Pobierz domyślny certyfikat osobisty:

```
-cert -getdefault -db filename
-pw password
```

-cert-modyfikowanie
Zmodyfikuj certyfikat.

Uwaga: Obecnie jedynym polem, które można modyfikować, jest pole Zaufanie certyfikatu.

```
-cert -modify -db filename
-pw password -label label
-trust enable|disable
```

-cert -setdefault

Uwaga: Certyfikat domyślny nie jest obsługiwany przez system IBM MQ 8.0 lub nowszy. Należy użyć konfiguracji etykiety certyfikatu zgodnie z opisem w sekcji "Cyfrowe etykiety certyfikatów, zrozumienie wymagań" na stronie 26.

Ustaw domyślny certyfikat osobisty:

```
-cert -setdefault -db filename
-pw password -label label
```

ULW Komenda dla baz danych kluczy CMS lub PKCS #12 w systemie UNIX, Linux, and Windows

Za pomocą komend runmqckm i runmqakm można zarządzać kluczami i certyfikatami bazy danych kluczy CMS lub bazy danych kluczy PKCS #12 .

Uwaga: IBM MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami rodziny algorytmów SHA-2 .

Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .

-keydb -changepw
Zmień hasło dla bazy danych kluczy:

```
-keydb -changepw -db filename -pw password -new_pw
new_password -expire days
```

-keydb -convert
przekształć bazę danych kluczy z jednego formatu na inny:

```
-keydb -convert -db filename -pw password
-old_format cms | pkcs12 -new_format cms
```

-keydb -create
Utwórz bazę danych kluczy:

```
-keydb -create -db filename -pw password -type cms
| pkcs12
```

-keydb -delete
Usuwanie bazy danych kluczy:

```
-keydb -delete -db filename -pw password
```

-keydb -list
Wyświetl aktualnie obsługiwane typy bazy danych kluczy:

```
-keydb -list
```

-cert -add
Dodaj certyfikat z pliku do bazy danych kluczy:

```
-cert -add -db filename -pw password -label label
-file filename
-format ascii | binary
```

-cert -create
Utwórz certyfikat samopodpisany:

```
-cert -create -db filename -pw password -label label
-dn distinguished_name
-size 1024 | 512 -x509version 3 | 1
| 2
-expire days -sig_alg 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
|
SHAWithRSA
```

-cert -delete
Usuń certyfikat:

```
-cert -delete -db filename -pw password -label label
```

-cert -details
Wyświetl szczegółowe informacje o konkretnym certyfikacie:

```
-cert -details -db filename -pw password -label label
```

-cert -export
Wyeksportuj certyfikat osobisty i powiązany z nim klucz prywatny z bazy danych kluczy do pliku PKCS #12 lub do innej bazy danych kluczy:

```
-cert -export -db filename -pw password -label label
-type cms | pkcs12
-target filename -target_pw password -target_type
cms | pkcs12
```

-cert -extract
Wyodrębnij certyfikat z bazy danych kluczy:

```
-cert -extract -db filename -pw password -label label
-target filename
-format ascii | binary
```

-cert -import
Zaimportuj certyfikat osobisty z bazy danych kluczy:

```
-cert -import -file filename -pw password -type
pkcs12 -target filename
-target_pw password -target_type cms -label
label
```

Opcja -label jest wymagana i określa etykietę certyfikatu, który ma zostać zaimportowany z źródłowej bazy danych kluczy.

Opcja -new_label jest opcjonalna i umożliwia zaimportowanie certyfikatu z inną etykietą w docelowej bazie danych kluczy niż etykieta w źródłowej bazie danych.

-cert -list
Wyświetl listę wszystkich certyfikatów w bazie danych kluczy:

```
-cert -list all | personal | CA
-db filename -pw password
```

-cert -receive
Pobierz certyfikat z pliku:

```
-cert -receive -file filename -db filename -pw password

-format ascii | binary -default_cert yes |
no
```

-cert -sign
Podpisz certyfikat:

```
-cert -sign -db filename -file filename -pw password
-label label -target filename
-format ascii | binary -expire days
-sig_alg 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 |
SHAWithRSA
```

-certreq -create
Utwórz żądanie certyfikatu:

```
-certreq -create -db filename -pw password
-label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg 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 |
SHAWithRSA
```

-certreq -delete
Usuń żądanie certyfikatu:

```
-certreq -delete -db filename -pw password -label
label
```

-certreq -szczegóły
Wyświetl szczegółowe informacje dotyczące konkretnego żądania certyfikatu:

```
-certreq -details -db filename -pw password -label
label
```

Wyświetl szczegółowe informacje o żądaniu certyfikatu i wyświetl pełne żądanie certyfikatu:

```
-certreq -details -showOID -db filename
-pw password -label label
```

-certreq -extract
Wyodrębnij żądanie certyfikatu z bazy danych żądań certyfikatów do pliku:

```
-certreq -extract -db filename -pw password
-label label -target filename
```

-certreq -list
Wyświetl wszystkie żądania certyfikatów w bazie danych żądań certyfikatów:

```
-certreq -list -db filename -pw password
```

-certreq -odtwórz
Ponownie utwórz żądanie certyfikatu:

```
-certreq -recreate -db filename -pw password
-label label -target filename
```

ULW Komendy dla operacji urządzenia szyfrującego w systemie UNIX, Linux, and Windows

Za pomocą komend runmqckm i runmqakm można zarządzać kluczami i certyfikatami na potrzeby operacji urządzeń szyfrujących.

Uwaga: IBM MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami rodziny algorytmów SHA-2 .

Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .

-keydb -changepw
Zmień hasło dla urządzenia szyfrującego:

```
-keydb -changepw -crypto module_name -tokenlabel token_label
-pw password -new_pw new_password
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-keydb -list
Wyświetl aktualnie obsługiwane typy bazy danych kluczy:

```
-keydb -list
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -add
Dodaj certyfikat z pliku do urządzenia szyfrującego:

```
-cert -add -crypto module_name -tokenlabel token_label
-pw password -label label -file filename -format
ascii | binary
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -create
Utwórz certyfikat samopodpisany na urządzeniu szyfrującym:

```
-cert -create -crypto module_name -tokenlabel token_label

-pw password -label label -dn distinguished_name
-size 1024 | 512
-x509version 3 | 1 | 2 -default_cert no
| yes -expire days
-sig_alg 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 |
SHAWithRSA
```

Uwaga: Nie można zaimportować certyfikatu zawierającego wiele atrybutów jednostki organizacyjnej (OU) w nazwie wyróżniającej.

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -delete
Usuwanie certyfikatu z urządzenia szyfrującego:

```
-cert -delete -crypto module_name -tokenlabel token_label
-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -details
Wyświetl szczegółowe informacje o konkretnym certyfikacie urządzenia szyfrującego:

```
-cert -details -crypto module_name -tokenlabel token_label

-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

Wyświetl szczegółowe informacje i wyświetl pełny certyfikat dla konkretnego certyfikatu na urządzeniu szyfrującym:

```
-cert -details -showOID -crypto module_name -tokenlabel
token_label
-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -extract
Wyodrębnij certyfikat z bazy danych kluczy:

```
-cert -extract -crypto module_name -tokenlabel token_label
-pw password -label label -target filename
-format ascii | binary
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -import
Zaimportuj certyfikat do urządzenia szyfrującego z obsługą dodatkowej bazy danych kluczy:

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Zaimportuj certyfikat PKCS #12 do urządzenia szyfrującego z obsługą dodatkowej bazy danych kluczy:

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Uwaga: Nie można zaimportować certyfikatu zawierającego wiele atrybutów jednostki organizacyjnej (OU) w nazwie wyróżniającej.

-cert -list
Wyświetl listę wszystkich certyfikatów na urządzeniu szyfrującym:

```
-cert -list all | personal | CA
-crypto module_name -tokenlabel token_label -pw
password
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-cert -receive
Pobierz certyfikat z pliku do urządzenia szyfrującego z obsługą dodatkowej bazy danych kluczy:

```
-cert -receive -file filename -crypto module_name -tokenlabel
token_label
-pw password -default_cert yes | no
-secondaryDB filename -secondaryDBpw password -format
ascii | binary
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

Za pomocą komendy **runmqakm** :

-certreq -create
Utwórz żądanie certyfikatu na urządzeniu szyfrującym:

```
-certreq -create -crypto module_name -tokenlabel token_label

-pw password -label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg 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 |
SHAWithRSA
```

Uwaga: Nie można zaimportować certyfikatu zawierającego wiele atrybutów jednostki organizacyjnej (OU) w nazwie wyróżniającej.

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-certreq -delete
Usuń żądanie certyfikatu z urządzenia szyfrującego:

```
-certreq -delete -crypto module_name -tokenlabel token_label

-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-certreq -szczegóły
Wyświetl szczegółowe informacje dotyczące konkretnego żądania certyfikatu w urządzeniu szyfrującym:

```
-certreq -details -crypto module_name -tokenlabel token_label

-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

Wyświetl szczegółowe informacje o żądaniu certyfikatu i wyświetl pełne żądanie certyfikatu na urządzeniu szyfrującym:

```
-certreq -details -showOID -crypto module_name -tokenlabel
```

```
token_label
-pw password -label label
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-certreq -extract
Wyodrębnij żądanie certyfikatu z bazy danych żądań certyfikatów na urządzeniu szyfrującym do pliku:

```
-certreq -extract -crypto module_name -tokenlabel token_label

-pw password -label label -target filename
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

-certreq -list
Wyświetl wszystkie żądania certyfikatów w bazie danych żądań certyfikatów na urządzeniu szyfrującym:

```
-certreq -list -crypto module_name -tokenlabel token_label

-pw password
```

Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11, należy zauważyć, że **runmqckm** i **strmqikm** 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 to jedyne wyjątki, ponieważ programy **strmqikm** i **runmqckm** na tych platformach są w wersjach 32-bitowych.

ULW Opcje runmqckm i runmqakm w systemie UNIX, Linux, and Windows

Do zarządzania kluczami, certyfikatami i żądaniami certyfikatów można użyć opcji wiersza komend **runmqckm** (iKeycmd) i **runmqakm** .

ULW Komenda `runmqakm` jest dostępna w systemie UNIX, Linux, and Windows.

Windows UNIX Komenda `runmqckm` jest dostępna w systemach UNIX i Windows.

Uwaga: IBM MQ nie obsługuje algorytmów SHA-3 ani SHA-5 . Można użyć nazw algorytmów podpisu cyfrowego SHA384WithRSA i SHA512WithRSA , ponieważ oba algorytmy są elementami rodziny algorytmów SHA-2 .

Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .

Znaczenie opcji może zależeć od obiektu i działania określonego w komendzie.

*Tabela 90. Opcje, których można używać z opcjami **runmqckm** i **runmqakm***	
Parametr	**Opis**
`-create`	Opcja tworzenia bazy danych kluczy.
`-crypto`	Nazwa modułu do zarządzania urządzeniem szyfrującym PKCS #11 . Wartość po **-crypto** jest opcjonalna, jeśli w pliku właściwości określono nazwę modułu. Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11 , należy pamiętać, że produkty **runmqckm** i **strmqikm** są uruchamiane przy użyciu wirtualnej maszyny języka Java (JVM) dostarczanej z instalacją produktu IBM MQ . Moduły zewnętrzne wymagane do obsługi standardu PKCS #11 zostaną załadowane do procesu maszyny JVM, dlatego należy zainstalować bibliotekę PKCS #11 na potrzeby administrowania sprzętem szyfrującym, który jest zgodny z wartością bitową maszyny JVM, i określić tę bibliotekę jako **runmqckm** lub **strmqikm**.
-db	Pełna nazwa ścieżki do bazy danych kluczy.
-default_cert	Ustawia certyfikat jako domyślny. Wartością może być `yes` (tak) lub `no (nie)`. Wartością domyślną jest `no`.
-dn	Nazwa wyróżniająca X.500 . Wartością jest łańcuch ujęty w cudzysłów, na przykład `"CN=John Smith,O=IBM,OU=Test,C=GB"`. Należy pamiętać, że wymagane są tylko atrybuty O i C. Określenie nazwy zwykłej (CN) jest opcjonalne.
-encryption	Siła szyfrowania używana w komendzie eksportowania certyfikatu. Wartością może być `strong` lub `weak`. Wartością domyślną jest `strong`.
-expire	Czas ważności (w dniach) certyfikatu lub hasła bazy danych. Wartością domyślną jest 365 dni dla hasła certyfikatu. Nie ma domyślnego czasu dla hasła bazy danych: należy użyć parametru **-expire** , aby jawnie ustawić czas ważności hasła bazy danych.
-file	Nazwa pliku certyfikatu lub żądania certyfikatu.
-fips	określa, że komenda jest uruchamiana 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.
-format	Format certyfikatu. Wartością może być `ascii` dla kodu ASCII Base64_encoded ASCII lub `binary` dla danych binarnych DER. Wartością domyślną jest `ascii`.
-label	Etykieta dołączona do certyfikatu lub żądania certyfikatu. Jeśli certyfikat jest certyfikatem osobistym używanym do identyfikowania aplikacji klienckiej lub menedżera kolejek produktu IBM MQ , etykieta musi odpowiadać ustawieniu etykiety certyfikatu IBM MQ (CERTLABL). Więcej informacji na ten temat zawiera sekcja “Cyfrowe etykiety certyfikatów, zrozumienie wymagań” na stronie 26.
-new_format	Nowy format bazy danych kluczy.
-new_label	Ta opcja użyta w komendzie importowania certyfikatu umożliwia zaimportowanie certyfikatu z inną etykietą niż etykieta, którą miał w źródłowej bazie danych kluczy. Jeśli certyfikat jest certyfikatem osobistym używanym do identyfikowania aplikacji klienckiej lub menedżera kolejek produktu IBM MQ , etykieta musi odpowiadać ustawieniu etykiety certyfikatu IBM MQ (CERTLABL). Więcej informacji na ten temat zawiera sekcja “Cyfrowe etykiety certyfikatów, zrozumienie wymagań” na stronie 26.

*Tabela 90. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**
-new_pw	Nowe hasło bazy danych.
-old_format	Stary format bazy danych kluczy.
-pw	Hasło do bazy danych kluczy lub pliku PKCS #12 .
-secondaryDB	Nazwa dodatkowej bazy danych kluczy dla operacji urządzenia PKCS #11 .
-secondaryDBpw	Hasło do dodatkowej bazy danych kluczy dla operacji urządzenia PKCS #11 .
-showOID	Wyświetla pełny certyfikat lub żądanie certyfikatu.
-sig_alg	Algorytm kodowania mieszającego używany podczas tworzenia żądania certyfikatu, certyfikatu samopodpisanego lub podpisywania certyfikatu. Ten algorytm kodowania mieszającego jest używany do tworzenia podpisu powiązanego z nowo utworzonym certyfikatem lub żądaniem certyfikatu. W systemie **runmqckm**może to być wartość MD2_WITH_RSA, MD2WithRSA, MD5_WITH_RSA, MD5WithRSA, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, SHA2/ECDSA, SHA224WithECDSA, SHA256_WITH_RSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithECDSA, SHA3/ECDSA, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, SHA3WithECDSA, SHA5/ECDSA, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHA5WithECDSA, SHA_WITH_DSA, SHA_WITH_RSA, SHAWithDSA, SHAWithRSA. Wartością domyślną jest SHA1WithRSA. W przypadku systemu **runmqakm**wartością może być 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_SHA384lub EC_ecdsa_with_SHA512. Wartością domyślną jest SHA1WithRSA.
-size	Wielkość klucza. W przypadku **runmqckm**wartość może wynosić 512, 1024 lub 2048. Wartością domyślną jest 1024 bity. W przypadku **runmqakm**wartość zależy od algorytmu podpisywania: • W przypadku algorytmów podpisu RSA (domyślny algorytm używany, jeśli nie podano parametru **-sig_alg**) wartością może być 512, 1024, 2048 lub 4096. Klucz RSA o wielkości 512 bitów nie jest dozwolony, jeśli parametr **-fips** jest włączony. Domyślna wielkość klucza RSA to 1024 bity. • W przypadku algorytmów krzywej eliptycznej wartość może wynosić 256, 384 lub 512. Domyślna wielkość klucza krzywej eliptycznej zależy od algorytmu podpisywania. W systemie SHA256jest to 256, w systemie SHA384-384, a w systemie SHA512-512.

*Tabela 90. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**
-stash	Zapisz hasło bazy danych kluczy w pliku. Dotyczy tylko baz danych typu CMS i PKCS12. **Uwaga: -stash** jest poprawna w przypadku komend **-keydb** -create nakazuje produktowi **runmqckm**/**runmqakm** utworzenie pliku zeskładowanego zawierającego hasło. Wprowadzenie komendy `$ runmqakm -help` powoduje wyświetlenie tylko parametrów pomocy wysokiego poziomu.
-stashed	Wskazuje, że hasło do bazy danych kluczy lub pliku PKCS #12 znajduje się w pliku ukrytych haseł. **Uwaga:** Opcja **-stashed** jest poprawna w wywołaniach innych niż komendy **-keydb** -create. Jeśli ta opcja nie zostanie podana, należy podać hasło za pomocą komendy **-pw**. Ponadto tylko wtedy, gdy zostanie podane polecenie, jakiego rodzaju działanie jest wykonywane, zostanie wyświetlona szczegółowa pomoc z opisem **-stashed** .
-target	Plik docelowy lub baza danych.
-target_pw	Hasło do bazy danych kluczy, jeśli **-target** określa bazę danych kluczy.
-target_type	Typ bazy danych określony przez operand **-target** . Dozwolone wartości zawiera opis parametru **-type** .
-tokenLabel	Etykieta urządzenia szyfrującego PKCS #11 .
-trust	Status zaufania certyfikatu ośrodka CA. Wartością może być `enable` lub `disable`. Wartością domyślną jest `enable`.
-type	Typ bazy danych. Możliwe wartości: • `cms` dla bazy danych kluczy CMS • `pkcs12` dla pliku PKCS #12 .
-x509version	Wersja certyfikatu X.509 do utworzenia. Wartością może być 1, 2 lub 3. Domyślną wartością jest 3.

-rfc3339	Ten parametr służy do wyprowadzania daty w formacie RFC 3339 dla komendy `runmqakm -cert -details` , która ma następujący format:
	`Not Before : 2015-08-26T08:53:37Z`
	`Not After : 2016-08-26T08:53:37Z`
	Należy zauważyć, że parametr **-rfc3339** musi występować w komendzie po dodatkowych parametrach:
	`runmqakm -cert -details -db exampleDB -stashed -label certficateLabel -rfc3339`

Uwaga: Właściwości dostarczane z parametrem IBM Global Security Kit (GSKit) dotyczącym szyfrowania z kluczem symetrycznym **-seckey** w programie narzędziowym **runmqckm** są ignorowane i nie są obsługiwane przez program IBM MQ.

ULW Kody błędów komendy runmqakm w systemie UNIX, Linux, and Windows

Tabela zawierająca liczbowe kody błędów wydane przez program runmqakm i ich znaczenie.

Kod błędu	Komunikat o błędzie
0	Powodzenie
1	Wystąpił nieznany błąd
2	Wystąpił błąd kodowania/dekodowania ASN.1 .
3	Wystąpił błąd podczas inicjowania kodera/ dekodera ASN.1 .
4	Wystąpił błąd kodowania/dekodowania ASN.1 z powodu indeksu poza zakresem lub nieistniejącego pola opcjonalnego.
5	Wystąpił błąd bazy danych.
6	Wystąpił błąd podczas otwierania pliku bazy danych. Sprawdź, czy plik istnieje i czy ma odpowiednie uprawnienia.
7	Wystąpił błąd podczas ponownego otwierania zbioru bazy danych.
8	Tworzenie bazy danych nie powiodło się.
9	Baza danych już istnieje.
10	Wystąpił błąd podczas usuwania zbioru bazy danych.
11	Nie można otworzyć bazy danych.
12	Wystąpił błąd podczas odczytywania zbioru bazy danych.
13	Wystąpił błąd podczas zapisywania danych do zbioru bazy danych.
14	Wystąpił błąd sprawdzania poprawności bazy danych.
15	Napotkano niepoprawną wersję bazy danych.
16	Napotkano niepoprawne hasło bazy danych.
17	Napotkano niepoprawny typ zbioru bazy danych.
18	Określona baza danych została uszkodzona.
19	Podano niepoprawne hasło lub baza danych kluczy została sfałszowana lub uszkodzona.
20	Wystąpił błąd integralności pozycji klucza bazy danych.
21	W bazie danych już istnieje duplikat certyfikatu.
22	W bazie danych już istnieje duplikat klucza (ID rekordu).

Kod błędu	Komunikat o błędzie
23	Certyfikat o takiej samej etykiecie już istnieje w bazie danych kluczy.
24	W bazie danych już istnieje duplikat klucza (sygnatura).
25	W bazie danych już istnieje duplikat klucza (certyfikat niepodpisany).
26	W bazie danych już istnieje duplikat klucza (wystawca i numer seryjny).
27	W bazie danych już istnieje duplikat klucza (informacje o kluczu publicznym podmiotu).
28	W bazie danych już istnieje duplikat klucza (niepodpisana lista CRL).
29	Etykieta została użyta w bazie danych.
30	Wystąpił błąd szyfrowania hasła.
31	Wystąpił błąd związany z LDAP. (LDAP nie jest obsługiwany przez ten program)
32	Wystąpił błąd szyfrowania.
33	Wystąpił błąd szyfrowania/deszyfrowania.
34	Znaleziono niepoprawny algorytm szyfrowania.
35	Wystąpił błąd podczas podpisywania danych.
36	Wystąpił błąd podczas weryfikowania danych.
37	Wystąpił błąd podczas obliczania streszczenia danych.
38	Znaleziono niepoprawny parametr szyfrujący.
39	Napotkano nieobsługiwany algorytm szyfrowania.
40	Podana wielkość wejściowa jest większa niż obsługiwana wielkość modułu.
41	Znaleziono nieobsługiwany rozmiar modułu.
42	Wystąpił błąd sprawdzania poprawności bazy danych.
43	Sprawdzanie poprawności pozycji klucza nie powiodło się.
44	Istnieje duplikat pola rozszerzenia.
45	Wersja klucza jest niepoprawna.
46	Wymagane pole rozszerzenia nie istnieje.
47	Okres ważności nie obejmuje dnia dzisiejszego lub nie mieści się w okresie ważności wystawcy.
48	Okres ważności nie obejmuje dnia bieżącego lub nie mieści się w okresie ważności wystawcy.

Kod błędu	Komunikat o błędzie
49	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia użycia klucza prywatnego.
50	Nie znaleziono wystawcy klucza.
51	Brak wymaganego rozszerzenia certyfikatu.
52	Znaleziono niepoprawne rozszerzenie ograniczenia podstawowego.
53	Sprawdzanie poprawności podpisu klucza nie powiodło się.
54	Klucz główny klucza nie jest zaufany.
55	Klucz został unieważniony.
56	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia identyfikatora klucza uprawnień.
57	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia użycia klucza prywatnego.
58	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia alternatywnej nazwy podmiotu.
59	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia alternatywnej nazwy wystawcy.
60	Wystąpił błąd podczas sprawdzania poprawności rozszerzenia użycia klucza.
61	Znaleziono nieznane rozszerzenie krytyczne.
62	Wystąpił błąd podczas sprawdzania poprawności pozycji par kluczy.
63	Wystąpił błąd podczas sprawdzania poprawności listy CRL.
64	Wystąpił błąd blokady mutex.
65	Znaleziono niepoprawny parametr.
78	Napotkano parametr o wartości NULL lub błąd przydzielania pamięci.
65	Liczba lub wielkość jest zbyt duża lub zbyt mała.
76	Stare hasło jest niepoprawne.
67	Nowe hasło jest niepoprawne.
80	Hasło utraciło ważność.
90	Wystąpił błąd związany z wątkiem.
66	Wystąpił błąd podczas tworzenia wątków.
73	Wystąpił błąd podczas oczekiwania wątku na zakończenie.
74	Wystąpił błąd we/wy.
75	Wystąpił błąd podczas ładowania CMS.

Kod błędu	Komunikat o błędzie
85	Wystąpił błąd związany ze sprzętem kryptograficznym.
77	Procedura inicjowania biblioteki nie została pomyślnie wywołana.
75	Wewnętrzna tabela uchwytów bazy danych jest uszkodzona.
79	Wystąpił błąd przydziału pamięci.
80	Znaleziono nierozpoznaną opcję.
81	Wystąpił błąd podczas pobierania informacji o czasie.
80	Wystąpił błąd tworzenia blokady mutex.
87	Wystąpił błąd podczas otwierania katalogu komunikatów.
84	Wystąpił błąd podczas otwierania katalogu komunikatów o błędach
85	Znaleziono pustą nazwę pliku.
87	Wystąpił błąd podczas otwierania plików. Sprawdź, czy plik istnieje i czy ma odpowiednie uprawnienia.
87	Wystąpił błąd podczas otwierania plików do odczytu.
88	Wystąpił błąd podczas otwierania plików do zapisu.
89	Nie ma takiego pliku.
90	Nie można otworzyć pliku z powodu jego ustawienia uprawnień.
91	Wystąpił błąd podczas zapisywania danych do plików.
92	Wystąpił błąd podczas usuwania plików.
93	Znaleziono niepoprawne dane Base64-encoded .
94	Znaleziono niepoprawny typ komunikatu Base64 .
95	Wystąpił błąd podczas kodowania danych przy użyciu reguły kodowania Base64 .
96	Wystąpił błąd podczas dekodowania danych Base64-encoded .
97	Wystąpił błąd podczas pobierania znacznika nazwy wyróżniającej.
98	Wymagane pole nazwy zwykłej jest puste.
o 99	Wymagane pole nazwy kraju lub regionu jest puste.
100	Znaleziono niepoprawny uchwyt bazy danych.
101	Baza danych kluczy nie istnieje.
102	Baza danych par kluczy żądania nie istnieje.

Kod błędu	Komunikat o błędzie
103	Plik haseł nie istnieje.
104	Nowe hasło jest identyczne ze starym.
105	W bazie danych kluczy nie znaleziono klucza.
106	Nie znaleziono klucza żądania.
107	Nie znaleziono zaufanego ośrodka CA.
108	Nie znaleziono klucza żądania dla certyfikatu.
109	W bazie danych kluczy nie ma klucza prywatnego.
110	W bazie danych kluczy nie ma klucza domyślnego.
111	W rekordzie klucza nie ma klucza prywatnego.
112	W rekordzie klucza nie ma certyfikatu.
113	Brak pozycji CRL.
114	Znaleziono niepoprawną nazwę pliku bazy danych kluczy.
115	Znaleziono nierozpoznany typ klucza prywatnego.
116	Znaleziono niepoprawną nazwę wyróżniającą.
117	Nie znaleziono pozycji klucza, która ma określoną etykietę klucza.
118	Lista etykiet kluczy została uszkodzona.
119	Dane wejściowe nie są poprawnymi danymi PKCS12 .
120	Hasło jest niepoprawne lub dane PKCS12 zostały uszkodzone lub utworzone w późniejszej wersji PKCS12
121	Znaleziono nierozpoznany typ eksportu klucza.
122	Znaleziono nieobsługiwany algorytm szyfrowania oparty na haśle.
123	Wystąpił błąd podczas przekształcania pliku kluczy w bazę danych kluczy CMS.
124	Wystąpił błąd podczas przekształcania bazy danych kluczy CMS w plik kluczy.
125	Wystąpił błąd podczas tworzenia certyfikatu dla żądania certyfikatu.
126	Nie można zbudować kompletnego łańcucha wystawców.
127	Znaleziono niepoprawne dane WEBDB.
128	Brak danych do zapisania w pliku kluczy.
129	Wprowadzona liczba dni wykracza poza dozwolony okres ważności.
130	Hasło jest zbyt krótkie, musi składać się z co najmniej {0} znaków.

Kod błędu	Komunikat o błędzie
131	Hasło musi zawierać co najmniej jedną cyfrę.
132	Wszystkie znaki w haśle są literami lub cyframi.
133	Podano nierozpoznany lub nieobsługiwany algorytm podpisu.
134	Napotkano niepoprawny typ bazy danych.
135	Podana dodatkowa baza danych kluczy jest używana przez inne urządzenie PKCS#11 .
136	Nie określono dodatkowej bazy danych kluczy.
137	Etykieta nie istnieje na urządzeniu PKCS#11 .
138	Hasło wymagane do uzyskania dostępu do urządzenia PKCS#11 .
139	Hasło nie jest wymagane do uzyskania dostępu do urządzenia PKCS#11 .
140	Nie można załadować biblioteki kryptograficznej.
141	Opcja PKCS#11 nie jest obsługiwana dla tej operacji.
142	Operacja na urządzeniu PKCS#11 nie powiodła się.
143	Użytkownik LDAP nie jest poprawnym użytkownikiem. (LDAP nie jest obsługiwany przez ten program)
144	Użytkownik LDAP nie jest poprawnym użytkownikiem. (LDAP nie jest obsługiwany przez ten program)
145	Zapytanie LDAP nie powiodło się. (LDAP nie jest obsługiwany przez ten program)
146	Znaleziono niepoprawny łańcuch certyfikatów.
147	Certyfikat główny nie jest zaufany.
148	Napotkano unieważniony certyfikat.
149	Funkcja obiektu szyfrującego nie powiodła się.
150	Brak dostępnego źródła danych listy odwołań certyfikatów.
151	Brak dostępnego tokenu szyfrującego.
152	Tryb FIPS jest niedostępny.
153	Wystąpił konflikt z ustawieniami trybu FIPS.
154	Wprowadzone hasło nie spełnia wymagań minimalnej mocy.
200	Wystąpił błąd podczas inicjowania programu.
201	Dzielenie na leksemy argumentów przekazanych do programu runmqakm nie powiodło się.

Kod błędu	Komunikat o błędzie
202	Obiekt zidentyfikowany w komendzie nie jest rozpoznawanym obiektem.
203	Przekazane działanie nie jest znanym działaniem -keydb.
204	Przekazane działanie nie jest znanym działaniem -cert.
205	Przekazane działanie nie jest znanym działaniem -certreq.
206	Brak znacznika dla żądanej komendy.
207	Wartość przekazana ze znacznikiem -version nie jest rozpoznawaną wartością.
208	Wartość przekazana ze znacznikiem -size nie jest rozpoznawaną wartością.
209	Wartość przekazana ze znacznikiem -dn ma niepoprawny format.
210	Wartość przekazana ze znacznikiem -format nie jest rozpoznawaną wartością.
211	Wystąpił błąd związany z otwieraniem pliku.
212	Na tym etapie PKCS12 nie jest obsługiwany.
213	Token szyfrujący, dla którego próbujesz zmienić hasło, nie jest chroniony hasłem.
214	Na tym etapie PKCS12 nie jest obsługiwany.
215	Wprowadzone hasło nie spełnia wymagań minimalnej mocy.
216	Tryb FIPS jest niedostępny.
217	Liczba dni podana jako data utraty ważności jest spoza dozwolonego zakresu.
218	Siła hasła nie spełnia minimalnych wymagań.
219	W żądanej bazie danych kluczy nie znaleziono certyfikatu domyślnego.
220	Napotkano niepoprawny status zaufania.
221	Napotkano nieobsługiwany algorytm podpisu. Na tym etapie obsługiwane są tylko algorytmy MD5 i SHA1 .
222	Opcja PCKS11 nie jest obsługiwana dla tej konkretnej operacji.
223	Przekazane działanie nie jest znanym działaniem losowym.
224	Długość mniejsza niż zero nie jest dozwolona.
225	Jeśli używany jest znacznik -strong, minimalna długość hasła wynosi 14 znaków.

Kod błędu	Komunikat o błędzie
226	Jeśli używany jest znacznik -strong, maksymalna długość hasła wynosi 300 znaków.
227	Algorytm MD5 nie jest obsługiwany w trybie FIPS.
228	Znacznik site nie jest obsługiwany dla komendy -cert -list. Ten atrybut jest dodawany w celu zapewnienia kompatybilności wstecznej i potencjalnego rozszerzenia w przyszłości.
229	Wartość powiązana ze znacznikiem -ca nie została rozpoznana. Wartością musi być 'true' lub 'false'.
230	Wartość przekazana ze znacznikiem -type jest niepoprawna.
231	Wartość przekazana ze znacznikiem -expire jest poniżej dozwolonego zakresu.
232	Używany lub żądany algorytm szyfrowania nie jest obsługiwany.
233	Element docelowy już istnieje.

Ochrona szczegółów uwierzytelniania bazy danych

Jeśli używane jest uwierzytelnianie za pomocą nazwy użytkownika i hasła w celu nawiązania połączenia z menedżerem bazy danych, można je zapisać w składnicy referencji produktu MQ XA, aby uniknąć zapisywania hasła w postaci jawnego tekstu w pliku `qm.ini` .

Zaktualizuj plik XAOpenString dla menedżera zasobów

Aby użyć składnicy referencji, należy zmodyfikować plik XAOpenString w pliku `qm.ini` . Łańcuch jest używany do nawiązywania połączenia z menedżerem bazy danych. W celu określenia miejsca, w którym nazwa użytkownika i hasło są podstawiane w łańcuchu XAOpenString , należy określić zastępowane pola.

- Pole +USER+ jest zastępowane wartością nazwy użytkownika zapisaną w składnicy XACreSklep.
- Pole +PASSWORD+ jest zastępowane wartością hasła zapisaną w składnicy XACreSklep.

W poniższych przykładach przedstawiono sposób modyfikowania parametru XAOpenString w celu użycia pliku referencji w celu nawiązania połączenia z bazą danych.

Nawiąże połączenie z bazą danych Db2

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
  XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t
  ThreadOfControl=THREAD
```

Nawiąże połączenie z bazą danych Oracle

```
XAResourceManager:
  Name=myoracle
  SwitchFile=oraswit
  XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35
            +LogDir=/tmp+threads=true
  ThreadOfControl=THREAD
```

Praca z referencjami dla bazy danych do składnicy referencji produktu MQ XA

Po zaktualizowaniu pliku `qm.ini` za pomocą zastępowanych łańcuchów referencji należy dodać nazwę użytkownika i hasło do składnicy referencji produktu MQ za pomocą komendy **setmqxacred** . Można również użyć produktu **setmqxacred** do modyfikowania istniejących referencji, usuwania referencji lub listy referencji. W poniższych przykładach przedstawiono typowe przypadki użycia:

Dodawanie informacji autoryzacyjnych

Poniższa komenda w bezpieczny sposób zapisuje nazwę użytkownika i hasło dla menedżera kolejek QM1 dla zasobu mqdb2.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

Aktualizowanie informacji autoryzacyjnych

Aby zaktualizować nazwę użytkownika i hasło używane do nawiązywania połączenia z bazą danych, wprowadź ponownie komendę **setmqxacred** z nową nazwą użytkownika i hasłem:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Aby zmiany zostały uwzględnione, należy zrestartować menedżer kolejek.

Usuwanie referencji

Następująca komenda usuwa dane uwierzytelniające:

```
setmqxacred -m QM1 -x mydb2 -d
```

Wyświetlanie informacji autoryzacyjnych

Poniższa komenda wyświetla informacje autoryzacyjne:

```
setmqxacred -m QM1 -l
```

Odsyłacze pokrewne

setmqxacred

zabezpieczanieManaged File Transfer

Bezpośrednio po instalacji i bez modyfikacji produkt Managed File Transfer ma poziom zabezpieczeń, który może być odpowiedni do celów testowych lub testowych w chronionym środowisku. Jednak w środowisku produkcyjnym należy odpowiednio kontrolować, kto może uruchamiać operacje przesyłania plików, którzy mogą odczytywać i zapisywać przesyłane pliki oraz jak chronić integralność plików.

Zadania pokrewne

Ograniczanie uprawnień grupowych dla zasobów specyficznych dla produktu MFT

Zarządzanie uprawnieniami dla zasobów specyficznych dla produktu MFT

“Używanie produktu Advanced Message Security z produktem Managed File Transfer” na stronie 623

W tym scenariuszu wyjaśniono, w jaki sposób można skonfigurować produkt Advanced Message Security w taki sposób, aby zapewniał prywatność komunikatów przesyłanych danych za pośrednictwem serwera Managed File Transfer.

Odsyłacze pokrewne

Uprawnienia MFT do dostępu do systemów plików

Właściwość commandPath MFT

Uprawnienie do publikowania dzienników i komunikatów statusu agentów MFT

Uwierzytelnianie połączenia MFT i IBM MQ

Uwierzytelnianie połączenia umożliwia skonfigurowanie menedżera kolejek w celu uwierzytelniania aplikacji przy użyciu podanego identyfikatora użytkownika i hasła. Jeśli powiązany menedżer kolejek ma włączone zabezpieczenia i wymaga szczegółów referencji (identyfikatora użytkownika i hasła), należy włączyć opcję uwierzytelniania połączenia, aby możliwe było pomyślne nawiązanie połączenia z menedżerem kolejek. Uwierzytelnianie połączenia może być uruchamiane w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Metody dostarczania szczegółów informacji autoryzacyjnych

Wiele komend produktu Managed File Transfer obsługuje następujące metody dostarczania szczegółów informacji autoryzacyjnych:

Szczegóły dostarczone przez argumenty wiersza komend.
Szczegóły referencji można określić za pomocą parametrów **-mquserid** i **-mqpassword** . Jeśli **-mqpassword** nie zostanie podany, użytkownik zostanie poproszony o podanie hasła, w którym dane wejściowe nie są wyświetlane.

Szczegóły dostarczone z pliku referencji: `MQMFTCredentials.xml`.
Szczegóły informacji autoryzacyjnych mogą być predefiniowane w pliku `MQMFTCredentials.xml` jako jawny tekst lub tekst zaciemniony.

Więcej informacji na temat konfigurowania pliku MQMFTCredentials.xml w systemie IBM MQ for Multiplatforms zawiera sekcja “Konfigurowanie produktu MQMFTCredentials.xml na wielu platformach” na stronie 559.

Więcej informacji na temat konfigurowania pliku MQMFTCredentials.xml w systemie IBM MQ for z/OS zawiera sekcja “Konfigurowanie produktu MQMFTCredentials.xml w systemie z/OS” na stronie 561.

Pierwszeństwo

Kolejność określania szczegółów informacji autoryzacyjnych jest następująca:

1. Argument wiersza komend.
2. `MQMFTCredentials.xml` indeksu przez powiązany menedżer kolejek i użytkownik uruchamiający komendę.
3. `MQMFTCredentials.xml` indeksu przez powiązany menedżer kolejek.
4. Domyślny tryb kompatybilności wstecznej, w którym nie są dostarczane żadne szczegóły referencji, co pozwala na kompatybilność z poprzednimi wersjami produktu IBM MQlub IBM WebSphere MQ .

Uwagi:

- Komendy **`fteStartAgent`** i **`fteStartLogger`** nie obsługują argumentu wiersza komend **-mquserid**ani **-mqpassword**, a szczegóły referencji mogą być określone tylko w pliku `MQMFTCredentials.xml` .
- z/OS

  W systemie z/OShasło musi być zapisane wielkimi literami, nawet jeśli hasło użytkownika ma małe litery. Na przykład, jeśli hasło użytkownika to "password", to należy wprowadzić je jako "PASSWORD".

Odsyłacze pokrewne

Która komenda MFT łączy się z menedżerem kolejek

Format pliku referencji produktu MFT

Konfigurowanie produktu `MQMFTCredentials.xml` na wielu platformach

Jeśli produkt Managed File Transfer (MFT) jest skonfigurowany z włączonymi zabezpieczeniami, uwierzytelnianie połączenia wymaga wszystkich komend produktu MFT , które łączą się z menedżerem kolejek w celu podania identyfikatora użytkownika i hasła. Podobnie, podczas nawiązywania połączenia

z bazą danych program rejestrujący produktu MFT może wymagać podania identyfikatora użytkownika i hasła. Te informacje autoryzacyjne mogą być zapisane w pliku referencji produktu MFT .

O tym zadaniu

Elementy w pliku `MQMFTCredentials.xml` muszą być zgodne ze schematem produktu `MQMFTCredentials.xsd` . Informacje na temat formatu produktu `MQMFTCredentials.xml`można znaleźć w sekcji Format pliku referencji MFT.

Przykładowy plik referencji można znaleźć w katalogu `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Dla menedżera kolejek koordynacji można mieć jeden plik referencji produktu MFT , jeden dla menedżera kolejek komend, jeden dla każdego agenta i jeden dla każdego programu rejestrującego. Alternatywnie można mieć jeden plik, który jest używany przez wszystkie elementy w topologii.

Domyślne położenie pliku referencji produktu MFT jest następujące:

UNIX and Linux

$HOME

Windows

%USERPROFILE% lub %HOMEDRIVE%%HOMEPATH%

Jeśli plik referencji jest zapisany w innym miejscu, można użyć następujących właściwości, aby określić, gdzie powinny być one przeznaczone dla komend:

Tabela 91. : Właściwości, które definiują położenie pliku MQMFTCredentials.xml dla różnych komend.

Typ komendy	Plik właściwości	Nazwa właściwości
Komenda łącząca się z menedżerem kolejek koordynacji	coordination.properties	Plik coordinationQMgrAuthenticationCredentials
Komenda, która łączy się z menedżerem kolejek komend	connection.properties	Plik connectionQMgrAuthenticationCredentials
Komenda łącząca się z procesem agenta	agent.properties	Plik agentQMgrAuthenticationCredentials
Komenda łącząca się z procesem programu rejestrującego	logger.properties	Plik loggerQMgrAuthenticationCredentials

Tabela 92. : Właściwości, które definiują położenie pliku MQMFTCredentials.xml dla agentów i procesów programu rejestrującego.

Typ komendy	Plik właściwości	Nazwa właściwości
Agenty MFT	agent.properties	Plik agentQMgrAuthenticationCredentials
MFT Programy rejestrujące	logger.properties	Plik loggerQMgrAuthenticationCredentials

Szczegółowe informacje na temat komend i procesów, z którymi łączy się menedżer kolejek, zawiera sekcja Jakie komendy i procesy produktu MFT łączą się z tym menedżerem kolejek.

Ponieważ plik referencji zawiera informacje o identyfikatorze użytkownika i haśle, wymaga specjalnych uprawnień, aby zapobiec dostępowi bez uprawnień do niego:

UNIX and Linux

```
chown <agent owner userid>
chmod 600
```

Windows

Upewnij się, że dziedziczenie nie jest włączone, a następnie usuń wszystkie identyfikatory użytkowników z wyjątkiem tych, w których działa agent lub program rejestrujący, który będzie używać pliku referencji.

Szczegóły informacji autoryzacyjnych używane do nawiązywania połączenia z menedżerem kolejek koordynacji produktu MFT w module dodatkowym IBM MQ Explorer Managed File Transfer zależą od typu konfiguracji:

Globalne (konfiguracja na dysku lokalnym)
Konfiguracja globalna korzysta z pliku referencji określonego we właściwościach koordynacji i komendy.

Lokalne (zdefiniowane w programie IBM MQ Explorer):
Konfiguracja lokalna korzysta z właściwości szczegółów połączenia powiązanego menedżera kolejek w produkcie IBM MQ Explorer.

Zadania pokrewne

“Włączanie uwierzytelniania połączenia dla produktu MFT” na stronie 563
Uwierzytelnianie połączenia wtyczki IBM MQ Explorer MFT podczas nawiązywania połączenia z menedżerem kolejek koordynacji lub menedżerem kolejek komend oraz uwierzytelnianie połączenia dla agenta Managed File Transfer łączącego się z menedżerem kolejek koordynacji lub menedżerem kolejek komend można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Odsyłacze pokrewne

Format pliku referencji produktu MFT
`fteObfuscate`: szyfrowanie danych poufnych

z/OS Konfigurowanie produktu `MQMFTCredentials.xml` w systemie z/OS

Jeśli produkt Managed File Transfer (MFT) jest skonfigurowany z włączonymi zabezpieczeniami, uwierzytelnianie połączenia wymaga od wszystkich agentów MFT i komend łączących się z menedżerem kolejek podania identyfikatora użytkownika i hasła.

Podobnie podczas nawiązywania połączenia z bazą danych mogą być wymagane programy rejestrujące MFT do określenia identyfikatora użytkownika i hasła.

Te informacje autoryzacyjne mogą być zapisane w pliku referencji MFT . Należy zauważyć, że pliki referencji są opcjonalne, ale łatwiej jest zdefiniować plik lub pliki, które są wymagane przed dostosowaniem środowiska.

Oprócz tego, jeśli masz pliki referencji, otrzymasz mniej komunikatów ostrzegawczych. Komunikaty ostrzegawcze informują o tym, że program MFT uważa, że zabezpieczenia menedżera kolejek są wyłączone i dlatego użytkownik nie podaje szczegółów uwierzytelniania.

Przykładowy plik referencji można znaleźć w katalogu `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Poniżej przedstawiono przykład pliku `MQMFTCredentials.xml`:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MFTCredentials.xsd">
  <tns:qmgr name="MQPH" user="ADMIN" mqUserId="JOHNDOEH" mqPassword="cXXXX" />
  <tns:qmgr name="MQPI" user="ADMIN" mqUserId="JOHNDOEI" mqPassword="yXXXX" />
  <tns:qmgr name="MQPH" mqUserId="NONEH" mqPassword="yXXXX" />
```

```
  <tns:qmgr name="MQPI" mqUserId="NONEI" mqPassword="yXXXX" />
</tns:mqmftCredentials>
```

Gdy zadanie o identyfikatorze ADMIN musi połączyć się z menedżerem kolejek MQPH, przekazuje ID użytkownika *JOHNDOEH* i używa hasła *cXXXX*.

Jeśli zadanie jest uruchamiane przez inny ID użytkownika i łączy się z MQPH, przekazuje ono ID użytkownika *NONEH* i hasło *yXXXX*.

Domyślnym położeniem pliku `MQMFTCredentials.xml` jest katalog osobisty użytkownika w systemie z/OS UNIX System Services (USS). Można również zapisać plik w innym położeniu w USS lub w elemencie w partycjonowanym zestawie danych.

Jeśli plik referencji jest przechowywany w innym położeniu, można użyć następujących właściwości, aby określić miejsce, w którym komendy powinny go szukać:

Tabela 93. : Właściwości definiujące położenie pliku MQMFTCredentials.xml dla różnych komend.

Typ komendy	**Plik właściwości**	**Nazwa właściwości**
Komenda łącząca się z menedżerem kolejek koordynacji	coordination.properties	Plik coordinationQMgrAuthenticationCredentials
Komenda łącząca się z menedżerem kolejek komend	connection.properties	Plik connectionQMgrAuthenticationCredentials
Komenda łącząca się z procesem agenta	agent.properties	Plik agentQMgrAuthenticationCredentials
Komenda łącząca się z procesem programu rejestrującego	logger.properties	Plik loggerQMgrAuthenticationCredentials

Tabela 94. : Właściwości definiujące położenie pliku MQMFTCredentials.xml dla agentów i procesów programu rejestrującego.

Typ komendy	**Plik właściwości**	**Nazwa właściwości**
Agenty MFT	agent.properties	Plik agentQMgrAuthenticationCredentials
MFT Programy rejestrujące	logger.properties	Plik loggerQMgrAuthenticationCredentials

Szczegółowe informacje na temat komend i procesów, które łączą się z którym menedżerem kolejek, zawiera sekcja Które komendy i procesy MFT łączą się z którym menedżerem kolejek.

Aby utworzyć plik referencji w partycjonowanym zestawie danych, wykonaj następujące kroki:

- Utwórz zestaw danych PDSE o formacie VB i długości rekordu logicznego (Lrecl) 200.
- Utwórz element w zestawie danych, zanotuj zestaw danych i element, a następnie dodaj do elementu następujący kod:

```
<?xml version="1.0" encoding="IBM-1047"?>
<tns:mqmftCredentials xmlns:tns="http://wmqfte.ibm.com/MQMFTCredentials"
xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://wmqfte.ibm.com/MFTCredentials MQMFTCredentials.xsd">
  <!—-credentials information goes here-->
</tns:mqmftCredentials>
```

Plik referencji można chronić za pomocą produktu zabezpieczeń, na przykład RACF, ale identyfikatory użytkowników uruchamiających komendy Managed File Transfer i administrujących procesami agenta i programu rejestrującego wymagają prawa do odczytu tego pliku.

Informacje w tym pliku można przesłonić przy użyciu kodu JCL w elemencie BFGCROBS. Spowoduje to, że plik będzie używany do szyfrowania identyfikatora i hasła użytkownika IBM MQ . Na przykład element BFGCROBS przyjmuje linię

```
<tns:qmgr name="MQPI" user="JOHNDOE2" mqUserId="JOHNDOE1" mqPassword="yXXXX" />
```

i tworzy

```
<tns:qmgr mqPasswordCipher="e977c61e9b9c363c" mqUserIdCipher="c394c5887867157c"
name="MQPI" user="JOHNDOE2"/>
```

Aby zachować odwzorowanie identyfikatora użytkownika na identyfikator IBM MQ , można dodać komentarze do pliku. Na przykład:

```
<!--      name="MQPI" user="ADMIN"    mqUserId="JOHNDOE1 -->
```

Te komentarze nie zostały zmienione przez proces zaciemniania.

Należy zauważyć, że treść jest zasłonięta i nie jest mocno zaszyfrowana. Należy ograniczyć identyfikatory użytkowników, którzy mają dostęp do pliku.

Zadania pokrewne

“Konfigurowanie produktu MQMFTCredentials.xml na wielu platformach” na stronie 559
Jeśli produkt Managed File Transfer (MFT) jest skonfigurowany z włączonymi zabezpieczeniami, uwierzytelnianie połączenia wymaga wszystkich komend produktu MFT , które łączą się z menedżerem kolejek w celu podania identyfikatora użytkownika i hasła. Podobnie, podczas nawiązywania połączenia z bazą danych program rejestrujący produktu MFT może wymagać podania identyfikatora użytkownika i hasła. Te informacje autoryzacyjne mogą być zapisane w pliku referencji produktu MFT .

Włączanie uwierzytelniania połączenia dla produktu MFT

Uwierzytelnianie połączenia wtyczki IBM MQ Explorer MFT podczas nawiązywania połączenia z menedżerem kolejek koordynacji lub menedżerem kolejek komend oraz uwierzytelnianie połączenia dla agenta Managed File Transfer łączącego się z menedżerem kolejek koordynacji lub menedżerem kolejek komend można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

O tym zadaniu

Przed IBM MQ 9.1.1tryb zgodności jest domyślnym ustawieniem uwierzytelniania połączenia. Można jednak wyłączyć domyślny tryb zgodności i włączyć tryb uwierzytelniania MQCSP.

V 9.1.1 W produkcie IBM MQ 9.1.1domyślnym trybem uwierzytelniania MQCSP jest tryb uwierzytelniania.

W przypadku uwierzytelniania połączenia dla wtyczki IBM MQ Explorer Managed File Transfer lub dla agentów Managed File Transfer , które łączą się z menedżerem kolejek przy użyciu transportu CLIENT, hasła dłuższe niż 12 znaków są obsługiwane tylko w trybie uwierzytelniania MQCSP. Jeśli zostanie podane hasło o długości większej niż 12 znaków podczas autoryzowania przy użyciu trybu zgodności, wystąpi błąd i agent nie będzie uwierzytelniany za pomocą menedżera kolejek. Informacje na ten temat zawiera komunikat BFGAG0187E w sekcji Komunikaty diagnostyczne: BFGAG0001 - BFGAG9999.

Procedura

- Aby wybrać tryb uwierzytelniania połączenia dla menedżera kolejek koordynacji lub menedżera kolejek komend w programie IBM MQ Explorer, wykonaj następujące kroki:
  a) Wybierz menedżer kolejek, z którym ma zostać nawiązane połączenie.
  b) Kliknij prawym przyciskiem myszy, a następnie z menu podręcznego wybierz opcję **Szczegóły połączenia-> Właściwości** .
  c) Kliknij kartę **ID użytkownika**.

d) Upewnij się, że pole wyboru dla trybu uwierzytelniania połączenia, które ma zostać użyte, jest zaznaczone:

   - V 9.1.0 W produkcie IBM MQ 9.1.0domyślnie pole wyboru **Tryb zgodności identyfikacji użytkownika** nie jest zaznaczone. Oznacza to, że jeśli pole wyboru **Włącz identyfikację użytkownika** jest zaznaczone, produkt IBM MQ Explorer będzie używać uwierzytelniania MQCSP podczas nawiązywania połączenia z menedżerem kolejek. Jeśli produkt IBM MQ Explorer musi nawiązać połączenie z menedżerem kolejek przy użyciu trybu zgodności zamiast uwierzytelniania MQCSP, należy upewnić się, że zaznaczone są pola wyboru **Włącz identyfikację użytkownika** i **Tryb zgodności identyfikacji użytkownika** .
   - Przed IBM MQ 9.1.0domyślnie zaznaczone jest pole wyboru **Tryb zgodności identyfikacji użytkownika** . Oznacza to, że jeśli pole wyboru **Włącz identyfikację użytkownika** jest zaznaczone, produkt IBM MQ Explorer będzie korzystać z trybu zgodności podczas nawiązywania połączenia z menedżerem kolejek. Jeśli produkt IBM MQ Explorer musi nawiązać połączenie z menedżerem kolejek przy użyciu uwierzytelniania MQCSP, należy upewnić się, że pole wyboru **Włącz identyfikację użytkownika** jest zaznaczone, a pole wyboru **Tryb zgodności identyfikacji użytkownika** nie jest zaznaczone.

- Aby włączyć lub wyłączyć tryb uwierzytelniania MQCSP dla agenta Managed File Transfer przy użyciu pliku `MQMFTCredentials.xml` , należy dodać parametr **useMQCSPAuthentication** do pliku `MQMFTCredentials.xml` dla odpowiedniego użytkownika.

  Parametr **useMQCSPAuthentication** ma następujące wartości:

  true
  Tryb uwierzytelniania MQCSP jest używany do uwierzytelniania użytkownika za pomocą menedżera kolejek.

  V 9.1.1 W przypadku wartości IBM MQ 9.1.1wartością domyślną jest `true` . Jeśli parametr **useMQCSPAuthentication** nie jest określony, domyślnie jest ustawiony na wartość `true` , a tryb uwierzytelniania MQCSP jest używany do uwierzytelniania użytkownika za pomocą menedżera kolejek.

  Fałsz
  Tryb zgodności jest używany do uwierzytelniania użytkownika w menedżerze kolejek.

  Przed IBM MQ 9.1.1, jeśli parametr **useMQCSPAuthentication** nie jest określony, domyślnie jest ustawiony na wartość `false` , a tryb zgodności jest używany do uwierzytelniania użytkownika w menedżerze kolejek.

  W poniższym przykładzie przedstawiono sposób ustawienia parametru **useMQCSPAuthentication** w pliku `MQMFTCredentials.xml` :

```
<tns:qmgr name="CoordQueueMgr" user="ernest" mqUserId="ernest"
    mqPassword="AveryL0ngPassw0rd2135" useMQCSPAuthentication="true"/>
```

Pojęcia pokrewne

“Ochrona hasłem protokołu MQCSP” na stronie 30
W produkcie IBM MQ 8.0można wysyłać hasła, które są zawarte w strukturze MQCSP, chronione, za pomocą funkcji IBM MQ lub zaszyfrowane przy użyciu szyfrowania TLS.

Odsyłacze pokrewne

“Uwierzytelnianie połączenia MFT i IBM MQ” na stronie 559
Uwierzytelnianie połączenia umożliwia skonfigurowanie menedżera kolejek w celu uwierzytelniania aplikacji przy użyciu podanego identyfikatora użytkownika i hasła. Jeśli powiązany menedżer kolejek ma włączone zabezpieczenia i wymaga szczegółów referencji (identyfikatora użytkownika i hasła), należy włączyć opcję uwierzytelniania połączenia, aby możliwe było pomyślne nawiązanie połączenia z menedżerem kolejek. Uwierzytelnianie połączenia może być uruchamiane w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Format pliku referencji produktu MFT

MFT przestrzenie prywatne

Można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp w ramach przesyłania. Obszar, do którego agent jest ograniczony, jest nazywany środowiskiem testowym. Istnieje możliwość zastosowania ograniczeń dla agenta lub użytkownika, który żąda przesłania.

Przestrzenie prywatne nie są obsługiwane, gdy agent jest agentem mostu protokołu lub agentem mostu Connect:Direct . Nie można używać funkcji sandboxing agenta dla agentów, które muszą przesyłać do lub z kolejek produktu IBM MQ .

Odsyłacze pokrewne

“Praca ze środowiskiem testowym agenta MFT” na stronie 565
Aby dodać dodatkowy poziom zabezpieczeń do produktu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp.

“Praca z przestrzeniach prywatnych użytkownika produktu MFT” na stronie 566
Można ograniczyć obszar systemu plików, do którego mogą być przesyłane pliki, a także poza nim, na podstawie nazwy użytkownika MQMD, która żąda przesłania.

Praca ze środowiskiem testowym agenta MFT

Aby dodać dodatkowy poziom zabezpieczeń do produktu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp.

Nie można użyć funkcji sandboxing agenta dla agentów, które przesyłają do lub z kolejek produktu IBM MQ . Ograniczenie dostępu do kolejek produktu IBM MQ przy użyciu środowiska testowego może zostać zaimplementowane zamiast użycia środowiska testowego użytkownika, który jest zalecanym rozwiązaniem dla wszystkich wymagań dotyczących przestrzeni prywatnej. Więcej informacji na temat przestrzeni prywatnej użytkownika zawiera sekcja “Praca z przestrzeniach prywatnych użytkownika produktu MFT” na stronie 566

Aby włączyć środowisko testowe agenta, dodaj następującą właściwość do pliku `agent.properties` dla agenta, który ma zostać ograniczony:

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

gdzie:

- *restricted_directory_name* jest ścieżką do katalogu, która ma być dozwolona lub odmowa.
- `!` jest opcjonalna i określa, że odmowa (wykluczona) następującej wartości dla *restricted_directory_name* . Jeśli wartość `!` nie jest określona, *restricted_directory_name* jest dozwoloną (dołączona) ścieżką.
- *separator* jest separatorem specyficznym dla platformy.

Na przykład, aby ograniczyć dostęp tylko do katalogu AGENT1 do katalogu `/tmp` , ale nie zezwalać na dostęp do podkatalogu `private` , należy ustawić właściwość w następujący sposób w pliku `agent.properties` należącym do AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

Właściwość sandboxRoot jest opisana w sekcji Zaawansowane właściwości agenta.

Zarówno agent, jak i sandboxing użytkownika nie są obsługiwane przez agenty mostu protokołu ani agenty mostu Connect:Direct .

Praca w przestrzeni prywatnej na platformach UNIX, Linuxi Windows

ULW Na platformach UNIX, Linuxi Windows środowisko prywatne ogranicza dostęp do katalogów, z których Managed File Transfer Agent może odczytywać i zapisywać dane. Po aktywowaniu przestrzeni prywatnej program Managed File Transfer Agent może odczytywać i zapisywać w katalogach określonych jako dozwolone, a także wszystkie podkatalogi, które zawierają określone katalogi, chyba że podkatalogi zostaną określone jako odrzucone w katalogu sandboxRoot. Sandboxing Managed File Transfer nie ma

pierwszeństwa przed bezpieczeństwem systemu operacyjnego. Użytkownik, który uruchomił Managed File Transfer Agent , musi mieć dostęp na poziomie systemu operacyjnego do dowolnego katalogu, który będzie mógł odczytywać lub zapisywać w tym katalogu. Jeśli dowiązany katalog nie znajduje się poza określonymi katalogami sandboxRoot (i podkatalogami), nie następuje po nim dowiązanie symboliczne do katalogu.

Praca w środowisku testowym w systemie z/OS

z/OS W systemie z/OSśrodowisko testowe ogranicza kwalifikatory nazwy zestawu danych, z których Managed File Transfer Agent może odczytywać i zapisywać dane. Użytkownik, który uruchomił serwer Managed File Transfer Agent , musi posiadać odpowiednie uprawnienia systemu operacyjnego do wszystkich zestawów danych. Jeśli wartość kwalifikatora nazwy zestawu danych sandboxRoot zostanie ujęta w podwójne cudzysłowy, wówczas wartość jest zgodna z normalną konwencją z/OS i jest traktowana jako pełnopormatowa. W przypadku pominięcia podwójnych cudzysłowów element sandboxRoot jest poprzedzony bieżącym identyfikatorem użytkownika. Jeśli na przykład właściwość sandboxRoot zostanie ustawiona w następujący sposób: `sandboxRoot=//test`, agent będzie mieć dostęp do następujących zestawów danych (w standardowej notacji z/OS) `//`*`username`*`.test.**` W czasie wykonywania, jeśli początkowe poziomy w pełni rozstrzygniętej nazwy zestawu danych nie są zgodne z sandboxRoot, żądanie transferu zostanie odrzucone.

Praca w przestrzeni prywatnej w systemach IBM i

IBM i W przypadku plików w zintegrowanym systemie plików w systemach IBM i , sandboxing ogranicza katalogi, z których Managed File Transfer Agent może odczytywać i zapisywać dane. Po aktywowaniu przestrzeni prywatnej program Managed File Transfer Agent może odczytywać i zapisywać w katalogach określonych jako dozwolone, a także wszystkie podkatalogi, które zawierają określone katalogi, chyba że podkatalogi zostaną określone jako odrzucone w katalogu sandboxRoot. Sandboxing Managed File Transfer nie ma pierwszeństwa przed bezpieczeństwem systemu operacyjnego. Użytkownik, który uruchomił Managed File Transfer Agent , musi mieć dostęp na poziomie systemu operacyjnego do dowolnego katalogu, który będzie mógł odczytywać lub zapisywać w tym katalogu. Jeśli dowiązany katalog nie znajduje się poza określonymi katalogami sandboxRoot (i podkatalogami), nie następuje po nim dowiązanie symboliczne do katalogu.

Odsyłacze pokrewne

“Dodatkowe sprawdzenia dotyczące przesyłania znaków wieloznacznych” na stronie 570
Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia lokalizacji, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia w przypadku przesyłania znaków wieloznacznych dla tego agenta.

“Praca ze środowiskiem testowym agenta MFT” na stronie 565
Aby dodać dodatkowy poziom zabezpieczeń do produktu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp.

Plik MFT `agent.properties`

Praca z przestrzeniach prywatnych użytkownika produktu MFT

Można ograniczyć obszar systemu plików, do którego mogą być przesyłane pliki, a także poza nim, na podstawie nazwy użytkownika MQMD, która żąda przesłania.

Przestrzenie prywatne użytkownika nie są obsługiwane, gdy agent jest agentem mostu protokołu lub agentem mostu Connect:Direct .

Aby włączyć tworzenie przestrzeni prywatnej dla użytkownika, dodaj następującą właściwość do pliku `agent.properties` dla agenta, który ma zostać ograniczony:

```
userSandboxes=true
```

Jeśli ta właściwość jest obecna i ustawiona na wartość true, agent używa informacji znajdujących się w pliku *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/agents/`

agent_name/UserSandboxes.xml w celu określenia, które części systemu plików mają mieć dostęp do użytkownika, który żąda transferu.

Plik XML produktu UserSandboxes.xml składa się z elementu <agent> , który zawiera zero lub więcej elementów <sandbox> . Te elementy opisują reguły, do których mają zastosowanie użytkownicy. Atrybut user elementu <sandbox> jest wzorcem, który jest używany do dopasowania do użytkownika MQMD żądania.

Plik UserSandboxes.xml jest okresowo ładowany przez agenta, a wszelkie poprawne zmiany wprowadzone w tym pliku będą miały wpływ na działanie agenta. Domyślny odstęp czasu przeładowywania wynosi 30 sekund. Ten odstęp czasu można zmienić, określając właściwość agenta xmlConfigReloadInterval w pliku agent.properties .

Jeśli zostanie określony atrybut lub wartość userPattern="regex" , atrybut user jest interpretowany jako wyrażenie regularne Java . Więcej informacji na ten temat zawiera sekcja Wyrażenia regularne używane przez MFT.

If you do not specify the userPattern="regex" attribute or value the user attribute is interpreted as a pattern with the following wildcard characters:

- gwiazdka (*), która reprezentuje zero lub więcej znaków
- znak zapytania (?), który reprezentuje dokładnie jeden znak

Dopasowania są wykonywane w kolejności, w jakiej elementy <sandbox> są wymienione w pliku. Zostanie użyte tylko pierwsze dopasowanie, wszystkie następujące potencjalne dopasowania w pliku są ignorowane. Jeśli żaden z elementów <sandbox> określonych w pliku nie jest zgodny z użytkownikiem MQMD powiązanym z komunikatem żądania przesyłania, to operacja przesyłania nie może uzyskać dostępu do systemu plików. W przypadku znalezienia zgodności między nazwą użytkownika MQMD i atrybutem user dopasowanie identyfikuje zestaw reguł wewnątrz elementu <sandbox> , które są stosowane do przesyłania. Ten zestaw reguł jest używany do określania, które plikilub zestawy danych mogą być odczytyowane lub zapisywane jako część przesyłania.

Każdy zestaw reguł może określać element <read> , który określa, które pliki mogą być odczytyowane, oraz element <write> , który identyfikuje pliki, które mogą być zapisywane. W przypadku pominięcia elementów <read> lub <write> z zestawu reguł, przyjmuje się, że użytkownik powiązany z tym zestawem reguł nie może wykonywać żadnych operacji odczytu lub zapisu, w zależności od przypadku.

Uwaga: Element <read> musi znajdować się przed elementem <write> , a element <include> musi znajdować się przed elementem <exclude> , w pliku UserSandboxes.xml .

Każdy element <read> lub <write> zawiera jeden lub więcej wzorców używanych do określenia, czy plik znajduje się w przestrzeni prywatnej i czy może zostać przesłany. Te wzorce należy określić za pomocą elementów <include> i <exclude> . Atrybut name elementu <include> lub <exclude> określa wzorzec, który ma być dopasowany. Opcjonalny atrybut type określa, czy wartość nazwy jest zbiorem, czy wzorcem kolejki. Jeśli atrybut type nie zostanie określony, agent będzie traktować wzorzec jako wzorzec ścieżki do pliku lub katalogu. Na przykład:

```
<tns:read>
    <tns:include name="/home/user/**"/>
    <tns:include name="USER.**" type="queue"/>
    <tns:exclude name="/home/user/private/**"/>
</tns:read>
```

The <include> and <exclude> name patterns are used by the agent to determine whether files, zestawy danych, or queues can be read from or written to. Operacja jest dozwolona, jeśli ścieżka do pliku kanonicznego, zestaw danych, lub nazwa kolejki jest zgodna z co najmniej jednym z zawartych wzorców i dokładnie zerem z wykluczonych wzorców. Wzorce określone za pomocą atrybutu name w elementach <include> i <exclude> używają separatorów ścieżek i konwencji właściwych dla platformy, na której działa agent. Jeśli zostaną podane ścieżki względne, ścieżki zostaną rozstrzygnięte względem właściwości transferRoot agenta.

W przypadku określania ograniczenia kolejki obsługiwana jest składnia QUEUE@QUEUEMANAGER , której reguły są następujące:

- Jeśli znak at (@) nie jest dostępny w pozycji, wzorzec jest traktowany jako nazwa kolejki, do której można uzyskać dostęp w dowolnym menedżerze kolejek. Jeśli na przykład wzorzec to `name` , jest on traktowany w taki sam sposób, jak produkt `name@**`.
- Jeśli znak at (@) jest pierwszym znakiem w pozycji, wzorzec jest traktowany jako nazwa menedżera kolejek, a dostęp do wszystkich kolejek w menedżerze kolejek jest możliwy. Na przykład, jeśli wzorzec to `@name` , jest traktowany w taki sam sposób, jak `**@name`.

Następujące znaki wieloznaczne mają specjalne znaczenie w przypadku określenia ich jako części atrybutu `name` elementów `<include>` i `<exclude>` :

*****
: Pojedyncza gwiazdka oznacza zero lub więcej znaków w nazwie katalogu lub w kwalifikatorze nazwy zestawu danych lub nazwy kolejki.

?
: Znak zapytania pasuje do dokładnie jednego znaku w nazwie katalogu lub w kwalifikatorze nazwy zestawu danych lub nazwy kolejki.

******
: Dwa znaki gwiazdki są zgodne z zerową lub większą liczbę nazw katalogów albo zero lub więcej kwalifikatorów w nazwie zestawu danych lub nazwie kolejki. Ponadto ścieżki, które kończą się znakiem separatora ścieżki, mają niejawne "**" dodane do końca ścieżki. Oznacza to, że produkt `/home/user/` jest taki sam jak `/home/user/**`.

Na przykład:

- `/**/test/**` jest zgodny z dowolnym plikiem, który ma w ścieżce katalog `test` .
- `/test/file?` jest zgodny z dowolnym plikiem w katalogu `/test` , który rozpoczyna się od łańcucha `file` , po którym następuje dowolny pojedynczy znak
- `c:\test\*.txt` jest zgodny z dowolnym plikiem w katalogu `c:\test` z rozszerzeniem `.txt` .
- `c:\test\**\*.txt` jest zgodny z dowolnym plikiem w katalogu `'c:\test` lub jednym z jego podkatalogów, który ma rozszerzenie `.txt` .
- z/OS `//'TEST.*.DATA'` jest zgodny z dowolnym zestawem danych, który ma pierwszy kwalifikator TEST, ma dowolny drugi kwalifikator i trzeci kwalifikator produktu DATA.
- Wartość *@QM1 jest zgodna z dowolną kolejką w menedżerze kolejek QM1 , która ma pojedynczy kwalifikator.
- Produkt TEST`.*.QUEUE@QM1` jest zgodny z dowolną kolejką w menedżerze kolejek QM1 , która ma pierwszy kwalifikator produktu TEST, ma dowolny drugi kwalifikator i trzeci kwalifikator produktu QUEUE.
- Wartość **@QM1 jest zgodna z dowolną kolejką w menedżerze kolejek QM1.

Dowiązania symboliczne

Należy w pełni rozstrzygnąć wszystkie dowiązania symboliczne używane w ścieżkach plików w pliku `UserSandboxes.xml` , podając twarde dowiązania w elementach `<include>` i `<exclude>` . Jeśli na przykład istnieje dowiązanie symboliczne, w którym program `/var` jest odwzorowywać na wartość `/SYSTEM/var`, należy określić tę ścieżkę jako `<tns:include name="/SYSTEM/var"/>`. W przeciwnym razie zamierzony transfer nie powiedzie się i zostanie wyświetlony błąd zabezpieczeń środowiska testowego użytkownika.

Przykład

W tym przykładzie przedstawiono sposób zezwalania użytkownikowi na nazwę użytkownika MQMD `guest` w celu przesłania dowolnego pliku z katalogu `/home/user/public` lub dowolnego jego podkatalogów

w systemie, w którym działa agent AGENT_JUPITER, przez dodanie następującego elementu <sandbox> do pliku UserSandboxes.xml w katalogu konfiguracyjnym AGENT_JUPITER:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
        xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
        xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="guest">
            <tns:read>
                <tns:include name="/home/user/public/**"/>
             </tns:read>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

Przykład

W tym przykładzie pokazano, w jaki sposób można zezwolić użytkownikowi o nazwie użytkownika MQMD account , po której następuje pojedyncza cyfra, na przykład account4, w celu wykonania następujących czynności:

- Prześlij dowolny plik z katalogu /home/account lub dowolnego z jego podkatalogów, z wyjątkiem katalogu /home/account/private w systemie, w którym działa agent AGENT_SATURN
- Prześlij dowolny plik do katalogu /home/account/output lub dowolnego z jego podkatalogów w systemie, w którym działa agent AGENT_SATURN.
- Odczytaj komunikaty z kolejek w lokalnym menedżerze kolejek, rozpoczynając od przedrostka ACCOUNT. , chyba że rozpoczyna się on od ACCOUNT.PRIVATE. (który ma PRIVATE na drugim poziomie).
- Przesyłaj dane do kolejek, zaczynając od przedrostka ACCOUNT.OUTPUT. w dowolnym menedżerze kolejek.

Aby umożliwić użytkownikowi z nazwą użytkownika MQMD account wykonanie tych czynności, należy dodać następujący element <sandbox> do pliku UserSandboxes.xmlw katalogu konfiguracyjnym AGENT_SATURN:

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:userSandboxes
            xmlns:tns="http://wmqfte.ibm.com/UserSandboxes"
            xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://wmqfte.ibm.com/UserSandboxes UserSandboxes.xsd">
    <tns:agent>
        <tns:sandbox user="account[0-9]" userPattern="regex">
            <tns:read>
                <tns:include name="/home/account/**"/>
                <tns:include name="ACCOUNT.**" type="queue"/>
                <tns:exclude name="ACCOUNT.PRIVATE.**" type="queue"/>
                <tns:exclude name="/home/account/private/**"/>
                                                        </tns:read>
            <tns:write>
                <tns:include name="/home/account/output/**"/>
                <tns:include name="ACCOUNT.OUTPUT.**" type="queue"/>
            </tns:write>
        </tns:sandbox>
    </tns:agent>
</tns:userSandboxes>
```

Odsyłacze pokrewne

“Dodatkowe sprawdzenia dotyczące przesyłania znaków wieloznacznych” na stronie 570
Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia lokalizacji, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia w przypadku przesyłania znaków wieloznacznych dla tego agenta.

Plik MFT agent.properties

Dodatkowe sprawdzenia dotyczące przesyłania znaków wieloznacznych

Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia lokalizacji, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia w przypadku przesyłania znaków wieloznacznych dla tego agenta.

Właściwość additionalWildcardSandboxChecking

Aby włączyć dodatkowe sprawdzanie pod kątem przesyłania znaków wieloznacznych, dodaj następującą właściwość do pliku `agent.properties` dla agenta, który ma zostać sprawdzony.

```
additionalWildcardSandboxChecking=true
```

Jeśli ta właściwość jest ustawiona na wartość true, a agent tworzy żądanie przesyłania, które próbuje odczytać położenie, które znajduje się poza zdefiniowaną przestrzenią prywatną w celu dopasowania pliku do pliku ze znakiem wieloznacznym, przesyłanie nie powiedzie się. Jeśli w ramach jednego żądania transferu istnieje wiele operacji przesyłania, a jedno z tych żądań nie powiedzie się z powodu próby odczytania położenia poza środowiskiem testowym, przesyłanie całego procesu przesyłania nie powiedzie się. Jeśli sprawdzanie nie powiedzie się, przyczyna niepowodzenia jest podana w komunikacie o błędzie.

Jeśli właściwość additionalWildcardSandboxChecking została pominięta w pliku `agent.properties` agenta lub jest ustawiona na wartość false, dla tego agenta nie są wykonywane żadne dodatkowe sprawdzenia dla przesyłania znaków wieloznacznych.

Komunikaty o błędach dla sprawdzania znaków wieloznacznych

Komunikaty, które są zgłaszane, gdy żądanie przesłania znaków wieloznacznych jest wysyłane do miejsca znajdującego się poza skonfigurowanym położeniem środowiska testowego, są następujące.

Następujący komunikat pojawia się, gdy ścieżka do pliku ze znakami wieloznacznymi w żądaniu przesyłania znajduje się poza zamkniętym środowiskiem testowym:

```
BFGSS0077E: Próba odczytania ścieżki do pliku: ścieżka została odrzucona.
Ścieżka do pliku znajduje się poza ograniczonym środowiskiem testowym
przesyłania.
```

Następujący komunikat występuje, gdy przesyłanie w ramach żądania przesłania wielokrotnego zawiera żądanie przesłania ze znakiem wieloznacznym, w którym ścieżka znajduje się poza zamkniętym środowiskiem testowym:

```
BFGSS0078E: Próba odczytania ścieżki do pliku: ścieżka została zignorowana jako inny transfer.
Element w zarządzanym przesyłaniu podjął próbę odczytu poza zamkniętym środowiskiem testowym
przesyłania.
```

Następujący komunikat pojawia się, gdy plik znajduje się poza zamkniętym środowiskiem testowym:

```
BFGSS0079E: Próba odczytania pliku ścieżka do pliku została odrzucona.
Plik znajduje się poza wyznaczonym środowiskiem
testowym przesyłania.
```

Następujący komunikat występuje w żądaniu wielokrotnego przesyłania, w którym inne żądanie przesłania znaków wieloznacznych spowodowało zignorowanie tego żądania:

```
BFGSS0080E: Próba odczytania pliku: ścieżka do pliku została zignorowana jako inny transfer.
Element w zarządzanym przesyłaniu podjął próbę odczytu poza zamkniętym środowiskiem testowym
przesyłania.
```

W przypadku przesyłania pojedynczych plików, które nie zawierają znaków wieloznacznych, komunikat zgłaszany, gdy operacja przesyłania obejmuje plik znajdujący się poza środowiskiem testowym, nie zmienia się z wcześniejszych wersji:

```
Nie powiodło się wykonanie komendy BFGIO0056E: Próba odczytania pliku "PLIK" została odrzucona.
Plik znajduje się poza wyznaczonym środowiskiem
testowym przesyłania.
```

Odsyłacze pokrewne

“Praca z przestrzeniach prywatnych użytkownika produktu MFT” na stronie 566

Można ograniczyć obszar systemu plików, do którego mogą być przesyłane pliki, a także poza nim, na podstawie nazwy użytkownika MQMD, która żąda przesłania.

“Praca ze środowiskiem testowym agenta MFT” na stronie 565
Aby dodać dodatkowy poziom zabezpieczeń do produktu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp.

Plik MFT `agent.properties`

Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT

Za pomocą protokołu SSL lub TLS można użyć programu IBM MQ Managed File Transfer w celu zabezpieczenia komunikacji między agentami i ich menedżerami kolejek agenta, komendami i menedżerami kolejek, z którymi nawiązują połączenie, oraz różnymi połączeniami menedżera kolejek z menedżerem kolejek w obrębie topologii.

Zanim rozpoczniesz

Do szyfrowania komunikatów przepływających przez topologię IBM MQ Managed File Transfer można używać szyfrowania SSL lub TLS. Są to:

- Komunikaty, które są przekazywane między agentem i jego menedżerem kolejek agenta.
- Komunikaty dla komend i menedżerów kolejek, z którymi są one nawiązane.
- Komunikaty wewnętrzne, które przepłyną między menedżerami kolejek agenta, menedżerami kolejek komend i menedżerem kolejek koordynacji w obrębie topologii.

O tym zadaniu

Ogólne informacje na temat używania protokołu SSL z produktem IBM MQzawiera sekcja “Praca z protokołem SSL/TLS” na stronie 282. W produkcie IBM MQ Managed File Transfer jest standardową aplikacją kliencką Java .

Aby użyć protokołu SSL w produkcie Managed File Transfer, wykonaj następujące kroki:

Procedura

1. Utwórz plik zaufanych certyfikatów i (opcjonalnie) plik kluczy (te pliki mogą być tym samym plikiem). Jeśli nie jest wymagane uwierzytelnianie klienta (to znaczy SSLCAUTH=OPTIONAL na kanałach), nie trzeba udostępniać magazynu kluczy. Wymagany jest magazyn zaufanych certyfikatów tylko w celu uwierzytelnienia certyfikatu menedżera kolejek.

   Algorytm klucza używany do tworzenia certyfikatów dla magazynu zaufanych certyfikatów i magazynów kluczy musi być RSA, aby pracować z produktem IBM MQ.
2. Skonfiguruj menedżera kolejek produktu IBM MQ w taki sposób, aby używany był protokół SSL.

   Informacje na temat konfigurowania menedżera kolejek pod kątem używania protokołu SSL za pomocą programu IBM MQ Explorer zawiera sekcja Konfigurowanie protokołu SSL w menedżerach kolejek.
3. Zapisz plik zaufanych certyfikatów i plik kluczy (o ile istnieje) w odpowiedniej lokalizacji. Sugerowane położenie to katalog *config_directory*/*coordination_qmgr*/agents/*agent_name* .
4. Ustaw właściwości protokołu SSL zgodnie z wymaganiami dla każdego menedżera kolejek z włączoną obsługą SSL w odpowiednim pliku właściwości produktu Managed File Transfer . Każdy zestaw właściwości odnosi się do osobnego menedżera kolejek (agenta, koordynacji i komendy), chociaż jeden menedżer kolejek może wykonać dwie lub więcej z tych ról.

   Jedna z właściwości **CipherSpec** lub **CipherSuite** jest wymagana, w przeciwnym razie klient próbuje nawiązać połączenie bez użycia protokołu SSL. Zarówno właściwości **CipherSpec** , jak i **CipherSuite** są udostępniane ze względu na różnice w terminologii między IBM MQ a Java. Produkt Managed File Transfer akceptuje dowolną właściwość i wykonuje niezbędną konwersję, dlatego nie ma potrzeby ustawiania obu właściwości. W przypadku określenia zarówno właściwości **CipherSpec** , jak i **CipherSuite** , pierwszeństwo ma **CipherSpec** .

Właściwość **PeerName** jest opcjonalna. Właściwość tę można ustawić na nazwę wyróżniającą menedżera kolejek, z którym ma zostać nawiązane połączenie. Produkt Managed File Transfer odrzuca połączenia z niepoprawnym serwerem SSL z niezgodnymi nazwami wyróżniającymi.

Ustaw właściwości **SslTrustStore** i **SslKeyStore** na nazwy plików, które wskazują na magazyn zaufanych certyfikatów i pliki kluczy. Jeśli te właściwości są ustanawiane dla agenta, który jest już uruchomiony, zatrzymaj i zrestartuj agenta, aby ponownie nawiązać połączenie w trybie SSL.

Pliki właściwości zawierają hasła w postaci tekstu jawnego, dlatego należy rozważyć ustawienie odpowiednich uprawnień systemu plików.

Więcej informacji na temat właściwości protokołu SSL zawiera sekcja Właściwości SSL dla produktu MFT.

5. Jeśli menedżer kolejek agenta używa protokołu SSL, nie można podać niezbędnych szczegółów podczas tworzenia agenta. Aby utworzyć agenta, wykonaj następujące kroki:
   a) Utwórz agenta za pomocą komendy **fteCreateAgent** . Zostanie wyświetlone ostrzeżenie o niemożności opublikowania informacji o istnieniu agenta w menedżerze kolejek koordynacji.
   b) Edytuj plik `agent.properties` utworzony przez poprzedni krok, aby dodać informacje o protokole SSL. Gdy agent zostanie pomyślnie uruchomiony, ponowna próba publikacji zostanie podjęta ponownie.
6. Jeśli agenty lub instancje programu IBM MQ Explorer są uruchomione, podczas gdy właściwości SSL w pliku `agent.properties` lub pliku `coordination.properties` zostaną zmienione, należy zrestartować agenta lub IBM MQ Explorer.

Odsyłacze pokrewne
Plik MFT `agent.properties`

Nawiąże połączenie z menedżerem kolejek w trybie klienta z uwierzytelnianiem kanału

Produkt IBM WebSphere MQ 7.1 wprowadził rekordy uwierzytelniania kanału w celu zapewnienia bardziej precyzyjnego sterowania dostępem na poziomie kanału. Ta zmiana w zachowaniu oznacza, że domyślnie nowo utworzone menedżery kolejek produktu IBM WebSphere MQ 7.1 lub późniejsze odrzucają połączenia klientów z komponentu Managed File Transfer .

Więcej informacji na temat uwierzytelniania kanału zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 50.

Jeśli konfiguracja uwierzytelniania kanału dla SVRCONN używana przez produkt Managed File Transfer określa nieuprawniony identyfikator MCAUSER, należy nadać odpowiednie rekordy uprawnień dla menedżera kolejek, kolejek i tematów, aby umożliwić poprawne działanie komendy Managed File Transfer Agent i komend. Aby utworzyć, zmodyfikować lub usunąć rekordy uwierzytelniania kanału, należy użyć komendy MQSC SET CHLAUTH lub komendy PCF Set Channel Authentication Record (Ustaw rekord uwierzytelniania kanału). Dla wszystkich agentów Managed File Transfer , które mają być połączone z menedżerem kolejek produktu IBM WebSphere MQ 7.1 lub nowszego, można skonfigurować identyfikator MCAUSER, który ma być używany dla wszystkich agentów, lub skonfigurować osobny identyfikator MCAUSER dla każdego agenta.

Nadaj każdemu identyfikatorowi MCAUSER następujące uprawnienia:

- Rekordy uprawnień wymagane dla menedżera kolejek:
  - connect
  - setid
  - inq
- Rekordy uprawnień wymagane dla kolejek.

  Dla wszystkich kolejek specyficznych dla agentów, czyli nazw kolejek, które kończą się na *nazwa_agenta* na poniższej liście, należy utworzyć te rekordy uprawnień dla każdego agenta, z którym ma zostać

nawiązane połączenie z menedżerem kolejek produktu IBM WebSphere MQ 7.1 lub nowszego przy użyciu połączenia klienckiego.

  - put, get, dsp (SYSTEM.DEFAULT.MODEL.QUEUE)
  - put, get, setid, browse (SYSTEM.FTE.COMMAND.*nazwa_agenta*)
  - put, get (SYSTEM.FTE.DATA.*nazwa_agenta*)
  - put, get (SYSTEM.FTE.REPLY.*nazwa_agenta*)
  - put, get, inq, browse (SYSTEM.FTE.STATE.*nazwa_agenta*)
  - put, get, browse (SYSTEM.FTE.EVENT.*nazwa_agenta*)
  - put, get (SYSTEM.FTE)
- Rekordy uprawnień wymagane dla tematów:
  - sub, pub (SYSTEM.FTE)
- Rekordy uprawnień wymagane do przesyłania plików.

  Jeśli istnieją oddzielne identyfikatory MCAUSER dla agenta źródłowego i docelowego, należy utworzyć rekordy uprawnień dla kolejek agentów zarówno w źródle, jak i w miejscu docelowym.

  Na przykład, jeśli identyfikator MCAUSER agenta źródłowego ma wartość **user1** , a identyfikatorem MCAUSER agenta docelowego jest **user2**, należy ustawić następujące uprawnienia dla użytkowników agenta:

Użytkownik AGENT	Kolejka	Wymagane uprawnienia
user1	SYSTEM.FTE.DATA.*nazwa_agenta_docelowego*	put
user1	SYSTEM.FTE.COMMAND.*nazwa_agenta_docelowego*	put
user2	SYSTEM.FTE.REPLY.*nazwa_agenta_źródłowego*	put
user2	SYSTEM.FTE.COMMAND.*nazwa_agenta_źródłowego*	put

Konfigurowanie protokołu SSL lub TLS między agentem mostu Connect:Direct a węzłem Connect:Direct

Skonfiguruj agent mostu Connect:Direct i węzeł Connect:Direct , aby połączyć się ze sobą za pośrednictwem protokołu SSL, tworząc magazyn kluczy i magazyn zaufanych certyfikatów, a także ustawiając właściwości w pliku właściwości agenta mostu Connect:Direct .

O tym zadaniu

Te kroki zawierają instrukcje dotyczące pobierania kluczy podpisanych przez ośrodek certyfikacji. Jeśli nie korzystasz z ośrodka certyfikacji, możesz wygenerować certyfikat samopodpisany. Więcej informacji na temat generowania samopodpisanego certyfikatu można znaleźć w sekcji “Praca z protokołem SSL/TLS w systemie UNIX, Linux, and Windows” na stronie 294.

Te kroki zawierają instrukcje dotyczące tworzenia nowego magazynu kluczy i magazynu zaufanych certyfikatów dla agenta mostu Connect:Direct . Jeśli agent mostu Connect:Direct ma już magazyn kluczy i magazyn zaufanych certyfikatów używany do bezpiecznego połączenia z menedżerami kolejek produktu IBM MQ , można użyć istniejącego magazynu kluczy i magazynu zaufanych certyfikatów podczas łączenia się bezpiecznie z węzłem produktu Connect:Direct . Aby uzyskać więcej informacji, zapoznaj się z sekcją: “Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT” na stronie 571.

Procedura

W przypadku węzła Connect:Direct wykonaj następujące kroki:

1. Wygeneruj klucz i podpisany certyfikat dla węzła Connect:Direct .

Można to zrobić za pomocą narzędzia IBM Key Management, które jest dostarczane razem z produktem IBM MQ. Więcej informacji na ten tematzawiera sekcja “Praca z protokołem SSL/TLS” na stronie 282.

2. Wyślij żądanie do ośrodka certyfikacji, aby mieć podpisany klucz. Otrzymujesz certyfikat w zamian.
3. Utwórz plik tekstowy, na przykład `/test/ssl/certs/CAcert`, który zawiera klucz publiczny ośrodka certyfikacji.
4. Zainstaluj opcję Secure + Option w węźle produktu Connect:Direct .

   Jeśli węzeł już istnieje, można zainstalować opcję Secure + Option, uruchamiając ponownie instalator, określając położenie istniejącej instalacji i wybierając opcję "Secure + Option".
5. Utwórz nowy plik tekstowy, na przykład `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.
6. Skopiuj odebrany certyfikat z ośrodka certyfikacji i klucz prywatny, który znajduje się w `/test/ssl/cd/privateKeys/`*node_name*`.key`, do pliku tekstowego.

   Zawartość pliku `/test/ssl/cd/keyCertFile/`*node_name*`.txt` musi mieć następujący format:

```
-----BEGIN CERTIFICATE-----
MIICnzCCAgigAwIBAgIBGjANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJHQjES
MBAGA1UECBMJSGFtcHNoaXJlMRAwDgYDVQQHEwdIdXJzbGV5MQwwCgYDVQQKEwNJ
Qk0xDjAMBgNVBAsTBU1RSVBUMQswCQYDVQQDEwJDQTAeFw0xMTAzMDExNjIwNDZa
Fw0yMTAyMjYxNjIwNDZaMFAxCzAJBgNVBAYTAkdCMRIwEAYDVQQIEwlIYW1wc2hp
cmUxDDAKBgNVBAoTA0lCTTEOMAwGA1UECxMFTVFGVEUxDzANBgNVBAMTBmJpbmJh
ZzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvgP1QIklU9ypSKD1XoODo1yk
EyMFXBOUpZRrDVxjoSEC0vtWNcJ199e+Vc4UpNybDyBu+NkDlMNofX4QxeQcLAFj
WnhakqCiQ+JIAD5AurhnrwChe0MV3kjA84GKH/rOSVqtl984mu/lDyS819XcfSSn
cOOMsK1KbneVSCIV2XECAwEAAaN7MHkwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0E
HxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFNXMIpSc
csBXUniW4A3UrZnCRsv3MB8GA1UdIwQYMBaAFDXY8rmj4lVz5+FVAoQb++cns+B4
MA0GCSqGSIb3DQEBBQUAA4GBAFc7klXa4pGKYgwchxKpE3ZF6FNwy4vBXS216/ja
8h/vl8+iv01OCL8t0ZOKSU95fyZLzOPKnCH7v+ItFSE3CIiEk9Dlz2U6WO9lICwn
l7PL72TdfaL3kabwHYVf17IVcuL+VZsZ3HjLggP2qHO9ZuJPspeT9+AxFVMLiaAb
8eHw
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,64A02DA15B6B6EF9

57kqxLOJ/gRUOIQ6hVK2YN13B4E1jAi1gSme0I5ZpEIG8CHXISKB7/0cke2FTqsV
lvI99QyCxsDWoMNt5fj51v7aPmVeS60bOm+UlGre8B/Ze18JVj2O4K2Uh72rDCXE
5e6eFxSdUM207sQDy20euBVELJtM2kOkL1ROdoQQSlU3XQNgJw/t3ZIx5hPXWEQT
rjRQO64BEhb+PzzxPF8uwzZ9IrUK9BJ/UUnqC6OdBR87IeA4pnJD1Jvb2ML7EN9Z
5Y+50hTKI8OGvBvWXO4fHyvIX5aslwhBoArXIS1AtNTrptPvoaP1zyIAeZ6OCVo/
SFo+A2UhmtEJeOJaZG2XZ3H495fAw/EHmjehzIACwukQ9nSIETgu4A1+CV64RJED
aYBCM8UjaAkbZDH5gn7+eBov0ssXAXWDyJBVhUOjXjvAj/e1h+kcSF1hax5D//AI
66nRMZzboSxNqkjcVd8wfDwP+bEjDzUaaarJTS7lIFeLLw7eJ8MNAkMGicDkycL0
EPBU9X5QnHKLKOfYHN/1WgUk8qt3UytFXXfzTXGF3EbsWbBupkT5e5+lYcX8OVZ6
sHFPNlHluCNy/riUcBy9iviVeodX8IomOchSyO5DKl8bwZNjYtUP+CtYHNFU5BaD
I+1uUOAeJ+wjQYKT1WaeIGZ3VxuNITJul8y5qDTXXfX7vxM5OoWXa6U5+AYuGUMg
/itPZmUmNrHjTk7ghT6i1IQOaBowXXKJBlMmq/6BQXN2IhkD9ys2qrvM1hdi5nAf
egmdiG50loLnBRqWbfR+DykpAhK4SaDi2F52Uxovw3Lhiw8dQP7lzQ==
-----END RSA PRIVATE KEY-----
```

7. Uruchom narzędzie administracyjne (Secure + Admin Tool).

   - W systemach Linux lub UNIX uruchom komendę **spadmin.sh**.
   - W systemach Windows należy kliknąć opcję **Start** > **Programy** > **Sterling Commerce Connect:Direct** > **CD Secure + Admin Tool** .

   Zostanie uruchomiony program CD Secure + Admin Tool.
8. W narzędziu CD Secure + Admin Tool kliknij dwukrotnie ikonę **.Lokalna** , aby edytować ustawienia głównego protokołu SSL lub TLS.

   a) Wybierz opcję **Włącz protokół SSL** lub **Włącz protokół TLS**, w zależności od używanego protokołu.

   b) Wybierz opcję **Wyłącz nadpisywanie**.

   c) Wybierz co najmniej jeden zestaw algorytmów szyfrowania.

   d) Jeśli wymagane jest uwierzytelnianie dwukierunkowe, należy zmienić wartość opcji **Włącz uwierzytelnianie klienta** na wartość `Yes`.

e) W polu **Zaufany certyfikat główny** wprowadź ścieżkę do publicznego pliku certyfikatu ośrodka certyfikacji, `/test/ssl/certs/CAcert`.

f) W polu **Key Certificate File** (Plik certyfikatu klucza) wprowadź ścieżkę do utworzonego pliku `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.

9. Kliknij dwukrotnie ikonę **.Klient** służy do edytowania głównych ustawień protokołu SSL lub TLS.

a) Wybierz opcję **Włącz protokół SSL** lub **Włącz protokół TLS**, w zależności od używanego protokołu.

b) Wybierz opcję **Wyłącz nadpisywanie**.

W przypadku agenta mostu Connect:Direct wykonaj następujące kroki:

10. Utwórz magazyn zaufanych certyfikatów. Można to zrobić, tworząc fikcyjny klucz, a następnie usuwając klucz fikcyjny.

Można użyć następujących komend:

```
keytool -genkey -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

```
keytool -delete -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

11. Zaimportuj certyfikat publiczny ośrodka certyfikacji do magazynu zaufanych certyfikatów.

Można użyć następującej komendy:

```
keytool -import -trustcacerts -alias myCA
        -file /test/ssl/certs/CAcert
        -keystore /test/ssl/fte/stores/truststore.jks
```

12. Edytuj plik właściwości agenta mostu Connect:Direct .

Uwzględnij następujące wiersze w dowolnym miejscu pliku:

```
cdNodeProtocol=protocol
cdNodeTruststore=/test/ssl/fte/stores/truststore.jks
cdNodeTruststorePassword=password
```

W przykładzie w tym kroku *protokół* jest protokołem, który jest używany, albo SSL, albo TLS, a *hasło* jest hasłem podanym podczas tworzenia magazynu zaufanych certyfikatów.

13. Jeśli uwierzytelnianie ma być dwukierunkowe, należy utworzyć klucz i certyfikat dla agenta mostu Connect:Direct .

a) Utwórz magazyn kluczy i klucz.

Można użyć następującej komendy:

```
keytool -genkey -keyalg RSA -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -validity 365
```

b) Wygeneruj żądanie podpisania.

Można użyć następującej komendy:

```
keytool -certreq -v -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks -storepass password
        -file /test/ssl/fte/requests/agent_name.request
```

c) Zaimportuj certyfikat otrzymany z poprzedniego kroku do magazynu kluczy. Certyfikat musi być w formacie x.509 .

Można użyć następującej komendy:

```
keytool -import -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -file certificate_file_path
```

d) Edytuj plik właściwości agenta mostu Connect:Direct .

Uwzględnij następujące wiersze w dowolnym miejscu pliku:

```
cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
cdNodeKeystorePassword=password
```

W przykładzie podanym w tym kroku *hasło* jest hasłem podanym podczas tworzenia magazynu kluczy.

Zadania pokrewne

Konfigurowanie mostu Connect:Direct

ULW Zabezpieczanie klientów AMQP

Użytkownik korzysta z szeregu mechanizmów zabezpieczeń do zabezpieczania połączeń z klientami AMQP i zapewnia, że dane są odpowiednio chronione w sieci. Zabezpieczenia można budować w aplikacjach MQ Light . Istnieje również możliwość użycia istniejących funkcji zabezpieczeń produktu IBM MQ z klientami AMQP w taki sam sposób, w jaki funkcje są używane dla innych aplikacji.

Reguły uwierzytelniania kanału (CHLAUTH)

Istnieje możliwość użycia reguł uwierzytelniania kanału w celu ograniczenia połączeń TCP do menedżera kolejek. Kanały AMQP obsługują korzystanie z reguł uwierzytelniania kanału, które są konfigurowane dla menedżera kolejek. Jeśli reguły uwierzytelniania kanału są zdefiniowane z profilem, który jest zgodny z dowolnymi kanałami AMQP w menedżerze kolejek, reguły te są stosowane do tych kanałów. Domyślnie uwierzytelnianie kanału jest włączone w nowych menedżerach kolejek produktu IBM® MQ , dlatego przed użyciem kanału AMQP należy wykonać co najmniej niektóre czynności konfiguracyjne.

Więcej informacji na temat konfigurowania reguł uwierzytelniania kanału w celu zezwolenia na połączenia AMQP z menedżerem kolejek można znaleźć w sekcji Tworzenie i używanie kanałów AMQP.

Uwierzytelnianie połączenia (CONNAUTH)

Uwierzytelniania połączenia można używać do uwierzytelniania połączeń z menedżerem kolejek. Kanały AMQP obsługują korzystanie z uwierzytelniania połączenia w celu kontrolowania dostępu do menedżera kolejek z aplikacji AMQP.

Protokół AMQP korzysta ze środowiska SASL (Simple Authentication and Security Layer) w celu określenia sposobu uwierzytelniania połączenia. Istnieją różne mechanizmy SASL, a produkt IBM MQ obsługuje dwa mechanizmy SASL: ANONYMOUS i PLAIN.

W przypadku wartości ANONYMOUS żadne informacje autoryzacyjne nie są przekazywane z klienta do menedżera kolejek w celu uwierzytelnienia. Jeśli obiekt MQ AUTHINFO określony w atrybucie CONNAUTH ma wartość CHCKCLNT REQUIRED lub REQDADM (jeśli nawiąże połączenie jako użytkownik administracyjny), to połączenie jest odrzucane. Jeśli wartością parametru CHCKCLNT jest NONE lub OPTIONAL, połączenie jest akceptowane.

W przypadku AIN, nazwa użytkownika i hasło są przekazywane z klienta do menedżera kolejek w celu uwierzytelnienia. Jeśli obiekt MQ AUTHINFO określony w atrybucie CONNAUTH ma wartość CHCKCLNT NONE, oznacza to, że połączenie zostało odrzucone. Jeśli wartością parametru CHCKCLNT jest OPTIONAL, REQUIRED lub REQDADM (w przypadku łączenia się jako użytkownik administracyjny), nazwa użytkownika i hasło są sprawdzane przez menedżer kolejek. Menedżer kolejek sprawdza system operacyjny (jeśli obiekt AUTHINFO jest obiektem typu IDPWOS) lub repozytorium LDAP (jeśli obiekt AUTHINFO jest typu IDPWLDAP).

Poniższa tabela zawiera podsumowanie tego działania uwierzytelniania:

Tabela 95. Podsumowanie mechanizmów SASL i uwierzytelnianie połączenia		
Mechanizm SASL	**Referencje przekazane od klienta do menedżera kolejek?**	**CHKCLNT, wartość**
anonimowe	Nie	REQUIRED lub REQDADM-odmowa połączenia NONE lub OPTIONAL-zaakceptowano połączenie
Zwykły tekst	Tak, nazwa użytkownika i hasło	Wymagane, REQDADM lub OPTIONAL-nazwa użytkownika i hasło sprawdzone przez menedżer kolejek NONE-odmowa połączenia

Jeśli używany jest klient MQ Light , można określić referencje, uwzględniając je w adresie AMQP, z którym nawiążesz połączenie, na przykład:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

Ustawienie MCAUSER na kanale

Kanały AMQP mają atrybut MCAUSER, którego można użyć do ustawienia identyfikatora użytkownika produktu IBM MQ , pod którym są autoryzowane wszystkie połączenia z tym kanałem. Wszystkie połączenia klientów AMQP z tym kanałem przyjmują skonfigurowany identyfikator MCAUSER. Ten identyfikator użytkownika jest używany do autoryzacji przesyłania komunikatów na różnych tematach.

Zaleca się użycie uwierzytelniania kanału (CHLAUTH) w celu zabezpieczenia połączeń z menedżerami kolejek. Jeśli używane jest uwierzytelnianie kanału, zalecane jest skonfigurowanie wartości parametru MCAUSER dla użytkownika nieuprawnionego. Dzięki temu, jeśli połączenie z kanałem nie jest zgodne z regułą CHLAUTH, to połączenie nie jest autoryzowane do wykonywania żadnych komunikatów w menedżerze kolejek.

Uwaga: Windows W systemie Windows, przed IBM MQ 9.1.1, ustawienie ID użytkownika MCAUSER jest obsługiwane tylko dla identyfikatorów użytkowników o długości do 12 znaków.

V 9.1.1 Od wersji IBM MQ 9.1.1 ten limit 12 znaków został usunięty.

Obsługa protokołu SSL/TLS

Kanały AMQP obsługują szyfrowanie SSL/TLS przy użyciu kluczy z repozytorium kluczy skonfigurowanego dla menedżera kolejek. Opcje konfiguracyjne kanału AMQP dla szyfrowania SSL/TLS obsługują te same opcje, co inne typy kanału MQ . Można określić specyfikację szyfru oraz to, czy menedżer kolejek wymaga certyfikatów z połączeń klienta AMQP.

Za pomocą atrybutów FIPS menedżera kolejek można sterować zestawami algorytmów szyfrowania SSL/TLS, które mogą być używane do zabezpieczania połączeń klientów AMQP.

Więcej informacji na temat konfigurowania repozytorium kluczy dla menedżera kolejek zawiera sekcja Praca z protokołem SSL lub TLS w systemach UNIX, Linux i Windows.

Informacje na temat konfigurowania obsługi protokołu SSL/TLS dla połączenia klienta AMQP można znaleźć w sekcji Tworzenie i używanie kanałów AMQP.

Java Authentication and Authorization Service (JAAS)

Opcjonalnie można skonfigurować kanały AMQP przy użyciu modułu logowania JAAS , który może sprawdzić nazwę użytkownika i hasło udostępnione przez klienta AMQP. Patrz sekcja “Konfigurowanie usługi JAAS dla kanałów AMQP” na stronie 579.

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie kanałów AMQP i korzystanie z nich

ULW Ograniczanie przejmowania klienta AMQP

Gdy połączenie klienta AMQP jest nawiązane z tym samym identyfikatorem klienta co istniejące połączenie klienta AMQP, to istniejące połączenie klienta jest domyślnie rozłączone. Można jednak skonfigurować menedżer kolejek w taki sposób, aby ograniczał zachowanie związane z przejęciem klienta, tak aby przejęcie było możliwe tylko wtedy, gdy spełnione są określone kryteria.

Na przykład odłączenie istniejącego połączenia klienckiego może nie być odpowiednie, jeśli istnieją aplikacje AMQP opracowywane przez różne zespoły i zdarzają się, że korzystają z tego samego identyfikatora klienta. Aby rozwiązać ten problem, można ograniczyć przejęcie klienta na podstawie nazwy używanego kanału AMQP, adresu IP klienta oraz identyfikatora użytkownika klienta (gdy uwierzytelnianie SASL jest włączone).

Użyj ustawień atrybutów menedżera kolejek **AdoptNewMCA** i **AdoptNewMCACheck** , aby określić wymagany poziom ograniczenia przejęcia klienta zgodnie z opisem w poniższej tabeli:

*Tabela 96. Ustawienia **AdoptNewMCA** i **AdoptNewMCACheck** w celu ograniczenia przejmowania klientów*

AdoptNewMCA	**AdoptNewMCACheck**	**Kryteria sprawdzane przed przejęciem klienta są dozwolone**
NIE lub niezdefiniowane	Nie dotyczy	Brak. Przejęcie klienta jest dozwolone dla wszystkich połączeń klienckich, które są uwierzytelniane i przekazują wszystkie reguły CHLAUTH.
ALL (lub wartość inna niż NO)	QM lub niezdefiniowana	Brak. Przejęcie klienta jest dozwolone dla wszystkich połączeń klienckich, które są uwierzytelniane i przekazują wszystkie reguły CHLAUTH.
ALL (lub wartość inna niż NO)	NAZWA	ID użytkownika (po włączeniu SASL) Nazwa kanału
ALL (lub wartość inna niż NO)	ADDRESS	ID użytkownika (po włączeniu SASL) Adres IP
ALL (lub wartość inna niż NO)	ALL	ID użytkownika (po włączeniu SASL) Nazwa kanału Adres IP

Atrybuty menedżera kolejek **AdoptNewMCA** i **AdoptNewMCACheck** są częścią konfiguracji menedżera kolejek, która jest zdefiniowana w sekcji CHANNELS. W systemie IBM MQ dla systemów Windows i IBM

MQ dla systemów Linux x86-64 należy zmodyfikować informacje konfiguracyjne przy użyciu IBM MQ Explorer. W innych systemach należy zmodyfikować informacje, edytując plik konfiguracyjny `qm.ini` . Informacje na temat modyfikowania informacji o kanałach menedżera kolejek można znaleźć w sekcji Atrybuty kanałów.

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie kanałów AMQP i korzystanie z nich

ULW Konfigurowanie usługi JAAS dla kanałów AMQP

Moduły niestandardowe Java Authentication and Authorization Service (JAAS) mogą być używane do uwierzytelniania referencji nazwy użytkownika i hasła przekazywanych do kanału AMQP przez klienta AMQP, gdy jest on połączony.

O tym zadaniu

Niestandardowy moduł JAAS może być używany, jeśli moduły JAAS są już używane do uwierzytelniania w innych systemach opartych na języku Java, a użytkownik chce ponownie wykorzystać te moduły w celu uwierzytelniania połączeń AMQP z produktem MQ. Alternatywnie można napisać niestandardowy moduł JAAS , jeśli funkcje uwierzytelniania wbudowane w produkt MQ nie obsługują mechanizmu uwierzytelniania, który ma być używany.

Konfiguracja modułów JAAS dla kanałów AMQP jest wykonywana na poziomie menedżera kolejek. Oznacza to, że jeśli konfigurowany jest moduł JAAS do uwierzytelniania połączeń AMQP z menedżerem kolejek, moduł będzie miał zastosowanie do wszystkich kanałów AMQP. Nazwa kanału, który wywołał moduł JAAS , jest przekazywany do modułu, co pozwala na zakodowanie różnych dzienników JAAS w zachowaniu różnych kanałów.

Inne informacje są również przekazywane do modułu JAAS :

- Identyfikator klienta klienta AMQP, który próbuje uwierzytelnić się.
- Adres sieciowy klienta AMQP.
- Nazwa kanału, który wywołał moduł JAAS .

Procedura

Aby skonfigurować moduł konfiguracji JAAS dla kanałów AMQP, należy wykonać następujące kroki:

1. Zdefiniuj plik `jaas.config` zawierający jedną lub większą liczbę sekcji konfiguracji modułu JAAS . W sekcji należy podać pełną nazwę klasy Java implementujący interfejs JAAS `javax.security.auth.spi.LoginModule` .
   - Z produktem dostarczany jest domyślny plik `jaas.config` , który znajduje się w katalogu *QM_data_directory*`/amqp/jaas.config`.
   - Wstępnie skonfigurowana sekcja o nazwie `MQXRConfig` jest już zdefiniowana w domyślnym pliku `jaas.config` .
2. Podaj nazwę sekcji, która ma być używana dla kanałów AMQP.
   - UNIX Dodaj właściwość do pliku `amqp_unix.properties` .
   - Windows Dodaj właściwość do pliku `amqp_win.properties` .

   Właściwość ma następującą postać:

   ```
   com.ibm.mq.MQXR.JAASConfig=JAAS_stanza_name
   ```

   Na przykład:

```
com.ibm.mq.MQXR.JAASConfig=MQXRConfig
```

3. Skonfiguruj środowisko menedżera kolejek w taki sposób, aby uwzględniał klasę modułu niestandardowego. Usługa AMQP musi mieć dostęp do klasy Java skonfigurowanej w sekcji konfiguracji JAAS .

   W tym celu należy dodać ścieżkę do klasy JAAS do pliku `service.env` produktu MQ . Edytuj plik `service.env` w katalogu konfiguracyjnym MQ (*katalog_konfiguracji_produktu_MQ*) lub w katalogu konfiguracji menedżera kolejek (*QM_config_directory*), aby ustawić zmienną CLASSPATH na położenie klasy modułu JAAS .

Co dalej

Przykładowy moduł logowania JAAS jest dostarczany razem z produktem w katalogu *mq_installation_directory*`/amqp/samples` . Przykładowy moduł logowania JAAS uwierzytelnia wszystkie połączenia klientów, niezależnie od nazwy użytkownika lub hasła, z którymi łączy się klient.

Można zmodyfikować kod źródłowy przykładu i zrekompilować go, aby spróbować uwierzytelniać tylko konkretnych użytkowników z określonym hasłem. Aby skonfigurować kanał AMQP w systemie UNIX do używania przykładowego modułu logowania JAAS dostarczanego razem z produktem:

1. Zmodyfikuj plik `/var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties` i ustaw właściwość `com.ibm.mq.MQXR.JAASConfig=MQXRConfig`.
2. Otwórz do edycji plik /var/mqm/service.env i ustaw właściwość CLASSPATH=*mq_installation_location*`/amqp/samples` .

Plik `jaas.config` zawiera już sekcję o nazwie `MQXRConfig` , która określa przykładową klasę `samples.JAASLoginModule` jako klasę modułu logowania. Przed próbą wykonania przykładowego modułu nie są wymagane żadne zmiany produktu `jaas.config` .

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie kanałów AMQP i korzystanie z nich

Advanced Message Security

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

Przegląd produktu Advanced Message Security

Aplikacje produktu IBM MQ mogą używać produktu 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 GSKit używane w komunikatach AMS

Funkcje i funkcje produktu Advanced Message Security

Produkt Advanced Message Security rozszerza usługi zabezpieczeń produktu IBM MQ , aby zapewnić podpisywanie danych i szyfrowanie na poziomie komunikatu. Rozszerzone usługi gwarantują, że dane komunikatu nie zostały zmodyfikowane między oryginalnie umieszczonym w kolejce a tym, kiedy jest on pobierany. Ponadto program AMS sprawdza, czy nadawca danych komunikatu ma uprawnienia do umieszczania podpisanych komunikatów w kolejce docelowej.

Produkt AMS udostępnia następujące funkcje:

- Zabezpieczy transakcje wrażliwe lub o wysokiej wartości przetworzone przez produkt IBM 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 IBM MQ.
- z/OS V 9.1.3 W produkcie IBM MQ 9.1.3produkt IBM MQ for z/OS umożliwia opcjonalne usuwanie i dodawanie zabezpieczeń AMS z lub do komunikatów, które przepływa przez sieć. Jest on znany jako *Intercepcja agenta kanału komunikatów serwera (MCA).*.
- ULW V 9.1.0.4 V 9.1.4 W przypadku produktów IBM MQ 9.1.4 i IBM MQ 9.1.0 Fix Pack 4do kodu biblioteki produktu IBM MQ , który jest uruchamiany w ramach aplikacji klienta, dodano sprawdzenie. Sprawdzenie jest uruchamiane na wczesnym etapie inicjowania w celu odczytania wartości zmiennej środowiskowej *AMQ_AMS_FIPS_OFF* , a jeśli jest ona ustawiona na dowolną wartość, to kod GSKit zostanie uruchomiony w trybie bez trybu FIPS w tej aplikacji.

Właściwości ochrony dostępne w produkcie AMS

Istnieją trzy właściwości ochrony dla produktów Advanced Message Security, `Integrity`, `Privacy`i `Confidentiality`.

Ochrona `Integrity` jest zapewniana przez podpisywanie cyfrowe, które zapewnia pewność, kto utworzył wiadomość, oraz że wiadomość nie została zmieniona ani nie została naruszona.

Ochrona systemu `Privacy` jest zapewniana przez połączenie cyfrowego podpisywania i szyfrowania. Szyfrowanie zapewnia, że dane komunikatu mogą być widoczne tylko dla zamierzonego odbiorcy lub odbiorców. Nawet jeśli nieautoryzowani odbiorcy uzyskują kopię zaszyfrowanych danych wiadomości, nie są w stanie wyświetlić samych danych komunikatu.

Ochrona `Confidentiality` jest zapewniana przez szyfrowanie tylko przy użyciu opcjonalnego klucza ponownego wykorzystania.

Wpływ na wydajność

Produkt AMS używa kombinacji procedur kryptograficznych symetrycznych i asymetrycznych w celu zapewnienia cyfrowego podpisywania i szyfrowania. Ponieważ kluczowe operacje klucza symetrycznego są bardzo szybkie w porównaniu z operacjami klucza asymetrycznego, które są intensywnie obciążające procesor, to z kolei może mieć istotny wpływ na koszty ochrony dużej liczby komunikatów za pomocą produktu AMS.

Procedury kryptograficzne asymetryczne

Na przykład przy umieszczaniu podpisanego komunikatu mieszanie komunikatów jest podpisywane przy użyciu operacji klucza asymetrycznego.

Podczas pobierania podpisanego komunikatu używana jest dalsza asymetryczna operacja klucza w celu zweryfikowania podpisanego komunikatu mieszającego.

Dlatego do podpisywania i weryfikowania danych komunikatu wymagane jest co najmniej dwie asymetryczne operacje kluczowe na komunikat.

Procedury kryptograficzne asymetryczne i symetryczne

Podczas umieszczania zaszyfrowanego komunikatu klucz symetryczny jest generowany, a następnie szyfrowany przy użyciu operacji klucza asymetrycznego dla każdego zamierzonego odbiorcy komunikatu.

Dane komunikatu są następnie szyfrowane za pomocą klucza symetrycznego. Podczas pobierania zaszyfrowanego komunikatu odbiorca musi użyć operacji klucza asymetrycznego, aby wykryć klucz symetryczny w użyciu dla komunikatu.

Wszystkie trzy zalety ochrony zawierają różne elementy operacji o asymetrycznej asymetrycznej pracy procesora, co znacząco wpływa na maksymalny możliwy do osiągnięcia szybkość przesyłania komunikatów dla aplikacji umieszczających i pobierających komunikaty.

Strategie produktu `Confidentiality` zezwalają jednak na ponowne wykorzystanie klucza symetrycznego w sekwencji komunikatów. Znaczne oszczędności w zakresie kosztów procesora mogą być dokonywane za pomocą strategii `Confidentiality` za pomocą symetrycznego klucza ponownego wykorzystania. Ten tryb działania nadal korzysta z formatu PKCS#7 w celu współużytkowania symetrycznego klucza szyfrowania. Nie istnieje jednak podpis cyfrowy, który eliminuje niektóre operacje klucza asymetrycznego komunikatu na komunikat. Klucz symetryczny nadal musi być szyfrowany za pomocą asymetrycznych operacji kluczowych dla każdego odbiorcy, ale klucz symetryczny może być opcjonalnie ponownie wykorzystany w wielu komunikatach przeznaczonych dla tych samych odbiorców. Jeśli ponowne wykorzystanie klucza jest dozwolone przez strategię, to tylko pierwszy komunikat wymaga operacji klucza asymetrycznego. Kolejne komunikaty muszą używać tylko operacji klucza symetrycznego.

Ponowne wykorzystanie klucza

W przypadku strategii produktu `Confidentiality` można użyć metody ponownego wykorzystania klucza symetrycznego w celu znacznego zmniejszenia kosztów związanych z szyfrowaniem pewnej liczby komunikatów umieszczonych w tej samej kolejce i przeznaczonych dla tego samego odbiorcy lub odbiorców.

Na przykład podczas umieszczania 10 zaszyfrowanych wiadomości do tego samego zestawu odbiorców generowany jest klucz symetryczny, a następnie szyfrowany dla pierwszego komunikatu, przy użyciu operacji klucza asymetrycznego dla każdego zamierzonego odbiorcy komunikatu.

Zaszyfrowany klucz symetryczny może być następnie ponownie wykorzystywany przez kolejne komunikaty, które są przeznaczone dla tych samych adresatów, jeśli są one sterowane przez strategie. Aplikacja, która pobiera zaszyfrowane wiadomości, może zastosować tę samą optymalizację, ponieważ aplikacja może wykryć, kiedy klucz symetryczny nie uległ zmianie i uniknąć wydatków związanych z pobieraniem klucza symetrycznego.

W tym przykładzie 90% operacji klucza asymetrycznego można uniknąć zarówno przez wprowadzenie, jak i pobieranie aplikacji za pomocą ponownego użycia tego samego klucza.

Więcej informacji na temat korzystania z ponownego wykorzystania klucza można znaleźć w sekcji:

- Komenda MQSC SET POLICY
- Komenda sterująca setmqspl
- IBM i Komenda IBM i SETMQMSPL

Kluczowe pojęcia w produkcie AMS

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 i Advanced Message Security

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 627
W celu zapewnienia przezroczystej ochrony kryptograficznej aplikacjom produktu IBM MQ produkt Advanced Message Security korzysta z pliku kluczy, w którym przechowywane są certyfikaty klucza publicznego i klucz prywatny. W systemie z/OSzamiast pliku kluczy używany jest plik kluczy SAF.

Certyfikaty cyfrowe w produkcie AMS

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 produkcie Java , jak i w aplikacjach rodzimych.

Pojęcia pokrewne

“Kryptografia” na stronie 7
Kryptografia to proces przekształcania tekstu w formie czytelnej, o nazwie *plaintext*i postaci nieczytelnej, o nazwie *ciphertext*.

Multi *Menedżer uprawnień do obiektów*

W przypadku wielu platform menedżer uprawnień do obiektów (Object Authority Manager-OAM) jest komponentem usługi autoryzacji dostarczonym z produktami IBM MQ .

Dostęp do obiektów Advanced Message Security jest kontrolowany za pomocą grup użytkowników IBM 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 (Message Queue Interface). 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

Interfejs kolejki komunikatów-przegląd

Technologia obsługiwana przez produkt Advanced Message Security

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 IBM MQ :

- Message Queue Interface (MQI)
- IBM MQ Java Message Service (JMS) 1.0.2 i 1.1.
- IBM MQ Klasy podstawowe dla Java
- Klasy IBM MQ dla. Net w trybie niezarządzanym

Uwaga: Produkt Advanced Message Security obsługuje uprawnienia do certyfikatów zgodnych ze standardem X.509 .

Znane ograniczenia produktu AMS

Istnieje wiele opcji produktu IBM MQ , które nie są obsługiwane lub mają ograniczenia dotyczące produktu Advanced Message Security.

- Następujące opcje produktu IBM MQ nie są obsługiwane lub mają ograniczenia:

  Publikowanie/subskrypcja
  Jedną z głównych zalet modelu przesyłania komunikatów w trybie publikowania/subskrypcji w punkcie punkt z punktem jest to, że aplikacje wysyłający i odbierający nie muszą wiedzieć nic o sobie nawzajem, aby dane były wysyłane i odbierane. Korzyści te są negowane przy użyciu strategii produktu Advanced Message Security , które muszą definiować zamierzonych odbiorców lub autoryzowanych osób podpisujących. Aplikacja może publikować w temacie przy użyciu definicji kolejki aliasowej, która jest chroniona przez strategię. Możliwe jest również, aby aplikacja subskrybująca otrzymała komunikaty z kolejki chronionej strategii. Nie można przypisać strategii bezpośrednio do łańcucha tematu, strategie mogą być przypisane tylko do definicji kolejek.

  Konwersja danych kanału
  Zabezpieczony ładunek zabezpieczonego komunikatu produktu Advanced Message Security jest przesyłany za pomocą formatu binarnego, co zapewnia, że konwersja danych w kanale między aplikacjami nie spowoduje unieważnienia skrótu komunikatu. Aplikacje pobierające komunikaty z kolejki chronionej strategii powinny żądać konwersji danych, a próba konwersji chronionego ładunku będzie podejmowana po pomyślnym zweryfikowaniu i niezabezpieczaniu komunikatów.

  Lista dystrybucyjna
  Strategie produktu Advanced Message Security mogą być używane podczas zabezpieczania aplikacji umieszczających komunikaty w listach dystrybucyjnych, pod warunkiem, że każda kolejka docelowa na liście ma zdefiniowaną identyczną strategię. Jeśli podczas otwierania przez aplikację listy dystrybucyjnej zostaną zidentyfikowane niespójne strategie, operacja otwarcia nie powiedzie się, a do aplikacji zostanie zwrócony błąd zabezpieczeń.

Segmentacja komunikatów aplikacji
Wielkość komunikatów chronionych strategii wzrośnie i nie jest możliwe, aby aplikacje precyzyjnie określały granice segmentów komunikatu.

Aplikacje korzystające z produktu IBM MQ classes for .NET w trybie zarządzanym (połączenia klienckie)
Aplikacje korzystające z produktu IBM MQ classes for .NET w trybie zarządzanym (połączenia klienckie) nie są obsługiwane.

Uwaga: Przechwytywanie MCA może być używane w celu umożliwienia nieobsługiwanym klientom korzystania z produktu AMS.

Klient usługi komunikatów dla aplikacji .NET (XMS) w trybie zarządzanym
Klient usługi komunikatów dla aplikacji .NET (XMS) w trybie zarządzanym nie jest obsługiwany.

Uwaga: Przechwytywanie MCA może być używane w celu umożliwienia nieobsługiwanym klientom użycia AMS.

Kolejki IBM MQ przetwarzane przez most IMS
Kolejki IBM MQ przetwarzane przez most IMS nie są obsługiwane.

Uwaga: Produkt AMS jest obsługiwany w kolejkach mostów CICS . Należy użyć tego samego identyfikatora użytkownika do wywołania MQPUT (encrypt) i MQGET (deszyfrowanie) w kolejkach mostów produktu CICS .

Umieść w oczekiwaniu na proces pobierający
Operacja umieszczania w oczekiwaniu nie jest obsługiwana w przypadku aplikacji pobierających dla kolejek, dla których zdefiniowano dla nich strategie AMS .

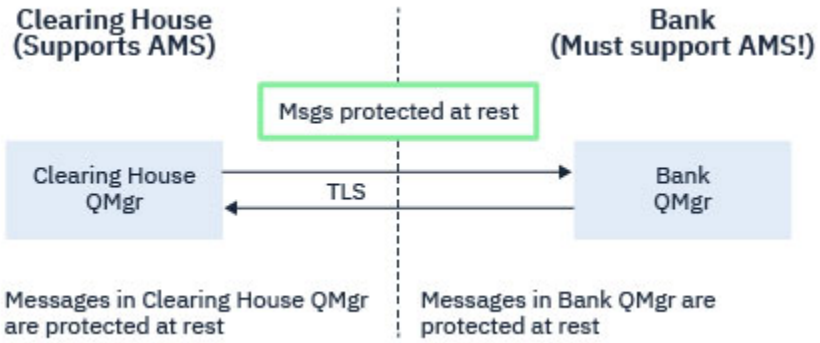
V 9.1.3 **Przechwytywanie serwera MCA serwera z serwerem**
W produkcie IBM MQ 9.1.3na serwerze IBM MQ for z/OSprzechwytywanie serwera MCA serwera z serwerem jest obsługiwane tylko dla typów kanałów nadawcy, serwera, odbiornika i requestera.

- Użytkownicy powinni unikać umieszczania więcej niż jednego certyfikatu o tej samej nazwie wyróżniającej w jednym pliku kluczy, ponieważ wybór certyfikatu, który ma być używany podczas zabezpieczania komunikatu, jest niezdefiniowany.
- Produkt AMS nie jest obsługiwany w produkcie JMS , jeśli właściwość **WMQ_PROVIDER_VERSION** jest ustawiona na wartość 6.
- Przechwytywacz AMS nie jest obsługiwany dla kanałów AMQP lub MQTT.

z/OS V 9.1.3 Przegląd informacji o przechwytywaniu produktu Advanced Message Security w kanałach komunikatów

On z/OS, Advanced Message Security (AMS) interception enhances the existing offering by adding an additional option of security policy protection (SPLPROT) to sender, server, receiver, and requester channels.

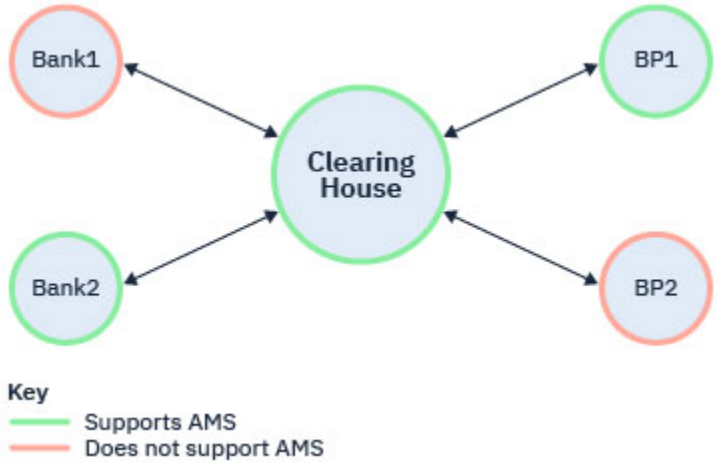
Obecnie, korzystając z przykładu izby rozliczeniowej komunikujących się z bankiem, obie strony systemu muszą obsługiwać AMS, jak pokazano na Rysunku 1.



Rysunek 32. Bieżące użycie AMS

Kluczowymi korzyścią dla dodatkowej opcji jest to, że jeśli w przedsiębiorstwie skonfigurowano produkt AMS , a nie wszyscy partnerzy biznesowi obsługują produkt AMS, można usunąć ochronę z komunikatów wychodzących i chronić komunikaty przychodzące w kanałach do i od tych partnerów biznesowych, które nie obsługują produktu AMS.

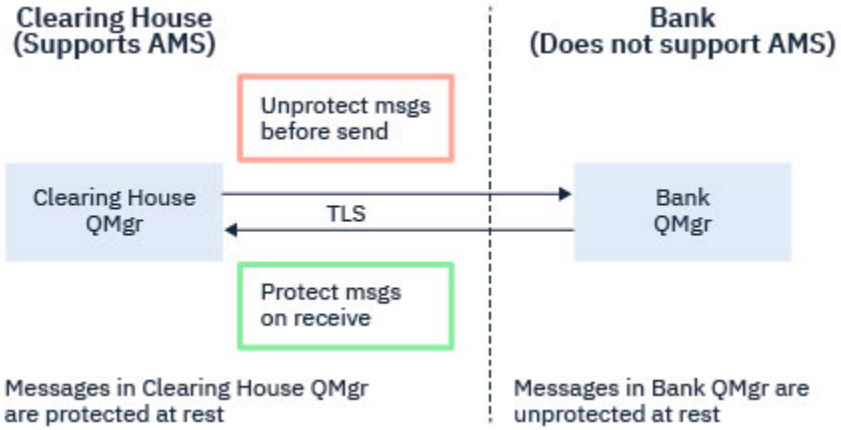
Za pomocą przykładu izby rozliczeniowej i banków scenariusz ten jest przedstawiony na Rysunku 2, w którym znajduje się przepływ komunikatów między izą rozliczeniową, bankami i partnerami biznesowymi, w których niektóre instytucje mają AMS, a inne nie.



Rysunek 33. Niektórzy partnerzy wspierają AMS, a niektórzy nie

Zwykle są to kanały z włączoną obsługą protokołu TLS.

Może jednak istnieć przypadek, w którym niektóre banki i partnerzy biznesowi nie obsługują produktu AMS, a istnieje wymaganie, aby móc wymieniać komunikaty między wszystkimi bankami i partnerami biznesowymi. Ten scenariusz jest przedstawiony na Rysunku 3



Rysunek 34. Przepływ komunikatów między partnerami biznesowymi

Zadania pokrewne

Przykładowe konfiguracje przechwycenia kanału komunikatów serwera z serwerem

z/OS V 9.1.3 *Przechwytywanie AMS w kanałach komunikatów serwer-serwer*

Przechwytywanie kanału komunikatów typu serwer z serwerem umożliwia sterowanie, czy w komunikatach powinny być zastosowane odpowiednie strategie Advanced Message Security (AMS), gdy agenty kanału komunikatów typu wysyłającego mają komunikaty z kolejek transmisji, a agenty kanału komunikatów typu odbiornika umieszczają komunikaty w kolejkach docelowych.

Umożliwia to włączenie zabezpieczeń produktu AMS w menedżerze kolejek podczas komunikowania się, przy użyciu kanałów komunikatów typu serwer-serwer typu nadawca, serwer, odbiornik i requester, z menedżerem kolejek, dla którego nie włączono AMS .

Oznacza to, że zabezpieczone komunikaty AMS w menedżerach kolejek z włączoną obsługą AMS mogą być niechronione przed wysłaniem do menedżerów kolejek z włączoną obsługąAMS , a niezabezpieczone komunikaty odebrane z menedżerów kolejek innych niżAMS mogą być chronione przez odpowiednie strategie produktu AMS w menedżerach kolejek z włączoną obsługą AMS .

Konfigurowanie przechwycenia kanału komunikatów serwera z serwerem

Przechwytywanie kanału komunikatów typu serwer z serwerem jest skonfigurowane za pomocą atrybutu SPLPROT w kanałach z typem kanału nadawcy, serwera, odbiornika lub requestera. Opcje dostępne do skonfigurowania zachowania zależą od podanego typu kanału:

PASSTHRU
: Wszystkie komunikaty wysłane lub odebrane przez agenta kanału komunikatów dla danego kanału są przekazywane bez zmian.

  Ta wartość jest poprawna dla kanałów o typie kanału (**CHLTYPE**) SDR, SVR, RCVR lub RQSTR i jest to wartość domyślna.

REMOVE
: W przypadku wybrania tej wartości cała ochrona AMS będzie usuwana z komunikatów pobieranych przez agent kanału komunikatów z kolejki transmisji przed ich wysłaniem do partnera.

  Gdy agent kanału komunikatów odbierze komunikat z kolejki transmisji, dla której zdefiniowano strategię AMS, zostanie ona zastosowana w celu usunięcia całej ochrony AMS z komunikatu przed wysłaniem go przez kanał. Jeśli dla kolejki transmisji nie zdefiniowano strategii AMS, komunikat zostanie wysłany w niezmienionej formie.

  Ta wartość jest poprawna tylko dla kanałów typu SDR lub SVR.

ASPOLICY

W przypadku wybrania tej wartości względem komunikatów przychodzących będzie stosowana ochrona AMS określana na podstawie strategii zdefiniowanej dla kolejki docelowej przed umieszczeniem ich w kolejce docelowej.

Gdy agent kanału komunikatów odbierze komunikat przychodzący, ochrona AMS zostanie zastosowana dla komunikatu przed umieszczeniem go w kolejce docelowej, jeśli dla kolejki docelowej zdefiniowano strategię AMS. Jeśli dla kolejki docelowej nie zdefiniowano strategii AMS, komunikat zostanie umieszczony w kolejce docelowej w niezmienionej formie.

Ta wartość jest poprawna tylko dla kanałów typu RCVR lub RQSTR.

Identyfikator użytkownika przechwycenia kanału komunikatów

Wymaganie dotyczące identyfikatorów użytkowników używanych z przechwytywaniem kanału komunikatów serwera z serwerem jest takie samo, jak w przypadku istniejących aplikacji z obsługą produktu AMS . W przypadku działającego kanału wysyłający agent kanału komunikatów pobiera komunikaty z kolejki transmisji, a odbierający agent kanału komunikatów umieszcza komunikaty w kolejkach docelowych. Pole Identyfikator użytkownika agenta kanału komunikatów (Message channel user ID-MCAUSER), ustawione na serwerze z kanałami serwera, definiuje ID użytkownika, pod którym agenty kanału komunikatów wykonują żądania umieszczania i pobierania.

W przypadku przechwytywania kanału komunikatów typu serwer z serwerem funkcje produktu AMS są wykonywane podczas pobierania i umieszczania żądań, podobnie jak w przypadku innych aplikacji obsługujących produkt AMS . Oznacza to, że identyfikatory użytkowników agenta kanału komunikatów mają takie same wymagania, jak te dla identyfikatorów użytkowników aplikacji AMS .

Element MCAUSER używany do wykonywania operacji umieszczania i pobierania jest konfigurowalny i zależny od tego, czy jest to kanał danych wychodzących, czy przychodzących. Szczegółowe informacje o tym, jak wybrany ID użytkownika wykonuje działania na agencie kanału komunikatów, zawiera sekcja MCAUSER . Identyfikator użytkownika, który uruchomił inicjator kanału, jest identyfikatorem użytkownika, który ma być używany na potrzeby funkcji AMS wykonywanych podczas przechwytywania kanału komunikatów serwera z serwerem. Z tego powodu te identyfikatory użytkowników mają takie same wymagania, jak te, które są używane dla identyfikatorów użytkowników aplikacji AMS .

Uwierzytelnianie odbywa się za pomocą istniejących reguł dla kanału szczegółowego dla kanałów z konfiguracją PUTAUT. Więcej informacji na ten temat zawiera sekcja Identyfikatory użytkowników używane przez inicjatora kanału .

Uwaga: Przechwytywanie kanału komunikatów typu serwer z serwerem nie uwzględnia wartości atrybutu kanału PUTAUT.

Wielkość komunikatu i MAXMSGL

Ze względu na ochronę produktu AMS wielkość komunikatów chronionych komunikatów będzie większa niż pierwotna wielkość komunikatu.

Komunikaty chronione są większe niż komunikaty niechronione. Dlatego wartość atrybutu **MAXMSGL** w przypadku obu kolejek i kanałów może wymagać zmiany w celu uwzględnienia wielkości chronionych komunikatów.

Odsyłacze pokrewne

Przykładowe konfiguracje przechwycenia kanału komunikatów serwera z serwerem

Obsługa błędów

Program IBM MQ 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-dostęp do nagłówka komunikatu Advanced Message Security (AMS) nie jest możliwy.
- 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 AMS korzysta z systemu SYSTEM.PROTECTION.ERROR.QUEUE jako swoją kolejkę obsługi błędów. Wszystkie komunikaty wprowadzone przez produkt IBM MQ AMS do systemu SYSTEM.PROTECTION.ERROR.QUEUE są poprzedzone nagłówkiem MQDLH.

Administrator produktu IBM MQ może również zdefiniować SYSTEM.PROTECTION.ERROR.QUEUE jako kolejka aliasowa wskazującą inną kolejkę.

z/OS V 9.1.3 W produkcie IBM MQ 9.1.3w systemie IBM MQ for z/OS, jeśli jest używany przechwytywanie agenta kanału komunikatów serwera (MCA), jeśli serwer jest używany:

- Jeśli z jednej z wcześniej podanych przyczyn program IBM MQ AMS przenosi komunikaty z kolejki transmisji do kolejki obsługi błędów, to agent MCA wysyłający po prostu kontynuuje przetwarzanie następnego dostępnego komunikatu w kolejce transmisji.
- Na ogół istniejące reguły kanału mają zastosowanie do następujących elementów:
  - Umieszczanie komunikatów w kolejce niedostarczanych komunikatów, oraz
  - Działania podejmowane w przypadku umieszczania w kolejce niedostarczanych komunikatów nie powinny kończyć się niepowodzeniem.

Więcej informacji na temat konkretnych scenariuszy zawiera sekcja “Niedostarczone komunikaty dla produktu AMS w systemie z/OS” na stronie 589 .

z/OS V 9.1.3 *Niedostarczone komunikaty dla produktu AMS w systemie z/OS*

Konkretne scenariusze związane z przechwytywaniem agenta kanału komunikatów serwera na serwerze IBM MQ for z/OS.

W produkcie IBM MQ 9.1.3w systemie IBM MQ for z/OS, jeśli jest używany przechwytywanie agenta kanału komunikatów serwera (MCA), jeśli serwer jest używany:

- Jeśli po wstaniu i niezabezpieczonym komunikacie nadawca MCA nie dostarczy komunikatu z jakiegoś powodu, na przykład, ponieważ komunikat jest zbyt duży dla kanału, jeśli atrybut kanału nadawczego USEDLQ jest ustawiony na wartość YES, nadawca MCA przenosi komunikat do lokalnej kolejki niedostarczanych komunikatów (DLQ).

  Jeśli SYSTEM.DEAD.LETTER.QUEUE jest używana jako lokalna kolejka DLQ, a komunikat jest umieszczany bez ochrony.

  Uwaga: Program IBM MQ AMS nie obsługuje ochrony komunikatów umieszczanych w kolejkach systemowych.

  Jeśli nazwa DLQ jest używana jako lokalna kolejka DLQ, komunikat zostanie zabezpieczony, jeśli zdefiniowano strategię IBM MQ AMS o takiej samej nazwie jak nazwa DLQ, która nie jest zabezpieczona, jeśli nie zdefiniowano odpowiedniej strategii.
- Jeśli z jakiegoś powodu komunikat nie może zostać umieszczony w lokalnym DLQ, to jeśli parametr NPMSPEED kanału ma wartość NORMAL lub komunikat jest komunikatem trwałym, tworzona jest wycofana bieżąca partia komunikatów, a kanał jest umieszczany w stanie RETRY. W przeciwnym razie

komunikat jest odrzucany, a nadawca MCA kontynuuje przetwarzanie następnego komunikatu w kolejce transmisji.

- Biorąc pod uwagę, że strategie bezpieczeństwa nie mają wpływu na SYSTEM.DEAD.LETTER.QUEUE, lub inne kolejki systemowe wymienione w “Ochrona kolejki systemowej w programie AMS” na stronie 663, jeśli SYSTEM.DEAD.LETTER.QUEUE jest używana, komunikaty umieszczane w tej kolejce przez MCAs są umieszczane w taki sposób, jak jest. Oznacza to, że jeśli wiadomości były wcześniej chronione, są one chronione; w przeciwnym razie są one niezabezpieczone.

  Jeśli atrybut DEADQ menedżera kolejek został ustawiony na nazwę alternatywnej (niesystemowej) kolejki niewysłanych komunikatów, a strategia AMS o takiej samej nazwie nie istnieje, komunikaty umieszczane w tej kolejce przez MCAs są umieszczane w takiej postaci. Oznacza to, że jeśli wiadomości były wcześniej chronione, są one chronione; w przeciwnym razie są one niezabezpieczone.

  Jeśli atrybut DEADQ menedżera kolejek został ustawiony na nazwę alternatywnej (niesystemowej) kolejki niewysłanych komunikatów oraz strategii AMS o takiej samej nazwie, jak nazwa DLQ, strategia ta jest używana do zabezpieczania komunikatów umieszczanych w tej kolejce przez MCAs. Jeśli wiadomość została już wcześniej zabezpieczona, nie jest ona ponownie chroniona. Ma to na celu uniknięcie podwójnej ochrony. Jeśli strategia AMS o takiej samej nazwie nie istnieje, komunikaty są umieszczane w postaci:-jest.
- Jeśli istnieje strategia dla DLQ z opcją tolerowania w komendzie setmqspl ustawioną na wartość off, to znaczy '**-t** O', operacja put to the DLQ nie powiedzie się, jeśli komunikat nie jest zabezpieczony przed AMS , a więc nie ma nagłówka PDMQ. Dzieje się tak wtedy, gdy komunikat dociera do odbiornika bez nagłówka PDMQ. To jest oryginalny program putter komunikatu, który nie ma strategii dla miejsca docelowego, a odbiornik nie ma ustawionego zestawu SPLPROT (ASPOLICY).
- Agent MCA może nie umieścić komunikatu w DLQ, jeśli strategia AMS zdefiniowana dla DLQ nie zezwala na identyfikator użytkownika, który uruchomił inicjator kanału w celu ochrony komunikatu.
- Kanały odbiorcze generalnie umieszczają niedostarczone komunikaty do lokalnego DLQ, podczas gdy kanały nadawcze zazwyczaj umieszczają komunikaty, których nie można przetworzyć z jakiegoś powodu, na przykład zbyt duży komunikat dla kolejki lub błędny nagłówek MQXQH, a więc na lokalny DLQ.
- Procedury obsługi DLQ zwykle patrzą tylko na nagłówek DLQ (DLH), a nie na sam ładunek komunikatu. Dlatego też fakt, że ładunek komunikatu może być chroniony, nie uniemożliwia procedur obsługi od określenia, dlaczego komunikat został umieszczony w kolejce DLQ.
- Jeśli kolejka DLQ nie jest zdefiniowana, kanał:
  - Kończy się nieprawidłowo (i przechodzi w stan ponawiania), jeśli nie można dostarczyć komunikatu trwałego.
  - Usuwa nietrwałe niedostarczone wiadomości i kontynuuje działanie.

Pojęcia pokrewne

“Obsługa błędów” na stronie 588

Program IBM MQ Advanced Message Security definiuje kolejkę obsługi błędów w celu zarządzania komunikatami, które zawierają błędy lub komunikaty, które nie mogą być niechronione.

Scenariusze użytkownika

Zapoznaj się z możliwami scenariuszami, aby zrozumieć, jakie cele biznesowe można osiągnąć za pomocą produktu Advanced Message Security.

Windows *Podręcznik Szybki start dla produktu AMS na platformach Windows*

Ten podręcznik służy do szybkiego konfigurowania produktu 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 MQ dla systemów Windows .

Informacje na temat inicjowania bieżącego środowiska za pomocą komendy **setmqenv** w taki sposób, aby odpowiednie komendy produktu IBM MQ mogły być zlokalizowane i wykonywane przez system operacyjny, należy zapoznać się z informacjami znajdującymi się w sekcji setmqenv (set IBM MQ environment).

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. Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są wprowadzane do infrastruktury produktu IBM MQ przy użyciu standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM MQ i jest skonfigurowana w poniższych krokach.

Za pomocą programu IBM MQ Explorer można utworzyć menedżer kolejek QM_VERIFY_AMS i jego kolejkę lokalną o nazwie TEST.Q , używając wszystkich domyślnych ustawień kreatora, lub użyć komend znalezionych w programie `C:\Program Files\IBM\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 również 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
```

Ostrzeżenie: Program IBM MQ optymalizuje wydajność przez strategie buforowania, dzięki czemu nie będzie konieczne przeglądanie rekordów w celu uzyskania szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Produkt IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Jeśli więc menedżer kolejek ma zdefiniowaną niewielką liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Jednak należy nadać uprawnienie do przeglądania tej kolejki, w przypadku, gdy istnieje duża liczba zdefiniowanych strategii lub jeśli używane są stare klienty. SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach wygenerowanych przez kod AMS. Uprawnienie do umieszczania w tej kolejce jest sprawdzane tylko przy próbie umieszczenia komunikatu o błędzie w kolejce. Uprawnienia użytkownika do umieszczenia w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki chronionej AMS.

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 595.

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 produktu AMS z klientami

Java” na stronie 614). W przypadku wszystkich innych języków oraz w przypadku aplikacji produktu Java korzystających z powiązań lokalnych kroki opisane w tym podręczniku są poprawne.

Procedura

1. Korzystanie z interfejsu GUI programu IBM Key Management (`strmqikm.exe`) , aby utworzyć 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** ; certyfikaty samopodpisane są używane w tym scenariuszu.
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 Advanced Message Security muszą wskazywać przechwytywacze do katalogu, w którym bazy danych kluczy i certyfikaty located.This są wykonywane za pośrednictwem pliku `keystore.conf` , który przechowuje te informacje w postaci zwykłego 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 = 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" (z miejscem na końcu) 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) dla systemu AMS” na stronie 628.
- *%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 627.
- 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/bob/AMS/bobkey.kdb" -pw passw0rd
   -label Bob_Cert -target bob_public.arm

   runmqakm -cert -add -db "C:/Documents and Settings/alice/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.

UNIX *Podręcznik Szybki start dla produktu AMS w systemie UNIX*

Ten podręcznik służy do szybkiego konfigurowania produktu Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów w systemie 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 Global Security Kit IBM
- Advanced Message Security

Nazwy komponentów na poszczególnych platformach można znaleźć w następujących tematach:

- Linux KomponentyIBM MQ dla systemów Linux
- AIX KomponentyIBM MQ dla systemów AIX
- Solaris KomponentyIBM 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. Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są wprowadzane do infrastruktury produktu IBM MQ przy użyciu standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM MQ i jest skonfigurowana w poniższych krokach.

Za pomocą programu IBM MQ Explorer można utworzyć menedżer kolejek QM_VERIFY_AMS i jego kolejkę lokalną o nazwie TEST.Q , używając wszystkich domyślnych ustawień kreatora, lub użyć komend znalezionych w programie *MQ_INSTALLATION_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 również 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
   ```

   Ostrzeżenie: Program IBM MQ optymalizuje wydajność przez strategie buforowania, dzięki czemu nie będzie konieczne przeglądanie rekordów w celu uzyskania szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

   Produkt IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Jeśli więc menedżer kolejek ma zdefiniowaną niewielką liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

   Jednak należy nadać uprawnienie do przeglądania tej kolejki, w przypadku, gdy istnieje duża liczba zdefiniowanych strategii lub jeśli używane są stare klienty. SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach wygenerowanych przez kod AMS. Uprawnienie do umieszczania w tej kolejce jest sprawdzane tylko przy próbie umieszczenia komunikatu o błędzie w kolejce. Uprawnienia użytkownika do umieszczenia w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki chronionej AMS.

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 602.

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 produktu AMS z klientami Java” na stronie 614). W przypadku wszystkich innych języków oraz w przypadku aplikacji produktu Java korzystających z powiązań lokalnych kroki opisane 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) dla systemu AMS” na stronie 628.
- `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 627.

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 `alice`umieść 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 `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` będą zawierać zaszyfrowane dane, które są w kolejce potwierdzające, że komunikat został zaszyfrowany.

z/OS *Przykładowe konfiguracje w systemie z/OS*

W tej sekcji przedstawiono przykładowe konfiguracje strategii i certyfikatów dla scenariuszy kolejkowania produktu Advanced Message Security w systemie z/OS.

Szczegółowe informacje na temat konfigurowania produktu Advanced Message Securityzawiera sekcja Konfigurowanie produktu Advanced Message Security for z/OS .

Przykłady te obejmują wymagane strategie produktu Advanced Message Security oraz certyfikaty cyfrowe, które muszą istnieć względem użytkowników i kluczy. W przykładach założono, że użytkownicy zaangażowani w scenariusze zostały skonfigurowane zgodnie z instrukcjami dostarczonym w sekcji Nadanie uprawnień do zasobów użytkownikom produktu Advanced Message Security.

V 9.1.3 Ponadto, począwszy od wersji IBM MQ 9.1.3 , należy zapoznać się z przykładami przechwytywania kanału komunikatów serwera z serwerem.

z/OS *Lokalne kolejkowanie komunikatów chronionych integralnością w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje na temat strategii i certyfikatów produktu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów zabezpieczonych przed integralnością do kolejki i z kolejki lokalnej w celu ich umieszczania i pobierania.

Przykładowe menedżery kolejek i kolejki to:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Użytkownicy ci są używani:

```
WMQBNK6  - AMS task user
```

```
TELLER5  - Sending user
FINADM2  - Recipient user
```

Tworzenie certyfikatów użytkownika

W tym przykładzie potrzebny jest tylko jeden certyfikat użytkownika. Jest to certyfikat użytkownika wysyłający, który jest potrzebny do podpisywania komunikatów chronionej integralności. Użytkownik wysyłający ma wartość 'TELLER5'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA). Certyfikat ośrodka CA to certyfikat ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, to wszystkie certyfikaty w łańcuchu są wymagane w pliku kluczy użytkownika zadania Advanced Message Security , w tym przypadku użytkownika WMQBNK6.

Certyfikat ośrodka CA można utworzyć za pomocą komendy RACF RACDCERT. Ten certyfikat jest używany do wystawiania certyfikatów użytkownika. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, który następnie może być używany do wydania certyfikatu użytkownika dla użytkownika 'TELLER5'. Na przykład:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Instalacja użytkownika będzie zawierać procedury wyboru lub utworzenia certyfikatu CA, a także procedury wydawania certyfikatów i dystrybucji ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów produkt Advanced Message Security wymaga:

- Certyfikat CA (łańcuch).
- Certyfikat użytkownika i jego klucz prywatny.

Jeśli używany jest produkt RACF, komenda RACDCERT EXPORT może być używana do eksportowania certyfikatów do zestawu danych, a do importowania certyfikatów z zestawu danych można użyć komendy RACDCERT ADD. Więcej informacji na temat tych i innych komend RACDCERT można znaleźć w podręczniku *z/OS: Security Server RACF Command Language Reference*.

Certyfikaty w tym przypadku są wymagane w systemie z/OS z uruchomionym menedżerem kolejek BNK6.

Jeśli certyfikaty zostały zaimportowane w systemie z/OS z uruchomionym BNK6, to certyfikat użytkownika wymaga atrybutu TRUST. Do dodania atrybutu TRUST do certyfikatu można użyć komendy RACDCERT ALTER. Na przykład:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

W tym przykładzie dla użytkownika odbiorcy nie jest wymagany certyfikat.

Połącz certyfikaty z odpowiednimi pierścieniami kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane, i ustawione jako zaufane, muszą być one połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS , na którym działa BNK6. Aby utworzyć pierścienie kluczy, użyj komend RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security (WMQBNK6) oraz pliku kluczy dla użytkownika wysyłającego: 'TELLER5'. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie jest rozróżniana wielkość liter.

Po utworzeniu pierścieni kluczy odpowiednie certyfikaty mogą być połączone:

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Certyfikat użytkownika wysyłającego musi być połączony jako DOMYŚLNY. Jeśli użytkownik wysyłający ma więcej niż jeden certyfikat w pliku drq.ams.keyring, domyślny certyfikat jest używany do podpisywania celów.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez produkt Advanced Message Security , dopóki menedżer kolejek nie zostanie zatrzymany i zrestartowany, albo komenda z/OS **MODIFY** zostanie użyta do odświeżenia konfiguracji certyfikatu produktu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH KEYRING
```

Tworzenie strategii produktu Advanced Message Security

W tym przykładzie komunikaty zabezpieczone przed integralnością są umieszczane w kolejce FIN.XFER.Q7 przez aplikację działającą jako użytkownik 'TELLER5', która została pobrana z tej samej kolejki przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagana jest tylko jedna strategia Advanced Message Security .

Strategie produktu Advanced Message Security są tworzone przy użyciu programu narzędziowego CSQ0UTIL , który jest udokumentowany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK6. Nazwa strategii i powiązana kolejka to FIN.XFER.Q7. Algorytm używany do generowania podpisu nadawcy to MD5, a nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US'.

Po zdefiniowaniu strategii należy zrestartować menedżer kolejek BNK6 lub użyć komendy z/OS **MODIFY** w celu odświeżenia konfiguracji strategii produktu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Lokalne kolejkowanie komunikatów chronionych prywatności w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje na temat strategii i certyfikatów produktu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów chronionych przez prywatność do kolejki oraz z kolejki lokalnej do aplikacji i pobierania ich z kolejki. Komunikaty chronione przez prywatność są podpisywane i szyfrowane.

Przykładowy menedżer kolejek i kolejka lokalna są następujące:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Użytkownicy ci są używani:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Kroki do skonfigurowania tego scenariusza są następujące:

Tworzenie certyfikatów użytkownika

W tym przykładzie wymagane są dwa certyfikaty użytkownika. Są to certyfikaty użytkownika wysyłającego wymagane do podpisywania komunikatów, a także certyfikat użytkownika odbiorcy, który jest potrzebny do szyfrowania i deszyfrowania danych komunikatu. Użytkownik wysyłający ma wartość 'TELLER5', a użytkownik odbiorcy ma wartość 'FINADM2'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA to certyfikat ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, to wszystkie certyfikaty w łańcuchu są wymagane w pliku kluczy użytkownika zadania Advanced Message Security , w tym przypadku użytkownika WMQBNK6.

Certyfikat ośrodka CA można utworzyć za pomocą komendy RACF RACDCERT. Ten certyfikat jest używany do wystawiania certyfikatów użytkownika. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, który może być następnie używany do wystawiania certyfikatów użytkowników dla użytkownikówTELLER5iFINADM2. Na przykład:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Instalacja użytkownika będzie zawierać procedury wyboru lub utworzenia certyfikatu CA, a także procedury wydawania certyfikatów i dystrybucji ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów produkt Advanced Message Security wymaga:

- Certyfikat CA (łańcuch).
- Wysyłający certyfikat użytkownika i jego klucz prywatny.
- Certyfikat użytkownika odbiorcy i jego klucz prywatny.

Jeśli używany jest produkt RACF, komenda RACDCERT EXPORT może być używana do eksportowania certyfikatów do zestawu danych, a do importowania certyfikatów z zestawu danych można użyć komendy RACDCERT ADD. Więcej informacji na temat tych i innych komend RACDCERT można znaleźć w podręczniku RACDCERT (Manage RACF digital certificates) w publikacji *z/OS: Security Server RACF Command Language Reference*.

Certyfikaty w tym przypadku są wymagane w systemie z/OS z uruchomionym menedżerem kolejek BNK6.

Jeśli certyfikaty zostały zaimportowane w systemie z/OS z uruchomionym BNK6, to certyfikaty użytkownika wymagają atrybutu TRUST. Do dodania atrybutu TRUST do certyfikatu można użyć komendy RACDCERT ALTER. Na przykład:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Połącz certyfikaty z odpowiednimi pierścieniami kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane, i ustawione jako zaufane, muszą być one połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS , na którym działa BNK6. Aby utworzyć pierścienie kluczy, użyj komendy RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security oraz kluczy dla użytkowników wysyłających i adresatów. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie jest rozróżniana wielkość liter.

Po utworzeniu kółek kluczy odpowiednie certyfikaty mogą być połączone.

```
RACDCERT ID(WMQBNK6) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))

RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Certyfikaty użytkownika wysyłającego i odbiorcy muszą być połączone jako domyślne. Jeśli jeden z użytkowników ma więcej niż jeden certyfikat w pliku drq.ams.keyring, certyfikat domyślny jest używany do podpisywania i deszyfrowania.

Certyfikat użytkownika odbiorcy musi być również połączony z głównym pierścieniem użytkownika zadania Advanced Message Security z USAGE (SITE). Dzieje się tak dlatego, że podczas szyfrowania danych komunikatu wymagane jest, aby zadanie zaawansowane Security Message Security (Zaawansowane zabezpieczenia komunikatów) było kluczem publicznym odbiorcy. Użycie parametru USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez produkt Advanced Message Security , dopóki menedżer kolejek nie zostanie zatrzymany i zrestartowany, albo komenda z/OS **MODIFY** zostanie użyta do odświeżenia konfiguracji certyfikatu produktu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH KEYRING
```

Tworzenie strategii produktu Advanced Message Security

W tym przykładzie komunikaty chronione przez prywatność są umieszczane w kolejce FIN.XFER.Q8 przez aplikację działającą jako użytkownik 'TELLER5', która została pobrana z tej samej kolejki przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagana jest tylko jedna strategia Advanced Message Security .

Strategie produktu Advanced Message Security są tworzone przy użyciu programu narzędziowego CSQ0UTIL , który jest udokumentowany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę:

```
setmqspl -m BNK6 -p FIN.XFER.Q8 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK6. Nazwa strategii i powiązana kolejka to FIN.XFER.Q8. Algorytmem, który jest używany do generowania podpisu nadawcy, jest SHA1, a nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US', a użytkownikiem odbiorcy jest 'CN=FinAdm2,O=BCO,C=US'. Algorytm używany do szyfrowania danych komunikatu to 3DES.

Po zdefiniowaniu strategii należy zrestartować menedżer kolejek BNK6 lub użyć komendy z/OS **MODIFY** w celu odświeżenia konfiguracji strategii produktu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Zdalne kolejkowanie komunikatów zabezpieczanych integralnością w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje na temat strategii i certyfikatów produktu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów zabezpieczonych przed integralnością do kolejek zarządzanych przez dwa różne menedżery kolejek. Dwa menedżery kolejek mogą być uruchomione w tym samym systemie z/OS lub w różnych systemach z/OS , albo jeden menedżer kolejek może znajdować się w systemie rozproszonym, na którym działa produkt Advanced Message Security.

Przykładowe menedżery kolejek i kolejki to:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Uwaga: w tym przykładzie BNK6 i BNK7 są menedżerami kolejek działaającymi w różnych systemach z/OS .

Użytkownicy ci są używani:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMStask user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Poniżej przedstawiono kroki, które należy wykonać, aby skonfigurować ten scenariusz:

Tworzenie certyfikatów użytkownika

W tym przykładzie potrzebny jest tylko jeden certyfikat użytkownika. Jest to certyfikat użytkownika wysyłający, który jest potrzebny do podpisania komunikatu zabezpieczonego integralnością. Użytkownik wysyłający ma wartość 'TELLER5'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA to certyfikat ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, to wszystkie certyfikaty w łańcuchu są wymagane w pliku kluczy użytkownika zadania Advanced Message Security , w tym przypadku użytkownika WMQBNK7.

Certyfikat ośrodka CA można utworzyć za pomocą komendy RACF RACDCERT. Ten certyfikat jest używany do wystawiania certyfikatów użytkownika. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, który następnie może być używany do wydawania certyfikatu użytkownika dla użytkownika 'TELLER5'. Na przykład:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
```

```
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Instalacja użytkownika będzie zawierać procedury wyboru lub utworzenia certyfikatu CA, a także procedury wydawania certyfikatów i dystrybucji ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów produkt Advanced Message Security wymaga:

- Certyfikat CA (łańcuch).
- Wysyłający certyfikat użytkownika i jego klucz prywatny.

Jeśli używany jest produkt RACF, komenda RACDCERT EXPORT może być używana do eksportowania certyfikatów do zestawu danych, a do importowania certyfikatów z zestawu danych można użyć komendy RACDCERT ADD. Więcej informacji na temat tych i innych komend RACDCERT można znaleźć w podręczniku RACDCERT (Manage RACF digital certificates) w publikacji *z/OS: Security Server RACF Command Language Reference*.

Certyfikaty w tym przypadku są wymagane w systemie z/OS z uruchomionym menedżerem kolejek BNK6 i BNK7.

W tym przykładzie certyfikat wysyłający musi być zaimportowany w systemie z/OS , na którym działa BNK6, a certyfikat ośrodka CA musi być zaimportowany na systemie z/OS , na którym działa BNK7. Gdy certyfikaty zostały zaimportowane, certyfikat użytkownika wymaga atrybutu TRUST. Do dodania atrybutu TRUST do certyfikatu można użyć komendy RACDCERT ALTER. Na przykład w systemie BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Połącz certyfikaty z odpowiednimi pierścieniami kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane, i ustawione jako zaufane, muszą być one połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS , na którym działają BNK6 i BNK7.

Aby utworzyć pierścienie kluczy, należy użyć komendy RACDCERT ADDRING, na stronie BNK6:

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika wysyłającego na serwerze BNK6. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie jest rozróżniana wielkość liter.

W systemie BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security w systemie BNK7. Dla 'TELLER5' na BNK7nie jest wymagany pierścień kluczy użytkownika.

Po utworzeniu kółek kluczy odpowiednie certyfikaty mogą być połączone.

W systemie BNK6:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

W systemie BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

Certyfikat użytkownika wysyłającego musi być połączony jako DOMYŚLNY. Jeśli użytkownik wysyłający ma więcej niż jeden certyfikat w pliku drq.ams.keyring, domyślny certyfikat jest używany do podpisywania celów.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez produkt Advanced Message Security , dopóki menedżer kolejek nie zostanie zatrzymany i zrestartowany, albo komenda z/OS **MODIFY** zostanie użyta do odświeżenia konfiguracji certyfikatu produktu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Tworzenie strategii produktu Advanced Message Security

W tym przykładzie komunikaty zabezpieczone przed integralnością są umieszczane w kolejce zdalnej FIN.XFER.Q7 w systemie BNK6 przez aplikację działającą jako użytkownik 'TELLER5' i pobieranej z kolejki lokalnej FIN.RCPT.Q7 w systemie BNK7 przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagane są dwie strategie produktu Advanced Message Security .

Strategie produktu Advanced Message Security są tworzone przy użyciu programu narzędziowego CSQ0UTIL , który jest udokumentowany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę, aby zdefiniować strategię integralności dla kolejki zdalnej w systemie BNK6:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK6. Nazwa strategii i powiązana kolejka to FIN.XFER.Q7. Algorytm używany do generowania podpisu nadawcy to MD5, a nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US'.

Należy również użyć programu narzędziowego CSQ0UTIL do uruchomienia następującej komendy w celu zdefiniowania strategii integralności dla kolejki lokalnej w systemie BNK7: .

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK7. Nazwa strategii i powiązana kolejka to FIN.RCPT.Q7. Oczekiwanym algorytmem dla sygnatury nadawcy jest MD5, a nazwa wyróżniająca (DN) użytkownika wysyłającego ma mieć wartość 'CN=Teller5,O=BCO,C=US'.

Po zdefiniowaniu dwóch strategii należy zrestartować menedżery kolejek BNK6 i BNK7 lub użyć komendy z/OS **MODIFY** w celu odświeżenia konfiguracji strategii produktu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS *Zdalne kolejkowanie komunikatów chronionych prywatności w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje na temat strategii i certyfikatów produktu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów chronionych przez prywatność do kolejek zarządzanych przez dwa różne menedżery kolejek oraz z kolejek zarządzanych przez te dwa. Dwa menedżery kolejek mogą być uruchomione w tym samym systemie z/OS lub w różnych systemach z/OS , albo jeden menedżer kolejek może znajdować się w systemie rozproszonym, na którym działa produkt Advanced Message Security.

Przykładowe menedżery kolejek i kolejki to:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Uwaga: w tym przykładzie BNK6 i BNK7 są menedżerami kolejek działaającymi w różnych systemach z/OS o tej samej nazwie.

Użytkownicy ci są używani:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMS task user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Poniżej przedstawiono kroki, które należy wykonać, aby skonfigurować ten scenariusz:

Tworzenie certyfikatów użytkownika

W tym przykładzie wymagane są dwa certyfikaty użytkownika. Są to certyfikaty użytkownika wysyłającego wymagane do podpisywania komunikatów, a także certyfikat użytkownika odbiorcy, który jest potrzebny do szyfrowania i deszyfrowania danych komunikatu. Użytkownik wysyłający ma wartość 'TELLER5', a użytkownik odbiorcy ma wartość 'FINADM2'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA to certyfikat ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, to wszystkie certyfikaty w łańcuchu są wymagane w pliku kluczy użytkownika zadania Advanced Message Security , w tym przypadku użytkownika WMQBNK7.

Certyfikat ośrodka CA można utworzyć za pomocą komendy RACF RACDCERT. Ten certyfikat jest używany do wystawiania certyfikatów użytkownika. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, który może być następnie używany do wystawiania certyfikatów użytkowników dla użytkownikówTELLER5iFINADM2. Na przykład:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(FINADM2) GENCERT SUBJECTSDN(CN('FinAdm2') O('BCO') C('US'))
WITHLABEL('FinAdm2') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

Instalacja użytkownika będzie zawierać procedury wyboru lub utworzenia certyfikatu CA, a także procedury wydawania certyfikatów i dystrybucji ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów produkt Advanced Message Security wymaga:

- Certyfikat CA (łańcuch).

- Wysyłający certyfikat użytkownika i jego klucz prywatny.
- Certyfikat użytkownika odbiorcy i jego klucz prywatny.

Jeśli używany jest produkt RACF, komenda RACDCERT EXPORT może być używana do eksportowania certyfikatów do zestawu danych, a do importowania certyfikatów z zestawu danych można użyć komendy RACDCERT ADD.

Więcej informacji na temat tych i innych komend RACDCERT zawiera sekcja RACDCERT (Zarządzanie certyfikatami cyfrowymi RACF) w publikacji *z/OS: Skorowidz języka komend serwera Security Server RACF*.

Certyfikaty w tym przypadku są wymagane w systemie z/OS z uruchomionym menedżerem kolejek BNK6 i BNK7.

W tym przykładzie certyfikaty nadawcze i odbiorcy muszą być importowane w systemie z/OS , na którym działa BNK6, a certyfikaty CA i odbiorcy muszą być zaimportowane w systemie z/OS , na którym działa BNK7. Gdy certyfikaty zostały zaimportowane, certyfikaty użytkownika wymagają atrybutu TRUST. Do dodania atrybutu TRUST do certyfikatu można użyć komendy RACDCERT ALTER. Na przykład:

W systemie BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

W systemie BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Połącz certyfikaty z odpowiednimi pierścieniami kluczy

Gdy wymagane certyfikaty zostały utworzone lub zaimportowane, i ustawione jako zaufane, muszą być one połączone z odpowiednimi pierścieniami kluczy użytkownika w systemach z/OS , na których działają BNK6 i BNK7.

Aby utworzyć pierścienie kluczy, użyj komendy RACDCERT ADDRING:

W systemie BNK6:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security oraz pliku kluczy dla użytkownika wysyłającego w systemie BNK6. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie jest rozróżniana wielkość liter.

W systemie BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security oraz pliku kluczy dla użytkownika będącego odbiorcą w systemie BNK7.

Po utworzeniu kółek kluczy odpowiednie certyfikaty mogą być połączone.

W systemie BNK6:

```
RACDCERT ID(WMQBNK6) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) USAGE(SITE))

RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

W systemie BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))

RACDCERT ID(FINADM2) CONNECT(ID(FINADM2) LABEL('FinAdm2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

Certyfikaty użytkownika wysyłającego i odbiorcy muszą być połączone jako domyślne. Jeśli jeden z użytkowników ma więcej niż jeden certyfikat w pliku drq.ams.keyring, certyfikat domyślny jest używany do podpisywania i szyfrowania/deszyfrowania.

W systemie BNK6certyfikat użytkownika odbiorcy musi być również połączony z głównym pierścieniem użytkownika zadania Advanced Message Security z użyciem funkcji USAGE (SITE). Dzieje się tak dlatego, że podczas szyfrowania danych komunikatu wymagane jest, aby zadanie zaawansowane Security Message Security (Zaawansowane zabezpieczenia komunikatów) było kluczem publicznym odbiorcy. Użycie parametru USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez produkt Advanced Message Security , dopóki menedżer kolejek nie zostanie zatrzymany i zrestartowany, albo komenda z/OS **MODIFY** zostanie użyta do odświeżenia konfiguracji certyfikatu produktu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Tworzenie strategii produktu Advanced Message Security

W tym przykładzie komunikaty chronione przez prywatność są umieszczane w kolejce zdalnej FIN.XFER.Q7 w systemie BNK6 przez aplikację działającą jako użytkownik 'TELLER5' i pobieranej z kolejki lokalnej FIN.RCPT.Q7 w systemie BNK7 przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagane są dwie strategie produktu Advanced Message Security .

Strategie produktu Advanced Message Security są tworzone przy użyciu programu narzędziowego CSQ0UTIL , który jest udokumentowany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę, aby zdefiniować strategię ochrony prywatności dla kolejki zdalnej w systemie BNK6:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK6. Nazwa strategii i powiązana kolejka to FIN.XFER.Q7. Algorytm używany do generowania podpisu nadawcy to SHA1, nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US', a użytkownikiem odbiorcy jest 'CN=FinAdm2,O=BCO,C=US'. Algorytm używany do szyfrowania danych komunikatu to 3DES.

Należy również użyć programu narzędziowego CSQ0UTIL do uruchomienia następującej komendy w celu zdefiniowania strategii ochrony prywatności dla kolejki lokalnej w systemie BNK7: .

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s SHA1 -e 3DES -a CN=Teller5,O=BCO,C=US -r
CN=FinAdm2,O=BCO,C=US
```

W tej strategii menedżer kolejek jest identyfikowany jako BNK7. Nazwa strategii i powiązana kolejka to FIN.RCPT.Q7. Oczekiwanym algorytmem dla sygnatury nadawcy jest SHA1, a oczekiwana nazwa wyróżniająca (DN) użytkownika wysyłającego ma wartość 'CN=Teller5,O=BCO,C=US', a użytkownikiem odbiorcy jest 'CN=FinAdm2,O=BCO,C=US'. Algorytm, który jest używany do deszyfrowania danych komunikatu, to 3DES.

Po zdefiniowaniu dwóch strategii należy zrestartować menedżery kolejek BNK6 i BNK7 lub użyć komendy z/OS **MODIFY** w celu odświeżenia konfiguracji strategii produktu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Podręcznik Szybki start dla produktu AMS z klientami Java

Ten podręcznik służy do szybkiego konfigurowania produktu Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów dla aplikacji produktu Java łączących się przy użyciu powiązań klienta. Po zakończeniu tego zadania utworzony zostanie magazyn kluczy w celu zweryfikowania 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. Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są wprowadzane do infrastruktury produktu IBM MQ przy użyciu standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM 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** wyświetla szczegółowe informacje na temat produktu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym scenariuszu pojawiają się dwaj użytkownicy: alice, nadawca i bob, odbiorca. Aby móc korzystać z kolejki aplikacji, użytkownicy ci muszą mieć uprawnienia do korzystania z niej. Aby pomyślnie korzystać ze strategii ochrony zdefiniowanych w tym scenariuszu, należy nadać tym użytkownikom 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 publikacji **Szybki start** (Windows lub UNIX) dla używanej 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 +browse
```

3. Należy również 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
```

Ostrzeżenie: Program IBM MQ optymalizuje wydajność przez strategie buforowania, dzięki czemu nie będzie konieczne przeglądanie rekordów w celu uzyskania szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Produkt IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Jeśli więc menedżer kolejek ma zdefiniowaną niewielką liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Jednak należy nadać uprawnienie do przeglądania tej kolejki, w przypadku, gdy istnieje duża liczba zdefiniowanych strategii lub jeśli używane są stare klienty. SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach wygenerowanych przez kod AMS. Uprawnienie do umieszczania w tej kolejce jest sprawdzane tylko przy próbie umieszczenia komunikatu o błędzie w kolejce. Uprawnienia użytkownika do umieszczenia w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki chronionej AMS.

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 619.

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 produkcie Java łączących się za pomocą powiązań klienta. Jeśli planowane jest korzystanie z aplikacji produktu Java przy użyciu 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 używanej platformy.

   Uwaga: Ten katalog jest określany 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 certyfikatów samopodpisanych, 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 UNIXsprawdź, czy magazyn kluczy jest dostępny do odczytu

   ```
   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` jest 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 jest 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 plik `keystore.conf` jest już zainstalowany, ponieważ zostały wykonane instrukcje zawarte w podręczniku Szybki start (Windows lub UNIX), można edytować istniejący plik w celu dodania tych wierszy.
- Więcej informacji na ten temat zawiera “Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf) dla systemu AMS” na stronie 628.

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 **strmqikm** (ikeyman) wprowadza rozróżnienie, które *wyodrębnij* certyfikaty (klucze publiczne) i *eksport* klucze prywatne. 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 IBM 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 IBM 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. Zapoznaj się z publikacją **Szybki start** (Windows lub UNIX) dla używanej platformy, aby uzyskać szczegółowe informacje na temat uruchamiania programów w różnych użytkownikach.

Procedura

1. Aby uruchomić te przykładowe aplikacje produktu JMS , należy użyć ustawienia CLASSPATH dla platformy, tak jak pokazano to w sekcji Zmienne środowiskowe używane przez produkt IBM MQ classes for JMS , aby upewnić się, że katalog przykładów jest dołączany.
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 kolejki zdalne, należy ustawić strategie w kolejce zdalnej i lokalnej, do której przesyłane są komunikaty.

Gdy komunikat jest umieszczany w kolejce zdalnej, program Advanced Message Security przechwytuje operację i przetwarza komunikat zgodnie z zestawem strategii dla kolejki zdalnej. Na przykład dla strategii szyfrowania komunikat jest szyfrowany, zanim zostanie przekazany do IBM MQ w celu jego obsługowania. Po przetworzeniu przez program Advanced Message Security komunikatu umieszczonego w kolejce zdalnej program IBM 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 IBM Integration Bus

Produkt Advanced Message Security może chronić komunikaty w infrastrukturze, w której zainstalowany jest produkt IBM Integration Buslub WebSphere Message Broker 8.0.0.1 (lub nowszy). Przed zastosowaniem zabezpieczeń w środowisku produktu IBM Integration Bus 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 IBM Integration Busmożna zezwolić IBM Integration Bus na przetwarzanie komunikatów bez znajomości ich treści (Scenariusz 1). lub uczynić go autoryzowanym użytkownikiem, który może odbierać i wysyłać wiadomości (Scenariusz 2).

Scenariusz 1- Integration Bus nie może wyświetlić treści komunikatu

Zanim rozpoczniesz

Produkt IBM Integration Bus 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 IBM Integration Bus. Produkt Advanced Message Security jest używany tylko przez *alice*, *bob* i *cecil*. Nie jest konieczne zainstalowanie lub skonfigurowanie go dla IBM Integration Bus.

Program IBM Integration Bus otrzymuje 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 IBM Integration Bus i nadejścia 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). Program IBM Integration Bus umieszcza kierowany komunikat w niezabezpieczonym aliasie. Odbiorcy pobierają komunikat z chronionej kolejki wyjściowej, w której produkt 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

[1] cecil

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 w konfiguracji kwalifikującej się do tej kolejki. Użyj tej samej konfiguracji dla kolejek QBOB, QCECIL i QDEF .

```
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 programie IBM Integration Bus utwórz przepływ komunikatów, aby skierować komunikaty przychodzące 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 środowiska wykonawczego produktu IBM Integration Bus .
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 składnik IBM Integration Bus z kolejki aliasowej produktu AIN . IBM Integration Bus decyduje, gdzie należy skierować komunikat odczytywanie właściwości routeTo , która jest, jak wszystkie właściwości, niezaszyfrowana. IBM Integration Bus 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.

Scenariusz 2- Integration Bus może wyświetlać treść komunikatu

O tym zadaniu

W tym scenariuszu grupa osób może wysyłać komunikaty do programu IBM Integration Bus. Inna grupa jest autoryzowana do odbierania komunikatów, które są tworzone przez produkt IBM Integration Bus. Transmisja między stronami i IBM Integration Bus nie może zostać usunięta.

Należy pamiętać, że program IBM Integration Bus odczytuje strategie ochrony i certyfikaty tylko po otwarciu kolejki, dlatego należy ponownie załadować grupę wykonawców po wprowadzeniu aktualizacji strategii ochrony, aby zmiany zostały uwzględnione.

```
mqsireload execution-group-name
```

Jeśli IBM Integration Bus jest uznawana za autoryzowaną stronę dopuszczalną do odczytu lub podpisania ładunku komunikatu, należy skonfigurować produkt Advanced Message Security dla użytkownika uruchamianego usługę IBM Integration Bus . Należy pamiętać, że nie musi to być ten sam użytkownik, który umieszcza/pobiera komunikaty do kolejek, ani użytkownik tworzący i wdrażający aplikacje produktu IBM Integration Bus .

Procedura

1. Skonfiguruj *alice*, *bob*, *cecil* i *dave* oraz użytkownika usługi IBM Integration Bus , 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. Podaj certyfikaty *alice*, *bob*, *cecil* i *dave's* dla użytkownika usługi IBM Integration Bus .

   W tym celu wyodrębnianie wszystkich certyfikatów identyfikujących *alice*, *bob*, *cecil* i *dave* do plików zewnętrznych, a następnie dodanie wyodrębnionych certyfikatów do magazynu kluczy IBM Integration Bus . Ważne jest, aby użyć metody opisanej w **Czynność 5. Współużytkowanie certyfikatów** w **Podręczniku szybkiego startu** (Windows lub UNIX).
3. Podaj certyfikat użytkownika usługi IBM Integration Bus na wartość *alice*, *bob*, *cecil* i *dave*.

   W tym celu należy użyć metody określonej w poprzednim kroku.

   Uwaga: *Alicja* i *jan* potrzebują certyfikatu użytkownika usługi IBM Integration Bus , aby poprawnie zaszyfrować komunikaty. Użytkownik usługi IBM Integration Bus potrzebuje certyfikatów *alice's* i *bob's* , aby zweryfikować autorów komunikatów. Użytkownik usługi IBM Integration Bus musi mieć

certyfikaty *cecil's* i *dave's* , aby szyfrować komunikaty dla nich. *cecil* i *dave* potrzebują certyfikatu użytkownika usługi IBM Integration Bus , aby sprawdzić, czy komunikat pochodzi z produktu IBM Integration Bus.

4. Zdefiniuj kolejkę lokalną o nazwie IN i zdefiniuj strategię bezpieczeństwa za pomocą *alice* i *bob* określonych jako autorzy, a także użytkownika usługi dla IBM Integration Bus określonego 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 OUTi zdefiniuj strategię bezpieczeństwa z użytkownikiem usługi dla IBM Integration Bus określonego jako autor, a *cecil* i *dave* określani 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 programie IBM Integration Bus 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 środowiska wykonawczego produktu IBM Integration Bus .
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 program IBM Integration Bus odczytany został. Produkt IBM Integration Bus akceptuje tylko komunikaty z *alice* i *bob* i odrzuca wszystkie inne komunikaty. Zaakceptowane komunikaty są odpowiednio przetwarzane, a następnie podpisywane i szyfrowane za pomocą kluczy *cecil* i *dave's* przed umieszczaniem ich w kolejce wyjściowej OUT. Tylko *cecil* i *dave* są w stanie go odczytać, komunikaty, które nie są podpisane przez IBM Integration Bus , są odrzucane.

Używanie produktu Advanced Message Security z produktem Managed File Transfer

W tym scenariuszu wyjaśniono, w jaki sposób można skonfigurować produkt Advanced Message Security w taki sposób, aby zapewniał prywatność komunikatów przesyłanych danych za pośrednictwem serwera Managed File Transfer.

Zanim rozpoczniesz

Upewnij się, że w instalacji produktu IBM MQ jest zainstalowany komponent Advanced Message Security , który udostępnia kolejki używane przez produkt Managed File Transfer , który ma być zabezpieczany.

Jeśli agenty Managed File Transfer łączą się w trybie powiązań, upewnij się, że w lokalnej instalacji jest zainstalowany komponent GSKit.

O tym zadaniu

Jeśli przesyłanie danych między dwoma agentami Managed File Transfer zostanie przerwane, prawdopodobnie poufne dane mogą pozostać niechronione w bazowych kolejkach produktu IBM MQ używanych do zarządzania przesyłaniem. W tym scenariuszu wyjaśniono sposób konfigurowania i używania produktu Advanced Message Security do ochrony tych danych w kolejkach produktu Managed File Transfer .

W tym scenariuszu rozważamy prostą topologię składającą się z jednej maszyny z dwiema kolejkami Managed File Transfer i dwoma agentami, AGENT1 i AGENT2, współużytkowaliśmy pojedynczy menedżer kolejek zgodnie z opisem w scenariuszu Przegląd scenariusza. 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 produktu Managed File Transfer Agent . 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 Managed File Transfer działają w trybie powiązań, komendy używane do tworzenia magazynu kluczy CMS (Cryptographic Message Syntax) są szczegółowo opisane w publikacji **Szybki start** (Windows lub UNIX). dla używanej platformy.
- Jeśli agenty Managed File Transfer działają w trybie klienta, komendy, które będą potrzebne do utworzenia pliku kluczy JKS (Java Keystore), są szczegółowo opisane w podręczniku “Podręcznik Szybki start dla produktu AMS z klientami Java” na stronie 614.

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=<organisation>, L=<location>, ST=<state>, C=<country>
   ```

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 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=<organisation>, L=<location>, ST=<state>, C=<country>"
   -e AES128 -r "CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>"
   ```

3. Upewnij się, że użytkownik uruchamiający proces Managed File Transfer Agent 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 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.

Advanced Message Security instalacja, przegląd

Zainstaluj komponent Advanced Message Security na różnych platformach.

O tym zadaniu

Informacje na temat procedur instalacyjnych można znaleźć w sekcji Instalowanie produktu Advanced Message Security na wielu platformach i Instalowanie produktu Advanced Message Security w systemie z/OS.

Zadania pokrewne

Deinstalacja produktuAdvanced Message Security

z/OS Kontrola w systemie z/OS

Advanced Message Security (AMS) for z/OS udostępnia możliwość opcjonalnej kontroli operacji przez aplikacje w kolejkach chronionych strategii. Jeśli ta opcja jest włączona, IBM kontroli SMF (System Management Facility) są generowane na potrzeby powodzenia i niepowodzenia tych operacji w kolejkach chronionych strategii. Kontrolowane operacje obejmują MQPUT, MQPUT1i MQGET.

Domyślnie kontrola jest wyłączona, można jednak aktywować kontrolę, konfigurując wartości _AMS_SMF_TYPE i _AMS_SMF_AUDIT w skonfigurowanym pliku środowiska językowego ® _CEE_ENVFILE dla przestrzeni adresowej AMS . Więcej informacji na ten temat zawiera sekcja Tworzenie procedur dla produktu Advanced Message Security. Zmienna _AMS_SMF_TYPE jest używana do wyznaczania typu rekordu SMF i jest liczbą z zakresu od 128 do 255. Typ rekordu SMF o wartości 180 jest zwykle używany, ale nie jest obowiązkowy. Kontrola jest wyłączona przez podanie wartości 0. Zmienna _AMS_SMF_AUDIT konfiguruje, czy rekordy kontroli są tworzone dla operacji, które się powiodły, operacji, które nie powiodły się, lub obu tych operacji. Opcje kontroli mogą być również dynamicznie zmieniane, gdy produkt AMS jest aktywny przy użyciu komend operatora. Więcej informacji na ten temat zawiera sekcja Operating Advanced Message Security.

Rekord SMF jest definiowany przy użyciu podtypów, a podtyp 1 jest generalnym zdarzeniem kontroli. Rekord SMF zawiera wszystkie dane istotne dla przetwarzanego żądania.

Rekord SMF jest odwzorowywany przez makro CSQ0KSMF (należy zwrócić uwagę na zero w nazwie makra), który jest udostępniany w bibliotece docelowej SCSQMACS. W przypadku pisania programów redukcji danych dla danych SMF można uwzględnić to odwzorowanie makra w celu uzyskania pomocy w opracowaniu i dostosowaniu procedur przetwarzania końcowego SMF.

W rekordach SMF utworzonych przez produkt Advanced Message Security for z/OSdane są zorganizowane w sekcje. Rekord składa się z:

- Standardowy nagłówek SMF
- Rozszerzenie nagłówka zdefiniowane przez Advanced Message Security dla z/OS
- sekcja produktu
- sekcja danych

Sekcja produktu w rekordzie SMF jest zawsze obecna w rekordach utworzonych przez produkt Advanced Message Security dla produktu z/OS. Sekcja danych różni się w zależności od podtypu. Obecnie definiowany jest jeden podtyp i dlatego używana jest jedna sekcja danych.

SMF jest opisany w podręczniku z/OS System Management Facilities (SA22-7630). Poprawne typy rekordów są opisane w elemencie SMFPRMxx zestawu danych PARMLIB systemu. Więcej informacji na ten temat zawiera dokumentacja SMF.

Generator raportów kontroli produktu Advanced Message Security (CSQ0USMF)

Produkt Advanced Message Security for z/OS udostępnia narzędzie generatora raportów kontroli o nazwie CSQ0USMF , które jest dostarczane w bibliotece SCSQAUTH instalacji. Przykładowy skrypt JCL do uruchomienia programu narzędziowego CSQ0USMF o nazwie CSQ40RSM znajduje się w bibliotece instalacji SCSQPROC.

Przed uruchomieniem programu narzędziowego CSQ0USMF rekordy SMF typu 180 muszą być zrzucane z systemowych zestawów danych SMF do sekwencyjnego zestawu danych. Na przykład ten skrypt JCL zrzuca rekordy SMF typu 180 z zestawu danych SMF i przesyła je do docelowego zestawu danych:

```
//IFAUDUMP EXEC PGM=IFASMFDP
//INDD1 DD DSN=SYSn.MANn.syst,DISP=SHR
//OUTDD1 DD DSN=your.target.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
INDD(INDD1,OPTIONS(DUMP))
OUTDD(OUTDD1,TYPE(180))
/*
```

Należy zweryfikować rzeczywiste nazwy zestawów danych SMF używane przez instalację. Docelowy zestaw danych dla rekordów po cenach dumpingowych musi mieć format rekordu VBS i długość rekordu 32760.

Uwaga: Jeśli używane są strumienie rejestrowania SMF, należy użyć programu IFASMFDL w celu zrzucenia strumienia dziennika do sekwencyjnego zbioru danych. Przykład użycia kodu JCL można znaleźć w sekcji Przetwarzanie rekordów SMF typu 116 .

Docelowy zestaw danych może być następnie użyty jako dane wejściowe dla programu narzędziowego CSQ0USMF w celu utworzenia raportu kontroli produktu AMS . Na przykład:

```
//STEP1 EXEC PGM=CSQ0USMF,
// PARM=('/ -SMFTYPE 180 -M qmgr')
//STEPLIB DD DSN=thlqual.SCSQANLE,DISP=SHR
//    DD DSN=thlqual.SCSQAUTH,DISP=SHR
//SMFIN DD DSN=your.target.dataset,DISP=SHR
//
```

Program CSQ0USMF akceptuje dwa opcjonalne parametry, które są wymienione w Tabela 97 na stronie 626:

Tabela 97. Parametry opcjonalne CSQ0USMF

Parametr	Wartość	Opis
TYP_MFP	nnn	Typ rekordu SMF, który ma zastosowanie do raportu kontroli. Program CSQ0USMF używa tylko rekordów SMF, które są zgodne z wartością parametru SMFTYPE podczas generowania raportu. Jeśli parametr SMFTYPE nie zostanie określony, zostanie użyta wartość domyślna 180.

Tabela 97. Parametry opcjonalne CSQ0USMF (kontynuacja)		
Parametr	**Wartość**	**Opis**
M	QMGR	Nazwa menedżera kolejek produktu IBM MQ , który ma zastosowanie do raportu kontroli. Jeśli parametr -M nie zostanie określony, raport kontroli będzie zawierał wszystkie rekordy kontroli dla wszystkich menedżerów kolejek reprezentowanych w zestawie danych SMFIN.

Korzystanie z magazynów kluczy i certyfikatów

W celu zapewnienia przezroczystej ochrony kryptograficznej aplikacjom produktu IBM MQ produkt Advanced Message Security korzysta z pliku kluczy, w którym przechowywane są certyfikaty klucza publicznego i klucz prywatny. W systemie z/OSzamiast pliku kluczy używany jest plik kluczy SAF.

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.

W systemach Windows i UNIX 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. Produkt Advanced Message Security akceptuje następujący format plików kluczy: `.kdb`, `.jceks`, `.jks`.

Domyślnym położeniem pliku `keystore.conf` jest:

- IBM i UNIX W systemach UNIX i IBM i: `$HOME/.mqs/keystore.conf`
- Windows W systemie Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

  Uwaga: Ścieżka na serwerze Windows może i powinna określać literę napędu, jeśli dostępna jest więcej niż jedna litera napędu.

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`*

Pojęcia pokrewne

“Nazwy wyróżniające nadawców w produkcie AMS” na stronie 654
Nazwy wyróżniające nadawców identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce. Przed umieszczeniem komunikatu w kolejce nadawca używa swojego certyfikatu do podpisania komunikatu.

“Nazwy wyróżniające odbiorców w programie AMS” na stronie 656
Nazwy wyróżniające odbiorców (DN) identyfikują użytkowników, którzy są uprawnieni do pobierania komunikatów z kolejki.

Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf) dla systemu AMS

Plik konfiguracyjny magazynu kluczy (`keystore.conf`) wskazuje Advanced Message Security położenie odpowiedniego magazynu kluczy.

Każdy z następujących typów plików konfiguracyjnych ma przedrostek:

CMS
System zarządzania certyfikatami, pozycje konfiguracji są poprzedzone przedrostkiem: `cms.`

PKCS#11
Public Key Cryptography Standard #11, pozycje konfiguracji są poprzedzone przedrostkiem: `pkcs11.`

IBM i **PEM**
Format poczty o zwiększonej prywatności, pozycje konfiguracji są poprzedzone przedrostkiem: `pem.`

JKS
Java KeyStore, pozycje konfiguracji są poprzedzone przedrostkiem: `jks.`

JCEKS
Java Cryptographic Encryption KeyStore, pozycje konfiguracji są poprzedzane przedrostkiem: `jceks.`

z/OS V 9.1.0 MQ Adv. VUE **JCERACFKS,**
Java Magazyn kluczy KeyStorepliku kluczy szyfrowania szyfrowania RACF, pozycje konfiguracji są poprzedzone przedrostkiem: `jceracfks`.

Ważne: Od IBM MQ 9.0 wartości `JCEKS.provider` i `JKS.provider` są ignorowane. Dostawca Bouncy Castle jest używany w połączeniu z dowolnym udostępnianiem JCE/JCE dostarczanym przez używane środowisko JRE. Więcej informacji na ten temat zawiera sekcja “Obsługa środowisk JRE innych niżIBM przy użyciu produktu AMS” na stronie 631.

Przykładowe struktury dla magazynów kluczy:

CMS

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
```

Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
jks.provider = IBMJCE
```

Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
jceks.provider = IBMJCE
```

V 9.1.0 Java JCERACFKS,

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

Tabela 98. Podsumowanie parametrów wymaganych dla każdego typu pliku konfiguracyjnego

Parametry	Wymagany	Typ pliku konfiguracyjnego			
		V 9.1.0 **Java (JKS, JCEKS i JCERACFKS)**	IBM i **PEM**	**PKCS#11**	**CMS**
keystore	✓	✓			✓
IBM i private	✓		IBM i ✓		
IBM i public	✓		IBM i ✓		
IBM i password	✓		IBM i ✓		
library	✓			✓	
certificate	✓	✓		✓	✓
token	✓			✓	
token_pin	✓			✓	
secondary_keystore	✓			✓	
encrypted		✓			
keystore_pass	✓	✓			
key_pass		✓			
provider		✓			

Komentarze można dodawać za pomocą symbolu # .

Parametry pliku konfiguracyjnego są zdefiniowane w następujący sposób:

keystore
Tylko konfiguracja CMS i Java . Ścieżka do pliku kluczy dla konfiguracji CMS, JKS i JCEKS.

z/OS V 9.1.0 MQ Adv. VUE Identyfikator URI pliku kluczy RACF dla konfiguracji JCERACFKS.

Ważne:

- Ścieżka do pliku kluczy nie może zawierać rozszerzenia nazwy pliku.
- z/OS V 9.1.0 MQ Adv. VUE Identyfikator URI pliku kluczy RACF musi mieć następującą postać:

  ```
  safkeyring://user/keyring
  ```

  gdzie:

  – *user* to identyfikator użytkownika, który jest właścicielem pliku kluczy.

  – *keyring* to nazwa pliku kluczy.

IBM i **private**
Tylko konfiguracja PEM. Nazwa pliku zawierającego klucz prywatny i certyfikat w formacie PEM.

IBM i **public**
Tylko konfiguracja PEM. Nazwa pliku zawierającego zaufane certyfikaty publiczne w formacie PEM.

IBM i **password**
Tylko konfiguracja PEM. Hasło używane do deszyfrowania zaszyfrowanego klucza prywatnego.

library
Tylko PKCS#11 . Nazwa ścieżki biblioteki PKCS#11 .

certificate
Tylko konfiguracja CMS, PKCS#11 i Java . Etykieta certyfikatu.

token
Tylko PKCS#11 . Etykieta tokenu.

token_pin
Tylko PKCS#11 . Numer PIN, aby odblokować token.

secondary_keystore
Tylko PKCS#11 . Nazwa ścieżki magazynu kluczy CMS (bez rozszerzenia `.kdb`), który zawiera certyfikaty serwera ujawniającego (certyfikaty główne) wymagane przez certyfikaty przechowywane w tokenie PKCS #11 . Dodatkowy magazyn kluczy może również zawierać certyfikaty pośrednie w łańcuchu zaufania, a także certyfikaty odbiorców zdefiniowane w strategii ochrony prywatności. Temu plikowi kluczy CMS musi towarzyszyć plik ukrytych haseł, który musi znajdować się w tym samym katalogu, co dodatkowy plik kluczy.

encrypted
Tylko konfiguracja Java . Status hasła.

keystore_pass
Tylko konfiguracja Java . Hasło do pliku kluczy.

Uwaga:

- W przypadku magazynu kluczy CMS AMS korzysta z plików ukrytych (`.sth`), podczas gdy JKS i JCEKS mogą wymagać hasła zarówno dla certyfikatu, jak i klucza prywatnego użytkownika.
- **Ważne:** Przechowywanie haseł w postaci jawnego tekstu stanowi zagrożenie dla bezpieczeństwa.

z/OS V 9.1.0 MQ Adv. VUE

Uwaga: Parametr jest ignorowany w przypadku systemu `jceracfks` , ponieważ dostęp nie jest kontrolowany przez hasło.

key_pass
Tylko konfiguracja Java . Hasło dla klucza prywatnego użytkownika.

Ważne: Przechowywanie haseł w postaci jawnego tekstu stanowi zagrożenie dla bezpieczeństwa.

z/OS V 9.1.0 MQ Adv. VUE

Uwaga: Parametr jest ignorowany w przypadku systemu `jceracfks` , ponieważ dostęp nie jest kontrolowany przez hasło.

`provider`
Tylko konfiguracja Java . Dostawca zabezpieczeń Java , który implementuje algorytmy szyfrowania wymagane przez certyfikat magazynu kluczy.

Ważne: Informacje przechowywane w magazynie kluczy mają kluczowe znaczenie dla bezpiecznego przepływu danych wysyłanych przy użyciu programu IBM MQ. Administratorzy bezpieczeństwa muszą zwracać szczególną uwagę podczas przypisywania uprawnień do tych plików.

Przykład pliku `keystore.conf` :

```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configurationjceks.keystore = c:/Documents and Settings/Alice/
AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

Zadania pokrewne

“Ochrona haseł w produkcie Java” na stronie 645
Zapisywanie haseł kluczy i kluczy prywatnych w postaci zwykłego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego program Advanced Message Security udostępnia narzędzie, które może je scalenizować przy użyciu klucza użytkownika, który jest dostępny w pliku kluczy.

Obsługa środowisk JRE innych niżIBM przy użyciu produktu AMS

IBM MQ classes for Java and IBM MQ classes for JMS support Advanced Message Security operation when running with non-IBM JREs.

Produkt Advanced Message Security (AMS) implementuje interfejs Cryptographic Message Syntax (CMS). Składnia CMS jest używana do cyfrowego podpisywania, streszczania, uwierzytelniania lub szyfrowania dowolnych treści wiadomości.

W produkcie IBM MQ 9.0obsługa Advanced Message Security w produkcie IBM MQ classes for Java i w produkcie IBM MQ classes for JMS korzysta z pakietów Open Source Bouncy Castle w celu obsługi CMS. Oznacza to, że klasy te mogą obsługiwać operację Advanced Message Security podczas pracy z JRE innymi niżIBM .

Przed IBM MQ 9.0produkt Advanced Message Security nie był obsługiwany w środowisku JRE innych niżIBM w klientach Java . Advanced Message Security support in the IBM MQ classes for Java and IBM MQ classes for JMS depended on CMS support specifically provided by the IBM implementation of the Java Cryptography Extensions (JCE). Ze względu na to ograniczenie funkcja była dostępna tylko wtedy, gdy używana jest Java runtime environment (JRE), które obejmował dostawcę JCE produktu Java .

Solaris Co ważne, wsparcie na platformach, takich jak Solaris , wymaga hybrydowego środowiska JRE, czyli standardowego środowiska JRE dla platformy z dodatkowymi elementami udostępnianymi przez produkt IBM. W szczególności, zamiast dostawcy JCE dostarczanego przez standardowe środowisko JRE dla platformy, wymagany był dostawca JCE IBM .

Numeracja lokalizacji i wersji dla plików JAR firmy Bouncy

Pliki JAR firmy Bouncy, które są potrzebne do obsługi środowisk JRE innych niżIBM , są dołączane jako część pakietu instalacyjnego produktu IBM MQ classes for Java i IBM MQ classes for JMS .

Używane pliki JAR firmy Bouncy to następujące pliki:

Plik JAR dostawcy, który ma podstawowe znaczenie dla operacji na zamku Bouncy.
Ten plik JAR nosi nazwę `bcprov-jdk15on.jar`.

Plik JAR "PKIX", który zawiera obsługę operacji CMS, które są używane przez produkt Advanced Message Security.
Ten plik JAR nosi nazwę `bcpkix-jdk15on.jar`.

V 9.1.0.9 **Plik JAR "util", który zawiera klasy używane przez inne pliki JAR firmy Bouncy Castle.**
Ten plik JAR nosi nazwę `bcutil-jdk15on.jar`.

Zależności

Klasy IBM MQ 9.1 i nowsze zostały przetestowane z IBM JREs i Oracle JREs. Prawdopodobnie działają one pomyślnie w dowolnym środowisku J2SE-compliant JRE. Należy jednak zwrócić uwagę na następujące zależności:

- Nie ma żadnych zmian w konfiguracji produktu Advanced Message Security .
- Klasy Castle Bouncy są używane tylko dla operacji CMS. Wszystkie inne operacje związane z bezpieczeństwem, na przykład dostęp do magazynu kluczy, rzeczywiste szyfrowanie danych i obliczanie sum kontrolnych podpisów, korzystają z funkcji udostępnianej przez środowisko JRE.

  Ważne: Z tego powodu używane środowisko JRE musi zawierać implementację dostawcy JCE.
- Aby użyć niektórych *silnych* algorytmów szyfrowania, może być konieczne zainstalowanie plików strategii *niezastrzeżonych* dla implementacji JCE środowiska JRE.

  Więcej informacji na ten temat zawiera dokumentacja środowiska JRE.
- Jeśli włączono zabezpieczenia produktu Java :
  - Dodaj `java.security.SecurityPermissioninsertProvider.BC` do aplikacji, aby klasy Castle Bouncy mogły być używane jako dostawca zabezpieczeń.
  - Nadaj `java.security.AllPermission` pliki JAR firmy Bouncy Castle, które są następujące:

    V 9.1.0.9 *mq_install_dir*`/java/lib/bcutil-jdk15on.jar`
    mq_install_dir`/java/lib/bcpkix-jdk15on.jar`
    mq_install_dir`/java/lib/bcprov-jdk15on.jar`

Pojęcia pokrewne

Co jest zainstalowane w przypadku klas produktu IBM MQ dla usługi JMS
Co jest zainstalowane dla klas IBM MQ dla języka Java

Multi Przechwytywanie agenta kanału komunikatów (MCA)

Przechwytywanie MCA umożliwia menedżerowi kolejek działającego w ramach produktu IBM MQ selektywne włączanie strategii, które mają być stosowane dla kanałów połączenia z serwerem.

Przechwytywanie MCA umożliwia klientom, którzy pozostają poza AMS , nadal nawiązywać połączenie z menedżerem kolejek, a ich komunikaty mają być szyfrowane i deszyfrowane.

Przechwytywanie agenta MCA ma na celu udostępnienie możliwości produktu AMS , jeśli na kliencie nie można włączyć programu AMS . Należy pamiętać, że użycie przechwytywania MCA i klienta z włączoną obsługą produktu AMSprowadzi do podwójnej ochrony komunikatów, które mogą być problematyczne w przypadku odbierania aplikacji. Więcej informacji na ten temat zawiera sekcja “Wyłączanie produktu Advanced Message Security na kliencie” na stronie 635.

Uwaga: Przechwytywacze MCA nie są obsługiwane dla kanałów AMQP lub MQTT.

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 AMS zawiera sekcja “Korzystanie z magazynów kluczy i certyfikatów” na stronie 627.

Aby włączyć przechwytywanie agenta MCA, należy podać nazwę kanału, który ma być używany w pliku konfiguracyjnym magazynu kluczy. W przypadku modułu MCA Interception można używać tylko typu magazynu kluczy cms.

Przykład konfigurowania przechwytywacza MCA zawiera sekcja “Przykład przechwycenia MCA Advanced Message Security” na stronie 633 .

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).

IBM i

Jeśli przedsiębiorstwo korzysta z produktu IBM i, a użytkownik wybrał komercyjny ośrodek certyfikacji (CA), który podpisuje swój certyfikat, to Certificate Manager utworzy żądanie certyfikatu w formacie PEM (Privacy-Enhanced Mail). Należy przekazać żądanie do wybranego ośrodka CA.

Aby to zrobić, należy użyć następującej komendy, aby wybrać poprawny certyfikat dla kanału określonego w programie `channelname`:

```
pem.certificate.channel.channelname
```

Przykład przechwycenia MCA Advanced Message Security

Przykładowe zadanie dotyczące konfigurowania przechwytywacza MCA produktu 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).

Jeśli przedsiębiorstwo korzysta z produktu IBM i, a użytkownik wybrał komercyjny ośrodek certyfikacji (CA), który podpisuje swój certyfikat, to Certificate Manager utworzy żądanie certyfikatu w formacie PEM (Privacy-Enhanced Mail). Należy przekazać żądanie do wybranego ośrodka CA.

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 7.5produkt AMS był produktem dodatkowym, który musi być oddzielnie zainstalowany, a przechwytywacze skonfigurowane do zabezpieczania aplikacji. Począwszy od wersji IBM WebSphere MQ 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 IBM WebSphere MQ 7.5 lub późniejszego, 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 bobmoże nie być konieczne.

```
INSTLOC=/opt/mq90
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 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 MQ 9.0 :

```
/opt/mq90/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 MQ 9.0 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Zadania pokrewne

“Podręcznik Szybki start dla produktu AMS z klientami Java” na stronie 614
Ten podręcznik służy do szybkiego konfigurowania produktu Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów dla aplikacji produktu Java łączących się przy użyciu powiązań klienta. Po zakończeniu tego zadania utworzony zostanie magazyn kluczy w celu zweryfikowania tożsamości użytkowników oraz zdefiniowanych strategii podpisywania i szyfrowania dla menedżera kolejek.

Odsyłacze pokrewne

“Znane ograniczenia produktu AMS” na stronie 584
Istnieje wiele opcji produktu IBM MQ , które nie są obsługiwane lub mają ograniczenia dotyczące produktu Advanced Message Security.

Wyłączanie produktu Advanced Message Security na kliencie

Jeśli do nawiązywania połączenia z menedżerem kolejek z wcześniejszej wersji produktu używany jest klient IBM WebSphere MQ 7.5 lub nowszy, należy wyłączyć program IBM MQ Advanced Message Security (AMS), a zgłaszany jest błąd 2085 （MQRC_UNKNOWN_OBJECT_NAME）.

O tym zadaniu

From IBM WebSphere MQ 7.5, IBM MQ Advanced Message Security (AMS) is automatically enabled in an IBM MQ client and so, by default, the client tries to check the security policies for objects at the queue manager. Jednak serwery we wcześniejszych wersjach produktu, na przykład IBM WebSphere MQ 7.1, nie mają włączonej opcji AMS , a powoduje to zgłoszenie błędu 2085 （MQRC_UNKNOWN_OBJECT_NAME）.

Jeśli ten błąd zostanie zgłoszony, podczas próby nawiązania połączenia z menedżerem kolejek z wcześniejszej wersji produktu można wyłączyć produkt AMS w następujący sposób:

- W przypadku klientów Java , w dowolny z następujących sposobów:
  - W tym celu należy ustawić zmienną środowiskową AMQ_DISABLE_CLIENT_AMS.
  - Ustawiając właściwość systemową Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - Za pomocą właściwości AMS DisableClient, w sekcji **Security** w pliku `mqclient.ini` .
- W przypadku klientów C wykonaj jedną z następujących czynności:
  - W tym celu należy ustawić zmienną środowiskową MQS_DISABLE_ALL_INTERCEPT.
  - Za pomocą właściwości AMS DisableClient, w sekcji **Security** w pliku `mqclient.ini` .

Uwaga: W produkcie IBM WebSphere MQ 7.5można również użyć zmiennej środowiskowej AMQ_DISABLE_CLIENT_AMS. dla klientów C. W produkcie IBM MQ 8.0nie można już używać zmiennej środowiskowej AMQ_DISABLE_CLIENT_AMS dla klientów C. Zamiast tego należy użyć zmiennej środowiskowej MQS_DISABLE_ALL_INTERCEPT.

Procedura

- Aby wyłączyć program AMS na kliencie, należy użyć jednej z następujących opcji:

  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 IBM WebSphere MQ 7.5 lub nowszy, klient IBM MQ classes for JMS lub IBM MQ classes for Java .

  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
  ```

  Właściwość systemowa Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS
  W przypadku klientów IBM MQ classes for JMS i IBM MQ classes for Java można ustawić 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.

  Zmienna środowiskowa MQS_DISABLE_ALL_INTERCEPT
  Tę zmienną należy ustawić w przypadku używania produktu IBM MQ 8.0 lub nowszego z klientami rodzimymi, a ponadto należy wyłączyć produkt AMS na kliencie.

  Utwórz zmienną środowiskową MQS_DISABLE_ALL_INTERCEPT i ustaw ją na wartość TRUE w środowisku, w którym działa klient. Na przykład:

  ```
  export MQS_DISABLE_ALL_INTERCEPT =TRUE
  ```

  Zmiennej środowiskowej MQS_DISABLE_ALL_INTERCEPT można użyć tylko dla klientów C. W przypadku klientów Java należy zamiast niej użyć zmiennej środowiskowej AMQ_DISABLE_CLIENT_AMS.

  Właściwość `DisableClientAMS` w pliku `mqclient.ini`
  Tej opcji można użyć dla klientów IBM MQ classes for JMS i IBM MQ classes for Java oraz dla klientów C.

  Dodaj nazwę właściwości `DisableClientAMS` w sekcji **`Security`** w pliku `mqclient.ini` , tak jak pokazano to w poniższym przykładzie:

  ```
  Security:
  DisableClientAMS=Yes
  ```

  Można również włączyć program AMS w sposób przedstawiony w poniższym przykładzie:

  ```
  Security:
  DisableClientAMS=No
  ```

Co dalej

Więcej informacji na temat problemów z otwieraniem kolejek chronionych produktu AMS zawiera sekcja Problemy z otwieraniem kolejek chronionych podczas korzystania z produktu AMS z produktem JMS.

Pojęcia pokrewne
“Przechwytywanie agenta kanału komunikatów (MCA)” na stronie 632

Przechwytywanie MCA umożliwia menedżerowi kolejek działającego w ramach produktu IBM 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 MQ classes for JMS

Wymagania dotyczące certyfikatu dla produktu 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 “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 45.

Rozszerzenia użycia klucza

Rozszerzenia dotyczące użycia kluczy nakładają dodatkowe ograniczenia na sposób, w jaki można używać certyfikatu.

W programie Advanced Message Securitykluczowe użycie certyfikatów X.509 v3 musi być ustawione zgodnie ze specyfikacją RFC 5280.

W celu zapewnienia jakości zabezpieczenia, jeśli ustawione są rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać co najmniej jedną z następujących wartości:

- **nonRepudiation**
- **digitalSignature**

W celu zapewnienia jakości ochrony prywatności, jeśli ustawione są rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać:

- **keyEncipherment**

W przypadku jakości poufności ochrony, jeśli ustawione są rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać:

- **dataEncipherment**

Rozszerzone użycie klucza dodatkowo ogranicza rozszerzenia użycia klucza. W przypadku wszystkich właściwości ochrony, jeśli ustawiono rozszerzone użycie klucza certyfikatu, zestaw musi zawierać:

- **emailProtection**

Pojęcia pokrewne

“Jakość ochrony” na stronie 657
Strategie ochrony danych Advanced Message Security oznaczają jakość ochrony (QOP).

Metody sprawdzania poprawności certyfikatów w produkcie AMS

Za pomocą programu 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 AMS umożliwia sprawdzenie poprawności certyfikatu przy użyciu protokołu OCSP (Online Certificate Status Protocol) lub listy odwołań certyfikatów (CRL).

Produkt AMS można skonfigurować zarówno dla sprawdzania OCSP, jak i sprawdzania listy CRL. Jeśli obie metody są włączone, ze względu na wydajność produkt AMS najpierw używa protokołu OCSP w celu uzyskania statusu odwołania. Jeśli status odwołania certyfikatu jest nieokreślony po sprawdzeniu OCSP, produkt AMS używa sprawdzania CRL.

Należy pamiętać, że sprawdzanie protokołu OCSP i CRL jest domyślnie włączone.

Pojęcia pokrewne

"Protokół OCSP (Online Certificate Status Protocol) w produkcie AMS" na stronie 638
Protokół OCSP (Online Certificate Status Protocol) określa, czy certyfikat został unieważniony i w związku z tym pomaga określić, czy certyfikat może być zaufany. Protokół OCSP jest włączony domyślnie.

"Listy odwołań certyfikatów (CRL) w produkcie AMS" na stronie 640
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) w produkcie AMS

Protokół OCSP (Online Certificate Status Protocol) określa, czy certyfikat został unieważniony i w związku z tym pomaga określić, czy certyfikat może być zaufany. Protokół OCSP jest włączony domyślnie.

Protokół OCSP nie jest obsługiwany w systemie IBM i sytems.

Włączanie sprawdzania protokołu OCSP w przechwytywaczy rodzimych produktu Advanced Message Security

Sprawdzanie protokołu OCSP (Online Certificate Status Protocol) w programie Advanced Message Security jest domyślnie włączone w oparciu o informacje zawarte w używanych certyfikatach.

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego magazynu kluczy:

Uwaga: Wszystkie sekcje OCSP są opcjonalne i mogą być określone niezależnie.

Opcja	Opis
`ocsp.enable=off`	Włącz sprawdzanie protokołu OCSP, jeśli sprawdzany certyfikat ma rozszerzenie AIA (Authority Info Access) z metodą dostępu PKIX_AD_OCSP zawierającą identyfikator URI miejsca, w którym znajduje się odpowiedź OCSP. Możliwe wartości: on lub `off`.
`ocsp.url=`*`responder_URL`*	Adres URL modułu odpowiadającego OCSP. Jeśli ta opcja zostanie pominięta, sprawdzanie OCSP inne niż AIA jest wyłączone.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	Adres URL serwera proxy OCSP. Jeśli ta opcja zostanie pominięta, wówczas serwer proxy nie będzie używany do sprawdzania certyfikatów online innych niż AIA.
`ocsp.http.proxy.port=`*`port_number`*	Numer portu serwera proxy OCSP. Jeśli ta opcja zostanie pominięta, zostanie użyty port domyślny o numerze 8080.
`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.

Opcja	Opis
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. Wartością domyślną jest off.
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.
ocsp.unknown=ACCEPT	Definiuje zachowanie, gdy serwer OCSP nie może zostać osiągnięty w okresie limitu czasu. Możliwe wartości: • ACCEPT Pozwala na wykonanie certyfikatu • WARN Pozwala na wyświetlenie certyfikatu i zarejestr. • REJECT Uniemożliwia użycie certyfikatu i zarejestr błędu

Włączanie sprawdzania protokołu OCSP w produkcie Java w produkcie AMS
Aby włączyć sprawdzanie protokołu OCSP dla produktu 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 zawiera rozszerzenie certyfikatu AIA (Authority Information Access).

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 produkt Java Security Manager, należy je również wykonać, dodając następujące uprawnienia 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, należy dodać następujące uprawnienia produktu 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) w produkcie AMS

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 zakotwiczenia zaufania. Baza zaufania jest zaufanym plikiem kluczy, który zawiera zaufany certyfikat lub zaufany certyfikat główny, który jest używany do potwierdzania zaufania certyfikatu. Program AMS weryfikuje ścieżkę certyfikatu przy użyciu algorytmu sprawdzania poprawności PKIX. Po utworzeniu i zweryfikowaniu łańcucha program 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, AMS sprawdza, czy ustawione są również wartości **digitalSignature** lub **nonRepudiation** . Jeśli nie są one, `MQRC_SECURITY_ERROR` jest raportowane i rejestrowane. Następnie program AMS pobiera listy CRL z plików lub z katalogu LDAP w zależności od wartości określonych w pliku konfiguracyjnym. 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 AMS nie sprawdza poprawności listy CRL. Dla każdego certyfikatu ośrodka CA AMS wysyła zapytania LDAP do list CRL przy użyciu 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
Należy zmodyfikować plik konfiguracyjny magazynu kluczy, tak aby program Advanced Message Security mógł pobrać CLRs z serwera LDAP (Lightweight Directory Access Protocol).

O tym zadaniu

IBM i Włączenie obsługi sprawdzania poprawności certyfikatu i listy odwołań certyfikatów w przechwytywakach rodzimych nie jest obsługiwane dla produktu Advanced Message Security w systemie IBM i.

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego:

Uwaga: Wszystkie sekcje CRL są opcjonalne i mogą być określone niezależnie.

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 AMS Java 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.
`crl.ldap.user=cn=`*`username`*	Zaloguj się do serwera 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.

Opcja	Opis
`crl.http.timeout=30`	Czas oczekiwania na odpowiedź serwera, w sekundach, po upływie którego AMS razy przekroczyli limit czasu.
`crl.http.cache_size=0`	Wielkość pamięci podręcznej HTTP w bajtach.
`crl.unknown=ACCEPT`	Definiuje zachowanie, gdy serwer listy odwołań certyfikatów nie może zostać osiągnięty w okresie limitu czasu. Możliwe wartości: • ACCEPT Pozwala na wykonanie certyfikatu • WARN Pozwala na wyświetlenie certyfikatu i zarejestr. • REJECT Uniemożliwia użycie certyfikatu i zarejestr błędu

Włączanie obsługi listy odwołań certyfikatów w produkcie Java w produkcie AMS
Aby włączyć obsługę list CRL w programie Advanced Message Security, należy zmodyfikować plik konfiguracyjny magazynu kluczy, aby umożliwić programowi 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 AMS Java pomyślnie nawiąże połączenie z serwerem LDAP, nie podejmuje próby pobrania list CRL z pozostałych udostępnionych serwerów. Produkt 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.
`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.

z/OS *Włączanie list odwołań certyfikatów (CRL) w systemie z/OS*

Produkt Advanced Message Security obsługuje sprawdzanie listy odwołań certyfikatów (CRL) w certyfikatach cyfrowych używanych do zabezpieczania komunikatów.

O tym zadaniu

Po włączeniu tej opcji program Advanced Message Security sprawdza poprawność certyfikatów odbiorcy, gdy komunikaty są umieszczane w kolejce chronionej prywatności i sprawdzają poprawność certyfikatów nadawcy, gdy komunikaty są pobierane z chronionej kolejki (integralność lub prywatność). Zatwierdzenie w tym przypadku obejmuje sprawdzenie, czy odpowiednie certyfikaty nie są zarejestrowane w odpowiedniej liście CRL.

Produkt Advanced Message Security korzysta z usług IBM System SSL w celu sprawdzenia poprawności certyfikatów nadawcy i odbiorcy. Szczegółowe informacje na temat sprawdzania poprawności certyfikatu SSL w systemie można znaleźć w podręczniku z/OS Cryptographic Services System Secure Sockets Layer Programming (SC24-5901).

Aby włączyć sprawdzanie listy CRL, należy określić położenie pliku konfiguracyjnego CRL za pomocą komendy CRLFILE DD w uruchomionym zadaniu JCL dla przestrzeni adresowej AMS. Przykładowy plik konfiguracyjny CRL, który można dostosować, jest dostępny w pliku *thlqual*.SCSQPROC (CSQ40CRL). Ustawienia dozwolone w tym pliku są następujące:

Tabela 99. Zmienne konfiguracyjne CRL Advanced Message Security

Zmienna	**Poprawne wartości**	**Opis**
crl.ldap.host[.n]	*hostname -or-hostname: port*	Nazwa ipaddr/nazwa hosta serwera LDAP, który udostępnia listy CRL certyfikatów wystawcy. Jeśli dla serwera LDAP nie zostanie podany numer portu, zostanie użyty numer portu określony przez parametr crl.ldap.port .
crl.ldap.port	*port*	Numer portu TCP/IP serwera LDAP.
crl.ldap.user	*użytkownik_ldap*	Nazwa użytkownika LDAP, która ma być używana podczas nawiązywania połączenia z serwerem LDAP.
crl.ldap.pass	*hasło_ldap*	Hasło LDAP powiązane z plikiem crl.ldap.user.

Można określić wiele nazw hostów i portów serwera LDAP w następujący sposób:

```
crl.ldap.host.1 = hostname -or hostname:port
crl.ldap.host.2 = hostname -or hostname:port
crl.ldap.host.3 = hostname -or hostname:port
```

Można podać maksymalnie 10 nazw hostów. Jeśli dla serwerów LDAP nie zostanie podany numer portu, zostanie użyty numer portu określony przez parametr crl.ldap.port . Każdy serwer LDAP musi używać tej samej kombinacji crl.ldap.user/password do uzyskania dostępu.

Jeśli określono wartość CRLFILE DD, konfiguracja jest ładowana podczas inicjowania przestrzeni adresowej Advanced Message Security , a sprawdzanie listy CRL jest włączone. Jeśli parametr CRLFILE DD nie został określony lub plik konfiguracyjny CRL jest niedostępny lub jest niepoprawny, sprawdzanie listy CRL jest wyłączone.

Program AMS sprawdza listę CRL za pomocą usług sprawdzania poprawności certyfikatów SSL systemu IBM w następujący sposób:

Tabela 100. Advanced Message Security sprawdzenia listy CRL

Operacja	**Jakość ochrony**	**Certyfikat (y) sprawdzony**
PUT	Ochrona prywatności	Odbiorca/-y
GET	Integralność/Prywatność	Nadawca

Jeśli operacja komunikatu nie powiedzie się, sprawdzenie listy CRL Advanced Message Security wykonuje następujące działania:

Tabela 101. Advanced Message Security Zachowanie sprawdzania niepowodzenia listy CRL	
Operacja	**Niepowodzenie sprawdzania listy CRL**
PUT	Komunikat nie jest umieszczany w kolejce docelowej. Do aplikacji zwracany jest kod zakończenia MQCC_FAILED i kod przyczyny MQRC_SECURITY_ERROR.
GET	Komunikat zostanie usunięty z kolejki docelowej i przeniesiony do kolejki błędów ochrony systemu. Do aplikacji zwracany jest kod zakończenia MQCC_FAILED i kod przyczyny MQRC_SECURITY_ERROR.

Produkt AMS for z/OS korzysta z usług IBM System SSL w celu sprawdzania poprawności certyfikatów, które obejmują listę CRL i sprawdzanie zaufania. IBM System SSL udostępnia zmienną środowiskową GSK_CRL_SECURITY_LEVEL w celu moderowania operacji sprawdzania listy CRL. Na przykład:

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

Ta zmienna została opisana w podręczniku z/OS Cryptographic Services System Secure Sockets Layer Programming. Do poprawnych przypisań należą:

- Sprawdzanie poprawności LOW-Certificate nie powiedzie się, jeśli nie można nawiązać kontaktu z serwerem LDAP.
- MEDIUM-Sprawdzanie poprawności certyfikatu wymaga, aby serwer LDAP mógł być kontaktowany, ale nie wymaga zdefiniowania listy CRL.
- HIGH-Certificate validation wymaga, aby serwer LDAP mógł być kontaktowany, a CRL ma być zdefiniowane.

Wartość domyślna dla systemowej implementacji SSL systemu IBM to MEDIUM. Tę zmienną można ustawić w pliku konfiguracyjnym określonym za pomocą DD ENVARS w uruchomionym zadaniu JCL dla przestrzeni adresowej AMS. Przykładowy plik konfiguracyjny zmiennej środowiskowej znajduje się w pliku *thlqual*.SCSQPROC (CSQ40ENV).

Uwaga: Obowiązkiem administratorów jest zapewnienie dostępu do odpowiednich usług LDAP oraz utrzymywanie wpisów CRL dla odpowiednich ośrodków certyfikacji.

Ochrona haseł w produkcie Java

Zapisywanie haseł kluczy i kluczy prywatnych w postaci zwykłego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego program Advanced Message Security udostępnia narzędzie, które może je scalenizować 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 627.

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
```

z/OS Korzystanie z certyfikatów w systemie z/OS

O tym zadaniu

Produkt Advanced Message Security implementuje trzy poziomy ochrony: integralność, poufność i prywatność.

W przypadku strategii integralności komunikaty są podpisywane przy użyciu klucza prywatnego inicjatora (aplikacji wykonującego operację MQPUT). Integralność zapewnia wykrywanie modyfikacji komunikatu, ale sam tekst komunikatu nie jest zaszyfrowany.

W przypadku strategii poufności komunikat jest szyfrowany, gdy jest umieszczany w kolejce. Komunikat jest szyfrowany przy użyciu klucza symetrycznego i algorytmu określonego w odpowiedniej strategii Advanced Message Security . Sam klucz symetryczny jest zaszyfrowany za pomocą klucza publicznego każdego odbiorcy (aplikacji wykonującego operację MQGET). Klucze publiczne są powiązane z certyfikatami zapisaną w pierścieniach kluczy.

W przypadku strategii ochrony prywatności komunikaty są podpisywane i szyfrowane.

Gdy komunikat, który jest chroniony przez prywatność, jest umieszczany w kolejce przez aplikację odbiorcy wykonującego operację MQGET, komunikat musi zostać zdeszyfrowany. Ponieważ został on zaszyfrowany przy użyciu klucza publicznego odbiorcy, musi on zostać zdeszyfrowany przy użyciu klucza prywatnego odbiorcy znalezionego w pliku kluczy.

z/OS *Korzystanie z plików kluczy SAF*

Produkt Advanced Message Security (AMS) korzysta z usług kluczy SAF produktu z/OS w celu definiowania certyfikatów potrzebnych do podpisywania i szyfrowania oraz do zarządzania nimi. Produkty bezpieczeństwa, które są funkcjonalnie równoważne produktowi RACF , mogą być używane zamiast produktu RACF , jeśli zapewniają one ten sam poziom obsługi.

Efektywne korzystanie z pierścieni kluczy może zmniejszyć administrację potrzebną do zarządzania certyfikatami.

Po wygenerowaniu certyfikatu (lub zaimportowaniu) musi on być podłączony do pliku kluczy, aby stał się dostępny. Ten sam certyfikat może być podłączony do więcej niż jednego pliku kluczy.

Produkt Advanced Message Security używa dwóch zestawów kluczy. Jeden zestaw składa się z kluczy należących do poszczególnych identyfikatorów użytkowników, które pochodzą lub odbierają komunikaty. Każdy pierścień kluczy zawiera klucz prywatny powiązany z certyfikatem identyfikatora użytkownika będącego właścicielem. Klucz prywatny każdego certyfikatu jest używany do podpisywania komunikatów dla kolejek chronionych integralności lub ochrony prywatności. Jest on również używany do deszyfrowania komunikatów z chronionych kolejek prywatności lub chronionych kolejek podczas odbierania komunikatów.

Drugi zestaw to pojedynczy klucz, którego właścicielem jest użytkownik przestrzeni adresowej AMS . Zawiera on łańcuch certyfikatów CA podpisujących certyfikaty niezbędne do sprawdzenia poprawności certyfikatów inicjatora i odbiorców wiadomości.

Gdy używana jest ochrona prywatności lub poufności, pierścień kluczy należący do użytkownika przestrzeni adresowej AMS również zawiera certyfikaty odbiorców wiadomości. Klucze publiczne w tych certyfikatach są używane do szyfrowania klucza symetrycznego, który był używany do szyfrowania danych komunikatu po umieszczanie komunikatu w chronionej kolejce. Po pobraniu tych komunikatów klucz prywatny odpowiednich odbiorców jest używany do deszyfrowania klucza symetrycznego, który jest następnie używany do deszyfrowania danych komunikatu.

Podczas wyszukiwania certyfikatów i kluczy prywatnych produkt Advanced Message Security korzysta z nazwy pliku kluczy **drq.ams.keyring** . Jest to przypadek zarówno dla użytkownika, jak i dla pierścieni kluczy przestrzeni adresowej AMS .

Aby uzyskać ilustrację i dalsze wyjaśnienia dotyczące certyfikatów i kluczy oraz ich roli w ochronie danych, należy zapoznać się z Podsumowanie operacji związanych z certyfikatami.

Klucz prywatny używany do podpisywania i deszyfrowania może mieć dowolną etykietę, ale musi być połączony jako certyfikat domyślny.

Certyfikaty cyfrowe i pierścienie kluczy są zarządzane w produkcie RACF głównie za pomocą komendy RACDCERT.

Więcej informacji na temat certyfikatów, etykiet i komend RACDCERT zawierają publikacje *z/OS: Security Server RACF Command Language Reference* i *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Autoryzowanie dostępu do komendy RACDCERT*

Autoryzacja do użycia komendy RACDCERT jest czynnością poinstalacyjną, która powinna zostać zakończona przez programistę systemu z/OS . To zadanie obejmuje nadawanie odpowiednich uprawnień administratorowi zabezpieczeń produktu Advanced Message Security .

Podsumowanie tych komend jest niezbędne, aby umożliwić dostęp do komendy RACDCERT produktu RACF :

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

W tym przykładzie parametr *admin* określa identyfikator użytkownika administratora zabezpieczeń lub dowolny użytkownik, który ma być użyty do użycia komendy RACDCERT.

z/OS *Tworzenie certyfikatów i kluczy*

W tej sekcji zostały opisane kroki wymagane do utworzenia certyfikatów i kluczy podstawowych niezbędnych dla użytkowników produktu z/OS w produkcie Advanced Message Security (AMS), przy użyciu ośrodka certyfikacji (CA) produktu RACF .

Rozwiązywanie problemów z certyfikatami podczas korzystania z produktu Advanced Message Security w systemie z/OS

Jeśli występują problemy z certyfikatami i brakującą pozycją w magazynach kluczy, można włączyć śledzenie GSKIT.

W pliku, do którego odwołuje się DD ENVARS w procedurze uruchomionego zadania AMS , dodaj:

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

Więcej informacji na ten temat zawiera sekcja Zmienne środowiskowe .

Dla każdego dostępu do magazynu kluczy dane są zapisywane do pliku śledzenia określonego w GSK_TRACE_FILE.

Aby sformatować plik śledzenia, użyj komendy:

```
gsktrace inputtrace file > output_file
```

Scenariusz

Scenariusz aplikacji wysyłającej i aplikacji odbierającej jest używany do wyjaśniania wymaganych kroków.

W poniższych przykładach program user1 jest inicjatorem komunikatu, a user2 jest odbiorcą. ID użytkownika przestrzeni adresowej Advanced Message Security to WMQAMSD.

Wszystkie komendy podane w tych przykładach są wydawane z opcji 6 ISPF przy użyciu identyfikatora użytkownika administracyjnego admin.

z/OS *Definiowanie certyfikatu lokalnego ośrodka certyfikacji*

Jeśli jako ośrodek CA używany jest produkt RACF , należy utworzyć certyfikat ośrodka certyfikacji, jeśli jeszcze tego nie zrobiono. Komenda wyświetlana w tym miejscu tworzy certyfikat ośrodka certyfikacji (lub osoby podpisującej). W tym przykładzie tworzony jest certyfikat o nazwie AMSCA, który ma być używany podczas tworzenia kolejnych certyfikatów, które odzwierciedlają tożsamość użytkowników i aplikacji produktu Advanced Message Security .

Ta komenda może być modyfikowana, w szczególności SUBJECTSDN, w celu odzwierciedlić strukturę nazewnictwa i konwencje używane podczas instalacji:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

Uwaga: Certyfikaty podpisane przy użyciu tego certyfikatu lokalnego ośrodka certyfikacji wskazują na wystawcę CN=AMSCA, O=ibm, C=us, jeśli są one wymienione za pomocą komendy RACDCERT LIST.

z/OS *Tworzenie certyfikatu cyfrowego za pomocą klucza prywatnego*

Dla każdego użytkownika produktu Advanced Message Security musi zostać wygenerowany certyfikat cyfrowy z kluczem prywatnym. W przedstawionym tutaj przykładzie komendy RACDCERT są używane do generowania certyfikatów dla użytkowników user1 i user2, które są podpisywane z lokalnym certyfikatem ośrodka CA identyfikowanym przez etykietę AMSCA.

```
RACDCERT ID(user1) GENCERT SUBJECTSDN(CN('user1') O('ibm') C('us'))
WITHLABEL('user1') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

RACDCERT ID(user2) GENCERT SUBJECTSDN(CN('user2') O('ibm') C('us'))
WITHLABEL('user2') SIGNWITH(CERTAUTH LABEL('AMSCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

```
RACDCERT ID(user1) ALTER (LABEL('user1')) TRUST
RACDCERT ID(user2) ALTER (LABEL('user2')) TRUST
```

Do dodania atrybutu TRUST do certyfikatu wymagane jest wykonanie komendy RACDCERT ALTER. Jeśli certyfikat zostanie najpierw utworzony przy użyciu tej procedury, ma on inny poprawny zakres dat niż certyfikat podpisywania. W rezultacie produkt RACF oznacza go jako NOTRUST, co oznacza, że certyfikat nie ma być używany. Aby ustawić atrybut TRUST, należy użyć komendy RACDCERT ALTER.

Atrybuty KEYUSAGE HANDSHAKE, DATAENCRYPT i DOCSIGN muszą być określone dla certyfikatów używanych przez produkt Advanced Message Security.

Tabela 102. RACDCERT KEYUSAGE wartości i wskaźniki

Wartość KEYUSAGE	**Zestaw wskaźników**
uzgadnianie	digitalSignature i keyEncipherment
SZYFROWANIE DANYCH	dataEncipherment
DOCSIGN	nonRepudiation
CERTSIGN	Znak keyCerti cRLSign

z/OS *Tworzenie plików kluczy produktu RACF*

Przedstawione tutaj komendy tworzą pierścień kluczy dla zdefiniowanych przez produkt RACFID użytkowników user1, user2i użytkownika zadania przestrzeni adresowej Advanced Message Security WMQAMSD. Nazwa pliku kluczy jest ustalana przez produkt Advanced Message Security i musi być zakodowana w sposób pokazany, bez cudzysłowów. W nazwie uwzględniana jest wielkość liter.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

z/OS *Łączenie certyfikatów z kluczowymi pierścieniami*

Połącz certyfikaty użytkownika i ośrodka CA z kluczowymi pierścieniami:

```
RACDCERT ID(WMQAMSD) CONNECT(CERTAUTH LABEL('AMSCA')
RING(drq.ams.keyring))
RACDCERT ID(user1) CONNECT(ID(user1) LABEL('user1')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(user2) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
RACDCERT ID(WMQAMSD) CONNECT(ID(user2) LABEL('user2')
RING(drq.ams.keyring) USAGE(SITE))
```

Certyfikat zawierający klucz prywatny używany do deszyfrowania musi być podłączony do pliku kluczy użytkownika jako certyfikat domyślny.

Atrybut RACDCERT USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy, natomiast atrybut RACDCERT USAGE (PERSONAL) pozwala na użycie klucza prywatnego, jeśli istnieje. Certyfikat User2musi być połączony z pierścieniem kluczy przestrzeni adresowej Advanced Message Security , ponieważ jego klucz publiczny jest potrzebny do szyfrowania komunikatów w miarę ich umieszczania w kolejce. UŻYCIE (SITE) ogranicza ekspozycję klucza prywatnego user2.

Certyfikat CERTAUTH z etykietą AMSCA musi być połączony z pierścieniem kluczy przestrzeni adresowej Advanced Message Security , ponieważ został on użyty do podpisania certyfikatu user1, który jest inicjatorem komunikatu. Jest on używany do sprawdzania poprawności certyfikatu podpisywania user1.

z/OS *Weryfikacja pierścienia kluczy*

Plik kluczy powinien zostać wyświetlony w sposób pokazany poniżej, po wprowadzeniu wszystkich komend:

```
RACDCERT ID(user1) LISTRING(drq.ams.keyring)
Digital ring information for user USER1:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
user1                          ID(USER1)    PERSONAL YES

RACDCERT ID(user2) LISTRING(drq.ams.keyring)
Digital ring information for user USER2:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
user2                          ID(USER2)    PERSONAL YES

RACDCERT ID(WMQAMSD) LISTRING(drq.ams.keyring)
Digital ring information for user WMQAMSD:
Ring:>drq.ams.keyring<:

Certificate Label Name           Cert Owner   USAGE    DEFAULT
------------------------------ ------------ -------- -------
AMSCA                          CERTAUTH     CERTAUTH NO
user2                          ID(USER2)    SITE     NO
```

Wyświetlenie listy poszczególnych certyfikatów pokazuje również powiązanie pierścieniowe.

```
RACDCERT ID(user2) LIST(label('user2'))
Digital certificate information for user USER2:

***
Label: user2
Certificate ID: 2QfH8Pny9/LzpKKFmfFA
Status: TRUST
Start Date: 2010/05/03 22:59:53
End Date:  2011/05/04 22:59:52
Serial Number:>15<:
Issuer's Name:>OU=AMSCA.O=ibm.C=us<:
Subject's Name:>CN=user2.O=ibm.C=us<:
Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
Ring Owner: USER2
Ring:>drq.ams.keyring<:
Ring Owner: WMQAMSD
Ring:>drq.ams.keyring<:
```

Aby zwiększyć wydajność, zawartość pliku drq.ams.keyring powiązana z przestrzenią adresową AMS jest buforowana w czasie życia przestrzeni adresowej. Zmiany w tym pliku kluczy nie stają się skuteczne automatycznie. Administrator może odświeżyć pamięć podręczną, wykonując jedną z następujących czynności:

- Zatrzymywanie i restartowanie menedżera kolejek.
- Za pomocą komendy z/OS MODIFY:

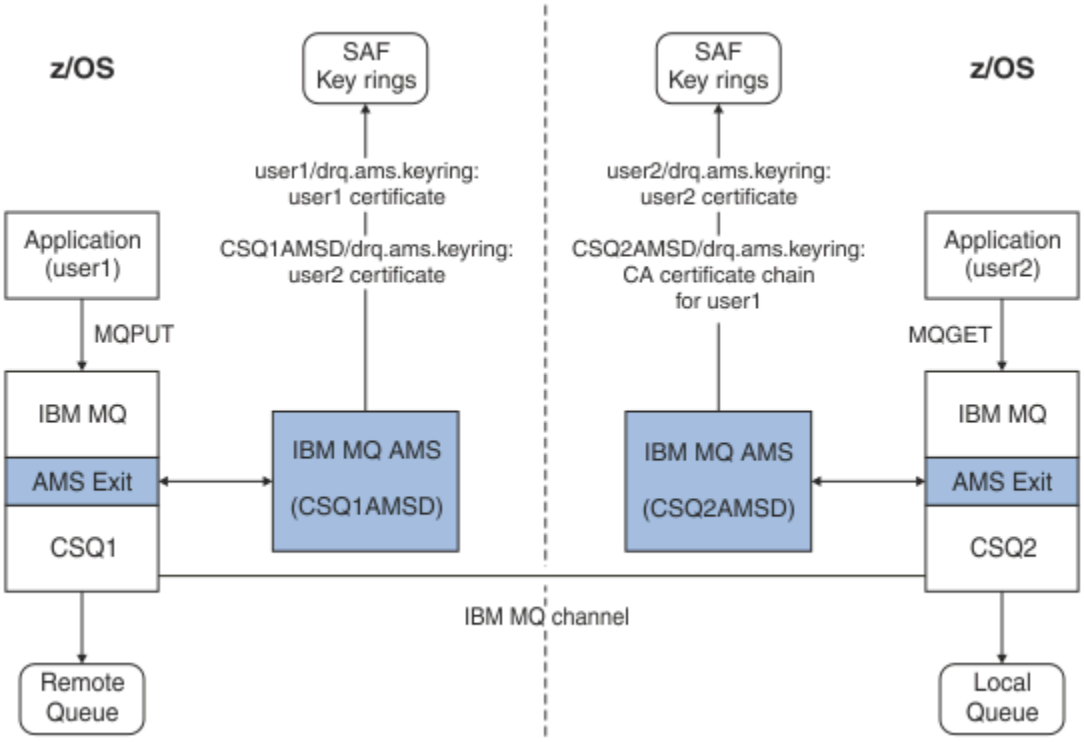
```
F qmgrAMSM,REFRESH KEYRING
```

Zadania pokrewne

Operacyjny Advanced Message Security

z/OS *Podsumowanie operacji związanych z certyfikatami*

Rysunek 35 na stronie 651 ilustruje relacje między aplikacjami wysyłających i odbierających oraz odpowiednimi certyfikatami. Ilustrowany scenariusz obejmuje zdalne kolejkowanie między dwoma menedżerami kolejek produktu z/OS przy użyciu strategii ochrony danych w zakresie ochrony prywatności. W programie Rysunek 35 na stronie 651"AMS" wskazuje " Advanced Message Security".



Rysunek 35. Relacje aplikacji i certyfikatów

Na tym diagramie aplikacja działająca jako 'user1' umieszcza komunikat w kolejce zdalnej zarządzanej przez menedżer kolejek CSQ1, który ma być pobrany przez aplikację działającą jako 'user2' z kolejki lokalnej zarządzanej przez menedżer kolejek CSQ2. Na diagramie założono, że strategia Advanced Message Security ma prywatność, co oznacza, że komunikat jest podpisany i zaszyfrowany.

Produkt Advanced Message Security przechwytuje komunikat po wystąpieniu operacji put i korzysta z certyfikatu użytkownika user2(zapisanego w pliku kluczy użytkownika przestrzeni adresowej AMS) w celu zaszyfrowania klucza symetrycznego używanego do szyfrowania danych komunikatu.

Należy zauważyć, że certyfikat user2jest połączony z pierścieniem kluczy użytkownika przestrzeni adresowej AMS z opcją USAGE (SITE). Oznacza to, że użytkownik przestrzeni adresowej AMS może uzyskać dostęp do certyfikatu i klucza publicznego, ale nie do klucza prywatnego.

Po zakończeniu odbierającego program Advanced Message Security przechwytuje komunikat wystawiony przez użytkownika user2i używa certyfikatu user2do deszyfrowania klucza symetrycznego, dzięki czemu może on deszyfrować dane komunikatu. Następnie sprawdza poprawność podpisu user1za pomocą łańcucha certyfikatów ośrodka CA user1, który jest zapisany w pliku kluczy użytkownika przestrzeni adresowej AMS.

Ze względu na ten scenariusz, ale ze strategią ochrony danych integralności, certyfikaty dla użytkownika user2 nie będą wymagane.

Aby można było używać produktu Advanced Message Security do wpisywania komunikatów w kolejkach zabezpieczonych IBM MQ, które mają strategię ochrony komunikatów dotyczącą prywatności lub integralności, produkt Advanced Message Security musi mieć dostęp do tych elementów danych:

- Certyfikat X.509 V2 lub V3 i klucz prywatny dla użytkownika umieszczającego w kolejce komunikat.

- Łańcuch certyfikatów używany do podpisywania certyfikatów cyfrowych wszystkich osób podpisujących komunikaty.
- Jeśli strategia ochrony danych to prywatność, certyfikat X.509 V2 lub V3 dla zamierzonych odbiorców. Zamierzone odbiorcy są wymieniani w strategii Advanced Message Security powiązanej z kolejką.

W przypadku procesów i aplikacji, które działają w systemie z/OS, produkt Advanced Message Security musi mieć certyfikaty w dwóch miejscach:

- W pliku kluczy zarządzanych przez SAF, który jest powiązany z tożsamością RACF aplikacji wysyłającej (aplikacji, która zawiera chroniony komunikat) lub odbierającej aplikację (jeśli używana jest prywatność).

  Certyfikat, który Advanced Message Security jest lokalizowany, jest certyfikatem domyślnym i musi zawierać klucz prywatny. Program Advanced Message Security przyjmuje tożsamość użytkownika produktu z/OS dla aplikacji wysyłającej. Oznacza to, że działa jak surogatka, więc może uzyskać dostęp do klucza prywatnego użytkownika.
- W pliku kluczy zarządzonym przez SAF powiązanym z użytkownikiem przestrzeni adresowej AMS.

  Podczas wysyłania wiadomości chronionych z prywatnością, ten pierścień kluczy zawiera certyfikaty kluczy publicznych odbiorców wiadomości. Podczas odbierania komunikatów zawiera on łańcuch certyfikatów ośrodka certyfikacji wymaganych do sprawdzenia poprawności podpisu nadawcy wiadomości.

Wcześniejsze pokazywane przykłady korzystały z RACF jako lokalnego ośrodka CA. Możliwe jest jednak użycie innego dostawcy PKI (ośrodka certyfikacji) w trakcie instalacji. Jeśli planowane jest użycie innego produktu PKI, należy pamiętać, że klucz prywatny i certyfikat muszą być zaimportowane do pliku kluczy powiązanego z identyfikatorami użytkowników z/OS RACF , które pochodzą z komunikatów programu IBM MQ chronionych przez produkt Advanced Message Security.

Za pomocą komendy RACF RACDCERT można użyć mechanizmu do generowania żądań certyfikatów, które mogą być eksportowane i wysyłane do dostawcy PKI, który ma zostać wydany.

Poniżej znajduje się podsumowanie kroków związanych z certyfikatem:

1. Zażądaj utworzenia certyfikatu ośrodka certyfikacji (CA), w którym RACF jest lokalnym ośrodkiem CA. Pomiń ten krok, jeśli używany jest inny dostawca PKI.
2. Wygeneruj certyfikaty użytkowników podpisane przez ośrodek CA.
3. Utwórz pierścienie kluczy dla użytkowników i identyfikator przestrzeni adresowej AMS produktu Advanced Message Security .
4. Połącz certyfikat użytkownika z pierścieniem kluczy użytkownika z atrybutem domyślnym.
5. Połącz certyfikaty odbiorców z pierścieniem klucza użytkownika przestrzeni adresowej AMS serwera Advanced Message Security przy użyciu atrybutu użycia (site) (Ten krok jest niezbędny tylko dla certyfikatów użytkowników, które ostatecznie będą odbiorcami komunikatów chronionych prywatności).
6. Połącz łańcuchy certyfikatów ośrodka CA pod kątem nadawców komunikatów z pierścieniem kluczy przestrzeni adresowej AMS Advanced Message Security . (Ten krok jest wymagany tylko w przypadku zadań AMS, które będą weryfikować podpisy nadawcy.)

z/OS *Konfigurowanie rezydentnego PKI innego niżz/OS*

Produkt Advanced Message Security for z/OSużywa certyfikatów cyfrowych X.509 V3 w przetwarzaniu zabezpieczania komunikatów umieszczanych na kolejkach IBM MQ lub odbieranych z nich. Sam produkt Advanced Message Security nie tworzy cyklu życia tych certyfikatów ani nie zarządza cyklem życia tych certyfikatów. Funkcja ta jest udostępniana przez infrastrukturę klucza publicznego (PKI). W przykładach tej publikacji ilustrujących użycie certyfikatów używany jest serwer z/OS Security Server RACF do wypełniania żądań certyfikatów.

Niezależnie od tego, czy używany jest serwer z/OS lub PKI inny niżz/OS , produkt AMS for z/OS używa tylko plików kluczy, które są zarządzane przez produkt RACF lub jego odpowiednik. Te pierścienie kluczy są oparte na narzędziu SAF (Security Authorization Facility) i są używane przez produkt AMS for z/OS do

pobierania certyfikatów dla inicjatorów i odbiorców komunikatów umieszczanych w kolejkach produktu IBM MQ lub odbieranych z nich.

W przypadku komunikatów pochodzących z produktu z/OS, które są chronione przez strategię integralności lub szyfrowania, certyfikat i klucz prywatny źródłowego identyfikatora użytkownika muszą być przechowywane w pliku kluczy zarządzanych przez SAF, który jest powiązany z identyfikatorem użytkownika produktu z/OS , który jest inicjatorem komunikatu.

Produkt RACF zawiera możliwość importowania certyfikatów i kluczy prywatnych do kluczy zarządzanych przez produkt RACF. Zapoznaj się z publikacjami z/OS Security Server RACF , aby uzyskać szczegółowe informacje oraz przykłady ładowania certyfikatów do plików kluczy zarządzanych RACF .

Jeśli instalacja korzysta z jednego z obsługiwanych produktów PKI, zapoznaj się z publikacjami, które towarzyszą produktowi, aby uzyskać informacje na temat sposobu jego wdrożenia.

Administrowanie policją zabezpieczeń produktu Advanced Message Security

Produkt 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 dla produktu AMS

Strategie bezpieczeństwa produktu Advanced Message Security są obiektami konceptualnymi opisujących sposób szyfrowania i podpisywania komunikatu.

Szczegółowe informacje na temat atrybutów strategii bezpieczeństwa można znaleźć w następujących podtematach:

Pojęcia pokrewne

“Jakość ochrony” na stronie 657
Strategie ochrony danych Advanced Message Security oznaczają jakość ochrony (QOP).

“Atrybuty strategii bezpieczeństwa w produkcie AMS” na stronie 657
Za pomocą programu Advanced Message Security można wybrać określony algorytm lub metodę w celu ochrony danych.

Nazwy strategii w produkcie AMS

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 Advanced Message Security (AMS) strategii i kolejki.

Tworząc strategię o tej samej nazwie, co kolejka, należy aktywować strategię dla tej kolejki. Kolejki bez zgodnych nazw strategii nie są chronione przez produkt 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 w produkcie AMS

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 w produkcie AMS

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 pamiętać, że strategia, która określa algorytm szyfrowania inny niż NONE , musi również określać co najmniej jedną nazwę wyróżniającą (DN) odbiorców i algorytm podpisu, ponieważ podpisywane są również zaszyfrowane komunikaty produktu Advanced Message Security .

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.

Tolerowanie w programie AMS

Atrybut tolerowania wskazuje, czy produkt 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 w produkcie AMS

Nazwy wyróżniające nadawców identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce. Przed umieszczeniem komunikatu w kolejce nadawca używa swojego certyfikatu do podpisania komunikatu.

Advanced Message Security (AMS) nie sprawdza, czy komunikat został umieszczony w kolejce zabezpieczonej przed danymi przez poprawnego użytkownika do czasu pobrania komunikatu. 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 AMS zwraca błąd do aplikacji odbierającej i umieszcza komunikat w kolejce błędów AMS.

Strategia może mieć określonych zero lub więcej nazw wyróżniających nadawców. Jeśli dla strategii nie określono nazw wyróżniających nadawcy, każdy nadawca może umieścić w kolejce komunikaty zabezpieczone danymi, udostępniając certyfikat nadawcy jako zaufany. Certyfikat nadawcy jest zaufany przez dodanie certyfikatu publicznego do magazynu kluczy dostępnego dla aplikacji odbierającej.

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 podane w kolejności przedstawionej w poniższej tabeli:

Nazwa komponentu	Wartość
CN	Nazwa zwykła obiektu tej nazwy wyróżniającej, taka jak pełna nazwa lub przeznaczenie urządzenia.
OU	Jednostka w organizacji, z którą powiązany jest obiekt nazwy wyróżniającej (DN), taka jak dział korporacyjny lub nazwa produktu.
O	Organizacja, z którą powiązany jest obiekt nazwy wyróżniającej, na przykład korporacja.
L	Miejscowość (miasto lub gmina), w której znajduje się obiekt nazwy wyróżniającej.
ST	Nazwa stanu lub prowincji, w której znajduje się obiekt nazwy wyróżniającej.
C	Kraj, w którym znajduje się obiekt nazwy 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.
- AMS obsługuje nazwy wyróżniające z wartościami tylko z zestawu znaków Latin-1 . Aby utworzyć nazwy wyróżniające zawierające znaki z zestawu, należy najpierw utworzyć certyfikat z nazwą wyróżniającą utworzoną w kodowaniu UTF-8 przy użyciu UNIX z włączonym kodowaniem UTF-8 lub przy użyciu interfejsu GUI systemu **strmqikm** . Następnie należy utworzyć strategię na platformie UNIX z włączonym kodowaniem UTF-8 lub użyć wtyczki AMS dla IBM MQ.
- Metoda używana przez AMSdo przekształcania nazwy nadawcy z formatu x.509 na format nazwy wyróżniającej (DN) zawsze używa dla wartości stanu lub prowincji znaku ST =.
- Następujące znaki specjalne wymagają znaków zmiany znaczenia:

```
, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)
```

- Jeśli nazwa wyróżniająca zawiera odstępy wewnętrzne, należy ująć nazwę wyróżniającą w podwójny cudzysłów.

Pojęcia pokrewne

“Nazwy wyróżniające odbiorców w programie AMS” na stronie 656
Nazwy wyróżniające odbiorców (DN) identyfikują użytkowników, którzy są uprawnieni do pobierania komunikatów z kolejki.

Nazwy wyróżniające odbiorców w programie AMS

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 za pomocą znaków zestawu, należy najpierw utworzyć certyfikat z nazwą wyróżniającą utworzoną w kodowaniu UTF-8 przy użyciu produktu UNIX z włączonym kodowaniem UTF-8 lub za pomocą interfejsu GUI programu **strmqikm** . Następnie należy utworzyć strategię z poziomu platformy UNIX z włączonym kodowaniem UTF-8 lub użyć wtyczki Advanced Message Security do programu IBM MQ.

Pojęcia pokrewne

“Nazwy wyróżniające nadawców w produkcie AMS” na stronie 654
Nazwy wyróżniające nadawców identyfikują użytkowników, którzy mają uprawnienia do umieszczania komunikatów w kolejce. Przed umieszczeniem komunikatu w kolejce nadawca używa swojego certyfikatu do podpisania komunikatu.

Atrybuty strategii bezpieczeństwa w produkcie AMS

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.

Tabela 103. Atrybuty strategii bezpieczeństwa w produkcie AMS

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 są uzupełniane o czwarty poziom w produkcie IBM MQ 9.0 i nowszym, a wszystkie zależą od algorytmów szyfrowania, które są używane 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.
- Poufność-komunikaty umieszczone w kolejce muszą być zaszyfrowane. Więcej informacji na ten temat zawiera sekcja “Właściwości ochrony dostępne w produkcie AMS” na stronie 581
- 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 określa, że komunikaty muszą być szyfrowane po umieszczonym w kolejce, ma QOP POUFNOŚCI. QOP of POUFNOŚCI oznacza, że strategia określa algorytm szyfrowania.

Strategia, która nie określa algorytmu podpisu lub algorytmu szyfrowania, ma wartość QOP (BRAK). Program Advanced Message Security nie zapewnia ochrony danych dla kolejek, dla których istnieje strategia z parametrem QOP o wartości NONE.

Zarządzanie strategiami bezpieczeństwa

Strategia bezpieczeństwa jest obiektem pojęciowym opisanym w sposób kryptograficznie zaszyfrowany i podpisany.

Miejsce, z którego uruchamiane są wszystkie zadania administracyjne związane ze strategiami bezpieczeństwa, zależy od platformy, która jest używana.

- ULW W systemach UNIXi Windowssłużą do zarządzania strategiami bezpieczeństwa przy użyciu komend DELETE POLICY, DISPLAY POLICYi SET POLICY (lub równoważnych PCF).
  - UNIX W systemie UNIXzadania administracyjne można uruchamiać z poziomu produktu *MQ_INSTALLATION_PATH*/bin.
  - Windows Na platformach Windows zadania administracyjne można uruchamiać z dowolnego miejsca, w którym zmienna środowiskowa PATH jest aktualizowana podczas instalacji.
- IBM i W systemie IBM ikomendy DSPMQMSPL, SETMQMSPLi WRKMQMSPL są instalowane w bibliotece systemowej QSYS dla języka podstawowego systemu, w którym zainstalowany jest produkt IBM MQ .

  Dodatkowe wersje języków narodowych są instalowane w bibliotekach QSYS29xx w zależności od obciążenia funkcji języka. Na przykład komputer z językiem angielskim (Stany Zjednoczone), jako język podstawowy i język koreański jako język dodatkowy, zawiera komendy języka angielskiego (Stany Zjednoczone) zainstalowane w bibliotece QSYS, a obciążenie koreańskiego języka dodatkowego w QSYS2962 jako 2962 jest obciążeniem języka koreańskiego.
- z/OS W systemie z/OSkomendy administracyjne są uruchamiane przy użyciu programu narzędziowego strategii bezpieczeństwa komunikatów (CSQ0UTIL). Gdy strategie są tworzone, modyfikowane lub usuwane w systemie z/OS, zmiany nie są rozpoznawane przez produkt Advanced Message Security , dopóki menedżer kolejek nie zostanie zatrzymany i zrestartowany, albo za pomocą komendy z/OS MODIFY służy do odświeżania konfiguracji strategii produktu Advanced Message Security . Na przykład:

  ```
  F <qmgr ssid>AMSM,REFRESH POLICY
  ```

Zadania pokrewne

“Tworzenie strategii bezpieczeństwa w produkcie AMS” na stronie 659
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 w produkcie AMS” na stronie 660
Za pomocą programu Advanced Message Security można zmieniać szczegóły strategii zabezpieczeń, które zostały już zdefiniowane.

“Wyświetlanie i zrzucanie strategii bezpieczeństwa w produkcie AMS” na stronie 660
Komenda **dspmqspl** służy do wyświetlania listy wszystkich strategii bezpieczeństwa lub szczegółów nazwanej strategii, w zależności od podanych parametrów wiersza komend.

“Usuwanie strategii bezpieczeństwa w produkcie AMS” na stronie 662
Aby usunąć strategie bezpieczeństwa w programie Advanced Message Security, należy użyć komendy `setmqspl` .

Operacyjny Advanced Message Security

Odsyłacze pokrewne

Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL)

Tworzenie strategii bezpieczeństwa w produkcie AMS

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 IBM MQ.
- Aby nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, użytkownik musi mieć uprawnienia niezbędne do połączenia się z menedżerem kolejek:
  - z/OS W systemie z/OSnależy nadać uprawnienia udokumentowane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na innych platformach innych niż z/OSnależy nadać niezbędne uprawnienia + connect, + inq i + chg za pomocą komendy setmqaut .

  Więcej informacji na temat konfigurowania zabezpieczeń zawiera sekcja “Konfigurowanie zabezpieczeń” na stronie 130.
- z/OS W systemie z/OSupewnij się, że wymagane obiekty systemowe zostały zdefiniowane zgodnie z definicjami w CSQ4INSM.

Przykład

Poniżej przedstawiono przykład tworzenia strategii dla menedżera kolejek QMGR. Strategia określa, że komunikaty są podpisywane przy użyciu algorytmu SHA256 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 SHA256 -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 3DES dla certyfikatów o nazwach wyróżniających: CN=john, O=IBM, C=US i CN=jeff, O=IBM, C=US i podpisanych przy użyciu algorytmu SHA256 dla certyfikatu o nazwie wyróżniającej: CN=phil, O=IBM, C=US

```
setmqspl -m QMGR -p MY.OTHER.QUEUE -s SHA256 -e 3DES -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 w produkcie AMS

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 nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, użytkownik musi mieć uprawnienia niezbędne do nawiązania połączenia z menedżerem kolejek.
  - z/OS W systemie z/OSnależy nadać uprawnienia udokumentowane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na innych platformach innych niż z/OSnależy nadać niezbędne uprawnienia + connect, + inq i + chg za pomocą komendy setmqaut .

  Więcej informacji na temat konfigurowania zabezpieczeń zawiera sekcja “Konfigurowanie zabezpieczeń” na stronie 130.

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 mają być szyfrowane przy użyciu algorytmu 3DES dla autorów (**-a**) posiadających certyfikaty o nazwie wyróżniającej CN=alice, O=IBM, C=US i podpisanych z algorytmem SHA256 dla odbiorców (**-r**) posiadających certyfikaty o nazwie wyróżniającej CN=jeff, O=IBM, C = US.

```
setmqspl -m QMGR -p MYQUEUE -e 3DES -s SHA256 -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 SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Odsyłacze pokrewne

setmqspl (ustawienie strategii bezpieczeństwa)

Wyświetlanie i zrzucanie strategii bezpieczeństwa w produkcie AMS

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 nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, użytkownik musi mieć uprawnienia niezbędne do nawiązania połączenia z menedżerem kolejek.

– z/OS W systemie z/OSnależy nadać uprawnienia udokumentowane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

– Multi Na innych platformach innych niż z/OSnależy nadać niezbędne uprawnienia + connect, + inq i + chg za pomocą komendy setmqaut .

Więcej informacji na temat konfigurowania zabezpieczeń zawiera sekcja “Konfigurowanie zabezpieczeń” na stronie 130.

O tym zadaniu

Poniżej znajduje się lista opcji komendy **dspmqspl** :

*Tabela 104. 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 poniższym przykładzie przedstawiono sposób tworzenia dwóch strategii bezpieczeństwa dla produktu `venus.queue.manager`:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s sha256 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s sha256 -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: SHA256
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: SHA256
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: SHA256
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 SHA256 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export
```

z/OS W systemie z/OSwyeksportowana informacja o strategii jest zapisywana przez CSQ0UTIL w DD EXPORT DD.

Multi Na platformach innych niż z/OSprzekieruj dane wyjściowe do pliku, na przykład:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Aby zaimportować strategię bezpieczeństwa:

- Windows W systemie Windowsuruchom komendę `policies.bat`.
- UNIX W systemie UNIX:
  1. Zaloguj się jako użytkownik, który należy do grupy administracyjnej `mqm` IBM MQ .
  2. Wydaj komendę `. policies.sh`.
- z/OS W systemie z/OS należy użyć programu narzędziowego CSQ0UTIL , określając w systemie SYSIN zestaw danych zawierający wyeksportowane informacje o strategii.

Odsyłacze pokrewne

Pełna lista atrybutów komendy dspmqspl

Usuwanie strategii bezpieczeństwa w produkcie AMS

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 nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, użytkownik musi mieć uprawnienia niezbędne do nawiązania połączenia z menedżerem kolejek.
  - z/OS W systemie z/OSnależy nadać uprawnienia udokumentowane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na innych platformach innych niż z/OSnależy nadać niezbędne uprawnienia + connect, + inq i + chg za pomocą komendy setmqaut .

  Więcej informacji na temat konfigurowania zabezpieczeń zawiera sekcja “Konfigurowanie zabezpieczeń” na stronie 130.

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 w programie AMS

Kolejki systemowe umożliwiają komunikację między programem IBM MQ a jego aplikacjami pomocniczymi. Za każdym razem, gdy tworzony jest menedżer kolejek, tworzona jest również kolejka systemowa do przechowywania wewnętrznych komunikatów i danych produktu IBM MQ . Można chronić kolejki systemowe za pomocą programu Advanced Message Security , aby tylko autoryzowani użytkownicy mieli dostęp do nich lub ich odszyfrowywanie.

Ochrona kolejki systemowej jest zgodna z tym samym wzorcem, co ochrona kolejek regularnych. Patrz “Tworzenie strategii bezpieczeństwa w produkcie AMS” na stronie 659.

Windows Aby użyć ochrony kolejki systemowej w systemie Windows, skopiuj plik `keystore.conf` do następującego katalogu:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

z/OS W systemie z/OS, 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 uzyskiwać 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 sprawdzenia 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 IBM MQ Explorer nie są chronione przez produkt AMS.

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
- z/OS SYSTEM.ADMIN.COMMAND.QUEUE
- 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

- z/OS SYSTEM.BROKER.CLIENTS.DATA
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- z/OS SYSTEM.BROKER.SUBSCRIPTIONS.DATA
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- z/OS SYSTEM.CHLAUTH.DATA.QUEUE
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- z/OS SYSTEM.COMMAND.INPUT
- z/OS SYSTEM.DDELAY.LOCAL.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
- z/OS SYSTEM.JMS.PS.STATUS.QUEUE
- z/OS SYSTEM.JMS.REPORT.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- z/OS SYSTEM.QSG.CHANNEL.SYNCQ
- z/OS SYSTEM.QSG.TRANSMIT.QUEUE
- z/OS SYSTEM.QSG.UR.RESOLUTION.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- z/OS 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 Advanced Message Security opiera się na menedżerze obiektów (Object Authority Manager-OAM) i każdej próbie wykonania tych komend przez użytkownika, który nie należy do grupy mqm, która jest grupą administracyjną IBM 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
```

Uwaga: Te uprawnienia OAM należy ustawić tylko wtedy, gdy klienty mają być podłączane do menedżera kolejek przy użyciu produktu Advanced Message Security 7.0.1.

Ostrzeżenie: Przeglądaj uprawnienia do SYSTEM.PROTECTION.POLICY.QUEUE nie jest obowiązkowa we wszystkich sytuacjach. Program IBM MQ optymalizuje wydajność przez strategie buforowania, dzięki czemu nie będzie konieczne przeglądanie rekordów w celu uzyskania szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Produkt IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Jeśli więc menedżer kolejek ma zdefiniowaną niewielką liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Jednak należy nadać uprawnienie do przeglądania tej kolejki, w przypadku, gdy istnieje duża liczba zdefiniowanych strategii lub jeśli używane są stare klienty. SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach wygenerowanych przez kod AMS. Uprawnienie do umieszczania w tej kolejce jest sprawdzane tylko przy próbie umieszczenia komunikatu o błędzie w kolejce. Uprawnienia użytkownika do umieszczenia w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki chronionej AMS.

Nadawanie uprawnień zabezpieczeń

W przypadku korzystania z zabezpieczeń zasobów komend należy skonfigurować uprawnienia, aby umożliwić funkcj Advanced Message Security . W tym temacie opisano komendy RACF w przykładach. Jeśli w przedsiębiorstwie używany jest inny zewnętrzny menedżer zabezpieczeń (ESM), należy użyć równoważnych komend dla tego programu ESM.

Aby nadać uprawnienia zabezpieczeń, należy wykonać trzy aspekty:

- “Przestrzeń adresowa AMSM” na stronie 665
- “CSQ0UTIL” na stronie 666
- “Korzystanie z kolejek, dla których zdefiniowano strategię Advanced Message Security” na stronie 666

Uwagi: Przykładowe komendy używają następujących zmiennych.

1. *QMgrName* -nazwa menedżera kolejek.

   z/OS W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejki.
2. *nazwa_użytkownika* -może to być nazwa grupy.
3. W przykładach przedstawiono klasę MQQUEUE. Może to być również MXQUEUE, GMQQUEUE lub GMXQUEUE. Więcej informacji na ten temat zawiera sekcja “Profile dla bezpieczeństwa kolejki” na stronie 203.

Ponadto, jeśli profil już istnieje, nie jest wymagane wykonanie komendy RDEFINE.

Przestrzeń adresowa AMSM

Należy wprowadzić pewne zabezpieczenia produktu IBM MQ do nazwy użytkownika, w ramach której działa przestrzeń adresowa produktu Advanced Message Security .

- Dla połączenia wsadowego z menedżerem kolejek, problem

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
           PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Aby uzyskać dostęp do SYSTEM.PROTECTION.POLICY.QUEUE, wprowadź:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
            PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

CSQ0UTIL

Program narzędziowy, który umożliwia użytkownikom uruchamianie komend **setmqspl** i **dspmqspl** , wymaga następujących uprawnień, w przypadku których nazwa użytkownika jest identyfikatorem użytkownika zadania:

- W przypadku połączenia wsadowego z menedżerem kolejek należy wykonać następujące czynności:

```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
            PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Aby uzyskać dostęp do SYSTEM.PROTECTION.POLICY.QUEUE, która jest wymagana dla komendy **setmqpol** , należy wprowadzić komendę:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
              PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- Aby uzyskać dostęp do SYSTEM.PROTECTION.POLICY.QUEUE, która jest wymagana dla komendy **dspmqpol** , należy wprowadzić komendę:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
                PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

Korzystanie z kolejek, dla których zdefiniowano strategię Advanced Message Security

Gdy aplikacja wykonuje dowolną pracę z kolejkami, dla których zdefiniowano strategię, ta aplikacja wymaga dodatkowych uprawnień, aby umożliwić Advanced Message Security ochronę komunikatów.

Aplikacja wymaga:

- Dostęp do odczytu do SYSTEM.PROTECTION.POLICY.QUEUE. W tym celu należy wykonać następujące czynności:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Umieść dostęp do SYSTEM.PROTECTION.ERROR.QUEUE. W tym celu należy wykonać następujące czynności:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
            PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

IBM i Konfigurowanie certyfikatów i pliku konfiguracyjnego magazynu kluczy w systemie IBM i

Pierwszym zadaniem podczas konfigurowania ochrony produktu Advanced Message Security jest utworzenie certyfikatu i powiązanie go ze środowiskiem. Powiązanie jest konfigurowane za pomocą pliku znajdującego się w zintegrowanym systemie plików (IFS).

Procedura

1. Aby utworzyć samopodpisany certyfikat za pomocą narzędzia OpenSSL dostarczanego z produktem IBM i, wprowadź następującą komendę z powłoki QShell:

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
$HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
```

   Komenda pyta o różne atrybuty nazwy wyróżniającej dla nowego certyfikatu samopodpisanego, w tym:

   - Nazwa zwykła (CN =)
   - Organizacja (O =)
   - Kraj (C =)

   Spowoduje to utworzenie niezaszyfrowanego klucza prywatnego i zgodnego certyfikatu, zarówno w formacie PEM (Privacy Enhanced Mail).

   Dla prostoty, wystarczy wprowadzić wartości dla nazwy zwykłej, organizacji i kraju. Te atrybuty i wartości są ważne podczas tworzenia strategii.

   Dodatkowe zapytania i atrybuty można dostosować, określając niestandardowy plik konfiguracyjny openssl w wierszu komend z parametrem **-config** . Więcej informacji na temat składni pliku konfiguracyjnego można znaleźć w dokumentacji OpenSSL .

   Na przykład następująca komenda dodaje dodatkowe rozszerzenia certyfikatu X.509 v3 :

```
/QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048
-keyout $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365 -config myconfig.cnf
```

   gdzie myconfig.cnf jest plikiem strumieniowym ASCII, który zawiera następujące informacje:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = myextensions

[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = GB
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Hants
localityName = Locality Name (eg, city)
localityName_default = Hursley
organizationName = Organization Name (eg, company)
organizationName_default = IBM United Kingdom
organizationalUnitName = Organizational Unit Name (eg, department)
organizationalUnitName_default = IBM MQ Development
commonName = Common Name (eg, Your Name)

[myextensions]
keyUsage = digitalSignature,nonRepudiation,dataEncipherment,keyEncipherment
extendedKeyUsage = emailProtection
```

2. Program AMS wymaga, aby zarówno certyfikat, jak i klucz prywatny były przechowywane w tym samym pliku. Wykonaj następującą komendę, aby to osiągnąć:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

   Plik `private.pem` w produkcie $HOME zawiera teraz pasujący klucz prywatny i certyfikat, natomiast plik `mycert.pem` zawiera wszystkie certyfikaty publiczne, dla których można szyfrować komunikaty i sprawdzać poprawność podpisów.

   Dwa pliki muszą być powiązane z danym środowiskiem, tworząc plik konfiguracyjny magazynu kluczy `keystore.conf`w domyślnym położeniu.

   Domyślnie program AMS szuka konfiguracji magazynu kluczy w podkatalogu `.mqs` katalogu osobistego użytkownika.

3. W QShell utwórz plik `keystore.conf` :

```
mkdir -p $HOME/.mqs
echo "pem.private = $HOME/private.pem" > $HOME/.mqs/keystore.conf
echo "pem.public = $HOME/mycert.pem" >> $HOME/.mqs/keystore.conf
echo "pem.password = unused" >> $HOME/.mqs/keystore.conf
```

IBM i *Tworzenie strategii w systemie IBM i*

Przed utworzeniem strategii należy utworzyć kolejkę, w której będą przechowywane komunikaty chronione.

Procedura

1. W wierszu komend wpisz komendę;

```
CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
```

   gdzie mqmname to nazwa menedżera kolejek.

   Użyj komendy DSPMQM, aby sprawdzić, czy menedżer kolejek może używać strategii bezpieczeństwa. Upewnij się, że **Security Policy Capability** ma wartość **YES*.

   Najprostszą strategią, którą można zdefiniować, jest strategia integralności, która jest osiągana przez utworzenie strategii z algorytmem podpisu cyfrowego, ale nie jest algorytmem szyfrowania.

   Komunikaty są podpisywane, ale nie są szyfrowane. Jeśli komunikaty mają być szyfrowane, należy określić algorytm szyfrowania i jeden lub więcej adresatów.

   Certyfikat w publicznym magazynie kluczy dla zamierzonego odbiorcy komunikatu jest identyfikowany za pomocą nazwy wyróżniającej.
2. Wyświetl nazwy wyróżniające certyfikatów w publicznym magazynie kluczy, `mycert.pem` w $HOME, za pomocą następującej komendy w QShell:

```
/QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
```

   Należy wprowadzić nazwę wyróżniającą jako zamierzony odbiorca, a nazwa strategii musi być zgodna z nazwą kolejki, która ma być chroniona.
3. W wierszu komend CL wpisz na przykład:

```
SETMQMSPL POLICY(PROTECTED) MQMNAME (mqmname)SIGNALG(*SHA256) ENCALG(*AES256) RECIP('CN=..,
O=.., C=..')
```

   gdzie mqmname to nazwa menedżera kolejek.

   Po utworzeniu strategii wszystkie komunikaty, które są umieszczane, przeglądane lub niszczone przez tę nazwę kolejki, podlegają strategii AMS .

Odsyłacze pokrewne

Wyświetlenie menedżera kolejek komunikatów (Display Message Queue Manager-DSPMQM)

Ustaw strategię bezpieczeństwa MQM (SETMQMSPL)

IBM i *Testowanie strategii w systemie IBM i*

Użyj przykładowych aplikacji udostępnionych z produktem w celu przetestowania strategii bezpieczeństwa.

O tym zadaniu

Przykładowych aplikacji udostępnionych z produktem IBM MQ , takich jak AMQSPUT4, AMQSGET4, AMQSGBR4, oraz narzędzi, takich jak WRKMQMMSG, można użyć do umieszczania, przeglądania i pobierania komunikatów za pomocą nazwy kolejki zabezpieczonej.

Jeśli wszystko zostało poprawnie skonfigurowane, nie powinno być różnicy w zachowaniu aplikacji w przypadku kolejki niechronionych dla tego użytkownika.

Użytkownik, który nie jest skonfigurowany dla produktu Advanced Message Security, lub użytkownik, który nie ma wymaganego klucza prywatnego do deszyfrowania komunikatu, nie będzie mógł wyświetlić komunikatu. Użytkownik otrzymuje kod zakończenia RCFAIL, który jest odpowiednikiem MQCC_FAILED (2) i kodem przyczyny RC2063 (MQRC_SECURITY_ERROR).

Aby sprawdzić, czy ochrona AMS jest w mocy, należy umieścić kilka komunikatów testowych w kolejce PROTECTED, na przykład za pomocą komendy AMQSPUT0. Następnie można utworzyć kolejkę aliasową w celu przeglądania surowych danych chronionych podczas pozostania w stanie spoczynku.

Procedura

Aby nadać użytkownikowi niezbędne uprawnienia, uruchom komendę:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

Przeglądanie za pomocą nazwy kolejki ALIAS, na przykład za pomocą komendy AMQSBCG4 lub WRKMQMMSG, powinno ujawnić większe komunikaty produktu `scrambled` , w przypadku których w kolejce chronionej wyświetlane są komunikaty jawne.

Komunikaty scrambled są widoczne, ale oryginalny tekst jawny nie jest rozszyfrowalny przy użyciu kolejki ALIAS, ponieważ nie ma strategii dla AMS w celu wymuszenia dopasowania tej nazwy. W związku z tym zwracane są surowe dane chronione.

Odsyłacze pokrewne

Ustaw strategię bezpieczeństwa MQM (SETMQMSPL)

Praca z komunikatami MQ (WRKMQMMSG)

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 IBM MQ to komunikaty formatu PCF wysłane do dedykowanych kolejek w menedżerze kolejek, w którym wystąpiło zdarzenie.

Komunikaty zdarzeń konfiguracji są wysyłane do systemu SYSTEM.ADMIN.CONFIG.EVENT .

Komunikaty zdarzeń komend są wysyłane do systemu SYSTEM.ADMIN.COMMAND.EVENT .

Zdarzenia są generowane niezależnie od narzędzi, które są używane 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 w produkcie AMS” na stronie 659, które generują dwa komunikaty zdarzeń produktu IBM MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy
- “Zmiana strategii bezpieczeństwa w produkcie AMS” na stronie 660, który generuje trzy komunikaty zdarzeń produktu IBM MQ :
  - Zdarzenie konfiguracyjne, które zawiera stare wartości strategii bezpieczeństwa

  - Zdarzenie konfiguracyjne, które zawiera nowe wartości strategii bezpieczeństwa.
  - Zdarzenie komendy
- "Wyświetlanie i zrzucanie strategii bezpieczeństwa w produkcie AMS" na stronie 660, który generuje jeden komunikat zdarzenia IBM MQ :
  - Zdarzenie komendy
- "Usuwanie strategii bezpieczeństwa w produkcie AMS" na stronie 662, który generuje dwa komunikaty zdarzeń produktu IBM MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy

Włączanie i wyłączanie rejestrowania zdarzeń

Zdarzenia komendy i konfiguracji są sterowane 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, ustaw wartość opcji **CONFIGEV** na ENABLED. Aby wyłączyć zdarzenia konfiguracji, ustaw wartość opcji **CONFIGEV** na DISABLED. Na przykład można włączyć zdarzenia konfiguracji przy użyciu następującej komendy MQSC:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Zdarzenia komendy

Aby włączyć zdarzenia komend, należy ustawić opcję **CMDEV** na wartość ENABLED. Aby włączyć zdarzenia komend dla komend z wyjątkiem komend **DISPLAY MQSC** i komendy Inquire PCF, należy ustawić parametr **CMDEV** na wartość NODISPLAY. Aby wyłączyć zdarzenia komendy, należy ustawić opcję **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 IBM 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 występują 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:

Identyfikator użytkownika EventUser

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:

MQEVO_CONSOLE
Komenda konsoli-wiersz komend.

MQEVO_MSG
Komunikat komendy z wtyczki IBM 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.

Znacznik EventAccounting

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.

Dane EventIdentity

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.

Typ EventAppl

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.

Nazwa EventAppl

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.

Źródło EventAppl

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.

Komenda

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 IBM MQ 8.0 `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 .

Możliwe wartości deskryptora komunikatu MQMD można znaleźć w sekcji 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. Możliwe 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.
Maksymalna długość:	DŁUGOŚĆ_CZASU_MQ.
Zwrócone:	Zawsze.

SecurityId

Opis:	Wartość MQMD.AccountingToken w przypadku komunikatów serwera komend lub identyfikatora SID produktu Windows dla komendy lokalnej.
Identyfikator:	**MQBACF_EVENT_SECURITY_ID**
Typ danych:	MQCBS.
Maksymalna długość:	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 IBM 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: 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 IBM MQ 8.0 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 IBM MQ 8.0 lub w pliku `cmqc.h` .

Maksymalna długość: MQ_OBJECT_NAME_LENGTH.

Zwrócone: Zawsze.

PolicyVersion

Opis: Wersja strategii produktu Advanced Message Security .

Identyfikator: **MQIA_POLICY_VERSION**

Typ danych: MQCFIN

Wartość **238** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Zwrócone: Zawsze

TolerateFlag

Opis: Opcja tolerowania strategii Advanced Message Security .

Identyfikator: **MQIA_TOLERATE_UNPROTECTED**

Typ danych: MQCFIN

Wartość **235** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 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 IBM MQ 8.0 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 IBM MQ 8.0 lub w pliku `cmqc.h` .

Zwrócone: Za każdym razem, gdy w strategii produktu IBM MQ jest zdefiniowany algorytm szyfrowania

SignerDNs

Opis: Temat DistinguishedName dozwolonych osób podpisujących.

Identyfikator: **MQCA_SIGNER_DN**

Typ danych: MQCFSL

Wartość: **2113** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Maksymalna długość: Najdłuższa nazwa wyróżniająca (DN) osoby podpisującej w strategii, ale nie ma już wartości MQ_DISTINGUISHED_NAME_LENGTH

Zwrócone: Zawsze, gdy jest zdefiniowana w strategii IBM MQ .

RecipientDNs

Opis: Temat DistinguishedName dozwolonych osób podpisujących.

Identyfikator: **MQCA_RECIPIENT_DN**

Typ danych: MQCFSL

Wartość: **2114** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Maksymalna długość:	Najdłuższa nazwa wyróżniająca (DN) odbiorcy w strategii, ale nie jest dłuższa niż wartość MQ_DISTINGUISHED_NAME_LENGTH.
Zwrócone:	Zawsze, gdy jest zdefiniowana w strategii IBM MQ .

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.

Ten podręcznik zawiera informacje na temat planowanych interfejsów programistycznych, które umożliwiają klientom pisanie programów w celu uzyskania dostępu do usług produktu 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: