9.3

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 753.

Niniejsze wydanie publikacji dotyczy wersji 9, wydania 3 produktu IBM® MQ oraz wszystkich jego późniejszych wydań i modyfikacji, aż do odwołania w nowych wydaniach publikacji.

Spis treści

zabezpieczanieIBM MQ.....7
przegląd zabezpieczeń.....7
Identyfikacja i uwierzytelnianie.....7
Niezaprzeczalność.....8
Autoryzacja.....9
Kontrola.....9
Poufność.....10
Integralność danych.....10
Pojęcia związane z szyfrowaniem.....11
Szyfrujące protokoły bezpieczeństwa: TLS.....18
IBM MQ mechanizmy zabezpieczeń.....24
Planowanie wymagań dotyczących bezpieczeństwa.....90
Planowanie identyfikacji i uwierzytelniania.....91
Planowanie autoryzacji.....94
Poufność planowania.....110
Planowanie integralności danych.....119
Planowanie kontroli.....119
Planowanie bezpieczeństwa według topologii.....120
Zapory firewall i Internet pass-thru.....135
Lista kontrolna implementacji zabezpieczeń systemu IBM MQ for z/OS.....136
Konfigurowanie zabezpieczeń.....139
Konfigurowanie zabezpieczeń w systemie AIX, Linux, and Windows.....139
Konfigurowanie zabezpieczeń w systemie IBM i.....165
Konfigurowanie zabezpieczeń w systemie z/OS.....196
Konfigurowanie zabezpieczeń systemu IBM MQ MQI client.....286
Konfigurowanie kanałów TLS za pomocą komend MQSC.....289
Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie IBM i.....291
Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie AIX, Linux, and Windows.....291
Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie z/OS.....292
Praca z protokołem SSL/TLS.....293
Identyfikowanie i uwierzytelnianie użytkowników.....365
Użytkownicy uprzywilejowani.....365
Identyfikowanie i uwierzytelnianie użytkowników przy użyciu struktury MQCSP.....367
Implementowanie identyfikacji i uwierzytelniania w wyjściach zabezpieczeń.....368
Odwzorowanie tożsamości w wyjściach komunikatów.....369
Odwzorowanie tożsamości w wyjściu funkcji API i wyjściu funkcji API.....370
Praca ze znacznikami uwierzytelniania.....371
Praca z odwołanymi certyfikatami.....382
Korzystanie z metody PAM (Pluggable Authentication Method).....394
Autoryzowanie dostępu do obiektów.....395
Określanie, który użytkownik jest używany do autoryzacji.....395
Kontrolowanie dostępu do obiektów za pomocą OAM w systemie AIX, Linux, and Windows.....397
Nadawanie wymaganego dostępu do zasobów.....408
Uprawnienia do administrowania systemem IBM MQ w systemie AIX, Linux, and Windows.....446
Uprawnienia do pracy z obiektami IBM MQ w systemie AIX, Linux, and Windows.....448
Implementowanie kontroli dostępu w wyjściach zabezpieczeń.....454
Implementowanie kontroli dostępu w wyjściach komunikatów.....456
Implementowanie kontroli dostępu w wyjściu funkcji API i wyjściu funkcji API.....456
Bezpieczeństwo kolejek strumieniowych.....456
Autoryzacja LDAP.....459
Ustawianie autoryzacji.....460
Wyświetlanie autoryzacji.....462

Inne uwagi dotyczące używania autoryzacji LDAP....462
Przełączanie między modelami autoryzacji systemu operacyjnego i LDAP....464
Administrowanie LDAP....464
Poufność komunikatów....466
Włączanie CipherSpecs....466
Resetowanie kluczy tajnych SSL i TLS....514
Implementowanie poufności w programach obsługi wyjścia użytkownika....515
Poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych. 517
Przegląd kroków szyfrowania zestawu danych IBM MQ for z/OS....517
Przykład szyfrowania aktywnych dzienników menedżera kolejek....518
Uwagi dotyczące szyfrowania zestawu danych z/OS w grupie współużytkowania kolejek....521
Uwagi dotyczące migracji wstecznej przy korzystaniu z szyfrowania zestawu danych z/OS....522
Integralność danych komunikatów....525
Kontrola....526
Zabezpieczanie klastrów....526
Zatrzymywanie nieautoryzowanych menedżerów kolejek wysyłających komunikaty....526
Zatrzymywanie nieautoryzowanych menedżerów kolejek umieszczanych w kolejkach....526
Autoryzowanie umieszczania komunikatów w zdalnych kolejkach klastra....527
Blokowanie dołączania menedżerów kolejek do klastra....528
Wymuszanie opuszczenia klastra przez niechciane menedżery kolejek....529
Blokowanie odbierania komunikatów przez menedżery kolejek....530
SSL/TLS i klastry....530
Zabezpieczenia publikowania/subskrypcji....533
Przykładowa konfiguracja zabezpieczeń publikowania/subskrypcji....541
Zabezpieczenia subskrypcji....554
Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek....556
Bezpieczeństwo systemów IBM MQ Console i REST API....559
Konfigurowanie użytkowników i ról....561
Zmiana certyfikatu udostępnionego przez IBM MQ Console w przeglądarce....574
Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console....577
Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API....581
Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API....582
Osadzanie IBM MQ Console w i-ramce....584
Konfigurowanie mechanizmu CORS dla serwera REST API....585
Konfigurowanie sprawdzania poprawności nagłówka hosta dla IBM MQ Console i REST API....586
Kontrola....587
Zagadnienia dotyczące zabezpieczeń produktów IBM MQ Console i REST API w systemie z/OS.. 588
Zarządzanie kluczami i certyfikatami w systemie AIX, Linux, and Windows....593
Komendy runmqckm i runmqakm w systemie AIX, Linux, and Windows....594
Opcje runmqckm i runmqakm w systemie AIX, Linux, and Windows....606
Kody błędów komendy runmqakm w systemie AIX, Linux, and Windows....610
Ochrona haseł w plikach konfiguracyjnych komponentu IBM MQ....617
Ograniczenia ochrony przez szyfrowanie haseł....625
Ochrona szczegółów uwierzytelniania w bazie danych....625
zabezpieczanieManaged File Transfer....627
Szyfrowanie zapisanych referencji w produkcie MFT....627
Uwierzytelnianie w systemach MFT i IBM MQ....630
MFT przestrzenie prywatne....636
Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT....642
Nawiązywanie połączenia z menedżerem kolejek w trybie klienta z uwierzytelnianiem kanału.... 644
Konfigurowanie protokołu SSL lub TLS między agentem mostu Connect:Direct i węzłem Connect:Direct....645
Zabezpieczanie klientów AMQP....648
Ograniczanie przejęcia klienta AMQP....650
Konfigurowanie usługi JAAS dla kanałów AMQP....651
Advanced Message Security....652
Przegląd produktu Advanced Message Security....652

Advanced Message Security instalacja, przegląd..... 697
Kontrola dla AMS w systemie z/OS.....697
Używanie magazynów kluczy i certyfikatów z programem AMS.....699
Administrowanie strategiami bezpieczeństwa Advanced Message Security.....728

Uwagi.....753
Informacje dotyczące interfejsu programistycznego..... 754
Znaki towarowe..... 755

zabezpieczanieIBM MQ

Bezpieczeństwo jest ważne zarówno dla programistów aplikacji IBM MQ , jak i dla administratorów systemu IBM MQ . Należy zadbać o to, aby cały sprzęt i oprogramowanie znajdujące się w bezpiecznej strefie i na stacjach roboczych operatora były objęte cyklem życia wsparcia, aby były aktualne z obowiązkowymi aktualizacjami oprogramowania oraz aby aktualizacje bezpieczeństwa były szybko zainstalowane.

Odsyłacze pokrewne

IBM Zarządzanie słabymi punktami zabezpieczeń

IBM Z i LinuxOne Security Portal

przegląd zabezpieczeń

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

Pojęcia i mechanizmy zabezpieczeń, które mają zastosowanie do dowolnego systemu komputerowego, zostały przedstawione jako pierwsze, a następnie omówienie tych mechanizmów zabezpieczeń w trakcie ich implementacji w produkcie IBM MQ.

Powszechnie akceptowane aspekty bezpieczeństwa są następujące:

- “Identyfikacja i uwierzytelnianie” na stronie 7
- “Autoryzacja” na stronie 9
- “Kontrola” na stronie 9
- “Poufność” na stronie 10
- “Integralność danych” na stronie 10

Mechanizmy zabezpieczeń są narzędziami technicznymi i technikami używanymi do implementowania usług zabezpieczeń. Mechanizm może działać samodzielnie lub z innymi w celu zapewnienia określonej usługi. Przykłady wspólnych mechanizmów bezpieczeństwa są następujące:

- “Kryptografia” na stronie 11
- “Streszczenia komunikatów i podpisy cyfrowe” na stronie 13
- “certyfikaty cyfrowe” na stronie 13
- “Infrastruktura klucza publicznego (PKI)” na stronie 18

Podczas planowania implementacji produktu IBM MQ należy rozważyć, które mechanizmy zabezpieczeń są wymagane do zaimplementowania istotnych dla użytkownika aspektów zabezpieczeń. Informacje na temat zagadnień, które należy wziąć pod uwagę po zapoznaniu się z tymi tematami, zawiera sekcja “Planowanie wymagań dotyczących bezpieczeństwa” na stronie 90.

Identyfikacja i uwierzytelnianie

Identyfikacja umożliwia jednoznaczną identyfikację użytkownika systemu lub aplikacji działającej w systemie. *Uwierzytelnianie* to zdolność do udowodnienia, że użytkownik lub aplikacja rzeczywiście jest osobą lub aplikacją, za którą się podaje.

Na przykład można rozważyć użytkownika, który loguje się do systemu, wprowadzając identyfikator użytkownika i hasło. System używa identyfikatora użytkownika do identyfikacji użytkownika. System uwierzytelnia użytkownika podczas logowania, sprawdzając, czy podane hasło jest poprawne.

Identyfikacja i uwierzytelnianie w programie IBM MQ

Gdy aplikacja łączy się z produktem IBM MQ, tożsamość użytkownika jest zawsze powiązana z połączeniem. Tożsamość użytkownika jest początkowo identyfikatorem użytkownika systemu

operacyjnego, który jest powiązany z procesem aplikacji. Ta tożsamość jest często wystarczająca dla aplikacji powiązanych lokalnie, które są udostępniane w tym samym systemie co menedżer kolejek. Jednak menedżer kolejek może również uwierzytelnić i zmodyfikować tożsamość powiązaną z połączeniem na kilka sposobów. Uwierzytelnianie tożsamości powiązanej z połączeniem jest ważne, gdy aplikacje klienckie, które nie mogą być traktowane jako zaufane, łączą się z menedżerem kolejek za pośrednictwem sieci.

Tożsamość powiązaną z połączeniem aplikacji z menedżerem kolejek produktu IBM MQ można ustanowić za pomocą dowolnego z następujących mechanizmów:

- Gdy aplikacja nawiązuje połączenie z menedżerem kolejek, może udostępnić ID użytkownika i hasło. Menedżer kolejek sprawdza poprawność referencji na podstawie swojej konfiguracji. Na przykład identyfikator użytkownika i hasło mogą zostać przekazane do systemu operacyjnego menedżera kolejek lub do serwera LDAP w celu uwierzytelnienia.
- V 9.3.4 W produkcie IBM MQ 9.3.4aplikacja może również dostarczyć znacznik uwierzytelniania, który uzyskuje z zewnętrznego serwera uwierzytelniania. Więcej informacji na temat znaczników uwierzytelniania zawiera sekcja “Praca ze znacznikami uwierzytelniania” na stronie 371.
- Kanał klienta można skonfigurować w taki sposób, aby korzystał z uwierzytelniania wzajemnego TLS, jeśli został skonfigurowany z poprawnym certyfikatem cyfrowym. Uwierzytelnianie TLS można połączyć z regułą uwierzytelniania kanału (CHLAUTH) w celu powiązania odpowiedniego ID użytkownika z połączeniem. Więcej informacji na ten temat zawiera sekcja “W jaki sposób protokół TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność” na stronie 20.
- Reguły uwierzytelniania kanału (CHLAUTH) mogą przesłonić tożsamość na podstawie informacji o połączeniu. Na przykład reguła uwierzytelniania kanału może ustawić identyfikator użytkownika powiązany z połączeniem na podstawie adresu IP klienta.
- Niestandardowy kod wyjścia może ustawić tożsamość na podstawie dowolnego wybranego kryterium.

Tożsamość i uwierzytelnianie mają również zastosowanie do kanałów między dwoma menedżerami kolejek. Te kanały są nazywane kanałami komunikatów. Po uruchomieniu kanału komunikatów agent kanału komunikatów (MCA) na każdym końcu kanału może uwierzytelnić swojego partnera. Ta technika jest nazywana *uwierzytelnianiem wzajemnym*. W przypadku wysyłającego agenta MCA zapewnia on, że partner, do którego mają być wysyłane komunikaty, jest prawdziwy. Podobnie odbierający agent MCA ma pewność, że będzie odbierał komunikaty od prawdziwego partnera.

Po ustanowieniu i uwierzytelnieniu tożsamości, jeśli jest to wymagane, jest ona używana przez produkt IBM MQ na kilka sposobów:

- Co ważne, domyślnie wszystkie kolejne sprawdzenia “Autoryzacja” na stronie 9 są wykonywane przy użyciu tej tożsamości. Jeśli na przykład aplikacja próbuje umieścić komunikat w kolejce, menedżer kolejek potwierdza, że tożsamość powiązana z aplikacją ma autoryzację put dla obiektu kolejki.
- Ponadto każdy komunikat może zawierać informacje o *kontekście komunikatu* . Te informacje są przechowywane w deskryptorze komunikatu (MQMD). Menedżer kolejek może automatycznie wygenerować kontekst komunikatu, gdy aplikacja umieści komunikat w kolejce. Alternatywnie aplikacja może dostarczyć kontekst komunikatu, jeśli ID użytkownika powiązany z aplikacją jest do tego uprawniony. Informacje o kontekście w komunikacie zawierają informacje o aplikacji, która odbiera informacje o nadawcy komunikatu. Zawiera na przykład nazwę aplikacji, która umieściła komunikat, oraz identyfikator użytkownika powiązany z aplikacją.

Niezaprzeczalność

Ogólnym celem usługi niezaprzeczalnej jest udowodnienie, że konkretny komunikat jest powiązany z konkretną osobą.

Usługa *non-repudiation* może być wyświetlana jako rozszerzenie usługi identyfikacji i uwierzytelniania. Ogólnie rzecz biorąc, niezaprzeczalność ma zastosowanie w przypadku, gdy dane są przekazywane drogą elektroniczną; na przykład, zamówienie do maklera giełdowego na zakup lub sprzedaż akcji lub zamówienie do banku na przelanie środków z jednego rachunku na drugi.

Usługa nieodrzucająca może zawierać więcej niż jeden komponent, przy czym każdy komponent udostępnia inną funkcję. Jeśli nadawca komunikatu odmawia jego wysłania, niezaprzeczalna usługa z *dowodem pochodzenia* może dostarczyć odbiorcy niezaprzeczalny dowód, że komunikat został wysłany przez tę konkretną osobę. Jeśli odbiorca komunikatu kiedykolwiek odmówi jego odebrania, usługa niezaprzeczalna z *dowodem dostarczenia* może dostarczyć nadawcy niezaprzeczalny dowód, że komunikat został odebrany przez tę konkretną osobę.

W praktyce, dowód z niemal 100% pewnością, 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 firmy. W takim środowisku bardziej realistyczne jest oczekiwanie, że służba non-repudiation będzie w stanie przedstawić dowody, które są dopuszczalne, i że uzasadnia to twoją sprawę w sądzie.

Niezaprzeczalność jest odpowiednią usługą zabezpieczeń w środowisku IBM MQ , ponieważ IBM MQ jest środkiem do przesyłania danych drogą elektroniczną. Na przykład można wymagać równoczesnego dowodu, że konkretny komunikat został wysłany lub odebrany przez aplikację powiązaną z określoną osobą.

Produkt IBM MQ z produktem Advanced Message Security nie udostępnia usługi niezaprzeczającej reputacji jako części swojej funkcji podstawowej. Jednak niniejsza dokumentacja produktu zawiera sugestie dotyczące sposobu, w jaki można udostępnić własną usługę nieodrzucania w środowisku IBM MQ , pisząc własne programy obsługi wyjścia.

Autoryzacja

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

Autoryzacja w produkcie IBM MQ

Za pomocą autoryzacji można ograniczyć możliwości poszczególnych osób lub aplikacji w środowisku IBM MQ .

Poniżej przedstawiono kilka przykładów autoryzacji w środowisku IBM MQ :

- Zezwalanie tylko autoryzowanemu administratorowi na wydawanie komend do zarządzania zasobami IBM MQ .
- Zezwalanie aplikacji na nawiązywanie połączenia z menedżerem kolejek tylko wtedy, gdy ID użytkownika powiązany z aplikacją jest do tego uprawniony.
- Zezwolenie aplikacji na otwieranie tylko tych kolejek, które są niezbędne dla jej funkcji.
- Zezwalanie aplikacji na subskrybowanie tylko tych tematów, które są niezbędne dla jej funkcji.
- Zezwalanie aplikacji na wykonywanie na kolejce tylko tych operacji, które są niezbędne dla jej funkcji. Na przykład aplikacja może potrzebować tylko przeglądania komunikatów w określonej kolejce, a nie umieszczania lub pobierania komunikatów.

Więcej informacji na temat konfigurowania autoryzacji zawiera sekcja “Planowanie autoryzacji” na stronie 94 i powiązane z nią tematy podrzędne.

Kontrola

Kontrola to proces rejestrowania i sprawdzania zdarzeń w celu wykrycia, czy wystąpiło nieoczekiwane lub nieautoryzowane działanie lub czy podjęto próbę wykonania takiego działania.

Kontrola w programie IBM MQ

Produkt IBM MQ może wysyłać komunikaty o zdarzeniach w celu zarejestrowania wystąpienia nietypowego działania.

Poniżej przedstawiono kilka przykładów kontroli w środowisku IBM MQ :

- Aplikacja próbuje otworzyć kolejkę, do której nie ma uprawnień. Generowany jest komunikat zdarzenia instrumentacji. Sprawdzając komunikat o zdarzeniu, można stwierdzić, że wystąpiła ta próba i zdecydować, jakie działanie jest konieczne.
- Aplikacja próbuje otworzyć kanał, ale próba nie powiedzie się, ponieważ połączenie TLS nie jest dozwolone. Generowany jest komunikat zdarzenia instrumentacji. Sprawdzając komunikat o zdarzeniu, można stwierdzić, że wystąpiła ta próba i zdecydować, jakie działanie jest konieczne.

Poufność

Usługa *poufności* chroni poufne informacje przed ujawnieniem bez uprawnień.

Jeśli dane wrażliwe są przechowywane lokalnie, mechanizmy kontroli dostępu mogą być wystarczające do ich zabezpieczenia przy założeniu, że dane nie mogą zostać odczytane, jeśli dostęp do nich nie jest możliwy. Jeśli wymagany jest wyższy poziom bezpieczeństwa, dane mogą być szyfrowane.

Szyfrowanie danych wrażliwych, gdy są one przesyłane przez sieć komunikacyjną, zwłaszcza przez niezabezpieczoną sieć, taką jak Internet. W środowisku sieciowym mechanizmy kontroli dostępu nie są skuteczne w przypadku prób przechwycenia danych, takich jak przechwytywanie danych.

Poufność w programie IBM MQ

Poufność w produkcie IBM MQ można zaimplementować, szyfrując komunikaty.

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

- Gdy wysyłający agent MCA otrzyma 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 umieści go w kolejce docelowej.
- Chociaż komunikaty są przechowywane w kolejce lokalnej, mechanizmy kontroli dostępu udostępniane przez produkt IBM MQ mogą być uznane za wystarczające do ochrony ich treści przed ujawnieniem bez uprawnień. Jednak w celu zwiększenia poziomu bezpieczeństwa można użyć programu Advanced Message Security do zaszyfrowania komunikatów przechowywanych w kolejkach.
- z/OS Komunikaty przechowywane w kolejkach lokalnych mogą być szyfrowane w spoczynku przy użyciu szyfrowania zestawu danych z/OS .

  Patrz sekcja poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych . :NONE.

Integralność danych

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

Istnieją dwa sposoby modyfikowania danych: przypadkowo, z powodu błędów sprzętu i transmisji lub z powodu zamierzonego ataku. Wiele produktów sprzętowych i protokołów transmisji ma mechanizmy wykrywania i korygowania błędów sprzętu i transmisji. Celem usługi integralności danych jest wykrycie zamierzonego ataku.

Celem usługi integralności danych jest tylko wykrycie, czy dane zostały zmodyfikowane. Nie ma na celu przywrócenia pierwotnego stanu danych, jeśli zostały one zmodyfikowane.

Mechanizmy kontroli dostępu mogą przyczynić się do zachowania integralności danych, ponieważ nie można modyfikować danych w przypadku odmowy dostępu. Jednak, podobnie jak w przypadku poufności, mechanizmy kontroli dostępu nie są skuteczne w środowisku sieciowym.

Integralność danych w produkcie IBM MQ

Integralność danych można zapewnić w środowisku IBM MQ w następujący sposób:

- Za pomocą protokołu TLS można wykryć, czy treść komunikatu została celowo zmodyfikowana podczas przesyłania przez sieć. W protokole TLS algorytm tworzenia skrótu komunikatu umożliwia wykrywanie zmodyfikowanych komunikatów podczas przesyłania.

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

  Produkt IBM MQ wykrywa zmodyfikowane komunikaty po ich odebraniu; po odebraniu zmodyfikowanego komunikatu IBM MQ w dzienniku błędów zapisywany jest komunikat o błędzie AMQ9661 , a kanał jest zatrzymywany.
- Podczas gdy komunikaty są przechowywane w kolejce lokalnej, mechanizmy kontroli dostępu udostępniane przez produkt IBM MQ mogą być uznane za wystarczające, aby zapobiec celowym modyfikacjom treści komunikatów.

  Jednak w celu zapewnienia wyższego poziomu bezpieczeństwa można użyć programu Advanced Message Security , aby wykryć, czy treść komunikatu została celowo zmodyfikowana między umieszczaniem komunikatu w kolejce a jego pobraniem z kolejki.

  W przypadku wykrycia zmodyfikowanego komunikatu aplikacja, która próbuje odebrać komunikat, odbiera kod powrotu MQRC_SECURITY_ERROR (2063). Jeśli aplikacja używa wywołania MQGET , komunikat jest również przenoszony do systemu SYSTEM.PROTECTION.ERROR.QUEUE .

Pojęcia związane z szyfrowaniem

Ta kolekcja tematów zawiera opis pojęć związanych z szyfrowaniem stosowanych w produkcie IBM MQ.

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

Kryptografia

Kryptografia jest procesem przekształcania tekstu możliwego do odczytania, nazywanego *tekstem jawnym*, i postaci nieczytelnej, nazywanej *tekstem zaszyfrowanym*.

Dzieje się tak w następujący sposób:

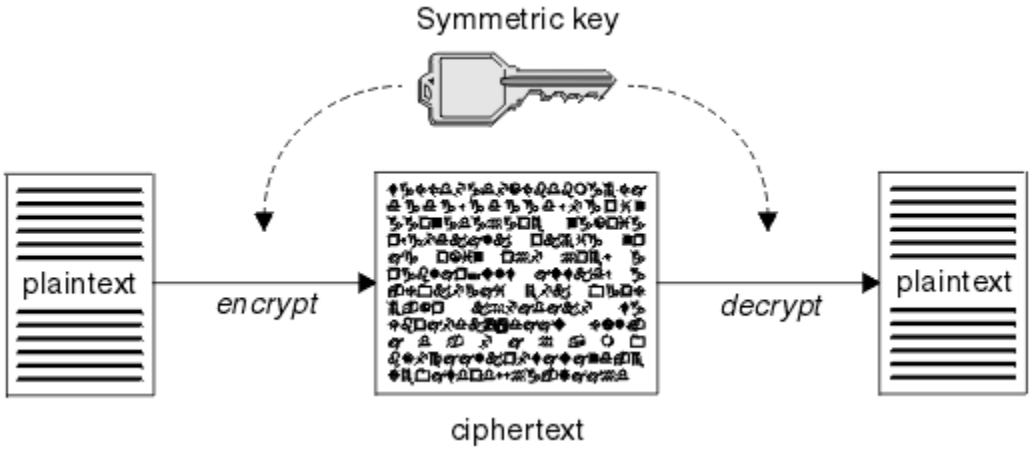
1. Nadawca przekształca komunikat jawnego tekstu w tekst zaszyfrowany. Ta część procesu jest nazywana *szyfrowaniem* (czasami *szyfrowaniem*).
2. Tekst zaszyfrowany jest przesyłany do odbiornika.
3. Odbiorca przekształca komunikat z tekstem zaszyfrowanym z powrotem do postaci jawnego tekstu. Ta część procesu jest nazywana *deszyfrowaniem* (czasami *deszyfrowaniem*).

Konwersja obejmuje sekwencję operacji matematycznych, które zmieniają wygląd komunikatu podczas transmisji, ale nie wpływają na treść. Techniki kryptograficzne mogą zapewnić poufność i chronić wiadomości przed nieautoryzowanym wyświetlaniem (podsłuchiwaniem), ponieważ zaszyfrowany komunikat nie jest zrozumiały. Podpisy cyfrowe, które zapewniają integralność komunikatów, używają technik szyfrowania. Więcej informacji zawiera sekcja “Podpisy cyfrowe w protokole SSL/TLS” na stronie 22.

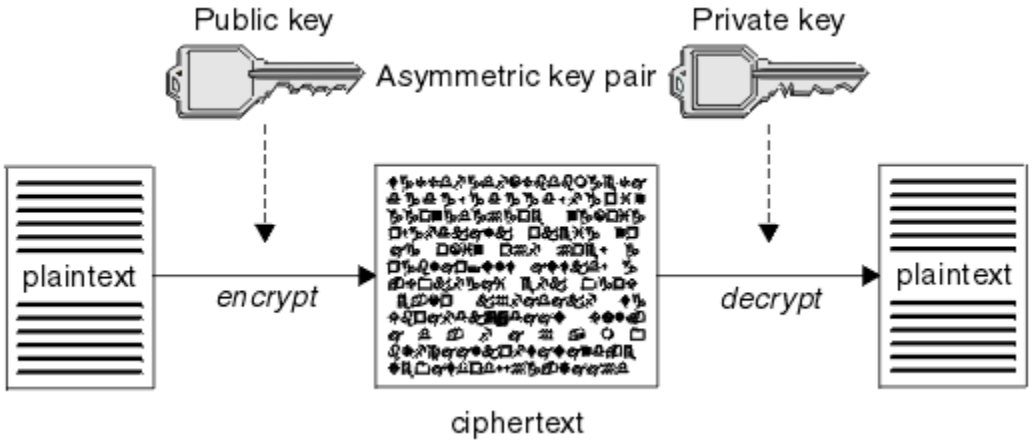
Techniki kryptograficzne obejmują ogólny algorytm, określony przez użycie kluczy. Istnieją dwie klasy algorytmów:

- Te, które wymagają, aby obie strony używały tego samego klucza tajnego. Algorytmy używające klucza współużytkowanego są nazywane algorytmami *symetrycznymi* . Rysunek 1 na stronie 12 przedstawia szyfrowanie z kluczem symetrycznym.
- Te, które używają jednego klucza do szyfrowania i innego klucza do deszyfrowania. Jedna z nich musi być tajna, ale druga może być publiczna. Algorytmy, które używają par kluczy publicznych i prywatnych, są nazywane algorytmami *asymetrycznymi* . Rysunek 2 na stronie 12 przedstawia szyfrowanie z kluczem asymetrycznym, które jest również nazywane *szyfrowaniami z kluczem publicznym*.

Używane algorytmy szyfrowania i deszyfrowania mogą być publiczne, ale współużytkowany klucz tajny i klucz prywatny muszą być tajne.



Rysunek 1. szyfrowanie za pomocą klucza symetrycznego



Rysunek 2. szyfrowanie z użyciem klucza niesymetrycznego

Rysunek 2 na stronie 12 przedstawia jawny tekst zaszyfrowany kluczem publicznym odbiorcy i zdeszyfrowany przy użyciu klucza prywatnego odbiorcy. Tylko zamierzony odbiornik przechowuje klucz prywatny do deszyfrowania tekstu zaszyfrowanego. Należy zauważyć, że nadawca może również szyfrować wiadomości za pomocą klucza prywatnego, co umożliwia każdemu, kto przechowuje klucz publiczny nadawcy, deszyfrowanie wiadomości z zapewnieniem, że wiadomość musi pochodzić od nadawcy.

W przypadku algorytmów asymetrycznych komunikaty są szyfrowane przy użyciu klucza publicznego lub prywatnego, ale mogą być deszyfrowane tylko przy użyciu innego klucza. Tylko klucz prywatny jest tajny, klucz publiczny może być znany przez każdego. W przypadku algorytmów symetrycznych klucz współużytkowany musi być znany tylko dwóm stronom. Jest to tzw. *problem z rozdzielaniem kluczy*. Algorytmy asymetryczne są wolniejsze, ale mają tę zaletę, że nie ma problemu z rozkładaniem 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	Asymetryczny klucz o średniej sile
4096 bitów	Klucz asymetryczny o dużej wytrzymałości

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

Algorytm szyfru blokowego
Algorytmy te szyfrują dane blokami. Na przykład algorytm RC2 firmy RSA Data Security Inc. używa bloków o długości 8 bajtów. Algorytmy blokowe są zwykle wolniejsze niż algorytmy strumieniowe.

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

Streszczenia komunikatów i podpisy cyfrowe

Skrót komunikatu jest stałą reprezentacją liczbową treści komunikatu. Skrót komunikatu jest obliczany przez funkcję mieszającą i może być szyfrowany, tworząc podpis cyfrowy.

Funkcja mieszająca używana do obliczania skrótu komunikatu musi spełniać dwa kryteria:

- To musi być jeden sposób. Nie może być możliwe odwrócenie funkcji w celu znalezienia komunikatu odpowiadającego konkretnemu skróceniu komunikatu, z wyjątkiem testowania wszystkich możliwych komunikatów.
- Znalezienie dwóch komunikatów, które mieszają się do tego samego streszczenia, musi być niewykonalne obliczeniowo.

Streszczenie komunikatu jest wysyłane razem z samym komunikatem. Odbiorca może wygenerować streszczenie dla komunikatu i porównać je ze streszczeniem nadawcy. Integralność komunikatu jest weryfikowana, gdy dwa streszczenia komunikatu są takie same. Każde manipulowanie wiadomością podczas transmisji prawie na pewno prowadzi do innego streszczenia wiadomości.

Skrót komunikatu utworzony przy użyciu tajnego klucza symetrycznego jest nazywany kodem uwierzytelniania komunikatu (Message Authentication Code-MAC), ponieważ może zapewnić, że komunikat nie został zmodyfikowany.

Nadawca może również wygenerować streszczenie komunikatu, a następnie zaszyfrować je przy użyciu klucza prywatnego pary kluczy asymetrycznych, tworząc podpis cyfrowy. Podpis musi zostać następnie zdeszyfrowany przez odbiorcę przed porównaniem go z lokalnie wygenerowanym streszczeniem.

Pojęcia pokrewne

“Podpisy cyfrowe w protokole SSL/TLS” na stronie 22
Podpis cyfrowy jest tworzony przez szyfrowanie reprezentacji komunikatu. Szyfrowanie wykorzystuje klucz prywatny sygnatariusza i ze względu na wydajność zwykle działa na streszczonym komunikacie, 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 jest to osoba fizyczna, menedżer kolejek, czy inna jednostka. Certyfikaty cyfrowe są również nazywane certyfikatami klucza publicznego, ponieważ dają pewność co do własności klucza publicznego, gdy używany jest schemat klucza asymetrycznego. Certyfikat cyfrowy zawiera klucz publiczny dla jednostki i jest oświadczeniem, że klucz publiczny należy do tej jednostki:

- Jeśli certyfikat jest przeznaczony dla pojedynczej jednostki, jest on nazywany *certyfikatem osobistym* lub *certyfikatem użytkownika*.
- Jeśli certyfikat jest przeznaczony dla ośrodka certyfikacji, jest on nazywany *certyfikatem ośrodka certyfikacji* lub *certyfikatem osoby podpisującej*.

Jeśli klucze publiczne są wysyłane bezpośrednio przez właściciela do innej jednostki, istnieje ryzyko przechwycenia komunikatu, a klucz publiczny jest zastępowany przez inny. Jest to tzw. *człowiek w ataku środkowym*. Rozwiązaniem tego problemu jest wymiana kluczy publicznych za pośrednictwem zaufanej osoby trzeciej, dając silne zapewnienie, że klucz publiczny rzeczywiście należy do jednostki, z którą się

komunikujesz. Zamiast wysyłać klucz publiczny bezpośrednio, należy poprosić zaufaną osobę trzecią o włączenie go do certyfikatu cyfrowego. Zaufana osoba trzecia, która wydaje certyfikaty cyfrowe, jest nazywana ośrodkiem certyfikacji (CA), zgodnie z opisem w sekcji "Ośrodki certyfikacji" na stronie 15.

Co znajduje się w certyfikacie cyfrowym

Certyfikaty cyfrowe zawierają konkretne informacje określone przez standard X.509 .

Certyfikaty cyfrowe używane przez IBM MQ są zgodne ze standardem X.509 , który określa wymagane informacje oraz format ich wysyłania. X.509 jest częścią struktury uwierzytelniania serii standardów X.500 .

Certyfikaty cyfrowe zawierają co najmniej następujące informacje o certyfikowanym podmiocie:

- 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 zdefiniowanego 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: żaden z dwóch certyfikatów podpisanych przez ten sam certyfikat ośrodka CA nie ma tego samego numeru seryjnego.

Certyfikat X.509 w wersji 2 zawiera również identyfikator wystawcy i identyfikator podmiotu, a certyfikat X.509 w wersji 3 może zawierać wiele rozszerzeń. Niektóre rozszerzenia certyfikatów, takie jak rozszerzenie Basic Constraint, są *standardowe*, ale inne są specyficzne dla implementacji. Rozszerzenie może być *krytyczne*, w którym to przypadku system musi być w stanie rozpoznać pole; jeśli nie rozpoznaje pola, musi odrzucić certyfikat. Jeśli rozszerzenie nie jest newralgiczne, system może je zignorować, jeśli nie zostanie rozpoznane.

Podpis cyfrowy w certyfikacie osobistym jest generowany przy użyciu klucza prywatnego ośrodka CA, który podpisał ten certyfikat. Każdy, kto musi zweryfikować certyfikat osobisty, może w tym celu użyć klucza publicznego ośrodka CA. Certyfikat ośrodka CA zawiera klucz publiczny.

Certyfikaty cyfrowe nie zawierają klucza prywatnego. Musisz zachować swój klucz prywatny w tajemnicy.

Wymagania dotyczące certyfikatów osobistych

IBM MQ obsługuje certyfikaty cyfrowe zgodne ze standardem X.509 . Wymaga opcji uwierzytelniania klienta.

Ponieważ system IBM MQ jest systemem typu każdy z każdym, jest on postrzegany jako uwierzytelnianie klienta w terminologii SSL/TLS. Oznacza to, że każdy certyfikat osobisty używany do uwierzytelniania SSL/TLS musi zezwalać na użycie klucza podczas uwierzytelniania klienta. Nie wszystkie certyfikaty serwera mają włączoną tę opcję, dlatego dostawca certyfikatów może wymagać włączenia uwierzytelniania klienta w głównym ośrodku CA dla certyfikatu zabezpieczonego.

Oprócz standardów, które określają format danych dla certyfikatu cyfrowego, istnieją również standardy określające, czy certyfikat jest poprawny. Standardy te były z biegiem czasu aktualizowane, aby zapobiec pewnym rodzajom naruszeń bezpieczeństwa. Na przykład starsze certyfikaty X.509 w wersji 1 i 2 nie wskazują, czy certyfikat może być używany do podpisywania innych certyfikatów. W związku z tym złośliwy użytkownik mógł uzyskać certyfikat osobisty z legalnego źródła i utworzyć nowe certyfikaty przeznaczone do imitowania innych użytkowników.

Jeśli używane są certyfikaty X.509 w wersji 3, rozszerzenia BasicConstraints i KeyUsage są używane do określenia, które certyfikaty mogą zgodnie z prawem podpisywać inne certyfikaty. Standard IETF RFC 5280 określa serię reguł sprawdzania poprawności certyfikatów, które muszą zostać zaimplementowane przez zgodne oprogramowanie aplikacji, aby zapobiec atakom personifikacji. Zestaw reguł certyfikatów jest nazywany strategią sprawdzania poprawności certyfikatów.

Więcej informacji na temat strategii sprawdzania poprawności certyfikatów w programie IBM MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w programie IBM MQ” na stronie 46.

Ośrodki certyfikacji

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

Role ośrodka CA są następujące:

- Po otrzymaniu żądania certyfikatu cyfrowego, aby zweryfikować tożsamość żądającego przed zbudowaniem, podpisaniem i zwróceniem certyfikatu osobistego
- Aby udostępnić własny klucz publiczny ośrodka CA w certyfikacie ośrodka CA
- Publikowanie listy certyfikatów, które nie są już zaufane na liście odwołań certyfikatów (CRL). Więcej informacji na ten temat zawiera sekcja “Praca z odwołanymi certyfikatami” na stronie 382.
- Zapewnianie dostępu do statusu odwołania certyfikatu przez działanie serwera odpowiadającego OCSP

Nazwy wyróżniające

Nazwa wyróżniająca (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 tych atrybutów nie jest dozwolone.

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

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

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

Standard X.509 umożliwia określenie nazwy wyróżniającej w formacie łańcucha. Na przykład:

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

Nazwa zwykła (CN) może opisywać pojedynczego użytkownika lub inną jednostkę, na przykład serwer WWW.

Nazwa wyróżniająca może zawierać wiele atrybutów OU i DC. Dozwolona jest tylko jedna instancja każdego z pozostałych atrybutów. Kolejność wpisów jednostki organizacyjnej jest istotna: kolejność określa hierarchię nazw jednostek organizacyjnych, z jednostką najwyższego poziomu jako pierwszą. Istotna jest również kolejność pozycji DC.

Produkt IBM MQ toleruje niektóre zniekształcone nazwy wyróżniające. Więcej informacji na ten temat zawiera sekcja Reguły dotyczące wartości SSLPEER w systemie IBM MQ.

Pojęcia pokrewne

“Co znajduje się w certyfikacie cyfrowym” na stronie 14
Certyfikaty cyfrowe zawierają konkretne informacje określone przez standard X.509 .

Uzyskiwanie certyfikatów osobistych z ośrodka certyfikacji

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

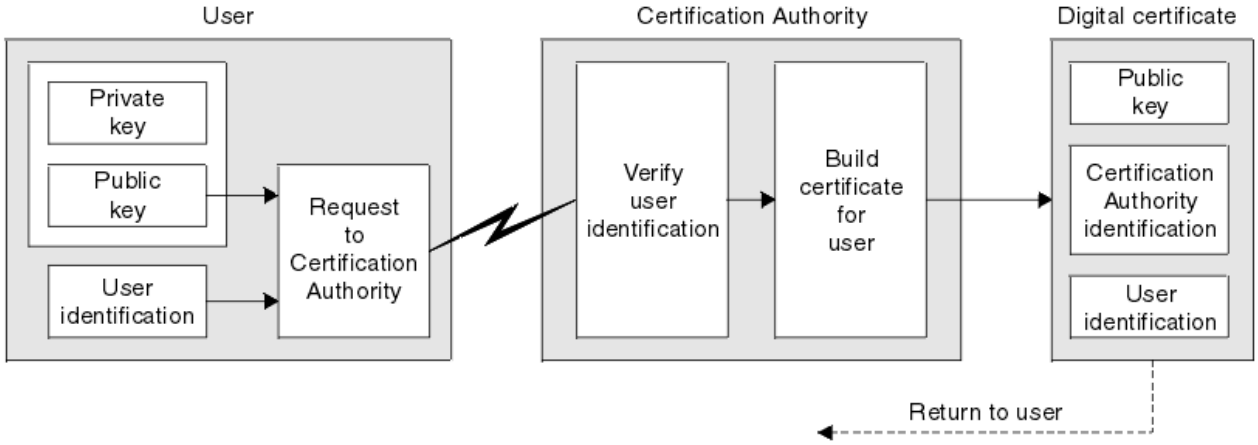
Certyfikat cyfrowy można uzyskać, wysyłając informacje do ośrodka CA w postaci żądania certyfikatu. Standard X.509 definiuje format tych informacji, ale niektóre ośrodki certyfikacji mają własny format. Żądania certyfikatów są zwykle generowane przez narzędzie do zarządzania certyfikatami używane przez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

- Multi Komenda **strmqikm** (narzędzieiKeyman) w systemie Wiele platformoraz komendy **runmqckm** i **runmqakm** w systemie AIX, Linux, and Windows.
- z/OS RACF na platformie z/OS.

Informacje te zawierają nazwę wyróżniającą i klucz publiczny. Gdy narzędzie do zarządzania certyfikatami generuje żądanie certyfikatu, generuje także klucz prywatny, który musi być bezpieczny. Nigdy nie dystrybuuj klucza prywatnego.

Gdy ośrodek CA otrzyma żądanie, weryfikuje tożsamość użytkownika przed utworzeniem certyfikatu i zwróceniem go jako certyfikatu osobistego.

Rysunek 3 na stronie 16 przedstawia proces uzyskiwania certyfikatu cyfrowego z ośrodka CA.



Rysunek 3. Uzyskiwanie certyfikatu cyfrowego

Na diagramie:

- Identyfikator użytkownika zawiera nazwę wyróżniającą podmiotu.
- Identyfikacja ośrodka certyfikacji obejmuje nazwę wyróżniającą ośrodka certyfikacji, który wystawia certyfikat.

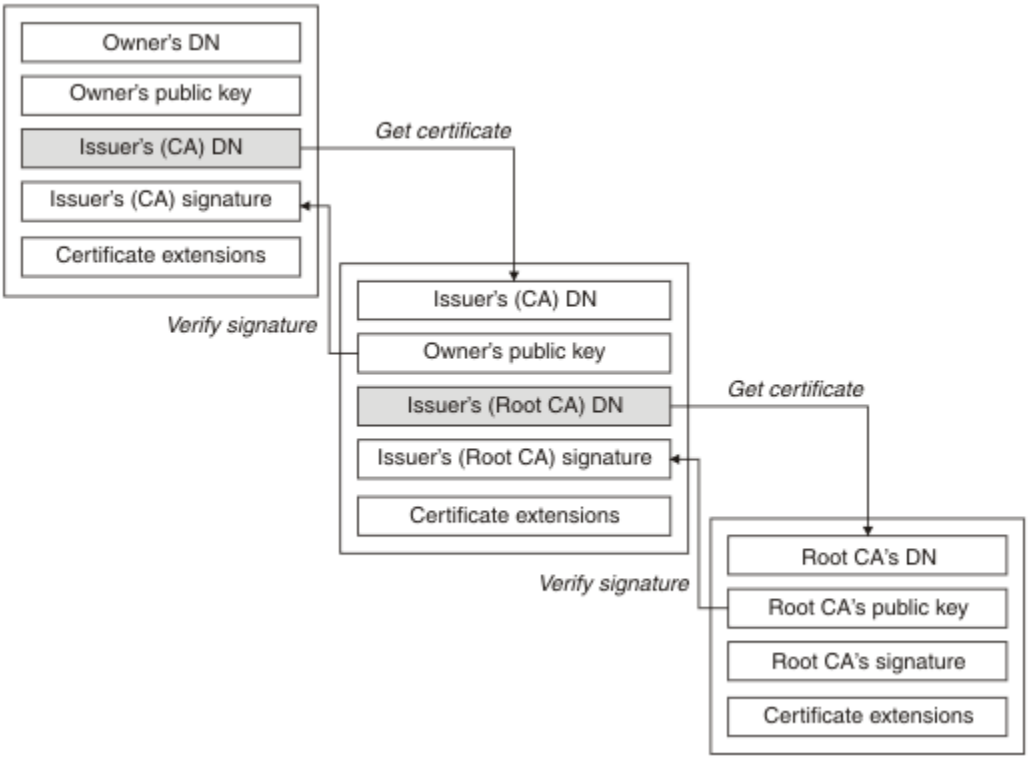
Certyfikaty cyfrowe zawierają dodatkowe pola inne niż przedstawione na diagramie. Więcej informacji na temat innych pól w certyfikacie cyfrowym zawiera sekcja “Co znajduje się w certyfikacie cyfrowym” na stronie 14.

Jak działają łańcuchy certyfikatów

Po otrzymaniu certyfikatu dla innej jednostki może być konieczne użycie *łańcucha certyfikatów* w celu uzyskania certyfikatu *głównego ośrodka CA* .

Łańcuch certyfikatów, zwany również *ścieżką certyfikacji*, jest listą certyfikatów używanych do uwierzytelniania jednostki. Łańcuch lub ścieżka rozpoczyna się certyfikatem tej jednostki, a każdy certyfikat w łańcuchu jest podpisany przez jednostkę identyfikowaną przez następny certyfikat w łańcuchu. Łańcuch kończy się certyfikatem głównego ośrodka CA. Certyfikat głównego ośrodka CA jest zawsze podpisywany przez sam ośrodek certyfikacji (CA). Podpisy wszystkich certyfikatów w łańcuchu muszą zostać zweryfikowane do czasu osiągnięcia certyfikatu głównego ośrodka CA.

Rysunek 4 na stronie 17 ilustruje ścieżkę certyfikacji od właściciela certyfikatu do głównego ośrodka CA, w którym rozpoczyna 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 ważne

Certyfikaty cyfrowe mogą utracić ważność lub zostać unieważnione.

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

Certyfikaty mogą zostać unieważnione z różnych powodów, w tym:

- Właściciel został przeniesiony do innej organizacji.
- Klucz prywatny nie jest już tajny.

Produkt IBM MQ może sprawdzić, czy certyfikat został unieważniony, wysyłając żądanie do programu odpowiadającego OCSP (Online Certificate Status Protocol) (tylko w systemie AIX, Linux, and Windows).

Mogą również uzyskać dostęp do listy odwołań certyfikatów (CRL) na serwerze LDAP. Informacje o odwołaniu OCSP i CRL są publikowane przez ośrodek certyfikacji. Więcej informacji na ten temat zawiera sekcja “Praca z odwołanymi certyfikatami” na stronie 382.

Infrastruktura klucza publicznego (PKI)

Infrastruktura klucza publicznego (Public Key Infrastructure-PKI) to system infrastruktury, strategii i usług, który obsługuje używanie szyfrowania z kluczem publicznym do uwierzytelniania stron uczestniczących w transakcji.

Nie istnieje pojedynczy standard definiujący komponenty infrastruktury klucza publicznego, ale infrastruktura PKI zwykle składa się z ośrodków certyfikacji (CA) i ośrodków rejestracji (AP). Ośrodki CA świadczą następujące usługi:

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

Standardy X.509 stanowią podstawę standardu branżowego Infrastruktura klucza publicznego.

Więcej informacji na temat certyfikatów cyfrowych i ośrodków certyfikacji (CA) zawiera sekcja “certyfikaty cyfrowe” na stronie 13 . RAs weryfikuje informacje podane podczas żądania certyfikatów cyfrowych. Jeśli ośrodek certyfikacji (RA) zweryfikuje te informacje, ośrodek certyfikacji (CA) może wydać żądającemu certyfikat cyfrowy.

Infrastruktura PKI może również udostępniać narzędzia do zarządzania certyfikatami cyfrowymi i kluczami publicznymi. Infrastruktura PKI jest czasami opisana jako *hierarchia zaufania* do zarządzania certyfikatami cyfrowymi, ale większość definicji obejmuje dodatkowe usługi. Niektóre definicje obejmują usługi szyfrowania i podpisu cyfrowego, ale te usługi nie są niezbędne do działania infrastruktury PKI.

Szyfrujące protokoły bezpieczeństwa: TLS

Protokoły szyfrujące zapewniają bezpieczne połączenia, umożliwiając dwóm stronom komunikację z ochroną prywatności i integralnością danych. Protokół TLS (Transport Layer Security) wyewoluował z protokołu SSL (Secure Sockets Layer). Produkt IBM MQ obsługuje protokół TLS.

Podstawowym celem obu protokołów jest zapewnienie poufności (czasem nazywanych *prywatnością*), integralności danych, identyfikacji i uwierzytelniania przy użyciu certyfikatów cyfrowych.

Chociaż te dwa protokoły są podobne, różnice są na tyle istotne, że protokół SSL 3.0 i różne wersje protokołu TLS nie współdziałają ze sobą.

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 wzajemne identyfikowanie się i uwierzytelnianie oraz komunikację z zachowaniem poufności i integralności danych. Protokół TLS oparty na protokole Netscape SSL 3.0 , ale protokoły TLS i SSL nie współdziałają ze sobą.

Protokół TLS zapewnia bezpieczeństwo komunikacji przez Internet i umożliwia aplikacjom typu klient/serwer komunikację w sposób poufny i niezawodny. Protokoły mają dwie warstwy: protokół rejestrowania i protokół uzgadniania, które są warstwowe nad protokołem transportowym, takim jak TCP/IP. Oba używają asymetrycznych i symetrycznych technik kryptograficznych.

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

Pełna lista CipherSpecs obsługiwanych przez produkt IBM MQ jest dostępna pod adresem “Włączanie CipherSpecs” na stronie 466.

Więcej informacji na temat protokołu SSL zawiera publikacja dostępna pod adresem https://developer.mozilla.org/docs/Mozilla/Projects/NSS. Więcej informacji na temat protokołu TLS zawierają informacje udostępniane przez grupę roboczą ds. protokołu TLS w serwisie WWW zespołu zadaniowego ds. inżynierii internetowej pod adresem https://www.ietf.org .

Przegląd uzgadniania SSL/TLS

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

Ta sekcja zawiera podsumowanie kroków, które umożliwiają komunikację między klientem i serwerem TLS.

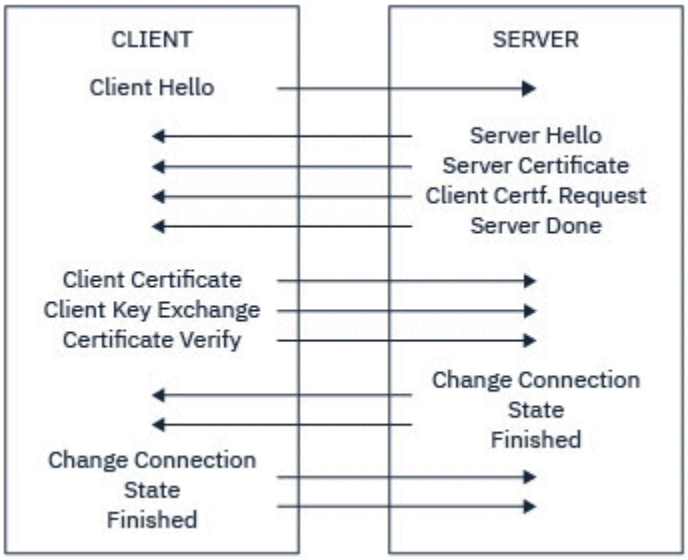
- Uzgodnić wersję protokołu, która ma być używana.
- Wybierz algorytmy szyfrowania.
- Uwierzytelniaj się wzajemnie, wymieniając i sprawdzając poprawność certyfikatów cyfrowych.
- Użyj technik szyfrowania asymetrycznego, aby wygenerować współużytkowany klucz tajny, co pozwala uniknąć problemu z dystrybucją kluczy. Następnie protokół TLS używa klucza współużytkowanego do symetrycznego szyfrowania komunikatów, które jest szybsze niż szyfrowanie asymetryczne.

Więcej informacji na temat algorytmów szyfrowania i certyfikatów cyfrowych zawierają informacje pokrewne.

W przeglądzie przedstawiono następujące kroki związane z uzgadnianiem TLS:

1. Klient TLS wysyła komunikat "client hello" , który wyświetla informacje kryptograficzne, takie jak wersja TLS i, w preferowanej kolejności, CipherSuites obsługiwane przez klienta. Komunikat zawiera również losowy łańcuch bajtowy, który jest używany w kolejnych obliczeniach. Protokół umożliwia "klientowi hello" uwzględnienie metod kompresji danych obsługiwanych przez klienta.
2. Serwer TLS odpowiada komunikatem "server hello" zawierającym zestaw algorytmów szyfrowania CipherSuite wybrany przez serwer z listy udostępnionej przez klienta, identyfikator sesji i inny losowy łańcuch bajtów. Serwer wysyła również swój certyfikat cyfrowy. Jeśli serwer wymaga certyfikatu cyfrowego do uwierzytelniania klienta, wysyła "żądanie certyfikatu klienta" zawierające listę obsługiwanych typów certyfikatów oraz nazwy wyróżniające akceptowalnych ośrodków certyfikacji (CA).
3. Klient TLS weryfikuje certyfikat cyfrowy serwera. Więcej informacji na ten temat zawiera “W jaki sposób protokół TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność” na stronie 20.
4. Klient TLS wysyła losowy łańcuch bajtów, który umożliwia zarówno klientowi, jak i serwerowi obliczenie klucza tajnego, który ma być używany do szyfrowania kolejnych danych komunikatu. Losowy łańcuch bajtów jest szyfrowany za pomocą klucza publicznego serwera.
5. Jeśli serwer TLS wysłał "żądanie certyfikatu klienta", klient wysyła losowy łańcuch bajtów zaszyfrowany kluczem prywatnym klienta wraz z certyfikatem cyfrowym klienta lub "alert braku 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 “W jaki sposób protokół TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność” na stronie 20.
7. Klient TLS wysyła do serwera komunikat "zakończony" , który jest zaszyfrowany kluczem tajnym, wskazujący, że część klienta uzgadniania została zakończona.
8. Serwer TLS wysyła do klienta komunikat "zakończony" , który jest zaszyfrowany kluczem tajnym, co oznacza, że część serwerowa uzgadniania została zakończona.
9. Przez czas trwania sesji TLS serwer i klient mogą teraz wymieniać komunikaty, które są symetrycznie zaszyfrowane za pomocą współużytkowanego klucza tajnego.

Rysunek 5 na stronie 20 przedstawia uzgadnianie TLS.



Rysunek 5. Przegląd uzgadniania TLS

W jaki sposób protokół TLS zapewnia identyfikację, uwierzytelnianie, poufność i integralność

Podczas uwierzytelniania zarówno klienta, jak i serwera, istnieje krok, który wymaga, aby dane były szyfrowane za pomocą jednego z kluczy w parze kluczy asymetrycznych i deszyfrowane za pomocą drugiego klucza pary. Do zapewnienia integralności używany jest skrót komunikatu.

Przegląd kroków związanych z uzgadnianiem TLS zawiera sekcja “Przegląd uzgadniania SSL/TLS” na stronie 19.

W jaki sposób protokół TLS zapewnia uwierzytelnianie

W przypadku uwierzytelniania serwera klient używa klucza publicznego serwera do zaszyfrowania danych używanych do obliczenia klucza tajnego. Serwer może wygenerować klucz tajny tylko wtedy, gdy może deszyfrować te dane przy użyciu poprawnego klucza prywatnego. Losowy łańcuch bajtów jest szyfrowany za pomocą klucza publicznego serwera (krok “4” na stronie 19 w przeglądzie).

W przypadku uwierzytelniania klienta serwer używa klucza publicznego w certyfikacie klienta do deszyfrowania danych wysyłanych przez klienta w kroku “5” na stronie 19 uzgadniania. Wymiana zakończonych wiadomości zaszyfrowanych za pomocą klucza tajnego (kroki “7” na stronie 19 i “8” na stronie 19 w przeglądzie) potwierdza, że uwierzytelnianie zostało zakończone.

Jeśli dowolny 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, zawierają informacje pokrewne. Wymagane są następujące certyfikaty, gdzie ośrodek CA X wystawia certyfikat klientowi TLS, a ośrodek CA Y wystawia certyfikat serwerowi TLS:

Tylko w przypadku uwierzytelniania serwera serwer TLS wymaga:

- Certyfikat osobisty wystawiony dla serwera przez ośrodek CA Y
- Klucz prywatny serwera

a klient TLS wymaga:

- Certyfikat CA dla ośrodka CA Y

Jeśli serwer TLS wymaga uwierzytelniania klienta, serwer weryfikuje tożsamość klienta, weryfikując certyfikat cyfrowy klienta za pomocą klucza publicznego 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 dla serwera przez ośrodek CA Y
- Klucz prywatny serwera
- Certyfikat CA dla ośrodka CA X

a klient potrzebuje:

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

Zarówno serwer, jak i klient TLS mogą potrzebować innych certyfikatów CA, aby utworzyć łańcuch certyfikatów do głównego certyfikatu CA. Więcej informacji na temat łańcuchów certyfikatów zawierają informacje pokrewne.

Co się dzieje podczas weryfikacji certyfikatu

Jak wspomniano w krokach “3” na stronie 19 i “6” na stronie 19 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 protokole SSL/TLS” na stronie 22).
2. Łańcuch certyfikatów jest sprawdzany; należy mieć certyfikaty pośrednie ośrodka CA (patrz sekcja “Jak działają łańcuchy certyfikatów” na stronie 17).
3. Sprawdzane są daty ważności i aktywacji oraz okres ważności.
4. Status odwołania certyfikatu jest sprawdzany (patrz “Praca z odwołanymi certyfikatami” na stronie 382).

Resetowanie klucza tajnego

Podczas uzgadniania TLS generowany jest *klucz tajny* do szyfrowania danych między klientem i serwerem TLS. Klucz tajny jest używany w formule matematycznej, która jest stosowana do danych w celu przekształcenia tekstu jawnego w nieczytelny tekst zaszyfrowany, a tekstu zaszyfrowanego w jawny tekst.

Klucz tajny jest generowany na podstawie losowego tekstu wysyłanego w ramach uzgadniania i jest używany do szyfrowania jawnego tekstu w tekst zaszyfrowany. Klucz tajny jest również używany w algorytmie MAC (Message Authentication Code), który służy do określania, czy komunikat został zmieniony. Więcej informacji zawiera sekcja “Streszczenia komunikatów i podpisy cyfrowe” na stronie 13.

Jeśli zostanie wykryty klucz tajny, jawny tekst komunikatu może zostać odszyfrowany z tekstu zaszyfrowanego lub może zostać obliczone streszczenie komunikatu umożliwiające zmianę komunikatów bez wykrywania. Nawet w przypadku złożonego algorytmu tekst jawny może zostać ostatecznie wykryty przez zastosowanie każdej możliwej transformacji matematycznej do tekstu zaszyfrowanego. Aby zminimalizować ilość danych, które mogą zostać odszyfrowane lub zmienione w przypadku uszkodzenia klucza tajnego, klucz tajny może być okresowo renegocjowany. Po renegocjacji klucza tajnego poprzedni klucz tajny nie może być już używany do deszyfrowania danych zaszyfrowanych za pomocą nowego klucza tajnego.

W jaki sposób protokół TLS zapewnia poufność

Protokół TLS używa kombinacji szyfrowania symetrycznego i asymetrycznego w celu zapewnienia prywatności komunikatów. Podczas uzgadniania TLS klient i serwer TLS uzgadniają algorytm szyfrowania i współużytkowany klucz tajny, które mają być używane tylko w 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 został przechwycony. Ponieważ protokół TLS używa szyfrowania asymetrycznego podczas transportowania współużytkowanego klucza tajnego, nie

ma problemu z dystrybucją klucza. Więcej informacji na temat technik szyfrowania zawiera sekcja “Kryptografia” na stronie 11.

W jaki sposób protokół TLS zapewnia integralność

Protokół TLS zapewnia integralność danych przez obliczanie skrótu komunikatu. Więcej informacji zawiera sekcja “Integralność danych komunikatów” na stronie 525.

Użycie protokołu TLS zapewnia integralność danych, pod warunkiem że specyfikacja szyfrowania CipherSpec w definicji kanału użytkownika używa algorytmu mieszającego zgodnie z opisem w tabeli w sekcji “Włączanie CipherSpecs” na stronie 466.

W szczególności, jeśli integralność danych jest problemem, należy unikać wybierania specyfikacji szyfrowania CipherSpec , której algorytm mieszania jest wymieniony jako "Brak". Użycie algorytmu MD5 jest również zdecydowanie niezalecane, ponieważ jest on obecnie bardzo stary i nie jest już bezpieczny w większości zastosowań praktycznych.

CipherSpecs i CipherSuites

Szyfrujące protokoły bezpieczeństwa muszą być zgodne z algorytmami używanymi przez bezpieczne połączenie. CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

CipherSpec identyfikuje kombinację algorytmu szyfrowania i algorytmu kodu uwierzytelniania komunikatu (Message Authentication Code-MAC). Aby komunikacja była możliwa, oba końce połączenia TLS muszą być zgodne z tą samą specyfikacją szyfrowania CipherSpec .

Produkt IBM MQ obsługuje protokoły TLS1.3 i TLS1.2 oraz CipherSpecs. W razie potrzeby można jednak włączyć nieaktualne CipherSpecs.

Więcej informacji na ten temat zawiera sekcja “Włączanie CipherSpecs” na stronie 466 :

- CipherSpecs obsługiwane przez produkt IBM MQ
- W jaki sposób włączyć nieaktualne specyfikacje szyfrowania SSL 3.0 i TLS 1.0 CipherSpecs

Ważne: Podczas pracy z kanałami produktu IBM MQ używana jest CipherSpec. Podczas pracy z kanałami Java , kanałami JMS lub kanałami MQTT należy określić opcję CipherSuite.

Więcej informacji na temat CipherSpecszawiera sekcja “Włączanie CipherSpecs” na stronie 466.

CipherSuite to zestaw algorytmów szyfrowania 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 skrótu komunikatu

Istnieje kilka opcji dla każdego komponentu pakietu, ale tylko niektóre kombinacje są poprawne, jeśli zostaną określone dla połączenia TLS. Nazwa poprawnego CipherSuite definiuje kombinację używanych algorytmów. Na przykład opcja CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA określa:

- Algorytm wymiany kluczy i uwierzytelniania RSA
- Algorytm szyfrowania AES używający 128-bitowego klucza i trybu łączenia zaszyfrowanych bloków (cipher block chaining-CBC)
- Kod uwierzytelniania komunikatu (Message Authentication Code-MAC) SHA-1

Podpisy cyfrowe w protokole SSL/TLS

Podpis cyfrowy jest tworzony przez szyfrowanie reprezentacji komunikatu. Szyfrowanie wykorzystuje klucz prywatny sygnatariusza i ze względu na wydajność zwykle działa na streszczonym komunikacie, a nie na samym komunikacie.

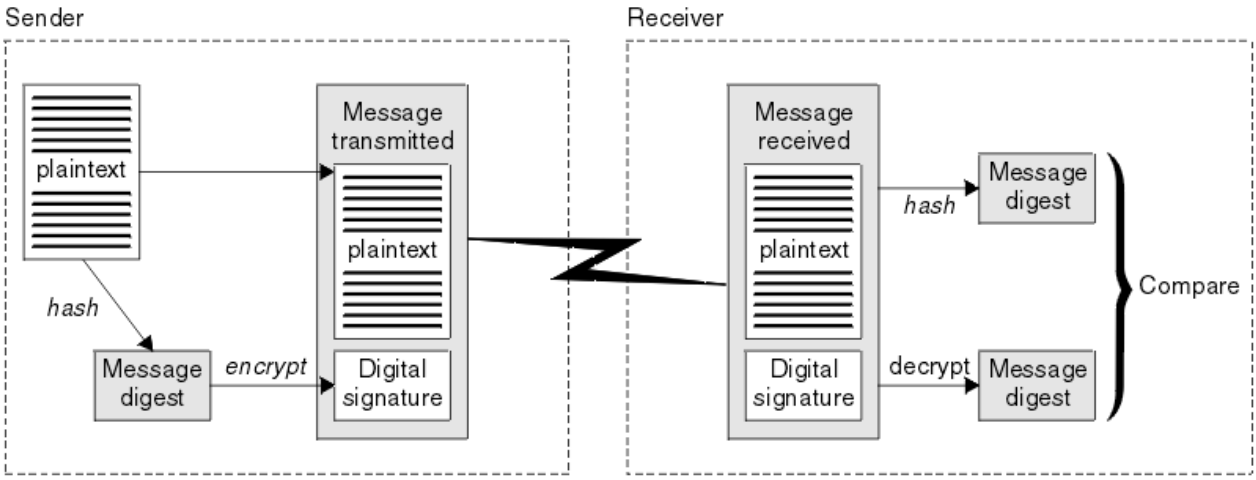
Podpisy cyfrowe różnią się w zależności od podpisywanych danych, w przeciwieństwie do podpisów odręcznych, które nie zależą od treści podpisywanego dokumentu. Jeśli dwie różne wiadomości są

podpisane cyfrowo przez tę samą jednostkę, obie podpisy różnią się, ale można je zweryfikować przy użyciu tego samego klucza publicznego, czyli klucza publicznego jednostki, która podpisała wiadomości.

Etapy procesu podpisywania cyfrowego są następujące:

1. Nadawca oblicza skrót wiadomości, a następnie szyfruje skrót przy użyciu klucza prywatnego nadawcy, tworząc podpis cyfrowy.
2. Nadawca przesyła podpis cyfrowy z komunikatem.
3. Odbiorca deszyfruje podpis cyfrowy przy użyciu klucza publicznego nadawcy, ponownie generując streszczenie komunikatu nadawcy.
4. Odbiorca oblicza streszczenie komunikatu na podstawie odebranych danych komunikatu i sprawdza, czy oba streszczenia są takie same.

Rysunek 6 na stronie 23 ilustruje ten proces.



Rysunek 6. Proces podpisu cyfrowego

Jeśli podpis cyfrowy jest zweryfikowany, odbiorca wie, że:

- Komunikat nie został zmodyfikowany podczas transmisji.
- Komunikat został wysłany przez jednostkę, która twierdzi, że go wysłała.

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

Uwaga: Można również zaszyfrować sam komunikat, co chroni poufność informacji zawartych w komunikacie.

Standardy FIPS (Federal Information Processing Standards)

Rząd Stanów Zjednoczonych udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. Krajowy Instytut Standardów i Technologii (NIST) jest ważnym organem zajmującym się systemami informatycznymi i bezpieczeństwem. NIST tworzy rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

Jednym z tych standardów jest standard FIPS 140-2, który wymaga użycia silnych algorytmów szyfrowania. Standard FIPS 140-2 określa również wymagania dotyczące algorytmów mieszających, które mają być używane do ochrony pakietów przed modyfikacją podczas przesyłania.

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

IBM MQ obsługuje standard FIPS 140-2, jeśli został w tym celu skonfigurowany.

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

Pojęcia pokrewne

"Kryptografia Suite B National Security Agency (NSA)" na stronie 24
Rząd Stanów Zjednoczonych Ameryki udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. US National Security Agency (NSA) zaleca zestaw interoperacyjnych algorytmów kryptograficznych w standardzie Suite B.

Kryptografia Suite B National Security Agency (NSA)

Rząd Stanów Zjednoczonych Ameryki udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. US National Security Agency (NSA) zaleca zestaw interoperacyjnych algorytmów kryptograficznych w standardzie Suite B.

Standard Suite B określa tryb działania, w którym używany jest tylko konkretny zestaw bezpiecznych algorytmów szyfrowania. 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)

Ponadto standard IETF RFC 6460 określa profile zgodne ze standardem Suite B, które definiują szczegółową konfigurację i zachowanie aplikacji niezbędne do zapewnienia zgodności ze standardem Suite B. Definiuje on dwa profile:

1. Profil zgodny z pakietem Suite B do użycia z protokołem TLS 1.2. W przypadku skonfigurowania dla operacji zgodnych z pakietem B używany jest tylko ograniczony zestaw wymienionych algorytmów szyfrowania.
2. Profil przejściowy do użycia z protokołem TLS 1.0 lub TLS 1.1. Ten profil umożliwia współdziałanie z serwerami niezgodnymi z pakietem Suite B. W przypadku skonfigurowania 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 zestaw włączonych algorytmów szyfrowania w celu zapewnienia pewnego poziomu bezpieczeństwa.

W systemach AIX, Linux, and Windows produkt IBM MQmożna skonfigurować w taki sposób, aby był zgodny z profilem 1.2 TLS zgodnym z pakietem Suite B, ale nie obsługuje profilu przejściowego Suite B. Więcej informacji zawiera sekcja "Szyfrowanie NSA Suite B w produkcie IBM MQ" na stronie 43.

Odsyłacze pokrewne

"Standardy FIPS (Federal Information Processing Standards)" na stronie 23
Rząd Stanów Zjednoczonych udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. Krajowy Instytut Standardów i Technologii (NIST) jest ważnym organem zajmującym się systemami informatycznymi i bezpieczeństwem. NIST tworzy rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

IBM MQ mechanizmy zabezpieczeń

Ta kolekcja tematów zawiera opis konkretnych mechanizmów w produkcie IBM MQ , które implementują różne pojęcia związane z bezpieczeństwem.

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 używać protokołu TLS do zapewnienia bezpieczeństwa na poziomie łącza. Wywołujący agent MCA jest klientem TLS, a odpowiadający agent MCA jest serwerem TLS.

IBM MQ obsługuje wersje 1.2 i 1.3 protokołu TLS. Wcześniejsze wersje protokołu TLS i SSL nie są domyślnie włączone, ale mogą być włączone w razie potrzeby. Algorytmy szyfrowania używane przez protokół TLS można określić, podając CipherSpec jako część definicji kanału.

Listę specyfikacji szyfrowania CipherSpecs obsługiwanych przez produkt IBM MQ i "Nieaktualne CipherSpecs" na stronie 482 dla nieaktualnych specyfikacji można znaleźć w sekcji "Włączanie CipherSpecs" na stronie 466 .

Za pomocą parametrów SECPROT i SSLCIPH można wyświetlić protokół zabezpieczeń i CipherSpec używane 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 partnerskiego agenta MCA na drugim końcu kanału. Kod IBM MQ na końcu kanału MQI klienta 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 serwera.

Menedżery kolejek i użytkownicy klienta IBM MQ nie muszą mieć powiązanych osobistych certyfikatów cyfrowych, jeśli działają jako klienty TLS, chyba że po stronie serwera kanału określono parametr SSLCAUTH (REQUIRED).

Certyfikaty cyfrowe są przechowywane w *repozytorium kluczy*. Atrybut menedżera kolejek **SSLKeyRepository** określa położenie repozytorium kluczy przechowującego certyfikat cyfrowy menedżera kolejek. W systemie klienckim IBM MQ zmienna środowiskowa MQSSLKEYR określa położenie repozytorium kluczy przechowującego certyfikat cyfrowy użytkownika. Alternatywnie aplikacja kliencka IBM MQ może określić swoje położenie w polu **KeyRepository** struktury opcji konfiguracyjnych TLS (MQSCO) w wywołaniu MQCONNX. Więcej informacji na temat repozytoriów kluczy i sposobu określania ich położenia zawierają tematy pokrewne.

Obsługa protokołu TLS

IBM MQ zapewnia obsługę protokołów TLS 1.2 i TLS 1.3 na wszystkich platformach. Więcej informacji na temat protokołu TLS można znaleźć w podtematach.

Klienty dla systemów Java i JMS
Te klienty używają maszyny JVM do obsługi protokołu TLS.

AIX, Linux, and Windows
Obsługa protokołu TLS jest instalowana razem z produktem IBM MQ.

IBM i
Obsługa protokołu TLS jest integralną częścią systemu operacyjnego IBM i .

z/OS
Obsługa protokołu TLS jest integralną częścią systemu operacyjnego z/OS . Obsługa protokołu TLS w systemie z/OS nosi nazwę *System SSL*.

Informacje na temat wymagań wstępnych dotyczących obsługi protokołu TLS w systemie IBM MQ zawiera sekcja Wymagania systemowe produktu IBM MQ.

Pojęcia pokrewne

"Szyfrujące protokoły bezpieczeństwa: TLS" na stronie 18
Protokoły szyfrujące zapewniają bezpieczne połączenia, umożliwiając dwóm stronom komunikację z ochroną prywatności i integralnością 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.

Informacje te używają terminu ogólnego *repozytorium kluczy* do opisania magazynu certyfikatów cyfrowych i powiązanych z nimi kluczy prywatnych. Repozytorium kluczy jest przywoływany przez różne nazwy na różnych platformach i w różnych środowiskach, które obsługują protokół TLS:

- IBM i W systemie IBM i: *baza certyfikatów*
- W systemach Java i JMS: *keystore* i *truststore*
- ALW W systemie AIX, 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 13 i “Pojęcia związane z protokołem TLS (Transport Layer Security)” na stronie 18.

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

- Liczba certyfikatów CA pochodzących z różnych ośrodków certyfikacji, które umożliwiają menedżerowi kolejek lub klientowi zweryfikowanie certyfikatów odebranych od partnera po zdalnym zakończeniu połączenia. Poszczególne certyfikaty mogą znajdować się w łańcuchu certyfikatów.
- Jeden lub więcej certyfikatów osobistych otrzymanych z ośrodka certyfikacji. Z każdym menedżerem kolejek lub programem IBM MQ MQI clientnależy powiązać osobny certyfikat osobisty. 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 osobistemu.
- Żądania certyfikatów oczekujące na podpisanie przez zaufany certyfikat ośrodka CA.

Więcej informacji na temat ochrony repozytorium kluczy zawiera sekcja “Ochrona repozytoriów kluczy IBM MQ” na stronie 27.

Położenie repozytorium kluczy zależy od używanej platformy:

IBM i **IBM i**

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

Alternatywnie można określić, że zamiast niej ma być używana baza certyfikatów systemu IBM i . W tym celu należy zmienić wartość atrybutu **SSLKEYR** menedżera kolejek na `*SYSTEM`. Wartość ta wskazuje, że menedżer kolejek musi używać bazy certyfikatów systemu, a menedżer kolejek jest zarejestrowany jako aplikacja w programie Digital Certificate Manager (DCM).

Baza certyfikatów zawiera również klucz prywatny menedżera kolejek.

ALW **Systemy AIX, Linux, and Windows**

Repozytorium kluczy jest plikiem bazy danych kluczy. Na przykład w systemie AIX 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`.

V 9.3.0 V 9.3.0 Aby uzyskać dostęp do pliku bazy danych kluczy IBM MQ , należy podać hasło do bazy danych kluczy. Można to zrobić bezpośrednio lub za pomocą pliku ukrytych haseł. Jeśli używany jest plik ukrytych haseł, musi on znajdować się w tym samym katalogu i mieć ten sam rdzeń, co baza danych kluczy, i musi kończyć się przyrostkiem `.sth`, na przykład `/var/mqm/qmgrs/QM1/ssl/key.sth`.

Uwaga: Karty sprzętowe szyfrowania PKCS #11 mogą zawierać certyfikaty i klucze, które są przechowywane w pliku bazy danych kluczy. Jeśli certyfikaty i klucze są przechowywane na kartach

PKCS #11 , program IBM MQ nadal wymaga dostępu zarówno do pliku bazy danych kluczy, jak i do pliku ukrytych haseł.

W systemach AIX, Linux, and Windows baza danych kluczy zawiera również klucz prywatny dla certyfikatu osobistego powiązanego z menedżerem kolejek lub programem IBM MQ MQI client.

z/OS

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

Inne zewnętrzne menedżery bezpieczeństwa (ESM) również używają pliku kluczy do przechowywania certyfikatów.

Klucze prywatne są zarządzane przez program RACF.

Ochrona repozytoriów kluczy IBM MQ
Repozytorium kluczy dla systemu IBM MQ jest plikiem. Upewnij się, że tylko zamierzony użytkownik może uzyskać dostęp do pliku repozytorium kluczy. Uniemożliwi to intruzowi lub innemu nieautoryzowanemu użytkownikowi skopiowanie pliku repozytorium kluczy do innego systemu, a następnie skonfigurowanie identycznego identyfikatora użytkownika w tym systemie w celu podszywania się pod zamierzonego użytkownika.

Uprawnienia do plików zależą od komendy umask użytkownika i używanego narzędzia. W systemie Windowskonta IBM MQ wymagają uprawnienia `BypassTraverseChecking` , co oznacza, że uprawnienia do folderów w ścieżce do pliku nie mają zastosowania.

Sprawdź uprawnienia do plików repozytorium kluczy i upewnij się, że pliki i folder zawierający nie są dostępne do odczytu dla wszystkich, najlepiej nawet dla grup.

Ustawienie magazynu kluczy w trybie tylko do odczytu jest dobrą praktyką w dowolnym systemie, w którym tylko administrator może włączyć operacje zapisu w celu przeprowadzenia konserwacji.

W praktyce należy chronić wszystkie magazyny kluczy, niezależnie od położenia i tego, czy są one chronione hasłem, czy nie; należy chronić repozytoria kluczy.

Etykiety certyfikatów cyfrowych, zrozumienie wymagań
Podczas konfigurowania protokołu TLS do korzystania z certyfikatów cyfrowych mogą być wymagane określone wymagania dotyczące etykiet, w zależności od używanej platformy i metody połączenia.

Co to jest etykieta certyfikatu?

Etykieta certyfikatu jest unikalnym identyfikatorem reprezentującym certyfikat cyfrowy przechowywany w repozytorium kluczy i udostępnia wygodną, czytelną dla człowieka nazwę, za pomocą której można odwoływać się do konkretnego certyfikatu podczas wykonywania funkcji zarządzania kluczami. Etykieta certyfikatu jest przypisywana podczas dodawania certyfikatu do repozytorium kluczy po raz pierwszy.

Etykieta certyfikatu jest oddzielona od pól **Subject Distinguished Name** lub **Subject Common Name** certyfikatu. Należy zauważyć, że pola **Subject Distinguished Name** i **Subject Common Name** są polami w samym certyfikacie. Są one definiowane podczas tworzenia certyfikatu i nie można ich zmieniać. W razie potrzeby można jednak 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 używających kodu EBCDIC katakana nie można używać małych liter.

Dodatkowe wymagania dotyczące wartości etykiet certyfikatów są określone w poniższych sekcjach.

W jaki sposób używana jest etykieta certyfikatu?

Program IBM MQ używa etykiet certyfikatów do zlokalizowania 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 wybraną wartość. Jeśli wartość nie zostanie ustawiona, zostanie użyta domyślna etykieta zgodna z konwencją nazewnictwa w zależności od używanej platformy. Szczegółowe informacje na ten temat zawierają poniższe sekcje dotyczące konkretnych platform.

Uwagi:

1. W systemach Java i JMS nie można samodzielnie ustawić etykiety certyfikatu.
2. Automatycznie definiowane kanały utworzone przez wyjście automatycznej definicji kanału (CHAD) nie mogą ustawić etykiety certyfikatu, ponieważ uzgadnianie TLS miało miejsce przed utworzeniem kanału. Ustawienie etykiety certyfikatu w wyjściu CHAD dla kanałów przychodzących nie ma wpływu.

W tym kontekście klient TLS odwołuje się do partnera połączenia inicjującego uzgadnianie, którym może być klient IBM MQ lub inny menedżer kolejek.

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

Serwer TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli został wysłany. Jeśli klient nie wyśle certyfikatu, uwierzytelnianie nie powiedzie się, jeśli koniec kanału, który działa jako serwer TLS, zostanie zdefiniowany z parametrem **SSLCAUTH** ustawionym na wartość *REQUIRED* lub wartością parametru **SSLPEER** .

Należy zauważyć, że kanały przychodzące (w tym kanały odbiornika, requestera, odbiornika klastra, niekwalifikowanego serwera i połączenia z serwerem) wysyłają skonfigurowany certyfikat tylko wtedy, gdy wersja IBM MQ zdalnego węzła sieci w pełni obsługuje konfigurację etykiety certyfikatu, a kanał używa CipherSpecTLS.

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

We wszystkich innych przypadkach parametr **CERTLABL** menedżera kolejek określa wysyłany certyfikat. W szczególności następujące elementy otrzymują tylko certyfikat skonfigurowany przez parametr **CERTLABL** menedżera kolejek, niezależnie od ustawienia etykiety specyficznej dla kanału:

- Klienty Java i JMS obsługujące protokół SNI (Server Name Indication), czyli certyfikaty dla poszczególnych kanałów.
- Wersje produktu IBM MQ wcześniejsze niż IBM MQ 8.0.
- Zarządzane klienty .NET

Ponadto certyfikat używany przez kanał musi być odpowiedni dla kanału CipherSpec -więcej informacji na ten temat zawiera sekcja “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48 .

Produkt IBM MQ 8.0 i nowsze wersje obsługują użycie wielu certyfikatów w tym samym menedżerze kolejek przy użyciu etykiety certyfikatu dla kanału określonej za pomocą atrybutu **CERTLABL** w definicji kanału. Kanały przychodzące do menedżera kolejek (na przykład połączenie z serwerem lub odbiornik) polegają na wykrywaniu nazwy kanału przy użyciu protokołu TLS Server Name Indication (SNI) w celu przedstawienia poprawnego certyfikatu z menedżera kolejek. Więcej informacji na temat używania wielu certyfikatów w menedżerze kolejek zawiera sekcja “Sposób, w jaki program IBM MQ udostępnia wiele certyfikatów” na stronie 30.

Jeśli kanał łączy się z docelowym menedżerem kolejek za pośrednictwem programu IBM MQ Internet Pass-Thru (MQIPT), a trasa MQIPT ma ustawione zarówno **SSLServer** , jak i **SSLClient** , istnieją dwie oddzielne sesje TLS między punktami końcowymi. W wersjach wcześniejszych niż IBM MQ 9.2.5dane

SNI nie przepływają przez przerwanie sesji. Zapobiega to użyciu certyfikatu dla kanału w docelowym menedżerze kolejek na potrzeby połączenia TLS między produktem MQIPT i menedżerem kolejek. Począwszy od produktu IBM MQ 9.2.5, produkt MQIPT można skonfigurować w taki sposób, aby umożliwić używanie wielu certyfikatów przez docelowy menedżer kolejek, ustawiając wartość SNI na nazwę kanału lub przekazując wartość SNI odebraną w połączeniu przychodzącym do trasy. Więcej informacji na temat obsługi wielu certyfikatów i MQIPTzawiera sekcja IBM MQ Obsługa wielu certyfikatów w produkcie MQIPT.

Więcej informacji na temat nawiązywania połączenia z menedżerem kolejek przy użyciu uwierzytelniania jednokierunkowego (jeśli klient TLS nie wysyła certyfikatu) zawiera sekcja Nawiązywanie połączenia z dwoma menedżerami kolejek przy użyciu uwierzytelniania jednokierunkowego.

Systemy wieloplatformowe

Multi

W systemie Wiele platformserwer TLS wysyła certyfikat do klienta.

W przypadku menedżerów kolejek i klientów następujące źródła są przeszukiwane w kolejności pod kątem niepustej wartości. Pierwsza niepusta wartość określa etykietę certyfikatu. Etykieta certyfikatu musi istnieć w repozytorium kluczy. Jeśli nie zostanie znaleziony zgodny certyfikat o poprawnej wielkości i formacie zgodnym 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 ma format: `ibmwebspheremq` z dodaną nazwą menedżera kolejek, jest zapisana 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 **`CertificateLabel`** struktury MQSCO.
3. Zmienna środowiskowa **MQCERTLABL**.
4. `.ini` Plik **`CertificateLabel`** klienta (w sekcji SSL), atrybut
5. Wartość domyślna (w formacie: `ibmwebspheremq`) z identyfikatorem użytkownika, który jest uruchamiany jako aplikacja kliencka, jest dodawana małymi literami. Na przykład dla identyfikatora użytkownika `USER1`domyślną etykietą certyfikatu jest `ibmwebspheremquser1`.

z/OS systemy

z/OS

IBM MQ Klienty nie są obsługiwane w systemie z/OS. Jednak menedżer kolejek systemu z/OS może pełnić rolę klienta TLS podczas inicjowania połączenia lub serwera TLS podczas akceptowania żądania połączenia. Wymagania dotyczące etykiet certyfikatów dla menedżerów kolejek w systemie z/OS mają zastosowanie w obu tych rolach i różnią się od wymagań w systemie Wiele platform.

W przypadku menedżerów kolejek i klientów następujące źródła są przeszukiwane w kolejności pod kątem niepustej wartości. Pierwsza niepusta wartość określa etykietę certyfikatu. Etykieta certyfikatu musi istnieć w repozytorium kluczy. Jeśli nie zostanie znaleziony zgodny certyfikat o poprawnej wielkości i formacie zgodnym z etykietą, wystąpi błąd i uzgadnianie TLS nie powiedzie się.

1. Atrybut etykiety certyfikatu kanału, **CERTLABL**.
2. W przypadku współużytkowania atrybut etykiety certyfikatu grupy współużytkowania kolejki **CERTQSGL**.

   Jeśli nie jest współużytkowany, atrybut etykiety certyfikatu menedżera kolejek **CERTLABL**.

3. Wartość domyślna, która ma format: `ibmWebSphereMQ` z dołączoną nazwą menedżera kolejek lub grupy współużytkowania kolejek. Należy zauważyć, że w tym łańcuchu jest rozróżniana wielkość liter i musi on zostać zapisany w sposób przedstawiony poniżej. Na przykład dla menedżera kolejek o nazwie `QM1`domyślną etykietą certyfikatu jest `ibmWebSphereMQQM1`.
4. Jeśli nie znaleziono certyfikatu w formacie podanym w opcji “3” na stronie 30, program IBM MQ spróbuje użyć certyfikatu oznaczonego jako domyślny w pliku kluczy.

Informacje na temat sposobu wyświetlania repozytorium kluczy zawiera sekcja “Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie z/OS” na stronie 354.

Klienty IBM MQ Java i IBM MQ JMS

Klienty IBM MQ Java i IBM MQ JMS używają narzędzi dostawcy JSSE (Java Secure Socket Extension) do wybrania certyfikatu osobistego podczas uzgadniania TLS i dlatego nie podlegają wymaganiom dotyczącym etykiet certyfikatów.

Domyślnie klient JSSE przeprowadza iterację przez certyfikaty w repozytorium kluczy, wybierając pierwszy znaleziony akceptowalny certyfikat osobisty. Jednak to zachowanie jest tylko domyślne i zależy od implementacji dostawcy JSSE.

Ponadto interfejs JSSE jest wysoce konfigurowalny dzięki konfiguracji i bezpośredniemu dostępowi aplikacji do środowiska wykonawczego. Szczegółowe informacje można znaleźć w dokumentacji dostarczonej przez dostawcę JSSE.

Aby rozwiązać problem 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, za pomocą konfiguracji lub wprowadzając w wierszu komend komendę `-Djavax.net.debug=ssl` .

Linux *Sposób, w jaki program IBM MQ udostępnia wiele certyfikatów*
Wskazanie nazwy serwera (Server Name Indication-SNI) jest rozszerzeniem protokołu TLS, które umożliwia klientowi wskazanie wymaganej usługi. W terminologii IBM MQ jest to równoznaczne z kanałem.

Rozszerzenie SNI jest używane przez IBM MQ w celu umożliwienia określenia wielu certyfikatów w różnych kanałach za pomocą parametru CERTLABL w definicji kanału.

Adres SNI używany przez IBM MQ jest oparty na żądanej nazwie kanału, po której następuje przyrostek `.chl.mq.ibm.com`.

Nazwy kanałów IBM MQ są odwzorowywane na poprawne nazwy SNI w następujący sposób:

- Wielkie litery A do Z są zawijane do małych liter
- Cyfry od `0` do 9 pozostają niezmienione
- Wszystkie inne znaki, w tym małe litery a na z, są konwertowane na dwucyfrowy szesnastkowy kod ASCII (małymi literami), po którym następuje łącznik.
  - Małe litery a do z odwzorowana na wartość szesnastkową `61-` na `7a-`
  - Wartość procentowa (%) jest odwzorowywana na wartość szesnastkową `25-`
  - łącznik (-) jest odwzorowywany na wartość szesnastkową `2d-`
  - kropka (.) jest odwzorowywana na wartość szesnastkową `2e-`
  - ukośnik (/) jest odwzorowywany na szesnastkowy `2f-`
  - Znak podkreślenia (_) jest odwzorowywany na wartość szesnastkową `5f-`

Na platformach EBCDIC nazwa kanału jest przekształcana w kod ASCII przed zastosowaniem tego odwzorowania.

Na przykład nazwa kanału `TO.QMGR1` jest odwzorowywana na adres SNI `to2e-qmgr1.chl.mq.ibm.com`.

Natomiast nazwa kanału `to.qmgr1` jest odwzorowywana na adres SNI `74-6f-2e-71-6d-67-72-1.chl.mq.ibm.com`.

Uwaga: W środowiskach, w których wygenerowany adres URL SNI musi być zgodny ze specyfikacjami formatowania adresu URL, na przykład gdy klient łączy się z menedżerem kolejek działającym w produkcie Red Hat® OpenShift® na trasie Red Hat OpenShift , nazwa kanału nie może kończyć się małą literą.

Właściwość **OutboundSNI** sekcji SSL umożliwia określenie, czy dla SNI nazwa docelowego kanału IBM MQ ma być ustawiona na system zdalny podczas inicjowania połączenia TLS, czy na nazwę hosta. Więcej informacji na temat właściwości **OutboundSNI** można znaleźć w sekcji Sekcja SSL pliku qm.ini i Sekcja SSL pliku konfiguracji klienta.

Wiele certyfikatów wymaga ustawienia SNI na nazwę kanału IBM MQ . Jeśli do nawiązania połączenia z kanałem IBM MQ ze skonfigurowaną etykietą certyfikatu zostanie użyta nazwa hosta, nazwa niestandardowa lub brak nazwy SNI, aplikacja nawiązująca połączenie zostanie odrzucona z błędem MQRC_SSL_INITIALIZATION_ERROR, a w dziennikach błędów menedżera kolejek zdalnych zostanie zapisany komunikat AMQ9673 .

V 9.3.0 Jeśli kanał łączy się z docelowym menedżerem kolejek za pośrednictwem programu IBM MQ Internet Pass-Thru (MQIPT), program MQIPT musi być skonfigurowany w taki sposób, aby albo ustawić SNI na nazwę kanału, albo przekazać przez SNI odebraną w połączeniu przychodzącym do trasy, aby umożliwić używanie wielu certyfikatów przez docelowy menedżer kolejek. Więcej informacji na temat obsługi wielu certyfikatów i MQIPTzawiera sekcja IBM MQ Obsługa wielu certyfikatów w produkcie MQIPT.

Więcej informacji na temat sposobu użycia tej właściwości zawiera sekcja Nawiązywanie połączenia z menedżerem kolejek wdrożonym w klastrze Red Hat OpenShift.

Odświeżanie repozytorium kluczy menedżera kolejek
Po zmianie treści repozytorium kluczy istniejące procesy menedżera kolejek nie pobierają nowej treści do czasu wydania komendy REFRESH SECURITY TYPE (SSL) lub zrestartowania menedżera kolejek.

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

Jeśli menedżer kolejek utworzy nowy proces kanału (przy użyciu produktu `amqrmppa` lub **runmqchl**) po zmianie zawartości magazynu kluczy, nowy proces natychmiast rozpocznie korzystanie z nowych certyfikatów, a istniejące procesy będą nadal używać kopii magazynu kluczy znajdującej się w pamięci podręcznej. Więcej informacji na temat zawiera sekcja “Gdy zmiany w certyfikatach lub w bazie certyfikatów zaczną obowiązywać w dniu AIX, Linux, and Windows” na stronie 326.

Należy zauważyć, że wiele działających kanałów może używać różnych wersji repozytorium kluczy do czasu wydania komendy REFRESH SECURITY TYPE (SSL).

Repozytorium kluczy można również odświeżyć za pomocą komend PCF lub programu IBM MQ Explorer. Więcej informacji na ten temat zawiera sekcja Komenda MQCMD_REFRESH_SECURITY oraz temat *Odświeżanie zabezpieczeń TLS* w sekcji IBM MQ Explorer dokumentacji tego produktu.

Pojęcia pokrewne
“Odświeżanie widoku klienta dla zawartości repozytorium kluczy SSL/TLS i ustawień SSl/TLS” na stronie 31
Aby zaktualizować aplikację kliencką przy użyciu odświeżonej zawartości repozytorium kluczy, należy zatrzymać i zrestartować aplikację kliencką.

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

Nie można odświeżyć zabezpieczeń w kliencie systemu IBM MQ ; nie istnieje odpowiednik komendy REFRESH SECURITY TYPE (SSL) dla klientów (patrz sekcja REFRESH SECURITY). aby uzyskać więcej informacji.

Po każdej zmianie certyfikatu bezpieczeństwa należy zatrzymać i zrestartować aplikację, aby zaktualizować aplikację kliencką przy użyciu odświeżonej zawartości repozytorium kluczy.

Jeśli restartowanie kanału powoduje odświeżenie konfiguracji i jeśli aplikacja ma logikę ponownego połączenia, możliwe jest odświeżenie zabezpieczeń na kliencie za pomocą komendy STOP CHL STATUS (INACTIVE).

Pojęcia pokrewne

“Odświeżanie repozytorium kluczy menedżera kolejek” na stronie 31
Po zmianie treści repozytorium kluczy istniejące procesy menedżera kolejek nie pobierają nowej treści do czasu wydania komendy REFRESH SECURITY TYPE (SSL) lub zrestartowania menedżera kolejek.

Zabezpieczenie hasłem MQCSP

Referencje uwierzytelniające, które są określone w strukturze MQCSP, mogą być chronione przy użyciu funkcji ochrony hasła MQCSP IBM MQ lub szyfrowane przy użyciu szyfrowania TLS.

Aplikacje IBM MQ client mogą podać identyfikator użytkownika i hasło podczas nawiązywania połączenia z menedżerem kolejek. V 9.3.4 W produkcie IBM MQ 9.3.4aplikacje mogą również dostarczyć znacznik uwierzytelniania jako alternatywną metodę uwierzytelniania. Te referencje są wysyłane do menedżera kolejek w strukturze MQCSP.

Jeśli kanał używa szyfrowania TLS, referencje w MQCSP są szyfrowane zgodnie ze specyfikacją szyfrowania TLS. Jeśli w produkcie IBM MQ 8.0kanał nie używa szyfrowania TLS, produkt IBM MQ może chronić te referencje przed ich wysłaniem przez sieć, aby uniknąć wysyłania referencji przez sieć w postaci jawnego tekstu. Składnik produktu IBM MQ , który chroni te referencje, jest nazywany zabezpieczeniem hasłem MQCSP.

Jeśli używane jest zabezpieczenie hasłem MQCSP, chronione są następujące dane w strukturze MQCSP:

- Hasło, jeśli w polu `MQCSP.AuthenticationType` ustawiono wartość `MQCSP_AUTH_USER_ID_AND_PW`.
- V 9.3.4 Znacznik uwierzytelniania, jeśli w polu `MQCSP.AuthenticationType` ustawiono wartość `MQCSP_AUTH_ID_TOKEN`.

Ważne: Zabezpieczenie hasłem MQCSP jest przydatne w celach testowych i programistycznych, ponieważ użycie zabezpieczenia hasłem MQCSP jest prostsze niż skonfigurowanie szyfrowania TLS, ale nie tak bezpieczne. Na potrzeby środowiska produkcyjnego należy używać szyfrowania TLS zamiast zabezpieczenia hasłem systemu IBM MQ , zwłaszcza gdy sieć między klientem a menedżerem kolejek jest niezaufana, ponieważ szyfrowanie TLS jest bezpieczniejsze.

Jeśli użytkownik jest zaniepokojony tym, jakie szyfrowanie jest używane i ile ochrony oferuje, należy użyć pełnego szyfrowania TLS. W przypadku protokołu TLS algorytmy są publicznie znane i można wybrać odpowiednie algorytmy dla danego przedsiębiorstwa, używając atrybutu kanału **SSLCIPH** .

Więcej informacji na temat struktury MQCSP zawiera sekcja Struktura MQCSP.

Referencje w strukturze MQCSP są chronione przy użyciu zabezpieczenia hasłem IBM MQ , jeśli spełnione są wszystkie następujące warunki:

- Oba końce połączenia używają systemu IBM MQ 8.0lub nowszego.
- Kanał nie używa szyfrowania TLS. Kanał nie używa szyfrowania TLS, jeśli kanał ma pusty atrybut **SSLCIPH** lub atrybut **SSLCIPH** jest ustawiony na specyfikację szyfru, która nie udostępnia szyfrowania. Puste szyfry, na przykład NULL_SHA, nie udostępniają szyfrowania.
- Pole `MQCSP.AuthenticationType` jest ustawione na wartość `MQCSP_AUTH_USER_ID_AND_PWD` lub `MQCSP_AUTH_ID_TOKEN`. Więcej informacji na temat pola `MQCSP.AuthenticationType` zawiera sekcja **`AuthenticationType`**.
- Jeśli klientem jest IBM MQ Explorer , a tryb zgodności identyfikacji użytkownika nie jest włączony. Ten tryb nie jest trybem domyślnym używanym przez program IBM MQ Explorer do wysyłania identyfikatora użytkownika i hasła. Ten warunek dotyczy tylko systemu IBM MQ Explorer.

Jeśli którykolwiek z tych warunków nie jest spełniony, referencje nie są chronione hasłem MQCSP. Jeśli wartość atrybutu **PasswordProtection** uniemożliwia wysyłanie referencji w postaci jawnego tekstu, a kanał nie używa szyfrowania TLS, połączenie nie powiedzie się i zostanie zwrócony kod przyczyny MQRC_PASSWORD_PROTECTION_ERROR (2594).

Ustawienie konfiguracyjne PasswordProtection

Atrybut **PasswordProtection** w sekcji **Channels** plików konfiguracyjnych klienta i menedżera kolejek może uniemożliwić wysyłanie referencji w postaci zwykłego tekstu.

Uwaga: Ten atrybut dotyczy tylko połączeń, które nie używają szyfrowania TLS. Referencje są szyfrowane przy użyciu protokołu TLS zamiast zabezpieczania hasłem MQCSP, jeśli połączenie używa szyfrowania TLS.

Atrybut można ustawić na jedną z następujących wartości. Wartością domyślną jest `compatible`.

Kompatybilny
Referencje są wysyłane w postaci jawnego tekstu, jeśli menedżer kolejek lub klient korzysta z wersji produktu IBM MQ wcześniejszej niż IBM MQ 8.0. Oznacza to, że referencje mogą być wysyłane przez sieć w postaci jawnego tekstu w celu zachowania zgodności z wersjami produktu IBM MQ , które nie obsługują zabezpieczenia hasłem MQCSP.

Referencje są chronione przez ochronę hasłem MQCSP, jeśli zarówno menedżer kolejek, jak i klient mają uruchomioną wersję produktu IBM MQ w wersji IBM MQ 8.0 lub nowszej.

Nawiązanie połączenia nie powiedzie się przed wysłaniem referencji, jeśli zarówno menedżer kolejek, jak i klient działają w systemie IBM MQ w wersji IBM MQ 8.0 lub nowszej, a pole `MQCSP.AuthenticationType` nie jest ustawione na wartość `MQCSP_AUTH_USER_ID_AND_PW` lub `MQCSP_AUTH_ID_TOKEN`.

zawsze
Referencje nie mogą być przesyłane przez sieć bez ochrony.

Referencje są chronione przez ochronę hasłem MQCSP, jeśli zarówno menedżer kolejek, jak i klient mają uruchomioną wersję produktu IBM MQ w wersji IBM MQ 8.0 lub nowszej.

Połączenie nie powiedzie się przed wysłaniem referencji w następujących przypadkach:

- Pole `MQCSP.AuthenticationType` nie jest ustawione na wartość `MQCSP_AUTH_USER_ID_AND_PW` lub `MQCSP_AUTH_ID_TOKEN`.
- Menedżer kolejek lub klient korzysta z wersji produktu IBM MQ wcześniejszej niż IBM MQ 8.0.

opcjonalne
Referencje są chronione przez ochronę hasłem MQCSP, jeśli zarówno menedżer kolejek, jak i klient działają w systemie IBM MQ w wersji IBM MQ 8.0 lub nowszej, a pole `MQCSP.AuthenticationType` jest ustawione na wartość `MQCSP_AUTH_USER_ID_AND_PW` lub `MQCSP_AUTH_ID_TOKEN`. W przeciwnym razie referencje są wysyłane w postaci zwykłego tekstu.

ostrzeżenie
Każdy klient może wysyłać referencje w postaci zwykłego tekstu. Jeśli zostaną odebrane referencje w postaci jawnego tekstu, w dziennikach błędów menedżera kolejek zostanie zapisany komunikat ostrzegawczy AMQ9297W .

Tę opcję można określić tylko w pliku konfiguracyjnym menedżera kolejek.

W przypadku klientów w systemach Java i JMS zachowanie atrybutu **PasswordProtection** zmienia się w zależności od tego, czy klient używa trybu zgodności, czy trybu MQCSP:

- Jeśli klienty Java i JMS działają w trybie zgodności, struktura MQCSP nie jest używana do wysyłania identyfikatora użytkownika i hasła podczas nawiązywania połączenia przez klient. Oznacza to, że zachowanie atrybutu **PasswordProtection** jest takie samo jak zachowanie opisane dla klientów z uruchomioną wersją IBM MQ wcześniejszą niż IBM MQ 8.0.
- Jeśli klienty Java i JMS działają w trybie MQCSP, zachowaniem atrybutu **PasswordProtection** jest zachowanie opisane poniżej.

Więcej informacji na temat uwierzytelniania połączenia z klientami Java i JMS zawiera sekcja “Uwierzytelnianie połączenia z klientem Java” na stronie 86.

Ochrona hasłem MQCSP i MQIPT

V 9.3.1

Jeśli klient łączy się z menedżerem kolejek za pośrednictwem programu IBM MQ Internet Pass-Thru (MQIPT), trasa MQIPT może być skonfigurowana do dodawania lub usuwania szyfrowania TLS. Oznacza to, że trasa MQIPT może być skonfigurowana z `SSLServer=true` i `SSLClient=false`lub `SSLServer=true` i `SSLClient=false`. W takiej sytuacji klient i menedżer kolejek mogą nie uzgodnić algorytmu ochrony hasła, ponieważ jeden koniec kanału używa szyfrowania TLS, a drugi nie. Powoduje to niepowodzenie połączenia z kodem przyczyny MQRC_PASSWORD_PROTECTION_ERROR (2594).

W produkcie IBM MQ 9.3.1produkt MQIPT może dodawać lub usuwać ochronę referencji w strukturach MQCSP w celu zachowania zgodności między klientem a menedżerem kolejek dla tras produktu MQIPT , które dodają lub usuwają szyfrowanie TLS. Zabezpieczenie hasłem MQCSP w produkcie MQIPT jest konfigurowane przy użyciu właściwości trasy **`PasswordProtection`** .

Wartością domyślną właściwości **`PasswordProtection`** jest `required`(wymagane). Ta wartość oznacza, że produkt MQIPT może dodać zabezpieczenie hasłem MQCSP, ale nie może go usunąć. Połączenia z trasą MQIPT , która dodaje szyfrowanie TLS, mogą zakończyć się niepowodzeniem z kodem przyczyny MQRC_PASSWORD_PROTECTION_ERROR (2594) o wartości **`PasswordProtection`**. Aby rozwiązać ten problem, należy ustawić wartość właściwości **`PasswordProtection`** na `compatible` (kompatybilne) w konfiguracji trasy MQIPT .

Więcej informacji na temat właściwości **`PasswordProtection`** w pliku MQIPTzawiera sekcja PasswordProtection.

menedżer certyfikatów cyfrowych (Digital Certificate Manager – DCM)

Program DCM służy do zarządzania certyfikatami cyfrowymi i kluczami prywatnymi w systemie IBM i.

Program Digital Certificate Manager (DCM) umożliwia zarządzanie certyfikatami cyfrowymi i używanie ich w bezpiecznych aplikacjach na serwerze IBM i . Za pomocą programu Digital Certificate Managermożna żądać i przetwarzać certyfikaty cyfrowe pochodzące z ośrodków certyfikacji (CA) lub innych firm. Można również działać jako lokalny ośrodek certyfikacji, aby tworzyć certyfikaty cyfrowe dla użytkowników i zarządzać nimi.

Program DCM obsługuje także używanie list odwołań certyfikatów (Certificate Revocation Lists-CRL) w celu zapewnienia silniejszego procesu sprawdzania poprawności certyfikatów i aplikacji. Można użyć programu DCM do zdefiniowania położenia, w którym znajduje się konkretna lista CRL ośrodka certyfikacji na serwerze LDAP, aby program IBM MQ mógł sprawdzić, czy konkretny certyfikat nie został unieważniony.

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

Program DCM udostępnia oparty na przeglądarce interfejs użytkownika, którego można użyć do zarządzania certyfikatami cyfrowymi dla 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 z nich korzystają. Niektóre pojedyncze zadania są wyświetlane bezpośrednio w głównej ramce nawigacyjnej, ale większość zadań w ramce nawigacyjnej jest podzielona na kategorie. Na przykład Zarządzanie certyfikatami jest kategorią zadań, która zawiera różne indywidualne zadania, takie jak wyświetlanie certyfikatu, odnawianie certyfikatu i importowanie certyfikatu. Jeśli element w ramce nawigacyjnej jest kategorią zawierającą więcej niż jedno zadanie, po jego lewej stronie wyświetlana jest strzałka. Strzałka wskazuje, że po wybraniu odsyłacza do kategorii zostanie wyświetlona rozwinięta lista zadań umożliwiająca wybór zadania do wykonania.

Ważne informacje na temat programu DCM można znaleźć w następujących publikacjach dotyczących produktu IBM Redbooks :

- *IBM i Ochrona sieci: OS/400 V5R1 Rozszerzenia DCM i Cryptographic Enhancements*, SG24-6168. Podstawowe informacje na temat konfigurowania systemu IBM i jako lokalnego ośrodka CA można znaleźć w załącznikach.
- *AS/400 Internet Security: Developing a Digital Certificate Infrastructure*, SG24-5659. W szczególności zob. rozdział 5. *Digital Certificate Manager dla systemu AS/400* , który wyjaśnia program DCM AS/400 .

Standardy FIPS (Federal Information Processing Standards)

W tym temacie przedstawiono program sprawdzania poprawności Cryptomodule FIPS (Federal Information Processing Standards) dla National Institute of Standards and Technology oraz funkcje kryptograficzne, które mogą być używane w kanałach TLS.

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Te informacje dotyczą następujących platform:

- ALW AIX, Linux, and Windows
- z/OS z/OS

ALW Więcej informacji na temat zgodności IBM MQ połączenia TLS w systemie AIX, Linux, and Windowsze standardem FIPS 140-2 zawiera sekcja “Standardy FIPS (Federal Information Processing Standards) dla AIX, Linux, and Windows” na stronie 36.

z/OS Więcej informacji na temat zgodności IBM MQ połączenia TLS w systemie z/OSze standardem FIPS 140-2 zawiera sekcja “Standardy FIPS (Federal Information Processing Standards) dla z/OS” na stronie 38.

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.

Z biegiem czasu standardy FIPS (Federal Information Processing Standards) są aktualizowane w celu odzwierciedlenia nowych ataków na algorytmy i protokoły szyfrowania. Na przykład niektóre CipherSpecs mogą przestać mieć certyfikat FIPS. W przypadku wystąpienia takich zmian 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 287
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

“Używanie komend runmqckm, runmqakm i strmqikm do zarządzania certyfikatami cyfrowymi” na stronie 312
W systemach AIX, Linux, and Windows można zarządzać kluczami i certyfikatami cyfrowymi za pomocą programu **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub 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 FIPS (Federal Information Processing Standards)” na stronie 23

Rząd Stanów Zjednoczonych udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. Krajowy Instytut Standardów i Technologii (NIST) jest ważnym organem zajmującym się systemami informatycznymi i bezpieczeństwem. NIST tworzy rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

ALW *Standardy FIPS (Federal Information Processing Standards) dla AIX, Linux, and Windows*

Jeśli szyfrowanie jest wymagane w kanale SSL/TLS w systemach AIX, Linux, and Windows , IBM MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach AIX, Linux, and Windows oprogramowanie ICC przeszło program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program) amerykańskiego National Institute of Standards and Technology na poziomie 140-2.

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Zgodność połączenia TLS IBM MQ z FIPS 140-2 w systemach AIX, Linux, and Windows 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 produktu IBM Global Security Kit (GSKit) ICC ma certyfikat zgodności ze standardem FIPS 140-2 dla zainstalowanej wersji systemu operacyjnego i architektury 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` .
  - Dostęp do wszystkich repozytoriów kluczy jest zapewniany przy użyciu pliku ukrytych haseł, a nie atrybutu **KEYRPWD** menedżera kolejek.
- Dla wszystkich aplikacji IBM MQ MQI client połączenie używa GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja produktu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 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 MQI.
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
  - Dostęp do wszystkich repozytoriów kluczy jest zapewniany za pomocą pliku zeskładowanego, a nie za pomocą mechanizmu haseł repozytorium kluczy.
- 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 korzysta ze standardu GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja produktu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 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 .NET .
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
  - Dostęp do wszystkich repozytoriów kluczy jest zapewniany za pomocą pliku zeskładowanego, a nie za pomocą mechanizmu haseł repozytorium kluczy.
- Dla niezarządzanych aplikacji klienckich XMS .NET połączenie korzysta ze standardu GSKit i jest zgodne ze standardem FIPS, jeśli spełnione są następujące warunki:
  - Zainstalowana wersja produktu GSKit ICC ma certyfikat zgodności ze standardem FIPS 140-2 dla zainstalowanej wersji systemu operacyjnego i architektury sprzętowej.
  - Określono, że ma być używane tylko szyfrowanie z certyfikatem FIPS, zgodnie z opisem w dokumentacji produktu XMS .NET .
  - Wszystkie repozytoria kluczy zostały utworzone i poddane operacjom przy użyciu tylko oprogramowania zgodnego ze standardem FIPS, takiego jak **runmqakm** z opcją `-fips` .
  - Dostęp do wszystkich repozytoriów kluczy jest zapewniany za pomocą pliku zeskładowanego, a nie za pomocą mechanizmu haseł repozytorium kluczy.

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 protokołu GSKitkomponent, który ma certyfikat FIPS 140-2, ma nazwę *ICC*. Jest to wersja tego komponentu, która określa zgodność produktu GSKit ze standardami FIPS na danej platformie. Aby określić aktualnie zainstalowaną wersję systemu ICC , uruchom komendę **dspmqver -p 64 -v** .

Poniżej przedstawiono przykładowy fragment danych wyjściowych komendy **dspmqver -p 64 -v** dotyczących komendy 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 certyfikacyjną NIST dla systemu GSKit ICC 8 (dołączoną do produktu 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 produkt IBM MQ można skonfigurować tak, aby były dostarczane przez producenta sprzętu. W takim przypadku konfiguracja jest zgodna ze standardem FIPS tylko wtedy, gdy te moduły szyfrujące mają certyfikat FIPS.

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 przez połączenie. Domyślnie program IBM MQ nie resetuje tajnego klucza sesji, dlatego należy go skonfigurować. Niepowodzenie włączenia resetowania klucza tajnego w przypadku używania Triple DES CipherSpec i zgodności ze standardem FIPS 140-2 powoduje zamknięcie połączenia 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 514.

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 w przypadku używania algorytmu szyfrowania Triple DES CipherSpecs w konfiguracji FIPS 140-2. Alternatywnie można uniknąć używania algorytmu Triple DES.

Pojęcia pokrewne

“Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.” na stronie 287
Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

“Używanie komend runmqckm, runmqakm i strmqikm do zarządzania certyfikatami cyfrowymi” na stronie 312
W systemach AIX, Linux, and Windows można zarządzać kluczami i certyfikatami cyfrowymi za pomocą programu **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub 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 FIPS (Federal Information Processing Standards)” na stronie 23
Rząd Stanów Zjednoczonych udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. Krajowy Instytut Standardów i Technologii (NIST) jest ważnym organem zajmującym się systemami informatycznymi i bezpieczeństwem. NIST tworzy rekomendacje i standardy, w tym standardy FIPS (Federal Information Processing Standards).

z/OS *Standardy FIPS (Federal Information Processing Standards) dla z/OS*
Jeśli szyfrowanie jest wymagane w kanale SSL/TLS w systemie z/OS , produkt IBM MQ używa usługi o nazwie System SSL. Celem systemowej implementacji protokołu SSL jest zapewnienie możliwości bezpiecznego wykonywania w trybie zaprojektowanym z myślą o przestrzeganiu programu sprawdzania poprawności Cryptomodule FIPS (Federal Information Processing Standards) w Instytucie Standardów i Technologii Stanów Zjednoczonych na poziomie 140-2.

Podczas implementowania połączeń zgodnych ze standardem FIPS 140-2 z połączeniami TLS IBM MQ należy rozważyć kilka punktów:

- Aby włączyć kanały komunikatów IBM MQ dla zgodności z FIPS, muszą być spełnione następujące warunki:
  - Zainstalowano i skonfigurowano identyfikator FMID poziomu 3 zabezpieczeń SSL systemu (patrz sekcja Planowanie instalacji produktu IBM MQ).

– Poprawność modułów systemowej implementacji protokołu SSL jest sprawdzana.
– Atrybut SSLFIPS menedżera kolejek został ustawiony na wartość **YES**.

Podczas pracy w trybie FIPS system SSL wykorzystuje asystę CP Assist for Cryptographic Function (CPACF), jeśli jest dostępna. Funkcje kryptograficzne wykonywane przez sprzęt obsługiwany przez ICSF w trybie innym niż FIPS są nadal wykorzystywane podczas wykonywania w trybie FIPS, z wyjątkiem generowania sygnatur RSA, które muszą być wykonywane w oprogramowaniu.

Tabela 2. Różnice między obsługą algorytmów trybu FIPS i trybu innego niż FIPS.

	Bez FIPS		**FIPS**	
Algorytm	**Wielkości kluczy**	**Wsparcie w obsłudze**	**Wielkości kluczy**	**Wsparcie w obsłudze**
RC2	40 i 128			
RC4	40 i 128			
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 w systemowej implementacji protokołu SSL mogą być używane tylko te certyfikaty, które używają algorytmów i wielkości kluczy przedstawionych w tabeli 1. Jeśli podczas sprawdzania poprawności certyfikatu X.509 zostanie napotkany algorytm, który jest niezgodny z trybem FIPS, nie można użyć tego certyfikatu i jest on traktowany jako niepoprawny.

W przypadku aplikacji klasy IBM MQ używających trybu klienta w produkcie WebSphere Application Server należy zapoznać się z sekcją Obsługa standardu FIPS (Federal Information Processing Standard).

Informacje na temat konfiguracji modułu SSL systemu zawiera sekcja Konfiguracja weryfikacji modułu SSL systemu .

Odsyłacze pokrewne

“Standardy FIPS (Federal Information Processing Standards)” na stronie 23
Rząd Stanów Zjednoczonych udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. Krajowy Instytut Standardów i Technologii (NIST) jest ważnym organem zajmującym się systemami informatycznymi i bezpieczeństwem. NIST tworzy 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, do którego odwołuje się atrybut **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 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 dostarczono etykiety certyfikatu do 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 komendy IBM Global Security Kit (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 w systemie IBM MQ MQI client

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

IBM MQ zapewnia obsługę protokołu TLS w produkcie IBM MQ MQI clients w systemach AIX, Linux, and Windows . W przypadku korzystania z bazy danych IBM MQ classes for Javanależy zapoznać się z sekcją Korzystanie z produktu IBM MQ classes for Java , a w przypadku korzystania z bazy danych IBM MQ classes for JMS-z sekcją Używanie produktu IBM MQ classes for JMS. Pozostała część tej sekcji nie dotyczy środowisk Java ani JMS .

Repozytorium kluczy dla IBM MQ MQI client można określić za pomocą wartości MQSSLKEYR w pliku konfiguracyjnym klienta IBM MQ lub podczas wykonywania wywołania MQCONNX przez aplikację. Istnieją trzy opcje określania, że kanał używa protokołu TLS:

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

Zmiennej środowiskowej MQSERVER nie można użyć do określenia, że kanał używa protokołu TLS.

Można kontynuować działanie istniejących aplikacji IBM MQ MQI client bez protokołu TLS, o ile protokół TLS nie zostanie określony na drugim końcu kanału.

Jeśli na komputerze klienta zostaną wprowadzone zmiany w zawartości repozytorium kluczy TLS, położeniu repozytorium kluczy TLS, informacjach uwierzytelniających lub parametrach sprzętu szyfrującego, należy zakończyć wszystkie połączenia TLS, aby odzwierciedlić te zmiany w kanałach połączeń klienckich używanych przez aplikację do nawiązania połączenia z menedżerem kolejek. Po zakończeniu wszystkich połączeń zrestartuj kanały TLS. Używane są wszystkie nowe ustawienia TLS. Te ustawienia są analogiczne do tych, które zostały odświeżone za pomocą komendy REFRESH SECURITY TYPE (SSL) w systemach menedżera kolejek.

Jeśli produkt IBM MQ MQI client działa w systemie AIX, Linux, and Windows ze sprzętem szyfrującym, należy go skonfigurować za pomocą zmiennej środowiskowej MQSSLCRYP. Ta zmienna jest równoważna

parametrowi SSLCRYP komendy ALTER QMGR MQSC. Opis parametru SSLCRYP komendy MQSC ALTER QMGR można znaleźć w sekcji ALTER QMGR . Jeśli używana jest wersja GSK_PCS11 parametru SSLCRYP, etykieta tokenu PKCS #11 musi być podana całkowicie małymi literami.

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 514 i “Standardy FIPS (Federal Information Processing Standards) dla AIX, Linux, and Windows” na stronie 36.

Więcej informacji na temat obsługi protokołu TLS w produkcie IBM MQ MQI clientszawiera sekcja “Konfigurowanie zabezpieczeń systemu IBM MQ MQI client” na stronie 286 .

Zadania pokrewne

IBM MQ MQI client plik konfiguracyjny, `mqclient.ini`

Określanie, że kanał MQI używa protokołu SSL/TLS

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

Istnieje możliwość zdefiniowania kanału połączenia klienckiego z wartością tego atrybutu w następujący sposób. Są one wymienione w kolejności malejącej kolejności wykonywania.

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

   Wyjście PreConnect może udostępniać nazwę CipherSpec w polu *SSLCipherSpec* struktury definicji kanału (MQCD). Ta struktura jest zwracana w polu **ppMQCDArrayPtr** struktury parametru wyjścia MQNXP używanej przez wyjście PreConnect .
2. Gdy aplikacja IBM MQ MQI client wysyła wywołanie MQCONNX.

   Aplikacja może określić nazwę CipherSpec w polu *SSLCipherSpec* struktury definicji kanału (MQCD).Ta struktura jest przywoływana przez strukturę opcji połączenia MQCNO, która jest parametrem wywołania MQCONNX.
3. Korzystanie z tabeli definicji kanału klienta (CCDT).

   Co najmniej jedna pozycja w tabeli definicji kanału klienta może określać nazwę CipherSpec.Jeśli na przykład pozycja jest tworzona za pomocą komendy MQSC DEFINE CHANNEL, można użyć parametru SSLCIPH w komendzie, aby określić nazwę CipherSpec.
4. Korzystanie z usługi Active Directory w systemie Windows.

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

Jeśli na przykład aplikacja kliencka udostępnia definicję kanału połączenia klienckiego w strukturze MQCD w wywołaniu MQCONNX, ta definicja jest używana zamiast wszystkich pozycji w tabeli definicji kanału klienta, do których klient IBM MQ może uzyskać dostęp.

Zmiennej środowiskowej MQSERVER nie można użyć do udostępnienia definicji kanału na końcu klienta kanału MQI używającego protokołu TLS.

Aby sprawdzić, czy certyfikat klienta przepłynął, należy wyświetlić status kanału na końcu serwera dla obecności wartości parametru nazwy węzła sieci.

Pojęcia pokrewne

“Określanie CipherSpec dla IBM MQ MQI client” na stronie 491
Istnieją trzy opcje określania parametru CipherSpec dla IBM MQ MQI client.

CipherSpecs i CipherSuites w produkcie IBM MQ

Produkt IBM MQ obsługuje algorytmy TLS1.3 i TLS 1.2 CipherSpecsoraz algorytmy RSA i Diffie-Hellman. W razie potrzeby można jednak włączyć nieaktualne CipherSpecs.

Więcej informacji na ten temat zawiera sekcja “Włączanie CipherSpecs” na stronie 466 :

- CipherSpecs obsługiwane przez produkt IBM MQ.

- W jaki sposób włączyć nieaktualne specyfikacje szyfrowania SSL 3.0 i TLS 1.0 CipherSpecs.

IBM MQ obsługuje algorytmy wymiany kluczy i uwierzytelniania RSA oraz Diffie-Hellman. Wielkość klucza używanego podczas uzgadniania TLS może zależeć od używanego certyfikatu cyfrowego, ale niektóre 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 22
Szyfrujące protokoły bezpieczeństwa muszą być zgodne z algorytmami używanymi przez bezpieczne połączenie. CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

Szyfrowanie NSA Suite B w produkcie IBM MQ

Ta sekcja zawiera informacje na temat konfigurowania produktu IBM MQ for AIX, Linux, and Windows w celu zapewnienia zgodności z profilem 1.2 zgodnym z protokołem TLS standardu Suite B.

Z biegiem czasu standard NSA Cryptography Suite B Standard jest aktualizowany w celu odzwierciedlenia nowych ataków na algorytmy i protokoły szyfrowania. Na przykład niektóre CipherSpecs mogą przestać mieć certyfikat Suite B. W przypadku wystąpienia takich zmian 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 Suite B wymuszonych przez każdy poziom konserwacyjny produktu. Jeśli produkt IBM MQ zostanie skonfigurowany w celu wymuszenia zgodności z pakietem Suite B, podczas planowania konserwacji należy zawsze zapoznać się z plikiem readme. Więcej informacji na ten temat zawiera sekcja IBM MQ, WebSphere MQi MQSeries -pliki readme.

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

Tabela 3. Poziomy zabezpieczeń standardu Suite B z dozwolonymi CipherSpecs i algorytmami podpisu cyfrowego

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 128-bitowego, jak i 192-bitowego poziomu bezpieczeństwa. Ponieważ konfiguracja Suite B określa minimalne akceptowalne algorytmy szyfrowania, skonfigurowanie obu poziomów zabezpieczeń jest równoważne skonfigurowaniu tylko 128-bitowego poziomu zabezpieczeń. Algorytmy szyfrowania na poziomie zabezpieczeń 192-bitowych są silniejsze niż minimum wymagane dla poziomu zabezpieczeń 128-bitowych, więc są one dozwolone dla poziomu zabezpieczeń 128-bitowych, nawet jeśli poziom zabezpieczeń 192-bitowych nie jest włączony.

Uwaga: Konwencje nazewnictwa używane dla poziomu zabezpieczeń nie muszą odzwierciedlać wielkości krzywej eliptycznej lub wielkości klucza algorytmu szyfrowania AES.

CipherSpec dla standardu Suite B

Mimo że domyślne zachowanie produktu IBM MQ nie jest zgodne ze standardem Suite B, produkt IBM MQ można skonfigurować w taki sposób, aby był zgodny z jednym lub z obydwoma poziomami zabezpieczeń

w systemach AIX, Linux, and Windows . Po pomyślnym skonfigurowaniu produktu IBM MQ do używania standardu Suite B każda próba uruchomienia kanału wychodzącego przy użyciu CipherSpec , która nie jest zgodna z standardem Suite B, spowoduje wystąpienie błędu AMQ9282. To działanie powoduje również, że klient MQI zwraca kod przyczyny MQRC_CIPHER_SPEC_NOT_SUITE_B. Podobnie próba uruchomienia kanału przychodzącego za pomocą atrybutu CipherSpec , który nie jest zgodny z konfiguracją pakietu B, powoduje wystąpienie błędu AMQ9616.

Więcej informacji na temat specyfikacji szyfrowania produktu IBM MQ CipherSpecszawiera sekcja “Włączanie CipherSpecs” na stronie 466 .

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 mogą zawierać certyfikaty. Dlatego produkt IBM MQ musi być skonfigurowany do używania certyfikatów, których algorytm podpisu cyfrowego i typ klucza publicznego są dozwolone przez skonfigurowany poziom zabezpieczeń Suite B partnera zdalnego. Certyfikaty cyfrowe, które nie spełniają wymagań poziomu bezpieczeństwa, są odrzucane, a połączenie kończy się niepowodzeniem z błędem AMQ9633 lub AMQ9285.

W przypadku 128-bitowego poziomu zabezpieczeń Suite B klucz publiczny podmiotu certyfikatu musi używać krzywej eliptycznej NIST P-256 lub krzywej eliptycznej NIST P-384 i musi być podpisany albo krzywą eliptyczną NIST P-256 , albo krzywą eliptyczną NIST P-384 . 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 .

Aby uzyskać certyfikat odpowiedni dla operacji zgodnej z pakietem Suite B, należy użyć komendy **runmqakm** i podać parametr **-sig_alg** w celu zażądania odpowiedniego algorytmu podpisu cyfrowego. Wartości parametrów EC_ecdsa_with_SHA256 i EC_ecdsa_with_SHA384 **-sig_alg** odpowiadają kluczom krzywej eliptycznej podpisanym przez dozwolone algorytmy podpisu cyfrowego Suite B.

Więcej informacji na temat komendy **runmqakm** zawiera sekcja Opcje runmqckm i runmqakm.

Uwaga: Komendy **runmqckm** i **strmqikm** nie obsługują tworzenia certyfikatów cyfrowych dla operacji zgodnych z pakietem Suite B.

Tworzenie i żądanie certyfikatów cyfrowych

Aby utworzyć samopodpisany certyfikat cyfrowy na potrzeby testowania pakietu Suite B, należy zapoznać się z sekcją “Tworzenie samopodpisanego certyfikatu osobistego w systemie AIX, Linux, and Windows” na stronie 327

Aby zażądać certyfikatu cyfrowego podpisanego przez ośrodek CA dla środowiska produkcyjnego pakietu Suite B, należy zapoznać się z sekcją “Żądanie certyfikatu osobistego w systemie AIX, Linux, and Windows” na stronie 330.

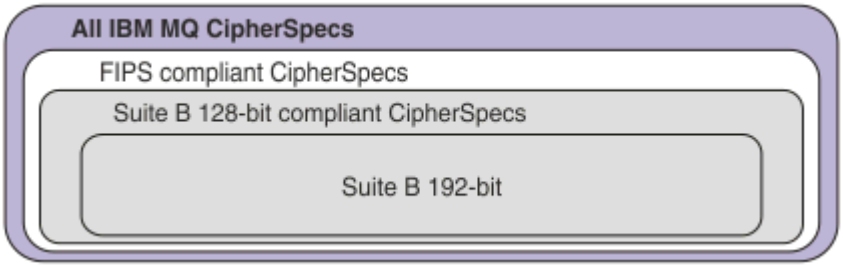
Uwaga: Używany ośrodek certyfikacji musi generować certyfikaty cyfrowe, które spełniają wymagania opisane w dokumencie IETF RFC 6460.

FIPS 140-2 i Suite B

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Standard Suite B jest koncepcyjnie podobny do standardu FIPS 140-2, ponieważ ogranicza zestaw włączonych algorytmów szyfrowania w celu zapewnienia gwarantowanego poziomu bezpieczeństwa. Obecnie obsługiwane CipherSpecs standardu Suite B mogą być używane, gdy parametr IBM MQ jest skonfigurowany dla operacji zgodnych ze standardem FIPS 140-2. Dlatego możliwe jest jednoczesne skonfigurowanie produktu IBM MQ pod kątem zgodności ze standardami FIPS i Suite B. W takim przypadku mają zastosowanie oba zestawy ograniczeń.

Na poniższym diagramie przedstawiono relację między tymi podzbiorami:



Konfigurowanie produktu IBM MQ na potrzeby operacji zgodnych z pakietem B

Informacje na temat konfigurowania produktu IBM MQ w systemie AIX, Linux, and Windows na potrzeby operacji zgodnych z pakietem Suite B zawiera sekcja “Konfigurowanie produktu IBM MQ dla pakietu B” na stronie 45.

System IBM MQ nie obsługuje operacji zgodnych z pakietem B na platformach IBM i i z/OS . Klienty IBM MQ Java i JMS nie obsługują również operacji zgodnych z pakietem Suite B.

Pojęcia pokrewne

“Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.” na stronie 287

Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

ALW *Konfigurowanie produktu IBM MQ dla pakietu B*

Produkt IBM MQ można skonfigurować do działania zgodnie ze standardem NSA Suite B na platformach AIX, Linux, and Windows .

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 “Kryptografia Suite B National Security Agency (NSA)” na stronie 24. Więcej informacji na temat konfiguracji Suite B i jej wpływu na kanały TLS zawiera sekcja “Szyfrowanie NSA Suite B w produkcie IBM MQ” na stronie 43.

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. Ustawiając pole EncryptionPolicySuiteB w strukturze MQSCO wywołania MQCONNX na jedną lub więcej z następujących wartości:
   - `MQ_SUITE_B_NONE`
   - `MQ_SUITE_B_128_BIT`
   - `MQ_SUITE_B_192_BIT`

Użycie MQ_SUITE_B_NONE z dowolną inną wartością jest niepoprawne.

Więcej informacji na temat struktury MQSCO zawiera sekcja MQSCO-opcje konfiguracyjne SSL.

2. Przez ustawienie zmiennej środowiskowej **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 na jedną lub więcej 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.

.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 programie IBM MQ

Strategia sprawdzania poprawności certyfikatu określa, w jakim stopniu sprawdzanie poprawności łańcucha certyfikatów jest zgodne z branżowymi standardami bezpieczeństwa.

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

- W przypadku aplikacji Java i JMS na wszystkich platformach strategia sprawdzania poprawności certyfikatu zależy od komponentu JSSE środowiska wykonawczego Java . Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera dokumentacja środowiska JRE.
- ALW W systemach AIX, Linux, and Windows strategia sprawdzania poprawności certyfikatu jest dostarczana przez IBM Global Security Kit (GSKit) i można ją skonfigurować. Obsługiwane są dwie różne strategie sprawdzania poprawności certyfikatów:
  - Wcześniejsza strategia sprawdzania poprawności certyfikatów, używana w celu zapewnienia maksymalnej kompatybilności wstecznej i współdziałania ze starymi certyfikatami cyfrowymi, które nie są zgodne z aktualnymi standardami sprawdzania poprawności certyfikatów IETF. Ta strategia jest nazywana strategią podstawową.
  - Ścisła strategia sprawdzania poprawności certyfikatu zgodna ze standardami, która wymusza stosowanie standardu RFC 5280. Ta strategia jest nazywana strategią standardową.

- IBM i W systemach IBM i strategia sprawdzania poprawności certyfikatów zależy od biblioteki bezpiecznych gniazd udostępnianej przez system operacyjny. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera dokumentacja systemu operacyjnego.
- z/OS W systemach z/OS strategia sprawdzania poprawności certyfikatów zależy od komponentu System SSL udostępnianego przez system operacyjny. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera dokumentacja systemu operacyjnego.

Informacje na temat konfigurowania strategii sprawdzania poprawności certyfikatów zawiera sekcja “Konfigurowanie strategii sprawdzania poprawności certyfikatów w programie IBM MQ” na stronie 47. Więcej informacji na temat różnic między podstawowymi i standardowymi strategiami sprawdzania poprawności certyfikatów zawiera sekcja Sprawdzanie poprawności certyfikatu i projektowanie zaufanych strategii w systemie AIX, Linux, and Windows.

Konfigurowanie strategii sprawdzania poprawności certyfikatów w programie IBM MQ

Istnieje kilka różnych sposobów określania, która strategia sprawdzania poprawności certyfikatów TLS jest używana do sprawdzania poprawności certyfikatów cyfrowych odebranych ze zdalnych systemów partnerskich.

O tym zadaniu

Strategia sprawdzania poprawności certyfikatu określa, w jakim stopniu sprawdzanie poprawności łańcucha certyfikatów jest zgodne z branżowymi standardami bezpieczeństwa. Strategia sprawdzania poprawności certyfikatów zależy od platformy i środowiska. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja “Strategie sprawdzania poprawności certyfikatów w programie IBM MQ” na stronie 46.

Procedura

- Aby ustawić strategię sprawdzania poprawności certyfikatu w menedżerze kolejek, należy użyć atrybutu menedżera kolejek **CERTVPOL**.

  Więcej informacji na temat ustawiania tego atrybutu zawiera sekcja ALTER QMGR (zmiana ustawień menedżera kolejek).
- Aby ustawić strategię sprawdzania poprawności certyfikatu na kliencie, należy użyć następujących metod.

  Jeśli do ustawienia strategii używana jest więcej niż jedna metoda, klient używa ustawień w następującej kolejności priorytetów:

  1. Użyj pola `CertificateValPolicy` w strukturze MQSCO klienta. Ustaw w polu jedną z następujących wartości:

     MQ_CERT_VAL_POLICY_ANY
     Zastosuj wszystkie strategie sprawdzania poprawności certyfikatów obsługiwane przez bibliotekę bezpiecznych gniazd. Zaakceptuj łańcuch certyfikatów, jeśli dowolna strategia uzna, że łańcuch certyfikatów jest poprawny.

     MQ_CERT_VAL_POLICY_RFC5280
     Zastosuj tylko strategię sprawdzania poprawności certyfikatu zgodną ze standardem RFC5280 . To ustawienie zapewnia bardziej rygorystyczne sprawdzanie poprawności niż ustawienie ANY, ale odrzuca niektóre starsze certyfikaty cyfrowe.

     Więcej informacji na temat używania tego pola zawiera sekcja MQSCO-opcje konfiguracyjne SSL.
  2. Użyj zmiennej środowiskowej klienta **MQCERTVPOL**. Aby ustawić tę zmienną środowiskową, użyj jednej z następujących komend:

     – Linux AIX W systemach AIX and Linux :

     ```
     export MQCERTVPOL= value
     ```

– Windows W systemach Windows :

```
SET MQCERTVPOL= value
```

– IBM i W systemach IBM i :

```
ADDENVVAR ENVVAR(MQCERTVPOL) VALUE(value)
```

3. Użyj atrybutu **CertificateValPolicy** w sekcji SSL pliku konfiguracyjnego klienta. Ustaw ten atrybut na jedną z następujących wartości:

   ANY
   Użyj dowolnej strategii sprawdzania poprawności certyfikatów obsługiwanej przez bazową bibliotekę bezpiecznych gniazd. Jest to ustawienie domyślne.

   RFC5280
   Należy używać tylko sprawdzania poprawności certyfikatu zgodnego ze standardem RFC 5280.

   Więcej informacji na temat używania tego atrybutu zawiera sekcja SSL pliku konfiguracyjnego klienta.

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

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

Tabela 4. Relacje między CipherSpecs i certyfikatami cyfrowymi (kontynuacja)					
Typ	**Przedrostek nazwy CipherSpec**	**Opis**	**Wymagany typ klucza publicznego**	**Algorytm szyfrowania podpisu cyfrowego**	**Metoda ustanawiania klucza tajnego**
2	EDHE_RSA_	CipherSpecs , które używają kluczy publicznych RSA, kluczy tajnych krzywej eliptycznej i algorytmów podpisu cyfrowego RSA.	RSA	RSA	ECDHE
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.

Należy upewnić się, że certyfikat wymieniony w etykiecie certyfikatu jest odpowiedni dla kanału CipherSpec. Oznacza to, że w przypadku skonfigurowania kanału z CipherSpec , który wymaga certyfikatu EC (Elliptic Curve), nie można nadać certyfikatowi RSA nazwy w etykiecie certyfikatu. W przypadku konfigurowania kanału z CipherSpec , który wymaga certyfikatu RSA, nie można nadać certyfikatowi EC nazwy w etykiecie certyfikatu.

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 .

Uruchomienie komendy **runmqakm** spowoduje wyświetlenie 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

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 w produkcie IBM MQ” na stronie 43. 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 CipherSpecs” na stronie 466
Włącz parametr CipherSpec , używając parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** lub **ALTER CHANNEL** MQSC.

“Określenie, że w czasie wykonywania na kliencie MQI będą używane tylko CipherSpecs z certyfikatem FIPS.” na stronie 287

Utwórz repozytoria kluczy przy użyciu oprogramowania zgodnego ze standardem FIPS, a następnie określ, że kanał musi używać CipherSpecsz certyfikatem FIPS.

"Szyfrowanie NSA Suite B w produkcie IBM MQ" na stronie 43
Ta sekcja zawiera informacje na temat konfigurowania produktu IBM MQ for AIX, Linux, and Windows w celu zapewnienia zgodności z profilem 1.2 zgodnym z protokołem TLS standardu Suite B.

"Kryptografia Suite B National Security Agency (NSA)" na stronie 24
Rząd Stanów Zjednoczonych Ameryki udziela porad technicznych w zakresie systemów informatycznych i bezpieczeństwa, w tym szyfrowania danych. US National Security Agency (NSA) zaleca zestaw interoperacyjnych algorytmów kryptograficznych w 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 dopiero zaczynasz pracę z przykładowymi aplikacjami działającymi jako klienty, zapoznaj się z sekcją Przygotowywanie i uruchamianie programów przykładowych , która zawiera 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
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 429.

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 identyfikatorów użytkowników” na stronie 430.

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 434.

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 433.

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 434.

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 “Odwzorowanie adresu IP na identyfikator użytkownika MCAUSER” na stronie 435.

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 “Odwzorowanie zdalnego menedżera kolejek na ID użytkownika MCAUSER” na stronie 431.

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 “Odwzorowanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER” na stronie 432.

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 “Odwzorowanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER” na stronie 432.

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 “Odwzorowanie zdalnego menedżera kolejek na ID użytkownika MCAUSER” na stronie 431.

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	Deprecated E=	Adres e-mail (nieaktualny, zastąpiony podłańcuchem MAIL)
4	UID=, USERID=	Identyfikator użytkownika
5	CN=	Nazwa zwykła
6	T=	Tytuł
7	OU=	Jednostka organizacyjna
8	DC=	Komponent domeny
9	O=	Organizacja
10	STREET=	Ulica / Pierwszy wiersz adresu
11	L=	Miejscowość
12	ST=, SP=, S=	Nazwa województwa lub rejonu
13	P=	Kod pocztowy
14	C=	Kraj

Tabela 7. Pierwszeństwo podłańcuchów (kontynuacja)		
Kolejność	**Podłańcuch nazwy wyróżniającej**	**Nazwa**
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 zdalnego przesyłania komunikatów” na stronie 106

W tej sekcji opisano aspekty zabezpieczeń związane ze zdalnym przesyłaniem komunikatów.

Interakcja CHLAUTH i CONNAUTH

W jaki sposób rekordy uwierzytelniania kanału (CHLAUTH) i uwierzytelnianie połączenia (CONNAUTH) współdziałają w produkcie IBM MQ, w przypadku pojedynczej konwersacji w kanale.

Różne typy powiązań

Produkt IBM MQ obsługuje dwie metody nawiązywania połączenia przez aplikację:

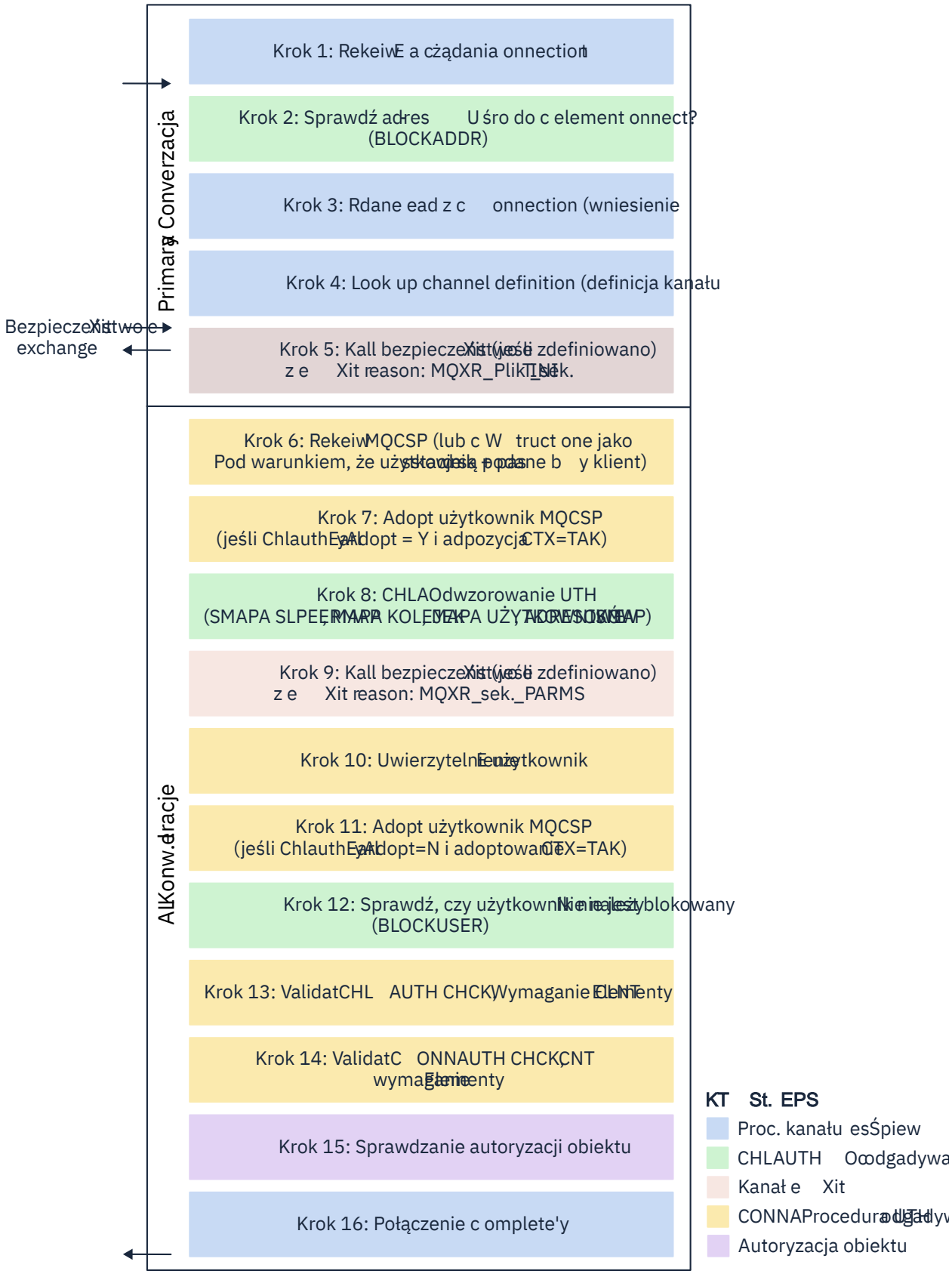
Powiązania lokalne
Ma zastosowanie, gdy aplikacja i menedżer kolejek znajdują się na tym samym obrazie operacyjnym. CHLAUTH nie jest odpowiednia dla tego typu połączenia aplikacji.

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

Wiązanie kroków odbierającego końca kanału

Gdy aplikacja nawiązuje połączenie z menedżerem kolejek, wykonywana jest znaczna liczba operacji sprawdzania, aby upewnić się, że oba końce kanału rozumieją, co jest obsługiwane przez drugi koniec. Odbierający koniec kanału wykonuje dodatkowe sprawdzenie, z udziałem CHLAUTH i CONNAUTH, aby upewnić się, że klient może nawiązać połączenie, a proces ten może również zawierać wyjście zabezpieczeń, ponieważ może to mieć wpływ na wynik. Ta faza łączenia kanału jest również nazywana *fazą powiązania*.

Na poniższym diagramie przedstawiono kroki wykonywane przez kanał SVRCONN po uruchomieniu serwera (w menedżerze kolejek):



Krok 1: Odbierz żądanie połączenia
Inicjator kanału lub program nasłuchujący odbiera żądanie połączenia z innego miejsca w sieci.

Krok 2: Czy adres może się łączyć?
Przed odczytaniem danych program IBM MQ sprawdza adres IP partnera w oparciu o reguły CHLAUTH, aby sprawdzić, czy adres znajduje się w regule *BLOCKADDR* . Jeśli adres nie zostanie znaleziony i nie zostanie zablokowany, przepływ przechodzi do następnego kroku.

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

Krok 4: Wyszukiwanie definicji kanału
W pierwszym przepływie danych produkt 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: Wywołanie wyjścia zabezpieczeń (jeśli zdefiniowano)
Jeśli dla kanału zdefiniowano wyjście zabezpieczeń (SCYEXIT), jest ono wywoływane z przyczyną wyjścia (MQCXP.**ExitReason**) ustawiony na wartość MQXR_INIT_SEC.

Krok 6: Odbierz MQCSP
Jeśli jest to konieczne, utwórz taką, jeśli klient dostarczył referencje uwierzytelniające.

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

Krok 7: Adoptuj użytkownika MQCSP (jeśli parametr `ChlauthEarlyAdopt` ma wartość *Y* , a parametr ADOPTCTX=YES)
Referencje dostarczone przez klienta są uwierzytelniane.

Jeśli CONNAUTH używa protokołu LDAP do odwzorowania sprawdzonej nazwy wyróżniającej na krótki identyfikator użytkownika, odwzorowanie jest wykonywane w tym kroku.

Jeśli uwierzytelnianie powiedzie się, ID użytkownika jest adoptowany przez kanał i używany w kroku odwzorowania CHLAUTH.

Uwaga: Parametr IBM MQ 9.0.4 **`ChlauthEarlyAdopt=`** *Y* jest automatycznie dodawany do sekcji channels 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 najbardziej zgodna z kanałem przychodzącym. Jeśli reguła ma **USERSRC***(CHANNEL)* lub *(MAP)*, kanał kontynuuje wiązanie.

Jeśli reguły CHLAUTH wartościują się do reguły z parametrem **USERSRC***(NOACCESS)*, aplikacja nie będzie mogła nawiązać połączenia z kanałem, chyba że referencje zostaną później przesłonięte poprawnymi referencjami w kroku 9.

Krok 9: Wywołanie wyjścia zabezpieczeń (jeśli zdefiniowano)
Jeśli dla kanału zdefiniowano wyjście zabezpieczeń (SCYEXIT), jest ono wywoływane z przyczyną wyjścia (MQCXP.**ExitReason**) Wartość ustawiona 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**). V 9.3.4 W produkcie IBM MQ 9.3.4struktura MQCSP zawiera również wskaźnik do znacznika uwierzytelniania (MQCSP.**TokenPtr**).

W wyjściu można zmienić identyfikator i hasło użytkownikaoraz znacznik uwierzytelniania . Poniższy przykład przedstawia sposób, w jaki wyjście zabezpieczeń drukuje wartości ID użytkownika i hasła do dziennika 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 spowodować, że produkt IBM MQ zamknie kanał, zwracając wartość *MQXCC_CLOSE_CHANNEL* w MQCXP.Pole **Exitresponse** . W przeciwnym razie przetwarzanie kanału będzie kontynuowane do fazy uwierzytelniania połączenia.

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

Krok 10: Uwierzytelnianie użytkownika

Faza uwierzytelniania ma miejsce, jeśli w menedżerze kolejek jest włączona opcja CONNAUTH.

Aby to sprawdzić, wydaj 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 jest nazwą obiektu **AUTHINFO** IBM MQ .

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

z/OS W poniższym przykładzie przedstawiono domyślny obiekt AUTHINFO z wartością **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 domyślny obiekt AUTHINFO z wartością **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)
```

Obiekt AUTHINFO TYPE (IDPWOS) ma atrybut o nazwie CHCKCLNT. Jeśli wartość zostanie zmieniona na *REQUIRED* , wszystkie aplikacje klienckie muszą podać poprawne referencje.

Jeśli użytkownik został uwierzytelniony w kroku 7, nie jest wykonywane kolejne sprawdzenie uwierzytelniania, chyba że:

- ID użytkownika, hasło lub znacznik uwierzytelniania w polu SecurityParms struktury MQCXP zostało zmienione przez wyjście zabezpieczeń w kroku 9.
- Aplikacja kliencka nawiązała połączenie z opcjami żądającymi funkcji z możliwością ponownego połączenia.

Krok 11: Adoptuj kontekst użytkownika MQCSP (jeśli `ChlauthEarlyAdopt=`*N* i adopcji TCTX=YES)
Można ustawić atrybut ADOPTCTX , który określa, czy kanał działa w ramach MCAUSER, czy też ID użytkownika podanego przez aplikację.

Jeśli ID użytkownika sprawdzony w polu MQCSP lub **`SecurityParms`** struktury MQXCP został pomyślnie uwierzytelniony i **ADOPTCTX** ma wartość *TAK*, kontekst użytkownika będący wynikiem kroków 7 i 8 jest adoptowany jako kontekst używany dla tej aplikacji, chyba że ID użytkownika, hasło lub znacznik uwierzytelniania w polu **`SecurityParms`** struktury MQCXP został zmieniony przez wyjście zabezpieczeń w kroku 9.

Ten sprawdzony ID użytkownika to ID użytkownika, który jest sprawdzany pod kątem autoryzacji do używania zasobów IBM MQ .

Na przykład nie ustawiono użytkownika MCAUSER w kanale SVRCONN, a klient działa w systemie '`johndoe`' na komputerze z systemem Linux . Aplikacja określa użytkownika '`fred`' w MQCSP, więc kanał jest uruchamiany z '`johndoe`' jako aktywnym użytkownikiem MCAUSER. Po sprawdzeniu CONNAUTH użytkownik '`fred`' jest adoptowany, a kanał jest uruchamiany z '`fred`' jako aktywnym użytkownikiem MCAUSER.

Krok 12: Sprawdź, 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.

Krok 13: Sprawdzanie poprawności wymagań CHLAUTH CHCKCLNT
Jeśli reguła CHLAUTH wybrana w kroku 8 dodatkowo określa wartość CHCKCLNT REQUIRED lub REQDADM, wykonywane jest sprawdzanie poprawności w celu zapewnienia, że w celu spełnienia tego wymagania podano poprawny identyfikator użytkownika CONNAUTH.

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

Uwagi:

1. Jeśli parametr CHCKCLNT (REQUIRED) lub CHCKCLNT (REQDADM) jest ustawiony, 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 został ponownie uwierzytelniony w tym kroku.

Krok 14: Sprawdź poprawność wymagań CONNAUTH CHCKCLNT.
Faza uwierzytelniania ma miejsce, jeśli w menedżerze kolejek jest włączona opcja CONNAUTH.

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

Uwaga: Użytkownik nie został ponownie uwierzytelniony w tym kroku.

Multi **Krok 15: Sprawdzanie autoryzacji obiektu**
Należy sprawdzić, czy aktywny użytkownik MCAUSER ma odpowiednie uprawnienia do nawiązywania połączenia z menedżerem kolejek.

ALW Więcej informacji na ten temat zawiera sekcja Menedżer uprawnień do obiektów.

IBM i Więcej informacji na ten temat zawiera sekcja “Menedżer uprawnień do obiektów w systemie IBM i” na stronie 166.

Krok 16: Połączenie zostało zakończone
Jeśli poprzednie kroki zakończą się pomyślnie, połączenie zostanie zakończone.

Pojęcia pokrewne
KONNAUTH
Menedżer kolejek można skonfigurować do uwierzytelniania referencji dostarczanych przez aplikację podczas nawiązywania połączenia.

Odsyłacze pokrewne
USTAW CHLAURA
ZMIEŃ INFORMACJE O AUTORYZACJI

Rozwiązywanie problemów z dostępem CHLAUTH
Kroki i przykłady rozwiązywania niektórych problemów z dostępem podczas używania rekordów uwierzytelniania kanału (CHLAUTH).

Zanim rozpoczniesz

Uwaga: Kroki w tym zadaniu wymagają uruchomienia komend MQSC. W jaki sposób można to zrobić, różnią się w zależności od platformy. Patrz sekcja Administrowanie produktem IBM MQ za pomocą komend MQSC.

O tym zadaniu

Istnieją trzy domyślne reguły przetwarzania CHLAUTH:

- Brak dostępu do wszystkich kanałów przez dowolnego użytkownika `MQ-admin*`
- Brak dostępu do całego SYSTEM.* kanały przez wszystkich użytkowników
- Zezwól na dostęp do SYSTEM.ADMIN.SVRCONN (użytkownicy inni niż `MQ-admin`)

Pierwsze dwie reguły blokują dostęp do wszystkich kanałów. Trzecia reguła jest bardziej specyficzna i dlatego ma pierwszeństwo przed pozostałymi dwoma, jeśli kanał jest systemem SYSTEM.ADMIN.SVRCONN , co umożliwia dostęp do tego kanału.

Reguły CSHAUTH są używane do określenia, czy kanał można uruchomić i czy umożliwiają one odwzorowanie za pośrednictwem użytkownika MCAUSER na inny identyfikator użytkownika. Jeśli nie można uruchomić kanału, 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

Należy ściśle zablokować dostęp, a następnie dodać więcej reguł CHLAUTH, aby kontrolować, kto może uzyskiwać dostęp do kanałów i je uruchamiać.

Aby tymczasowo rozwiązać problemy z wymienionymi błędami, wykonaj dowolny z poniższych kroków.

Procedura

- **Wyłącz reguły CHLAUTH**

  Jako miara tymczasowa, a także w celu rozwiązania powyższych błędów, można wyłączyć reguły CHLAUTH. Reguły można ponownie włączyć w dowolnym momencie, a jeśli wyłączenie reguł CHLAUTH rozwiąże problem z połączeniem, wiadomo, że to była przyczyna.

  Aby wyłączyć reguły CHLAUTH, uruchom następującą komendę MQSC:

```
ALTER QMGR CHLAUTH (DISABLED)
```

  Należy zauważyć, że można również ustawić parametr CHLAUTH na wartość *WARN*, która umożliwia dostęp i rejestrowanie wyników reguły.

- **Modyfikowanie lub usuwanie reguł CHLAUTH**

  Można również usunąć lub zmodyfikować regułę CHLAUTH lub reguły powodujące problem.

  Aby zmodyfikować regułę CHLAUTH, należy użyć komendy SET CHLAUTH z opcją ACTION (REPLACE). Na przykład, aby zmodyfikować domyślną regułę, która powoduje, że żaden użytkownik `MQ-admin` nie ma dostępu do wszystkich kanałów na poziomie WARN, zamiast być blokowanym, uruchom następującą komendę MQSC:

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

  Aby usunąć regułę CHLAUTH, należy użyć komendy SET CHLAUTH z opcją ACTION (REMOVE). Na przykład, aby usunąć domyślną regułę, która powoduje brak dostępu do wszystkich kanałów przez użytkowników `MQ-admin` , uruchom następującą komendę MQSC:

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

- **Testuj dostęp przy użyciu komendy MATCH (RUNCHECK)**

  Wynik reguł CHLAUTH można przetestować za pomocą opcji MATCH (*RUNCHECK*) reguły CHLAUTH. Opcja **MATCH** (*RUNCHECK*) zwraca rekord zgodny z konkretnym kanałem przychodzącym w czasie wykonywania, jeśli ten kanał nawiązuje połączenie z tym menedżerem kolejek. Należy podać:

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

  W poniższym przykładzie uruchamiana jest komenda MQSC służąca do sprawdzania, która reguła CHLAUTH (z regułami domyślnymi) powoduje, że `MQ-admin` użytkownik `johndoe` uzyskuje dostęp do kanału o nazwie `CHAN1`:

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

AMQ8878: Display channel authentication record details.
```

```
CHLAUTH(*) TYPE(BLOCKUSER)
USERLIST(*MQADMIN)
```

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

W poniższym przykładzie uruchamiana jest komenda MQSC w celu sprawdzenia, jaka reguła CHLAUTH (z regułami domyślnymi) powoduje, że użytkownik `alice` , który nie jest użytkownikiem produktu `MQ-admin` , uzyskuje dostęp do kanału o nazwie `CHAN1`:

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

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

Dla użytkownika `alice`kanał jest uruchamiany, a kanał przekazuje `alice` jako MCAUSER. MCAUSER jest identyfikatorem użytkownika używanym do sprawdzania uprawnień do obiektów IBM MQ .

Odsyłacze pokrewne

USTAW CHLAURA

WYŚWIETL_LICZ_LAUTH

Tworzenie nowych reguł CHLAUTH dla użytkowników

Niektóre typowe scenariusze dla użytkowników i przykładowe reguły CHLAUTH do ich realizacji.

Zanim rozpoczniesz

Uwaga: Kroki w tym zadaniu wymagają uruchomienia komend MQSC. W jaki sposób można to zrobić, różnią się w zależności od platformy. Patrz sekcja Administrowanie produktem IBM MQ za pomocą komend MQSC.

O tym zadaniu

Istnieją trzy domyślne reguły przetwarzania CHLAUTH:

- Brak dostępu do wszystkich kanałów przez dowolnego użytkownika `MQ-admin*`
- Brak dostępu do całego SYSTEM.* kanały przez wszystkich użytkowników
- Zezwól na dostęp do SYSTEM.ADMIN.SVRCONN (użytkownicy inni niż `MQ-admin`)

Pierwsze dwie reguły blokują dostęp do wszystkich kanałów. Trzecia reguła jest bardziej specyficzna i dlatego ma pierwszeństwo przed pozostałymi dwoma, jeśli kanał jest systemem SYSTEM.ADMIN.SVRCONN , co umożliwia dostęp do tego kanału.

Aby utworzyć nowe reguły CHLAUTH dla użytkowników, należy skonfigurować co najmniej jeden z następujących scenariuszy.

Procedura

- **Kontrola praw dostępu dla konkretnych użytkowników `MQ-admin`**
  a) Skonfiguruj kanał połączenia z serwerem, który ma być używany wyłącznie na potrzeby perspektywy administracyjnej, czyli do nawiązywania połączenia z poziomu produktu IBM MQ Explorer.

  Istnieje konkretny kanał dla tego użycia i zdefiniowany adres IP lub adresy, z których mają być akceptowane połączenia, oraz dostęp zablokowany dla identyfikatora `'mqm'` , jeśli połączenie nie pochodzi z jednego z podanych adresów IP.

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

  Uruchom następującą komendę MQSC:

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

c) Na potrzeby testowania należy upewnić się, że użytkownik jest zdefiniowany w grupie `MQ-admin` , a nie w grupie.

W tym scenariuszu `mqadm` znajduje się w grupie `MQ-admin` , a `alice` nie.

d) Potwierdź, że istnieją domyślne reguły CHLAUTH .

e) Dodaj trzy reguły, aby umożliwić konkretna użytkownikowi dostęp do grupy ADMIN.CHAN jako `MQ-admin` z określonych adresów IP:

- Ustaw NOACCESS z dowolnego adresu
- Ustaw parametr BLOCKUSER dla tego kanału na wartość blokową tylko dla użytkownika `nobody`, która przesłania wartość *MQADMIN BLOCKUSER
- Zezwól na dostęp do użytkownika `mqadm` w konkretnej podsieci adresów i odwzoruj na uprawnienie użytkownika `mqadm`

W tym celu uruchom następujące komendy MQSC:

```
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 użytkownika ADMIN.CHAN z podanego zakresu adresów IP.

f) Opcjonalne: W dowolnym momencie można uruchomić komendę MQSC MATCH (RUNCHECK), aby wyświetlić wyniki każdej z następujących komend:

```
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, którzy mają rekord CHLAUTH, mogą uzyskać dostęp przy użyciu grupy ADMIN.CHAN.

- **Kontrola praw dostępu dla konkretnego użytkownika i aplikacji klienckiej IBM MQ**

W tym scenariuszu domyślne reguły CHLAUTH są odpowiednie, przy założeniu, że dla konkretnego użytkownika należy ustawić uprawnienie IBM MQ , aby zapewnić poprawne uprawnienie IBM MQ (przy użyciu komendy setmqaut).

W tym scenariuszu uprawnienia są ustawiane dla użytkownika `mqapp1`, który nie jest użytkownikiem produktu `MQ-admin` .

a) Użyj następującej komendy MQSC, aby utworzyć kanał SVRCONN, APP1.CHAN, do użycia przez konkretną aplikację i konkretnego użytkownika.

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

b) Po umieszczeniu domyślnych reguł CHLAUTH użytkownik `mqapp1` może uruchomić APP1.CHAN .

Identyfikator użytkownika pochodzący z aplikacji klienckiej IBM MQ jest używany do sprawdzania uprawnień do obiektów IBM MQ . W tym przypadku, zakładając, że użytkownik `mqapp1` uruchamia aplikację kliencką IBM MQ , jest ona używana do sprawdzania uprawnień do obiektów IBM MQ . Dlatego, jeśli program `mqapp1` ma dostęp do obiektów IBM MQ wymaganych przez aplikację, wszystko jest w porządku; jeśli nie, wystąpią błędy uprawnień.

Można dodatkowo zwiększyć bezpieczeństwo, tworząc konkretne reguły CHLAUTH dla identyfikatora użytkownika `mqapp1` , ale zgodnie z regułami domyślnymi, żaden członek grupy `MQ-admin` nie może uzyskać dostępu do tego kanału.

Uruchom następujące komendy MQSC:

```
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)
```

- **Kontrola dostępu dla konkretnego użytkownika za pomocą nazwy wyróżniającej certyfikatu (DN) tego użytkownika**

  W tym scenariuszu użytkownik musi mieć certyfikat, który został przełożony do menedżera kolejek. Następnie nazwa wyróżniająca jest dopasowywana do ustawienia SSLPEER reguły CHLAUTH, a SSLPEER może używać znaków wieloznacznych.

  W przypadku dopasowania użytkownik może zostać odwzorowany na innego użytkownika MCAUSER w celu sprawdzenia uprawnień do obiektu IBM MQ . Odwzorowanie użytkownika MCAUSER może zminimalizować liczbę użytkowników, którzy muszą być zarządzani w menedżerze uprawnień do obiektów (object authority manager-OAM) systemu IBM MQ .

  a) Istnieje kanał TLS z używanymi certyfikatami i wymagane są reguły w celu:

  – Blokuj wszystkich użytkowników dla konkretnego kanału
  – Zezwala tylko użytkownikom o określonym parametrze SSLPEER, którzy używają klienta tego użytkownika do uzyskania dostępu do usługi IBM MQ OAM.

  Uruchom następujące komendy MQSC:

```
.
# 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 łączącego się w kanale jest używany dla uprawnień IBM MQ OAM obiektów IBM MQ , dlatego identyfikator użytkownika musi mieć odpowiednie uprawnienia IBM MQ .

  b) Opcjonalne: Odwzoruj na inny identyfikator użytkownika IBM MQ .

  Ponownie uruchom poprzednią komendę MQSC, zastępując `USERSRC(MAP) MCAUSER('mquser1')` komendą `USERSRC(CHANNEL)`.

- **Odwzoruj konkretnego użytkownika na użytkownika `mqm`**

  Jest to dodatek lub modyfikacja opcji Control access for specific MQ-admin users(Kontrola dostępu dla konkretnych użytkowników produktu WebSphere MQ).

Użyj komend MQSC, aby dodać następującą regułę CHLAUTH w celu odwzorowania konkretnych użytkowników na użytkownika mqm lub ID użytkownika MQ-admin , który ma konfigurację uprawnień do obiektów IBM MQ w systemie IBM MQ OAM.

```
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 odwzorowanie użytkownika johndoe na użytkownika mqm dla konkretnego kanału ADMIN.CHAN.

Pojęcia pokrewne

“Tworzenie nowych reguł CHLAUTH dla kanałów” na stronie 70
Aby ułatwić tworzenie własnych reguł CHLAUTH, poniżej przedstawiono kilka typowych scenariuszy dla kanałów, a także przykładowe reguły CHLAUTH służące do ich realizacji.

Zadania pokrewne

“Rozwiązywanie problemów z dostępem CHLAUTH” na stronie 65
Kroki i przykłady rozwiązywania niektórych problemów z dostępem podczas używania rekordów uwierzytelniania kanału (CHLAUTH).

Odsyłacze pokrewne

USTAW CHLAURA
WYŚWIETL_LICZ_LAUTH

Tworzenie nowych reguł CHLAUTH dla kanałów
Aby ułatwić tworzenie własnych reguł CHLAUTH, poniżej przedstawiono kilka typowych scenariuszy dla kanałów, a także przykładowe reguły CHLAUTH służące do ich realizacji.

Ten temat zawiera następujące scenariusze:

- “Zezwól na dostęp do konkretnego kanału tylko z określonego zakresu adresów IP.” na stronie 70
- “W przypadku konkretnego kanału blokuj wszystkich użytkowników, ale zezwalaj konkretnym użytkownikom na nawiązywanie połączeń.” na stronie 70
- “Korzystanie z CHLAUTH dla kanałów odbierających i wysyłających” na stronie 71

Zezwól na dostęp do konkretnego kanału tylko 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 pochodzi z określonego zakresu adresów IP.

Użytkownik łączący się jako MCAUSER jest odwzorowany na mqapp2i dlatego otrzymuje uprawnienie IBM MQ OAM dla tego użytkownika.

W przypadku konkretnego kanału blokuj wszystkich użytkowników, ale zezwalaj konkretnym użytkownikom na nawiązywanie połączeń.

Istnieją trzy domyślne reguły przetwarzania CHLAUTH:

- Brak dostępu do wszystkich kanałów przez dowolnego użytkownika `MQ-admin*`
- Brak dostępu do całego SYSTEM.* kanały przez wszystkich użytkowników
- Zezwól na dostęp do SYSTEM.ADMIN.SVRCONN (użytkownicy inni niż `MQ-admin`)

Pierwsze dwie reguły blokują dostęp do wszystkich kanałów. Trzecia reguła jest bardziej specyficzna i dlatego ma pierwszeństwo przed pozostałymi dwoma, jeśli kanał jest systemem SYSTEM.ADMIN.SVRCONN , co umożliwia dostęp do tego kanału.

W tym scenariuszu dostęp do kanału MY.SVRCONN ma ustawione domyślne reguły CHLAUTH.

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 połączenie z serwerem MY.SVRCONN, a następnie kod zezwala na uruchomienie tylko kanału MY.SVRCONN , gdy połączenie pochodzi z określonego identyfikatora użytkownika `johndoe`.

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

W razie potrzeby można odwzorować inny identyfikator użytkownika IBM MQ , używając:

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

zamiast `USERSRC(CHANNEL)`.

Korzystanie z CHLAUTH dla kanałów odbierających i wysyłających

Za pomocą reguł CHLAUTH można dodać dodatkowe zabezpieczenia do kanałów odbiorczych i nadawczych, aby ograniczyć dostęp do kanału odbiorczego. Należy zauważyć, że w przypadku dodawania lub wprowadzania zmian w regułach CHLAUTH zaktualizowane reguły CHLAUTH mają zastosowanie tylko podczas uruchamiania kanału, dlatego jeśli kanały są już uruchomione, należy je zatrzymać i zrestartować, aby aktualizacje CHLAUTH zostały zastosowane.

Reguły HLAUTH mogą być używane w dowolnym kanale, ale istnieją pewne ograniczenia. Na przykład reguły USERMAP mają zastosowanie tylko do kanałów SVRCONN.

Ten przykład umożliwia nawiązanie połączenia tylko z określonego adresu IP w celu uruchomienia TO.MYSVR1 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 dozwolone jest połączenie tylko z określonego menedżera 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)
```

Zadania pokrewne

“Rozwiązywanie problemów z dostępem CHLAUTH” na stronie 65
Kroki i przykłady rozwiązywania niektórych problemów z dostępem podczas używania rekordów uwierzytelniania kanału (CHLAUTH).

“Tworzenie nowych reguł CHLAUTH dla użytkowników” na stronie 67
Niektóre typowe scenariusze dla użytkowników i przykładowe reguły CHLAUTH do ich realizacji.

Odsyłacze pokrewne

USTAW CHLAURA
WYŚWIETL_LICZ_LAUTH

Tworzenie reguły zatrzymania wstecz CHLAUTH
Podczas myślenia o sterowaniu połączeniami przychodzącymi do menedżera kolejek dostępne są dwie opcje. Można podjąć próbę wyświetlenia listy wszystkich połączeń, które nie są dozwolone, lub rozpocząć od stwierdzenia, że wszystkie połączenia są niedozwolone, a następnie podjąć próbę wyświetlenia listy wszystkich połączeń, które są dozwolone. Ta druga opcja jest opisana w tym miejscu.

O tym zadaniu

Przyczyną użycia drugiej opcji jest to, że jeśli zostanie podjęta próba wyświetlenia listy wszystkich połączeń, które nie są dozwolone, a w związku z tym wszystkie połączenia, które nie są wymienione na liście są dozwolone, wynikiem braku połączenia z listy jest to, że połączenie, które nie powinno być dozwolone, jest w stanie nawiązać połączenie, co może spowodować naruszenie bezpieczeństwa.

I odwrotnie, jeśli zamiast tego zaczniesz od stwierdzenia, że każde połączenie nie jest dozwolone, a następnie wymień te, które są, wynik braku jednego z tej listy nie jest naruszeniem bezpieczeństwa. Jeśli przedsiębiorstwo wymaga dodania dodatkowych połączeń, jest to stosunkowo proste zadanie, ale nie ma możliwości naruszenia zabezpieczeń.

Pierwszą rzeczą, którą należy zrobić, jest utworzenie reguły *back-stop* , która przechwytuje połączenia niezgodne z bardziej szczegółowymi regułami. Ta reguła powoduje, że wszystkie połączenia zdalne nie mogą zostać w ogóle przyłączone do menedżera kolejek.

Jeśli jednak użytkownik jest zaniepokojony tym podejściem, może skonfigurować regułę *back-stop* w trybie ostrzegawczym; patrz krok “2” na stronie 72 .

Procedura

1. Aby utworzyć regułę zatrzymania, która zatrzymuje połączenia zdalne przyłączające się do menedżera kolejek, wydaj następującą komendę:

   ```
   SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
   USERSRC(NOACCESS) DESCR('Back-stop rule')
   ```

   Po zamknięciu drzwi we wszystkich połączeniach zdalnych można rozpocząć wprowadzanie bardziej szczegółowych reguł, aby umożliwić nawiązywanie określonych połączeń. Na przykład:

   ```
   SET CHLAUTH('APPL1.SVRCONN') TYPE(ADDRESSMAP) ADDRESS('9.20.1-3.*') USERSRC(CHANNEL)
   SET CHLAUTH('SYSTEM.ADMIN.*') TYPE(SSLPEERMAP) SSLPEER('O=IBM') USERSRC(CHANNEL)
   SET CHLAUTH('TO.QM2') TYPE(QMGRMAP) QMNAME('QM1') USERSRC(MAP) MCAUSER('QM1USER')
   SET CHLAUTH('*.SVRCONN') TYPE(USERMAP) CLNTUSER('johndoe') MCAUSER('johndoe@yourdomain')
   SET CHLAUTH('*') TYPE(SSLPEERMAP) SSLPEER('CN="John Doe"') ADDRESS('9.*') MCAUSER('johndoe')
   ```

2. Aby utworzyć regułę postprocesora w trybie ostrzegawczym, wprowadź następującą komendę:

   ```
   SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
   USERSRC(NOACCESS) DESCR('Back-stop rule') WARN(YES)
   ```

Teraz możesz kontynuować i wprowadzić wszystkie swoje pozytywne zasady. Jeśli uważasz, że wszystkie potrzebne reguły zostały utworzone, włącz zdarzenia kanału, wydając następującą komendę:

```
ALTER QMGR CHLEV(EXCEPTION)
```

i monitoruj system SYSTEM.ADMIN.CHANNEL.EVENT dla zdarzeń z parametrem **Reason** ustawionym na wartość MQRC_CHANNEL_BLOCKED_WARNING.

Te zdarzenia szczegółowo określają połączenia, które są zgodne z regułą "back-stop", ale ponieważ komenda jest uruchomiona w trybie ostrzegawczym, nie zostały na razie zablokowane.

Przejrzyj każde z tych zdarzeń i określ, czy to połączenie powinno mieć poprawną regułę pozytywną, czy też zostało poprawnie dopasowane do reguły *back-stop* . Można uruchomić ten tryb, przeglądając utworzone zdarzenia do czasu, aż wszystkie kanały przychodzące będą widoczne i będą mieć odpowiednie reguły pozytywne dla nich wszystkich.

W tym momencie można zmienić regułę *back-stop* , aby uruchomić zgodne z nią połączenia blokujące, wprowadzając następującą komendę:

```
SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
USERSRC(NOACCESS) DESCR('Back-stop rule') WARN(NO)
ACTION(REPLACE)
```

Tworzenie nieuprzywilejowanego administratora IBM MQ
Sposób tworzenia nieuprzywilejowanego administratora systemu IBM MQ za pomocą komendy CHLAUTH.

O tym zadaniu

W kontekście tego zadania terminy:

użytkownik uprzywilejowany
Oznacza użytkownika, który ma uprawnienia do wykonania operacji bez jawnie nadanego dostępu do tej operacji. Przykładami tych użytkowników uprzywilejowanych są użytkownicy należący do grupy mqm.

IBM MQAdministrator
Oznacza użytkownika, który musi wydać komendy administracyjne dla IBM MQ, na przykład **DEFINE QLOCAL** lub **START CHANNEL**.

Poniższe kroki umożliwiają utworzenie nieuprzywilejowanego administratora IBM MQ .

Procedura

1. Utwórz ID użytkownika na komputerze menedżera kolejek przy użyciu odpowiednich komend dla platformy lub platform używanych w przedsiębiorstwie.

   W tym przykładzie używana jest nazwa użytkownika `alice` .
2. Nadaj temu nowemu użytkownikowi uprawnienie do wydawania wszystkich komend administracyjnych IBM MQ , wykonując następującą procedurę:
   a) Uruchom program IBM MQ Explorer jako użytkownik uprzywilejowany.
   b) Przejdź do *kreatora opartego na rolach* , wybierając odpowiedni menedżer kolejek, a następnie opcję `Uprawnienia do obiektu` i opcję `Dodaj uprawnienia oparte na rolach`.
   c) Na panelu kreatora, który zostanie wyświetlony, wprowadź identyfikator użytkownika utworzony w pierwszym kroku lub, jeśli chcesz pracować z grupami, wprowadź nazwę grupy dla użytkownika lub zestawu użytkowników, którzy mają zostać przekształceni w nieuprzywilejowanych administratorów IBM MQ .
   d) Skonfiguruj kreator pod kątem pełnego dostępu administracyjnego.
   e) Zaznacz to pole wyboru, jeśli chcesz, aby nieuprzywilejowany administrator IBM MQ mógł przeglądać komunikaty w kolejkach.
   f) Przejrzyj komendy na panelu podglądu w dolnej części kreatora.

Te komendy można wycinać i wklejać w celu zbudowania własnych skryptów.

Jednym z powodów, dla których warto to zrobić za pomocą własnego skryptu, jest ograniczenie dostępu, jaki jest przyznawany temu użytkownikowi. Być może zamiast nadawania dostępu do wszystkich obiektów, preferowane jest nadawanie dostępu tylko do określonej grupy obiektów.

Kliknięcie przycisku **OK** w kreatorze powoduje wykonanie komend w takiej postaci, w jakiej są wyświetlane.

g) Należy skonfigurować niektóre reguły CHLAUTH, aby umożliwić zdalny dostęp dla tego ID użytkownika, jeśli wymaganie dotyczące nieuprzywilejowanego administratora IBM MQ dotyczy również zdalnego dostępu.

Zakładając, że przedsiębiorstwo korzysta ze wskazówek zawartych w sekcji "Tworzenie reguły zatrzymania wstecz CHLAUTH" na stronie 72, wystarczy dodać regułę włączania.

Tworzona reguła zależy raczej od sposobu uwierzytelniania zdalnych administratorów IBM MQ .

Jeśli używane jest słabe uwierzytelnianie TCP/IP, można skonfigurować regułę CHLAUTH, która wygląda następująco:

```
  SET CHLAUTH(admin-channel-name)      TYPE(ADDRESSMAP)
ADDRESS('1.2.3.4')      USERSRC(MAP) MCAUSER('alice')
DESCR('Admin Channel - Weak TCP/IP authentication')
```

9. Jeśli używane jest uwierzytelnianie TLS, można skonfigurować regułę CHLAUTH, która wygląda następująco:

```
SET CHLAUTH(admin-channel-name)      TYPE(SSLPEERMAP)
SSLPEER('CN=Alice') ADDRESS('1.2.3.4')      USERSRC(MAP) MCAUSER('alice')
DESCR('Admin Channel - TLS authentication'
```

Teraz, gdy użytkownik łączy się z produktem `admin-channel-name` (i jest zgodny z regułami CHLAUTH), może wydawać komendy dla identyfikatora użytkownika `alice` w menedżerze kolejek, dlatego uprzywilejowany dostęp zdalny nie jest wymagany.

Uwierzytelnianie połączenia

Uwierzytelnianie połączenia umożliwia aplikacjom podawanie referencji uwierzytelniających podczas nawiązywania połączenia z menedżerem kolejek. Menedżer kolejek sprawdza poprawność referencji. ID użytkownika podany w referencjach może być również adoptowany do użycia podczas sprawdzania autoryzacji dla zasobów, do których aplikacja uzyskuje dostęp.

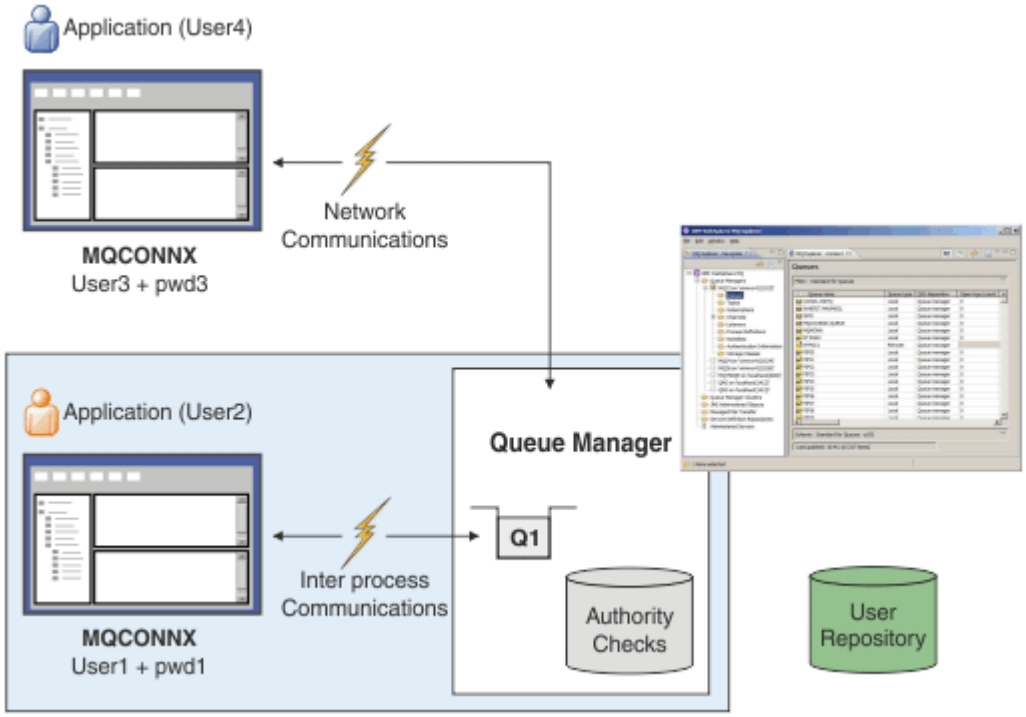
Aplikacje mogą podać identyfikator użytkownika i hasło na potrzeby uwierzytelniania podczas nawiązywania połączenia z menedżerem kolejek.

V 9.3.4 W produkcie IBM MQ 9.3.4aplikacje IBM MQ client mogą również dostarczyć znacznik uwierzytelniania jako alternatywną metodę uwierzytelniania.

Menedżer kolejek można skonfigurować w taki sposób, aby sprawdzany był poprawność referencji dostarczanych przez aplikację.

Identyfikator użytkownika i hasło podane przez aplikację są sprawdzane przy użyciu repozytorium użytkowników w konfiguracji menedżera kolejek. Więcej informacji na temat repozytorium używanego do sprawdzania identyfikatorów użytkowników i haseł zawiera sekcja Repozytoria użytkowników.

V 9.3.4 Poprawność znaczników uwierzytelniania jest sprawdzana przy użyciu certyfikatów i kluczy symetrycznych w magazynie kluczy uwierzytelniania znacznika menedżera kolejek w celu sprawdzenia poprawności podpisu znacznika. Więcej informacji na temat uwierzytelniania użytkowników za pomocą znaczników uwierzytelniania zawiera sekcja "Praca ze znacznikami uwierzytelniania" na stronie 371.



Na diagramie dwie aplikacje nawiązują połączenia z menedżerem kolejek, jedna aplikacja jako klient, a druga przy użyciu powiązań lokalnych. Aplikacje mogą używać różnych funkcji API do nawiązywania połączeń z menedżerem kolejek, ale wszystkie mają możliwość podania identyfikatora użytkownika i hasła. Identyfikator użytkownika, który jest używany przez aplikację, `User2` i `User4` na diagramie, który jest zwykłym identyfikatorem użytkownika systemu operacyjnego przedstawionym w sekcji IBM MQ, może różnić się od identyfikatora użytkownika podanego w aplikacji `User1` i `User3`.

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

Pojęcia pokrewne

“Uwierzytelnianie połączenia: konfiguracja” na stronie 75
Menedżer kolejek można skonfigurować do uwierzytelniania referencji dostarczanych przez aplikację podczas nawiązywania połączenia.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 80

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 81
Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Uwierzytelnianie połączenia: konfiguracja

Menedżer kolejek można skonfigurować do uwierzytelniania referencji dostarczanych przez aplikację podczas nawiązywania połączenia.

Włączanie uwierzytelniania połączenia w menedżerze kolejek

W przypadku obiektu menedżera kolejek atrybut **CONNAUTH** można ustawić na nazwę obiektu informacji uwierzytelniającej (AUTHINFO). Atrybut **AUTHTYPE** obiektu AUTHINFO określa typ obiektu. Obiekty AUTHINFO, które są używane do uwierzytelniania połączenia, mogą być jednego z następujących dwóch typów:

IDPWOS,
Menedżer kolejek używa lokalnego systemu operacyjnego do uwierzytelniania ID użytkownika i hasła, które są dostarczane przez aplikację nawiązującą połączenie.

V 9.3.4 Linux AIX W produkcie IBM MQ 9.3.4ten typ obiektu AUTHINFO umożliwia również menedżerowi kolejek, który działa w systemie AIX lub Linux , sprawdzanie poprawności znaczników uwierzytelniania. Oprócz obiektu AUTHINFO, który jest używany do konfigurowania uwierzytelniania połączenia, menedżer kolejek musi być skonfigurowany do akceptowania znaczników uwierzytelniania w sekcji **AuthInfo** pliku `qm.ini` . Więcej informacji na temat konfigurowania menedżera kolejek do akceptowania znaczników uwierzytelniania zawiera sekcja “Konfigurowanie menedżera kolejek w celu akceptowania znaczników uwierzytelniania” na stronie 376.

IDPWLDAP,
Menedżer kolejek używa serwera LDAP do uwierzytelniania ID użytkownika i hasła, które są dostarczane przez aplikację nawiązującą połączenie.

Uwaga: W atrybucie **CONNAUTH** menedżera kolejek nie można określić żadnego innego typu obiektu informacji uwierzytelniającej.

Obiekty AUTHINFO typu `IDPWOS` i `IDPWLDAP` są podobne w kilku atrybutach. Opisane tutaj atrybuty są wspólne dla obu typów obiektów.

Poniższe przykładowe komendy MQSC włączają uwierzytelnianie połączenia przy użyciu następujących operacji:

1. Zdefiniuj obiekt AUTHINFO o nazwie `USE.PW`.
2. Zmień atrybut **CONNAUTH** menedżera kolejek tak, aby odwoływał się do tego obiektu AUTHINFO.
3. Uruchom komendę **REFRESH SECURITY** , aby odświeżyć konfigurację uwierzytelniania połączenia menedżera kolejek. Aby menedżer kolejek rozpoznał zmiany w konfiguracji uwierzytelniania połączenia, należy wprowadzić komendę **REFRESH SECURITY** .

```
DEFINE AUTHINFO(USE.PW) +
AUTHTYPE(IDPWOS) +
FAILDLAY(10) +
CHCKLOCL(OPTIONAL) +
CHCKCLNT(REQUIRED)

ALTER QMGR CONNAUTH(USE.PW)

REFRESH SECURITY TYPE(CONNAUTH)
```

Aby określić, czy referencje mają być sprawdzane dla połączeń nawiązywanych przez aplikacje powiązane lokalnie, należy użyć atrybutu AUTHINFO **CHCKLOCL** (sprawdzanie połączeń lokalnych). Aby kontrolować, czy informacje autoryzacyjne są sprawdzane dla połączeń nawiązywanych przez aplikacje klienckie, należy użyć atrybutu AUTHINFO **CHCKCLNT** (sprawdzenie połączeń klienckich).

CHCKLOCL akceptuje wartości `NONE` i `OPTIONAL`, a **CHCKCLNT** zezwala na skonfigurowanie wartości `NONE` dla wymagań uwierzytelniania:

Brak
Referencje uwierzytelniające, które są dostarczane przez aplikacje, nie są sprawdzane.

opcjonalne
Zapewnia, że wszystkie informacje autoryzacyjne, które są udostępniane przez aplikację, są poprawne. Jednak podawanie referencji uwierzytelniających przez aplikacje nie jest obowiązkowe. Ta opcja może być przydatna na przykład podczas migracji.

W przypadku:

- Podaj nazwę użytkownika i hasło, zostaną one uwierzytelnione.
- Nie podawaj nazwy użytkownika i hasła, połączenie jest dozwolone.
- Podaj nazwę użytkownika, ale nie hasło, dla którego wystąpił błąd.

Ważne: OPCJONALNE to minimalna wartość, którą można ustawić, aby ustawić bardziej restrykcyjną opcję w regułach uwierzytelniania kanału (CHLAUTH).

Jeśli zostanie wybrana opcja BRAK , a połączenie klienta jest zgodne z rekordem CHLAUTH z wartością **CHCKCLNT** ustawioną na 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.

Więcej informacji na temat używania reguł uwierzytelniania kanału do ustawiania bardziej restrykcyjnych opcji **CHCKCLNT** dla niektórych połączeń klienckich zawiera sekcja "Granulacja konfiguracji" na stronie 77.

WYMAGANE
Wymaga, aby wszystkie aplikacje dostarczyli poprawne informacje autoryzacyjne. Patrz także poniższa uwaga.

metodyka REQDADM
Użytkownicy uprzywilejowani muszą podać poprawne referencje, ale użytkownicy nieuprzywilejowani są traktowani zgodnie z ustawieniem OPTIONAL . Patrz także poniższa uwaga. z/OS To ustawienie nie jest dozwolone w systemach z/OS .

Uwaga:

Ustawienie parametru **CHCKLOCL** na wartość REQUIRED lub REQDADM oznacza, że nie można lokalnie administrować menedżerem kolejek przy użyciu parametru **runmqsc** (błąd AMQ8135: Brak uprawnień), chyba że użytkownik określi parametr **-u** w celu określenia identyfikatora użytkownika w komendzie **runmqsc** . Jeśli ten parametr jest ustawiony, program **runmqsc** pyta o hasło użytkownika na konsoli.

Podobnie dla użytkownika, który uruchamia program IBM MQ Explorer w systemie lokalnym, podczas próby nawiązania połączenia z menedżerem kolejek zostanie wyświetlony błąd AMQ4036 . Aby określić ID użytkownika i hasło, kliknij prawym przyciskiem myszy obiekt lokalnego menedżera kolejek i wybierz opcję **Szczegóły połączenia** > **Właściwości ...** z menu. W sekcji **ID użytkownika** wprowadź ID użytkownika i hasło, które mają być używane, a następnie kliknij przycisk **OK**.

Podobne uwagi dotyczą zdalnych połączeń z systemem **CHCKCLNT**.

Atrybut **CONNAUTH** menedżera kolejek jest pusty dla menedżerów kolejek, które zostały zmigrowane z wersji wcześniejszych niż IBM MQ 8.0, ale są ustawione na wartość *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* dla nowo utworzonych menedżerów kolejek. Ta domyślna definicja **AUTHINFO** ma domyślnie właściwość **CHCKCLNT** ustawioną na wartość REQDADM .

Oznacza to, że wszystkie istniejące klienty, które używają identyfikatora użytkownika uprzywilejowanego do nawiązania połączenia, muszą podać poprawne informacje autoryzacyjne.

Ostrzeżenie: Referencje w strukturze MQCSP dla aplikacji klienckiej są czasami przesyłane przez sieć w postaci zwykłego tekstu. Aby upewnić się, że referencje klienta są chronione, patrz sekcja "Zabezpieczenie hasłem MQCSP" na stronie 32.

Granulacja konfiguracji

Atrybuty **CHCKLOCL** i **CHCKCLNT** obiektu AUTHINFO ustawiają wymagania uwierzytelniania dla wszystkich połączeń z menedżerem kolejek. Oprócz tych atrybutów, reguły atrybutu **CHCKCLNT** w uwierzytelnianiu kanału (CHLAUTH) umożliwiają ustawienie bardziej rygorystycznych wymagań uwierzytelniania dla konkretnych połączeń klienckich zgodnych z regułą CHLAUTH.

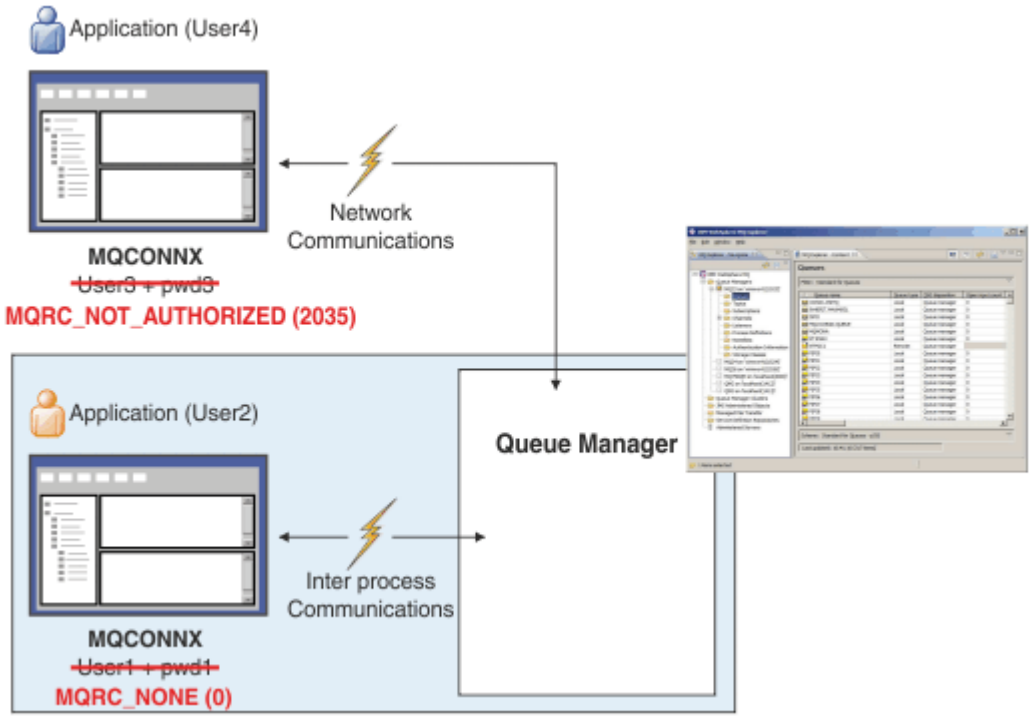
Ogólną wartość parametru **CHCKCLNT** można ustawić na OPTIONAL, na przykład dla obiektu AUTHINFO, a następnie można ją zaktualizować, aby była bardziej rygorystyczna dla niektórych kanałów, ustawiając parametr **CHCKCLNT** na wartość REQUIRED lub REQDADM w regule CHLAUTH. Domyślnie reguły CHLAUTH są definiowane przy użyciu parametru **CHCKCLNT(ASQMGR)**, dlatego ta granulacja nie musi być używana. Na przykład te komendy MQSC definiują jedną regułę CHLAUTH, która nadpisuje atrybut **CHCKCLNT** obiektu AUTHINFO, oraz jedną regułę CHLAUTH, która nie:

```
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)
```

Więcej informacji na temat reguł CHLAUTH zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.

Powiadomienie o błędzie



Błąd jest rejestrowany w następujących sytuacjach:

- Aplikacja nie dostarcza wymaganych referencji uwierzytelniających.
- Aplikacja dostarcza niepoprawne referencje uwierzytelniające. Ta sytuacja jest traktowana jako błąd, nawet jeśli konfiguracja określa, że podanie referencji przez aplikacje jest opcjonalne.

Uwaga: Jeśli parametr **CHCKLOCL** lub **CHCKCLNT** ma wartość NONE, niepoprawne informacje autoryzacyjne, które są dostarczane przez aplikacje, nie są wykrywane.

Nieudane uwierzytelnienia są wstrzymywane przez liczbę sekund określoną przez atrybut **FAILDLAY** , zanim błąd zostanie zwrócony do aplikacji. To opóźnienie zapewnia pewną ochronę przed wielokrotną próbą nawiązania połączenia przez aplikację.

Błąd jest rejestrowany na kilka sposobów:

Aplikacja
Do aplikacji zwracany jest kod przyczyny MQRC_NOT_AUTHORIZED (2035).

Administrator
Administrator IBM MQ widzi zdarzenie zgłoszone w dzienniku błędów. Komunikat o błędzie wskazuje, że połączenie zostało odrzucone, ponieważ referencje są niepoprawne, a nie na przykład dlatego, że użytkownik nie ma uprawnień do połączenia.

Narzędzie monitorowania
Narzędzie monitorowania może również zostać powiadomione o niepowodzeniu, jeśli zostaną włączone zdarzenia uprawnień, za pomocą komunikatu zdarzenia w kolejce

SYSTEM.ADMIN.QMGR.EVENT . Aby włączyć zdarzenia uprawnień, wydaj następującą komendę MQSC:

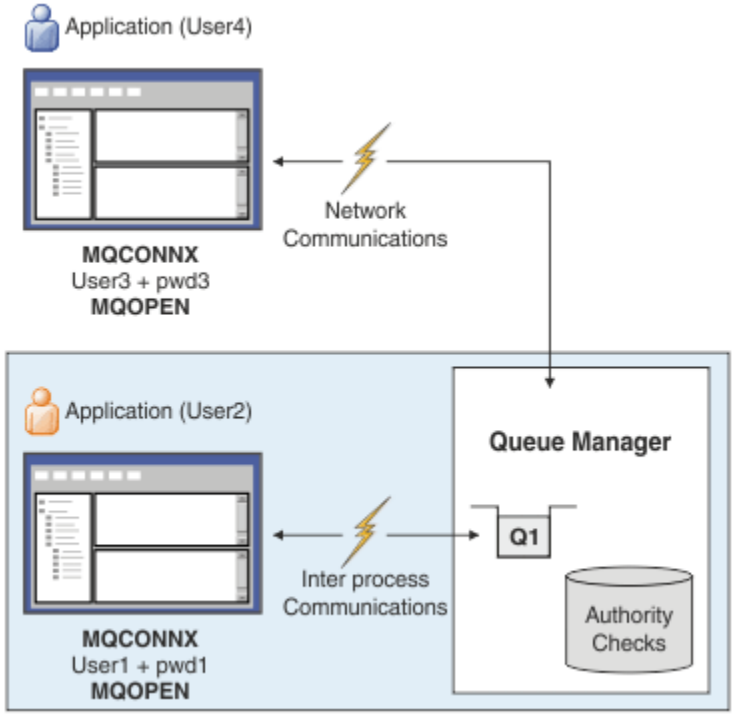
```
ALTER QMGR AUTHOREV(ENABLED)
```

To zdarzenie "Nieautoryzowane" jest zdarzeniem połączenia typu 1 i udostępnia te same pola, co inne zdarzenia typu 1, z dodatkowym polem, podanym identyfikatorem użytkownika MQCSP. Jeśli aplikacja podała hasło, nie jest ono uwzględniane w komunikacie zdarzenia. Oznacza to, że komunikat zdarzenia zawiera dwa identyfikatory użytkowników:

- Identyfikator użytkownika, w ramach którego działa aplikacja.
- Identyfikator użytkownika w referencjach prezentowanych przez aplikację.

Więcej informacji na temat tego komunikatu o zdarzeniu zawiera sekcja Brak uprawnień (typ 1).

Adoptowanie użytkowników do autoryzacji



Menedżer kolejek można skonfigurować w taki sposób, aby adoptować referencje prezentowane przez aplikację jako kontekst połączenia. Adoptowanie referencji oznacza, że ID użytkownika podany w referencjach uwierzytelniania jest używany do sprawdzania autoryzacji, wyświetlany na ekranach administracyjnych i wyświetlany w komunikatach. Atrybut **ADOPTCTX** obiektu AUTHINFO określa, czy referencje są adoptowane jako kontekst dla aplikacji. Na przykład następujące komendy MQSC definiują obiekt AUTHINFO o nazwie USE.PWD , który jest używany do uwierzytelniania połączenia, i ustawiają atrybut **ADOPTCTX** na wartość YES:

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

ALTER QMGR CONNAUTH(USE.PWD)
```

Dla atrybutu **ADOPTCTX** można podać następujące wartości:

Adoptowanie TCTX (TAK)
Referencje dostarczane przez aplikację są adoptowane jako kontekst aplikacji na czas trwania połączenia. Wszystkie operacje sprawdzania autoryzacji dla aplikacji są wykonywane przy użyciu ID użytkownika w uwierzytelnionych referencjach.

Ostrzeżenie: Jeśli używane są identyfikatory użytkowników systemu **ADOPTCTX(YES)** i lokalnego systemu operacyjnego, należy upewnić się, że adoptowany identyfikator użytkownika spełnia wymagania dotyczące identyfikatorów użytkowników podane w sekcji IBM MQ. Więcej informacji na ten tematzawiera sekcja “Identyfikatory użytkownika” na stronie 93.

ADOPTOWANIE TCTX (NIE)
Referencje, które są dostarczane przez aplikację, są używane tylko do uwierzytelniania w czasie połączenia. ID użytkownika, dla którego aplikacja jest uruchomiona, będzie nadal używany na potrzeby 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 (MCAUSER).

Interakcja z uwierzytelnianiem kanału

Reguły uwierzytelniania kanału mogą być używane do zmiany identyfikatora użytkownika, który jest używany jako kontekst dla połączenia aplikacji, na podstawie identyfikatora użytkownika odebranego od klienta. Przykład użycia reguły uwierzytelniania kanału do zmiany identyfikatora użytkownika powiązanego z połączeniem zawiera sekcja “Odwzorowanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER” na stronie 432.

Kolejność przetwarzania reguł uwierzytelniania połączenia i uwierzytelniania kanału jest istotnym czynnikiem przy określaniu kontekstu zabezpieczeń dla połączeń aplikacji klienckiej IBM MQ . Parametr **ChlauthEarlyAdopt** w sekcji **channels** pliku `qm.ini` steruje kolejnością, w jakiej menedżer kolejek adoptuje kontekst na podstawie referencji dostarczonych przez aplikację i stosuje reguły uwierzytelniania kanału. Więcej informacji na temat opcji **ChlauthEarlyAdopt**zawiera sekcja Atrybuty sekcji kanałów.

Ostrzeżenie: Jeśli w obiekcie informacji uwierzytelniającej używany jest parametr **ADOPTCTX(YES)** , kontekst adoptowany z referencji dostarczanych przez aplikację może zostać zmieniony przez reguły uwierzytelniania kanału tylko wtedy, gdy parametr **ChlauthEarlyAdopt** ma wartość Y.

Więcej informacji na temat interakcji uwierzytelniania połączenia i uwierzytelniania kanału oraz kolejności sprawdzania, w jakiej aplikacja kliencka nawiązuje połączenie z menedżerem kolejek, zawiera sekcja “Interakcja CHLAUTH i CONNAUTH” na stronie 60.

Pojęcia pokrewne
“Uwierzytelnianie połączenia” na stronie 74
Uwierzytelnianie połączenia umożliwia aplikacjom podawanie referencji uwierzytelniających podczas nawiązywania połączenia z menedżerem kolejek. Menedżer kolejek sprawdza poprawność referencji. ID użytkownika podany w referencjach może być również adoptowany do użycia podczas sprawdzania autoryzacji dla zasobów, do których aplikacja uzyskuje dostęp.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 80

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 81
Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Uwierzytelnianie połączenia: zmiany aplikacji

Aplikacja używająca interfejsu kolejki komunikatów (MQI) może udostępnić identyfikator użytkownika i hasło w strukturze parametrów zabezpieczeń połączenia (MQCSP) podczas wywołania MQCONNX. W innych aplikacyjnych interfejsach programistycznych struktura MQCSP jest zwykle tworzona w imieniu aplikacji przez biblioteki produktu IBM MQ .

V 9.3.4 Z poziomu produktu IBM MQ 9.3.4aplikacje klienckie nawiązujące połączenie z menedżerem kolejek, który działa w systemie AIX lub Linux , mogą również wysłać znacznik uwierzytelniania w strukturze MQCSP jako alternatywny sposób identyfikacji.

Identyfikator użytkownika i hasłolub znacznik uwierzytelniania są przekazywane w celu sprawdzenia do menedżera uprawnień do obiektów (object authority manager-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 hasłolub znacznik uwierzytelniania, do wyjść zabezpieczeń po stronie klienta i po stronie serwera w celu przetworzenia jest również przekazywany parametr . Można ich również użyć do ustawienia atrybutu identyfikatora użytkownika agenta kanału komunikatów (MCAUSER) instancji kanału.

Ostrzeżenie: Referencje w strukturze MQCSP dla aplikacji klienckiej są czasami przesyłane przez sieć w postaci zwykłego tekstu. Aby upewnić się, że referencje aplikacji klienckiej są chronione, należy zapoznać się z sekcją “Zabezpieczenie hasłem MQCSP” na stronie 32.

Używając łańcucha XAOPEN do podania identyfikatora użytkownika i hasła, można uniknąć konieczności zmiany kodu aplikacji.

Uwaga:

W produkcie IBM WebSphere MQ 6.0wyjście zabezpieczeń umożliwia ustawienie protokołu MQCSP. Oznacza to, że klienty na tym poziomie lub w nowszej wersji nie muszą być aktualizowane.

Jednak w wersjach produktu IBM MQ starszych niż IBM MQ 8.0protokół MQCSP nie nakładały żadnych ograniczeń na identyfikator użytkownika i hasło, które zostały udostępnione przez aplikację. W przypadku używania tych wartości z opcjami udostępnionymi przez IBM MQ istnieją ograniczenia, które mają zastosowanie w przypadku korzystania z tych opcji, ale jeśli użytkownik przekazuje je tylko do własnych wyjść, limity te nie mają zastosowania.

Pojęcia pokrewne

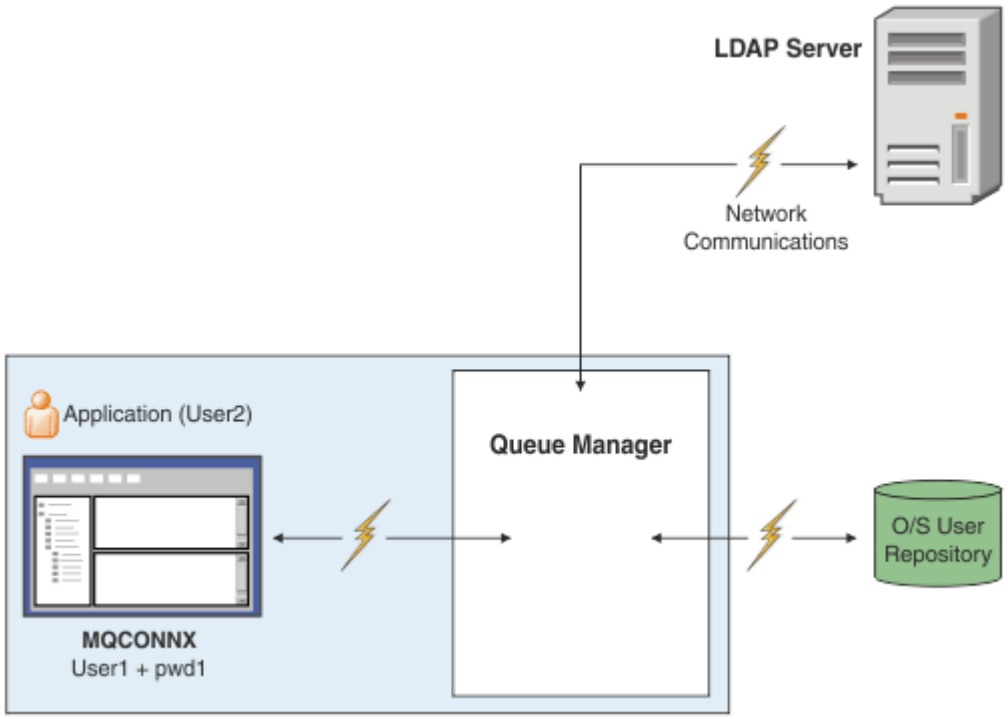
“Uwierzytelnianie połączenia” na stronie 74
Uwierzytelnianie połączenia umożliwia aplikacjom podawanie referencji uwierzytelniających podczas nawiązywania połączenia z menedżerem kolejek. Menedżer kolejek sprawdza poprawność referencji. ID użytkownika podany w referencjach może być również adoptowany do użycia podczas sprawdzania autoryzacji dla zasobów, do których aplikacja uzyskuje dostęp.

“Uwierzytelnianie połączenia: konfiguracja” na stronie 75
Menedżer kolejek można skonfigurować do uwierzytelniania referencji dostarczanych przez aplikację podczas nawiązywania połączenia.

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 81
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 .

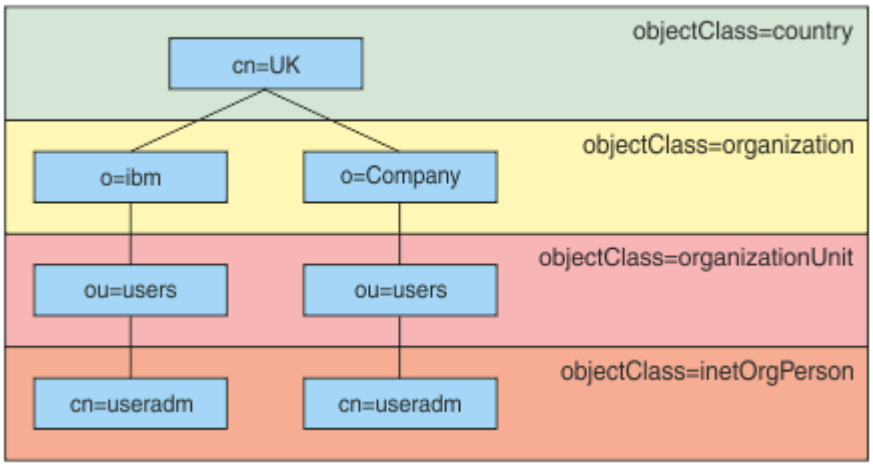
Repozytorium użytkowników LDAP

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 83 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 74
Uwierzytelnianie połączenia umożliwia aplikacjom podawanie referencji uwierzytelniających podczas nawiązywania połączenia z menedżerem kolejek. Menedżer kolejek sprawdza poprawność referencji. ID użytkownika podany w referencjach może być również adoptowany do użycia podczas sprawdzania autoryzacji dla zasobów, do których aplikacja uzyskuje dostęp.

“Uwierzytelnianie połączenia: konfiguracja” na stronie 75
Menedżer kolejek można skonfigurować do uwierzytelniania referencji dostarczanych przez aplikację podczas nawiązywania połączenia.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 80

Wyjście zabezpieczeń po stronie klienta służące do wstawiania identyfikatora użytkownika i hasła (`mqccred`)

Jeśli istnieją aplikacje klienckie, które muszą wysłać identyfikator użytkownika lub hasło, ale nie można jeszcze zmienić źródła, istnieje wyjście zabezpieczeń dostarczane z produktem IBM MQ 8.0 o nazwie **mqccred** , którego można użyć. **mqccred** udostępnia ID użytkownika i hasło w imieniu aplikacji klienckiej z pliku `.ini` . Ten ID użytkownika i hasło są wysyłane do menedżera kolejek, który je uwierzytelnia, jeśli jest w tym celu skonfigurowany.

Przegląd

mqccred jest wyjściem zabezpieczeń, które działa na tym samym komputerze, co aplikacja kliencka. Umożliwia ona podanie identyfikatora użytkownika i hasła w imieniu aplikacji klienckiej, w przypadku gdy informacje te nie są dostarczane przez samą aplikację. Informacje o identyfikatorze użytkownika i haśle są podawane w strukturze zwanej parametrami zabezpieczeń połączenia (MQCSP) i będą uwierzytelniane przez menedżer kolejek, jeśli skonfigurowano uwierzytelnianie połączenia .

Informacje o ID użytkownika i haśle są pobierane z pliku `.ini` na komputerze klienta. Hasła w pliku są chronione przez zaciemnienie za pomocą komendy **runmqccred** , a także przez zapewnienie, że uprawnienia do pliku `.ini` są ustawione w taki sposób, że tylko ID użytkownika uruchamiającego aplikację kliencką (a więc wyjście) może je odczytać.

Położenie

mqccred jest zainstalowany:

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

AIX and Linux platformy
W katalogu *installation_directory*/samp/mqccred

Uwagi: Wyjście:

1. Działa wyłącznie jako wyjście kanału zabezpieczeń i musi być jedynym takim wyjściem zdefiniowanym w kanale.
2. Nazwa jest zwykle nadawana za pośrednictwem tabeli definicji kanału klienta (CCDT), ale klient Java może mieć wyjście wymienione bezpośrednio w obiektach JNDI lub wyjście może być skonfigurowane dla aplikacji, które ręcznie tworzą strukturę MQCD .
3. Należy skopiować programy **mqccred** i **mqccred_r** do katalogu `var/mqm/exits` .

   Na przykład w 64-bitowym systemie AIX lub Linux wprowadź następującą komendę:

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

Więcej informacji na ten temat zawiera sekcja Przykład testowania mqccred krok po kroku .

4. Może działać w poprzednich wersjach produktu IBM MQ, nawet w wersji 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, identyfikator użytkownika oraz jawny tekst lub zaciemnione hasło.

Plik `.ini` należy edytować ręcznie przy użyciu dowolnego edytora i dodać atrybut hasła w postaci jawnego tekstu do sekcji. Uruchom podany program **runmqccred** , który pobiera plik `.ini` i zastępuje atrybut **Password** atrybutem **OPW** (zaciemniona postać hasła).

Opis komendy i jej parametrów zawiera sekcja runmqccred .

Plik `mqccred.ini` zawiera identyfikator i hasło użytkownika.

Plik szablonu `.ini` znajduje się w tym samym katalogu, co wyjście, aby zapewnić punkt początkowy dla przedsiębiorstwa.

Domyślnie ten plik będzie wyszukiwany w katalogu `$HOME/.mqs/mqccred.ini`. Aby znaleźć ją w innym miejscu, można użyć zmiennej środowiskowej *MQCCRED* , aby ją wskazać:

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

Jeśli używana jest komenda *MQCCRED*, zmienna musi zawierać pełną nazwę pliku konfiguracyjnego, w tym dowolny typ pliku `.ini` . Ponieważ ten plik zawiera hasła (nawet jeśli są zaciemnione), należy chronić plik przy użyciu uprawnień systemu operacyjnego, aby zapewnić, że nieautoryzowane osoby nie będą mogły go odczytać. Jeśli nie masz odpowiednich uprawnień do pliku, wyjście nie zostanie pomyślnie wykonane.

Jeśli aplikacja już dostarczyła strukturę MQCSP , wyjście zwykle uwzględnia tę strukturę i nie wstawia żadnych informacji z pliku `.ini` . Można to jednak zmienić, używając atrybutu **Force** w sekcji.

Ustawienie parametru **Force** na wartość *TRUE* powoduje usunięcie ID użytkownika i hasła dostarczonych przez aplikację i zastąpienie ich wersją pliku ini.

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

Wartością domyślną parametru **Force** jest *FALSE*.

Identyfikator użytkownika i hasło można podać dla wszystkich menedżerów kolejek lub dla poszczególnych menedżerów 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. Definicje poszczególnych menedżerów kolejek mają pierwszeństwo przed ustawieniem globalnym.
2. W atrybutach nie jest rozróżniana wielkość liter.

Ograniczenia

Jeśli to wyjście jest używane, identyfikator użytkownika lokalnego osoby, która uruchomiła aplikację, nie przepływa z klienta do serwera. Jedyne dostępne informacje o tożsamości pochodzą z zawartości pliku ini.

Dlatego należy skonfigurować menedżer kolejek w taki sposób, aby używał produktu **ADOPTCTX(YES)**, lub odwzorować żądanie połączenia przychodzącego na odpowiedni identyfikator użytkownika za pomocą jednego z dostępnych mechanizmów, na przykład "Rekordy uwierzytelniania kanału" na stronie 53.

Ważne: Po dodaniu nowych haseł lub zaktualizowaniu starych, komenda **runmqccred** przetwarza tylko hasła w postaci jawnej, pozostawiając niezmienione hasła w postaci ukrytej.

Debugowanie

Jeśli ta opcja jest włączona, wyjście zapisuje dane do standardowego śledzenia IBM MQ .

Aby pomóc w debugowaniu problemów z konfiguracją, wyjście może również zapisywać bezpośrednio do wyjścia standardowego.

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

BŁĄD
Drukuj tylko informacje o błędach, takich jak brak możliwości znalezienia pliku konfiguracyjnego.

DEBUGOWANIE
Wyświetla te warunki błędu i dodatkowe instrukcje śledzenia.

BRAK KONTROLI
Pomija ograniczenia dotyczące uprawnień do pliku oraz dalsze ograniczenie, że plik `.ini` nie powinien zawierać żadnych niechronionych haseł.

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

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

Użycie `mqccred`

Po skonfigurowaniu pliku 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 jest funkcją programu IBM MQ , która umożliwia skonfigurowanie menedżerów kolejek w taki sposób, aby menedżer kolejek mógł uwierzytelniać aplikacje przy użyciu podanego identyfikatora użytkownika i hasła. Jeśli aplikacja jest aplikacją Java korzystającą z transportu klienta, uwierzytelnianie połączenia można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Identyfikator użytkownika i hasło do uwierzytelnienia są określane przez aplikację za pomocą jednej z następujących metod:

- W aplikacji IBM MQ classes for Java , w klasie `MQEnvironment` lub we właściwościach Hashtable, które są przekazywane do konstruktora `com.ibm.mq.MQQueueManager` .
- W aplikacji IBM MQ classes for JMS : jako argumenty metody `createConnection(String username, String Password)` lub `createContext(String username, String password)` .

Tryb uwierzytelniania MQCSP

W tym trybie identyfikator użytkownika po stronie klienta, w ramach którego działa aplikacja, jest wysyłany do menedżera kolejek, a także identyfikator użytkownika i hasło do uwierzytelnienia. Produkt IBM MQ classes for Java i produkt IBM MQ classes for JMS wysyłają identyfikator użytkownika i hasło w celu uwierzytelnienia do menedżera kolejek w strukturze MQCSP .

Identyfikator użytkownika i hasło są dostępne dla wyjścia zabezpieczeń połączenia z serwerem w strukturze MQCSP. Adres struktury MQCSP można znaleźć w polu **SecurityParms** struktury MQCXP dla kanału.

Tryb uwierzytelniania MQCSP ma następujące zalety:

- Maksymalna długość ID użytkownika do uwierzytelnienia wynosi 1024 znaki.
- Maksymalna długość hasła dla uwierzytelniania wynosi 256 znaków.
- Sprawdzanie autoryzacji pod kątem dostępu do zasobów IBM MQ może być wykonywane przy użyciu identyfikatora użytkownika po stronie klienta, pod którym działa aplikacja, gdy obiekt informacji uwierzytelniającej, który jest używany do sterowania uwierzytelnianiem połączenia w menedżerze kolejek, jest skonfigurowany z adoptującą wartością TCTX (NO).

Tryb zgodności

W przypadku wersji wcześniejszych niż IBM MQ 8.0klient Java mógł wysłać identyfikator użytkownika i hasło przez kanał 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.

Można użyć tego trybu w połączeniu z uwierzytelnianiem połączenia i przeprowadzić migrację poza wszystkie wyjścia zabezpieczeń, które były wcześniej używane do wykonania tego samego zadania.

W tym trybie obowiązują następujące ograniczenia:

- Długość identyfikatora użytkownika i hasła nie może przekraczać 12 znaków. Identyfikatory użytkowników dłuższe niż 12 znaków są obcinane do 12 znaków. Może to spowodować niepowodzenie połączenia z kodem przyczyny MQRC_NOT_AUTHORIZED.
- Identyfikator użytkownika po stronie klienta, pod którym działa aplikacja, nie jest wysyłany do menedżera kolejek. Należy albo ustawić parametr ADOPTCTX (YES) dla obiektu informacji uwierzytelniających, który jest używany do sterowania uwierzytelnianiem połączenia w menedżerze kolejek, albo użyć innej metody, takiej jak reguła uwierzytelniania kanału oparta na certyfikacie TLS, aby ustawić identyfikator użytkownika MCA kanału sprawdzany pod kątem autoryzacji w celu korzystania z zasobów IBM MQ .

Domyślny tryb uwierzytelniania

Domyślny tryb uwierzytelniania używany przez aplikację kliencką w systemie IBM MQ classes for Java lub IBM MQ classes for JMS zależy od tego, czy aplikacja określa identyfikator użytkownika i hasło.

- V 9.3.0 W produkcie IBM MQ 9.2.1, jeśli określono identyfikator użytkownika i hasło, domyślnie używane jest uwierzytelnianie MQCSP.
- W wersjach wcześniejszych niż IBM MQ 9.2.1, jeśli podano ID użytkownika i hasło, tryb domyślny jest następujący:
  - Uwierzytelnianie MQCSP jest domyślnie używane przez aplikacje korzystające z produktu IBM MQ classes for Java.

  - Tryb zgodności jest domyślnie używany przez aplikacje korzystające z produktu IBM MQ classes for JMS.
- Jeśli ID użytkownika, ale nie podano hasła, domyślnie używany jest tryb zgodności.
- Jeśli nie określono identyfikatora użytkownika, zawsze używany jest tryb zgodności.

W przypadku określenia identyfikatora użytkownika aplikacja może wybrać konkretny tryb uwierzytelniania dla każdego pojedynczego połączenia lub ustawić globalnie przed uruchomieniem aplikacji, zgodnie z opisem w sekcji "Wybieranie trybu uwierzytelniania" na stronie 88.

Uwaga: V 9.3.0 Zmiana domyślnego trybu uwierzytelniania w produkcie IBM MQ 9.3.0może mieć wpływ na aplikacje korzystające z produktu IBM MQ classes for JMS . Po zaktualizowaniu produktu IBM MQ classes for JMS do wersji IBM MQ 9.3.0aplikacje, które wcześniej domyślnie używały trybu zgodności, będą używały uwierzytelniania MQCSP. Może to spowodować, że aplikacje, które wcześniej pomyślnie nawiązywały połączenie z menedżerem kolejek, nie nawiąże połączenia z bazą danych `JMSException` zawierającą kod przyczyny 2035 (MQRC_NOT_AUTHORIZED). W takim przypadku należy użyć jednej z metod opisanych w sekcji "Wybieranie trybu uwierzytelniania" na stronie 88 , aby określić, że aplikacja używa trybu zgodności.

Aplikacje produktu Java , które łączą się z menedżerem kolejek przy użyciu powiązań lokalnych, zawsze używają trybu uwierzytelniania MQCSP.

Wybieranie trybu uwierzytelniania

Tryb uwierzytelniania używany przez aplikacje klienckie Java , które określają identyfikator użytkownika podczas nawiązywania połączenia z menedżerem kolejek, można określić przy użyciu jednej z następujących metod. Metody te są wymienione w kolejności malejącej. Jeśli tryb uwierzytelniania nie zostanie określony przy użyciu żadnej z tych metod, zostanie użyty domyślny tryb uwierzytelniania.

Uwaga: V 9.3.0 Użycie tych metod do wybrania trybu uwierzytelniania zostało wyjaśnione w sekcji IBM MQ 9.3.0. W niektórych przypadkach tryb uwierzytelniania używany przez aplikację kliencką Java może ulec zmianie, gdy produkt IBM MQ classes for Java lub IBM MQ classes for JMS zostanie zaktualizowany do wersji IBM MQ 9.3.0. Może to spowodować, że aplikacje, które wcześniej pomyślnie nawiązywały połączenie z menedżerem kolejek, nie nawiąże połączenia z bazą danych `JMSException` zawierającą kod przyczyny 2035 (MQRC_NOT_AUTHORIZED). W takim przypadku należy użyć jednej z następujących metod, aby wybrać wymagany tryb uwierzytelniania.

- Określ tryb uwierzytelniania dla każdego pojedynczego połączenia, ustawiając odpowiednią właściwość w aplikacji przed nawiązaniem połączenia z menedżerem kolejek.
  - Jeśli używana jest właściwość IBM MQ classes for Java, należy ustawić właściwość *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* we właściwościach Hashtable, które są przekazywane do konstruktora `com.ibm.mq.MQQueueManager` .
  - Jeśli używany jest parametr IBM MQ classes for JMS, należy ustawić właściwość *JmsConstants.USER_AUTHENTICATION_MQCSP* w odpowiedniej fabryce połączeń przed utworzeniem połączenia.

  Ustaw wartości tych właściwości na jedną z następujących wartości:

  Prawda
  Użyj trybu uwierzytelniania MQCSP podczas uwierzytelniania w menedżerze kolejek.

  Fałsz
  Użyj trybu zgodności podczas uwierzytelniania w menedżerze kolejek.
- Tryb uwierzytelniania dla wszystkich połączeń klienckich nawiązywanych przez aplikację należy określić, ustawiając właściwość systemową *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* Java podczas uruchamiania aplikacji. Ustaw wartość właściwości na jedną z następujących wartości:

  Y
  Użyj trybu uwierzytelniania MQCSP podczas uwierzytelniania w menedżerze kolejek.

N
Użyj trybu zgodności podczas uwierzytelniania w menedżerze kolejek.

Na przykład następująca komenda ustawia właściwość w celu wybrania trybu zgodności i uruchamia aplikację Java :

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

- Należy określić tryb uwierzytelniania dla wszystkich połączeń klienckich nawiązywanych przez aplikacje uruchomione w tym samym środowisku, ustawiając zmienną środowiskową *com.ibm.mq.jmqi.useMQCSPauthentication* w środowisku, w którym aplikacja jest uruchamiana. Ustaw wartość zmiennej środowiskowej na jedną z następujących wartości:

  Y
  Użyj trybu uwierzytelniania MQCSP podczas uwierzytelniania w menedżerze kolejek.

  N
  Użyj trybu zgodności podczas uwierzytelniania w menedżerze kolejek.
- Określ tryb uwierzytelniania dla wszystkich aplikacji, które używają konkretnego pliku konfiguracyjnego klienta IBM MQ MQI client , podając atrybut **useMQCSPauthentication** w sekcji JMQI pliku konfiguracyjnego klienta. Ustaw wartość atrybutu na jedną z następujących wartości:

  YES
  Użyj trybu uwierzytelniania MQCSP podczas uwierzytelniania w menedżerze kolejek.

  NO
  Użyj trybu zgodności podczas uwierzytelniania w menedżerze kolejek.

  Więcej informacji na temat atrybutu **useMQCSPauthentication** zawiera sekcja JMQI w pliku konfiguracyjnym klienta.

Wybieranie trybu uwierzytelniania w produkcie IBM MQ Explorer

Aplikacja IBM MQ Explorer jest aplikacją Java , więc te dwa tryby (tryb zgodności i tryb uwierzytelniania MQCSP) również mają do niej zastosowanie.

W produkcie IBM MQ 9.1.0domyślnym trybem uwierzytelniania jest MQCSP. W systemach wcześniejszych niż IBM MQ 9.1tryb zgodności jest trybem domyślnym.

Na panelach, na których podano identyfikator użytkownika, dostępne jest pole wyboru umożliwiające włączenie lub wyłączenie trybu zgodności:

- W produkcie IBM MQ 9.1.0to pole wyboru nie jest domyślnie zaznaczone. Aby użyć trybu zgodności, zaznacz to pole wyboru.
- W produkcie IBM MQ 9.1.0to pole wyboru jest domyślnie włączone. Aby użyć uwierzytelniania MQCSP, należy usunąć zaznaczenie tego pola wyboru.

Pojęcia pokrewne

“Uwierzytelnianie połączenia” na stronie 74
Uwierzytelnianie połączenia umożliwia aplikacjom podawanie referencji uwierzytelniających podczas nawiązywania połączenia z menedżerem kolejek. Menedżer kolejek sprawdza poprawność referencji. ID użytkownika podany w referencjach może być również adoptowany do użycia podczas sprawdzania autoryzacji dla zasobów, do których aplikacja uzyskuje dostęp.

“Uwierzytelnianie połączenia: zmiany aplikacji” na stronie 80

“Uwierzytelnianie połączenia: repozytoria użytkowników” na stronie 81
Dla każdego menedżera kolejek można wybrać różne typy obiektów informacji uwierzytelniającej na potrzeby uwierzytelniania identyfikatorów użytkowników i haseł.

Zabezpieczenia komunikatów w produkcie IBM MQ

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

Advanced Message Security (AMS) Rozszerza usługi zabezpieczeń systemu IBM MQ , aby zapewnić podpisywanie i szyfrowanie danych na poziomie komunikatu. Rozwinięte usługi gwarantują, że dane komunikatu nie zostały zmodyfikowane między umieszczaniem ich w kolejce a pobraniem. Ponadto produkt AMS sprawdza, czy nadawca danych komunikatu ma uprawnienia do umieszczania podpisanych komunikatów w kolejce docelowej.

Pojęcia pokrewne

"Advanced Message Security" na stronie 652
Advanced Message Security (AMS) jest komponentem produktu IBM MQ , który zapewnia wysoki poziom ochrony danych wrażliwych przepływających przez sieć IBM MQ , nie wpływając jednocześnie na aplikacje końcowe.

Planowanie wymagań dotyczących bezpieczeństwa

W tej kolekcji tematów wyjaśniono, co należy wziąć pod uwagę podczas planowania ochrony w środowisku IBM MQ .

Produkt IBM MQ może być używany dla wielu różnych aplikacji na różnych platformach. Wymagania dotyczące bezpieczeństwa mogą być różne dla każdej aplikacji. Dla niektórych bezpieczeństwo będzie krytycznym czynnikiem.

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

Planując instalację produktu IBM MQ, należy wziąć pod uwagę pewne aspekty bezpieczeństwa:

- Multi W systemie Wiele platform, jeśli te aspekty zostaną zignorowane i nie zostaną użyte żadne działania, nie można użyć komendy IBM MQ.
- z/OS W systemie z/OSignorowanie tych aspektów powoduje, że zasoby IBM MQ nie są chronione. Oznacza to, że wszyscy użytkownicy mogą uzyskiwać dostęp do wszystkich zasobów IBM MQ i zmieniać je.

Uprawnienia do administrowania systemem IBM MQ

Administratorzy IBM MQ muszą mieć uprawnienia do:

- Wydawanie komend do administrowania produktem IBM MQ
- Zamiast nich użyj atrybutówIBM MQ Explorer
- IBM i Użyj paneli i komend administracyjnych IBM i .
- z/OS Korzystanie z operacji i paneli sterowania 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:

- ALW "Uprawnienia do administrowania systemem IBM MQ w systemie AIX, Linux, and Windows" na stronie 446
- IBM i "Uprawnienia do administrowania systemem IBM MQ w systemie IBM i" na stronie 95
- z/OS "Uprawnienia do administrowania systemem IBM MQ w systemie z/OS" na stronie 96

Uprawnienia do pracy z obiektami IBM MQ

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

- Menedżery kolejek

- Kolejki
- Procesy
- Listy nazw
- Tematy

Aplikacje mogą również używać komend Programmable Command Format (PCF) do uzyskiwania dostępu do tych obiektów IBM MQ oraz do kanałów i obiektów informacji uwierzytelniającej. Te obiekty mogą być chronione przez produkt IBM MQ , tak aby identyfikatory użytkowników powiązane z aplikacjami wymagały uprawnień dostępu do tych obiektów.

Więcej informacji na ten temat zawiera sekcja “Autoryzacja aplikacji do korzystania z produktu IBM MQ” na stronie 98.

Zabezpieczenia kanału

Identyfikatory użytkowników powiązane z agentami kanału komunikatów (MCA) wymagają uprawnień dostępu do różnych zasobów systemu IBM MQ . Na przykład agent MCA musi mieć możliwość nawiązania połączenia z menedżerem kolejek. Jeśli jest to wysyłający agent MCA, musi mieć możliwość otwarcia kolejki transmisji dla kanału. Jeśli jest to odbierający agent MCA, musi mieć możliwość otwierania kolejek docelowych. Identyfikatory użytkowników powiązane z aplikacjami, które muszą administrować kanałami, inicjatorami kanałów i nasłuchiwaniem, wymagają uprawnień do używania odpowiednich komend PCF. Jednak większość aplikacji nie potrzebuje takiego dostępu.

Więcej informacji na ten temat zawiera sekcja “Autoryzacja kanału” na stronie 120.

Dodatkowe uwarunkowania

Należy wziąć pod uwagę następujące aspekty bezpieczeństwa tylko wtedy, gdy używane są określone rozszerzenia funkcji lub produktu podstawowego IBM MQ :

- “Zabezpieczenia klastrów menedżera kolejek” na stronie 133
- “Zabezpieczenia mechanizmu publikowania/subskrypcji produktu IBM MQ” na stronie 134
- “zabezpieczenia dlaIBM MQ Internet Pass-Thru” na stronie 135

Planowanie identyfikacji i uwierzytelniania

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

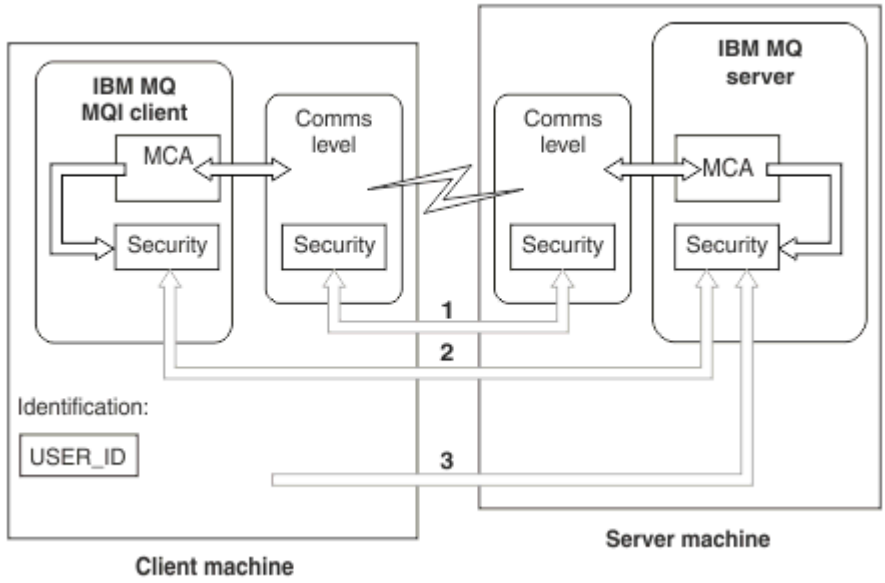
Należy zdecydować, w jaki sposób użytkownicy aplikacji IBM MQ będą identyfikowani, pamiętając, że różne systemy operacyjne obsługują identyfikatory użytkowników o różnych długościach. Rekordów uwierzytelniania kanału można użyć do odwzorowania jednego identyfikatora użytkownika na inny lub do określenia identyfikatora użytkownika na podstawie pewnego atrybutu połączenia. Kanały IBM MQ używające protokołu TLS używają certyfikatów cyfrowych jako mechanizmu identyfikacji i uwierzytelniania. Każdy certyfikat cyfrowy ma nazwę wyróżniającą podmiotu, którą można odwzorować na konkretne tożsamości przy użyciu rekordów uwierzytelniania kanału. Ponadto certyfikaty ośrodka CA w repozytorium kluczy określają, które certyfikaty cyfrowe mogą być używane do uwierzytelniania w programie IBM MQ. Więcej informacji na ten temat zawierają następujące sekcje:

- “Odwzorowanie zdalnego menedżera kolejek na ID użytkownika MCAUSER” na stronie 431
- “Odwzorowanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER” na stronie 432
- “Odwzorowanie nazwy wyróżniającej SSL lub TLS na identyfikator użytkownika MCAUSER” na stronie 432
- “Odwzorowanie adresu IP na identyfikator użytkownika MCAUSER” na stronie 435

Planowanie uwierzytelniania dla aplikacji klienckiej

Elementy sterujące uwierzytelniania można stosować na czterech poziomach: na poziomie komunikacji, w wyjściach zabezpieczeń, z rekordami uwierzytelniania kanału oraz w kontekście identyfikacji przekazywanej do wyjścia zabezpieczeń.

Należy wziąć pod uwagę cztery poziomy bezpieczeństwa. Diagram przedstawia 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 “Szyfrujące protokoły bezpieczeństwa: TLS” na stronie 18.

2. Rekordy uwierzytelniania kanału

   Patrz strzałki 2 i 3. Uwierzytelnianiem można sterować za pomocą adresu IP lub nazw wyróżniających TLS na poziomie zabezpieczeń. Identyfikator użytkownika może być również zablokowany lub może być odwzorowany na poprawny identyfikator użytkownika. Pełny opis znajduje się w sekcji “Rekordy uwierzytelniania kanału” na stronie 53.

3. Uwierzytelnianie połączenia

   Patrz strzałka 3. Klient wysyła identyfikator użytkownika i hasłolub znacznik uwierzytelniania. Więcej informacji na ten temat zawiera sekcja “Uwierzytelnianie połączenia: konfiguracja” na stronie 75.

4. Wyjścia zabezpieczeń kanału

   Patrz strzałka 2. Wyjścia zabezpieczeń kanału dla komunikacji między klientami i serwerami mogą działać w taki sam sposób, jak dla komunikacji między serwerami. W celu zapewnienia wzajemnego uwierzytelniania klienta i serwera można zapisać niezależną od protokołu parę wyjść. Pełny opis znajduje się w sekcji Programy obsługi wyjścia zabezpieczeń kanału.

5. Identyfikator przekazywany do wyjścia zabezpieczeń kanału

   Patrz strzałka 3. W komunikacji między klientem a serwerem wyjścia zabezpieczeń kanału nie muszą działać jako para. Wyjście po stronie klienta IBM MQ można pominąć. W takim przypadku identyfikator użytkownika jest umieszczany w deskryptorze kanału (MQCD), a w razie potrzeby może on zostać zmieniony przez wyjście zabezpieczeń po stronie serwera.

   IBM MQ MQI clients wysyła również dodatkowe informacje w celu ułatwienia identyfikacji.

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

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

Z poziomu produktu IBM MQ 8.0można wysyłać hasła, które są uwzględnione w strukturze MQCSP.

V 9.3.4 Linux AIX Z poziomu produktu IBM MQ 9.3.4produkt IBM MQ MQI clients łączący się z menedżerami kolejek systemu IBM MQ działającymi w systemach AIX lub Linux może również wysyłać znaczniki uwierzytelniania w strukturze MQCSP.

Ostrzeżenie: W niektórych przypadkach hasło lub znacznik uwierzytelniania w strukturze MQCSP dla aplikacji klienckiej jest przesyłane przez sieć w postaci jawnego tekstu. Aby upewnić się, że hasła aplikacji klienckiej i znaczniki uwierzytelniania są odpowiednio chronione, należy zapoznać się z sekcją “Zabezpieczenie hasłem MQCSP” na stronie 32.

Identyfikatory użytkownika

Podczas tworzenia identyfikatorów użytkowników dla aplikacji klienckich nie mogą one być dłuższe niż maksymalna dozwolona długość. Nie można używać zarezerwowanych identyfikatorów użytkowników UNKNOWN i NOBODY. Jeśli serwer, z którym łączy się klient, jest serwerem IBM MQ for Windows , należy zmienić znaczenie znaku @. Dozwolona długość identyfikatorów użytkowników zależy od platformy używanej dla serwera:

- z/OS Linux AIX W systemach z/OSi AIX 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 IBM MQ są w systemie Windows, a serwer ma dostęp do domeny, w której zdefiniowano ID użytkownika klienta, maksymalna długość ID użytkownika wynosi 20 znaków. Jeśli jednak serwer IBM MQ nie jest serwerem Windows , ID użytkownika jest obcinany do 12 znaków.
- Jeśli do przekazywania referencji używana jest struktura MQCSP, maksymalna długość identyfikatora użytkownika wynosi 1024 znaki. Identyfikator użytkownika struktury MQCSP nie może być używany w celu obejścia maksymalnej długości identyfikatora użytkownika używanego przez produkt IBM MQ na potrzeby autoryzacji. Więcej informacji na temat struktury MQCSP zawiera sekcja “Identyfikowanie i uwierzytelnianie użytkowników przy użyciu struktury MQCSP” na stronie 367.

W systemach AIX and Linux domyślnie do uwierzytelniania używane są identyfikatory użytkowników, a do autoryzacji używane są grupy. Można jednak skonfigurować te systemy w taki sposób, aby autoryzować je przy użyciu identyfikatorów użytkowników. Więcej informacji na ten temat zawiera sekcja “Uprawnienia OAM oparte na użytkownikach w systemie AIX and Linux” na stronie 397. Systemy Windows mogą używać zarówno identyfikatorów użytkowników do uwierzytelniania i autoryzacji, jak i grup do autoryzacji.

Jeśli konta usług są tworzone bez zwracania uwagi na grupy i autoryzowania wszystkich identyfikatorów użytkowników 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 systemu IBM MQ. Utworzenie ID użytkownika w systemie operacyjnym o nazwie UNKNOWN lub grupy o nazwie NOBODY może mieć niezamierzone skutki.

Identyfikatory użytkowników podczas nawiązywania połączenia z serwerem IBM MQ for Windows

Windows

Serwer IBM MQ for Windows nie obsługuje połączenia IBM MQ MQI client , jeśli klient działa z ID użytkownika, który zawiera znak @, na przykład `abc@d`. Kod powrotu do wywołania `MQCONN` na kliencie to MQRC_NOT_AUTHORIZED.

Można jednak podać ID użytkownika, używając dwóch znaków @, na przykład `abc@@d`. Preferowaną procedurą jest użycie formatu `id@domain` , aby zapewnić spójne rozstrzyganie identyfikatora użytkownika w poprawnej domenie, a zatem `abc@@d@domain`.

Planowanie autoryzacji

Zaplanuj użytkowników, którzy będą mieli uprawnienia administracyjne, oraz zaplanuj sposób autoryzowania użytkowników aplikacji do odpowiedniego używania obiektów IBM MQ , w tym obiektów łączących się z serwera IBM MQ MQI client.

Aby można było korzystać z produktu IBM MQ, należy przyznać dostęp pojedynczym użytkownikom lub aplikacjom. Wymagane przez nie prawa dostępu zależą od ról, jakie pełnią, oraz od zadań, które muszą wykonywać. Autoryzacja w systemie IBM MQ może być podzielona na dwie główne kategorie:

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

Obie klasy operacji są kontrolowane przez ten sam komponent i można nadać użytkownikowi uprawnienie do wykonywania obu kategorii operacji.

Więcej informacji na temat konkretnych obszarów autoryzacji, które należy wziąć pod uwagę, zawierają następujące tematy:

Uprawnienia do administrowania systemem IBM MQ

Administratorzy IBM MQ muszą mieć uprawnienia do wykonywania różnych funkcji. Uprawnienia te są uzyskiwane na różne sposoby na różnych platformach.

Administratorzy IBM MQ muszą mieć uprawnienia do:

- Wydaj komendy, aby administrować produktem IBM MQ.
- Windows Linux Należy używać komponentu IBM MQ Explorer.
- z/OS Korzystanie z operacji i paneli sterowania 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 zawiera temat odpowiedni dla danego systemu operacyjnego.

ALW *Uprawnienia do administrowania produktem IBM MQ w systemach AIX, Linux, and Windows*

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

Aby użytkownik mógł być administratorem systemu IBM MQ w systemach AIX, Linux, and Windows , musi być członkiem *grupy mqm*. Ta grupa jest tworzona automatycznie podczas instalowania produktu IBM MQ. Aby umożliwić użytkownikom wydawanie komend sterujących, należy dodać ich do grupy mqm. Dotyczy to również użytkownika root w systemie AIX and Linux.

Użytkownicy, którzy nie są członkami grupy mqm, mogą mieć nadane uprawnienia administracyjne, ale nie mogą wydawać komend sterujących produktu IBM MQ i są uprawnieni do wykonywania tylko tych komend, do których im nadano dostęp.

Ponadto 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 tym możliwość administrowania dowolnym menedżerem kolejek działającym w systemie. Ten dostęp można odebrać tylko przez usunięcie użytkownika z grupy mqm. W systemach Windows członkowie grupy Administratorzy mają również dostęp do wszystkich zasobów IBM MQ .

Administratorzy mogą używać komendy sterującej **runmqsc** do wywoływania komend skryptowych IBM MQ (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 uprawnienia wymagane do przetwarzania komend MQSC przez zdalny menedżer kolejek.

Program IBM MQ Explorer wydaje komendy PCF w celu wykonania zadań administracyjnych. Administratorzy nie wymagają dodatkowych uprawnień, aby używać programu IBM MQ Explorer do administrowania menedżerem kolejek w systemie lokalnym. Jeśli program IBM MQ Explorer jest używany do administrowania menedżerem kolejek w innym systemie, administratorzy muszą mieć uprawnienia wymagane do przetwarzania komend PCF przez zdalny menedżer kolejek.

Więcej informacji na temat sprawdzania uprawnień podczas przetwarzania komend PCF i MQSC zawierają następujące tematy:

- Komendy, które działają na menedżerach kolejek, kolejkach, kanałach, procesach, listach nazw i obiektach informacji uwierzytelniającej, zawiera sekcja “Autoryzacja aplikacji do korzystania z produktu IBM MQ” na stronie 98.
- Informacje o komendach, które działają na kanałach, inicjatorach kanałów, programach nasłuchujących i klastrach, zawiera sekcja Zabezpieczenia kanału.
- z/OS Informacje na temat komend MQSC przetwarzanych przez serwer komend w systemie IBM MQ for z/OSzawiera sekcja “Bezpieczeństwo komend i ochrona zasobów komend w systemie z/OS” na stronie 96.

Więcej informacji na temat uprawnień wymaganych do administrowania systemami IBM MQ for AIX, Linux, and Windows zawierają informacje pokrewne.

IBM i *Uprawnienia do administrowania systemem IBM MQ w systemie IBM i*

Aby być administratorem produktu IBM MQ w systemie IBM i, należy być członkiem *grupy QMQMADM*. Ta grupa ma właściwości podobne do właściwości grupy mqm z systemów AIX, Linux, and Windows . W szczególności grupa QMQMADM jest tworzona podczas instalowania produktu IBM MQ for IBM i, a członkowie grupy QMQMADM mają dostęp do wszystkich zasobów produktu IBM MQ w systemie. Użytkownik ma również dostęp do wszystkich zasobów systemu IBM MQ , jeśli ma uprawnienia *ALLOBJ.

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

Istnieją dwie grupy komend CL udostępnianych przez IBM MQ for IBM i:

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

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

- Aby użyć tej komendy, użytkownik musi mieć uprawnienie IBM i . Uprawnienie to jest nadawane za pomocą komendy GRTOBJAUT.
- Użytkownik wymaga uprawnienia IBM MQ , aby uzyskać dostęp 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 Uwierzytelniającej MQM
- CRTMQMCHL, Tworzenie kanału MQM

Więcej informacji na temat tej grupy komend zawiera sekcja “Autoryzacja aplikacji do korzystania z produktu IBM MQ” na stronie 98.

Pełną listę komend grupy 1 i grupy 2 zawiera sekcja “Uprawnienia dostępu do obiektów IBM MQ w systemie IBM i” na stronie 168

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

z/OS *Uprawnienia do administrowania systemem IBM MQ w systemie z/OS*

W tej kolekcji tematów opisano różne aspekty uprawnień wymaganych do administrowania produktem IBM MQ for z/OS.

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

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

Zakłada się, że jako menedżera ESM używany jest produkt RACF . Jeśli używany jest inny moduł ESM, może być konieczne zinterpretowanie informacji podanych dla systemu RACF w sposób, który jest istotny dla tego modułu ESM.

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

W przypadku włączenia zabezpieczeń podsystemu dla konkretnego menedżera kolejek, sprawdzanie uprawnień może być wykonywane na dwóch poziomach:

Zabezpieczenia na poziomie grupy współużytkowania kolejki
Podczas sprawdzania uprawnień używane są profile produktu RACF , które są współużytkowane przez wszystkie menedżery kolejek w grupie współużytkowania kolejek. Oznacza to, że istnieje mniej profili do zdefiniowania i obsługi, co ułatwia administrowanie bezpieczeństwem.

zabezpieczenia na poziomie menedżera kolejek
Podczas sprawdzania uprawnień używane są profile produktu RACF specyficzne dla menedżera kolejek.

Można użyć kombinacji grupy współużytkowania kolejek i zabezpieczeń na poziomie menedżera kolejek. Na przykład można zorganizować profile specyficzne dla menedżera kolejek, aby przesłonić profile grupy współużytkowania kolejek, do której należy menedżer kolejek.

Zabezpieczenia podsystemu, zabezpieczenia na poziomie grupy współużytkowania kolejki i zabezpieczenia na poziomie menedżera kolejek są włączane lub wyłączane przez zdefiniowanie *profili przełącznika*. Profil przełącznika to normalny profil systemu RACF , który ma specjalne znaczenie dla systemu IBM MQ.

z/OS *Bezpieczeństwo komend i ochrona zasobów komend w systemie z/OS*

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

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

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

Niektóre komendy MQSC wykonują operację na zasobie IBM MQ , na przykład komendę DEFINE QLOCAL, aby utworzyć kolejkę lokalną. Gdy administrator wydaje komendę MQSC, wykonywane są sprawdzenia uprawnień w celu określenia, czy żądana operacja może zostać wykonana na zasobie określonym w komendzie. Jest to nazywane *ochroną zasobów komend*.

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

Bezpieczeństwo komend i bezpieczeństwo zasobów komend są niezależne. Na przykład, gdy administrator wyda komendę:

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

przeprowadzane są następujące sprawdzenia uprawnień:

- Bezpieczeństwo komendy sprawdza, czy administrator ma uprawnienia do wydania komendy DEFINE QLOCAL.
- Bezpieczeństwo zasobów komend sprawdza, czy administrator ma uprawnienia do wykonania operacji na kolejce lokalnej o nazwie MOON.EUROPA.

Zabezpieczenia komend i zabezpieczenia zasobów komend można włączać i wyłączać, definiując profile przełączników.

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

W tym temacie opisano, w jaki sposób 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 systemowych.Identyfikator użytkownika, który jest używany do sprawdzania uprawnień, znajduje się w polu *UserIdentifier* w deskryptorze komunikatu zawierającego komendę MQSC. Ten ID użytkownika musi mieć wymagane uprawnienia w menedżerze kolejek, w którym przetwarzana jest komenda. Więcej informacji na temat pola *UserIdentifier* oraz sposobu jego ustawiania zawiera sekcja Kontekst komunikatu.

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

- Operacje i panele sterowania wysyłają komendy MQSC do kolejki wejściowej komend systemowych docelowego menedżera kolejek. Komendy MQSC odpowiadają działaniom wybranym na panelach. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator administratora TSO.
- Funkcja COMMAND programu narzędziowego IBM MQ , CSQUTIL, wysyła komendy MQSC w zestawie danych wejściowych do kolejki wejściowej komend systemowych 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 jest połączony inicjator kanału. Pole *UserIdentifier* w każdym komunikacie jest ustawione na identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

  Podczas wywoływania komend MQSC z zestawów danych CSQINP1 i CSQINP2 nie są wykonywane żadne sprawdzenia uprawnień. Użytkownik może kontrolować, kto może aktualizować te zestawy danych przy użyciu ochrony zestawu danych RACF .
- W obrębie grupy współużytkowania kolejek inicjator kanału może wysyłać komendy START CHANNEL do kolejki wejściowej komend systemowych menedżera kolejek, z którym jest połączony. Komenda jest wysyłana, gdy kanał wychodzący korzystający ze współużytkowanej kolejki transmisji zostanie

uruchomiony przez wyzwolenie. 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 ustawione na identyfikator użytkownika powiązany z aplikacją.
- W systemach AIX, Linux, and Windows komendy sterującej **runmqsc** można używać 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 administratora, który wydał komendę **runmqsc** .

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

Administratorzy IBM MQ for z/OS muszą mieć uprawnienia dostępu do zestawów danych menedżera kolejek. Ten temat zawiera informacje o tym, które zestawy danych wymagają ochrony RACF .

Do tych zestawów danych należą:

- Zestawy danych, do których odwołują się komendy CSQINP1, CSQINP2i CSQINPT w procedurze uruchomionego zadania menedżera kolejek.
- Zestawy stron menedżera kolejek, zestawy danych aktywnego dziennika, archiwalne zestawy danych dziennika i zestawy danych programu startowego (BSD)
- Zestawy danych, do których odwołują się CSQXLIB i CSQINPX w procedurze uruchomionego zadania inicjatora kanału

Należy chronić zestawy danych, aby żaden nieautoryzowany użytkownik nie mógł uruchomić menedżera kolejek ani uzyskać dostępu do danych menedżera kolejek. W tym celu należy użyć ochrony zestawu danych RACF .

Autoryzacja aplikacji do korzystania z produktu IBM MQ

Gdy aplikacje uzyskują dostęp do obiektów, identyfikatory użytkowników powiązane z aplikacjami wymagają odpowiednich uprawnień.

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

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

Aplikacje mogą również używać komend PCF do administrowania obiektami IBM MQ . Podczas przetwarzania komendy PCF używany jest kontekst uprawnień ID użytkownika, który umieścił komunikat PCF.

Aplikacje w tym kontekście obejmują aplikacje napisane przez użytkowników i dostawców oraz aplikacje dostarczone wraz z produktem IBM MQ for z/OS. Aplikacje dostarczane z produktem IBM MQ for z/OS obejmują:

- Operacje i panele sterowania
- Program narzędziowy IBM MQ , CSQUTIL
- Program narzędziowy do obsługi niedostarczonych komunikatów, CSQUDLQH

Aplikacje używające środowisk IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NETlub klientów usługi komunikatów dla środowisk C/C++ i .NET używają pośrednio interfejsu MQI.

Adaptery MCA również wywołują wywołania MQI i identyfikatory użytkowników powiązane z tymi konsolami MCA wymagają 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 120.

W systemie z/OSaplikacje mogą również używać komend MQSC do uzyskiwania dostępu do tych obiektów IBM MQ , ale zabezpieczenia komend i zasobów komend zapewniają sprawdzanie uprawnień w tych okolicznościach. z/OS Aby uzyskać więcej informacji, patrz “Bezpieczeństwo komend i ochrona zasobów komend w systemie z/OS” na stronie 96 i “Komendy MQSC i kolejka wejściowa komend systemowych w systemie z/OS” na stronie 97.

W systemie IBM iużytkownik, który wydaje komendę CL w grupie 2, może wymagać uprawnień dostępu do obiektu IBM MQ powiązanego z komendą. Więcej informacji na ten temat zawiera sekcja “Gdy wykonywane są sprawdzenia uprawnień” na stronie 99.

Gdy wykonywane są sprawdzenia uprawnień

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

W systemie IBM isprawdzanie uprawnień może być również wykonywane, gdy użytkownik wprowadza komendę CL w grupie 2, która uzyskuje dostęp do dowolnego z tych obiektów IBM MQ . Kontrole są przeprowadzane w następujących okolicznościach:

Gdy aplikacja łączy się z menedżerem kolejek za pomocą wywołania MQCONN lub MQCONNX

Menedżer kolejek pyta system operacyjny o identyfikator użytkownika powiązany z aplikacją. Następnie menedżer kolejek sprawdza, czy ID użytkownika jest autoryzowany do nawiązywania z nim połączenia i zachowuje ID użytkownika na potrzeby przyszłych sprawdzeń.

Użytkownicy nie muszą wpisywać się do IBM MQ. W systemie IBM MQ założono, że użytkownicy są wpisani do bazowego systemu operacyjnego i są przez niego uwierzytelniani.

Gdy aplikacja otwiera obiekt IBM MQ za pomocą wywołania MQOPEN lub MQPUT1

Wszystkie operacje sprawdzania uprawnień są wykonywane, gdy obiekt jest otwierany, a nie wtedy, gdy dostęp do niego jest uzyskiwany później. Na przykład sprawdzanie uprawnień jest wykonywane, gdy aplikacja otwiera kolejkę. Nie są one wykonywane, gdy aplikacja umieszcza komunikaty w kolejce lub pobiera komunikaty z kolejki.

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

Gdy aplikacja otwiera kolejkę, wykonywane są sprawdzenia uprawnień dla obiektu określonego w polu `ObjectName` deskryptora obiektu. Pole `ObjectName` jest używane w wywołaniach `MQOPEN` lub `MQPUT1` . Jeśli obiekt jest kolejką aliasową lub definicją kolejki zdalnej, sprawdzanie uprawnień jest wykonywane dla samego obiektu. Nie są one wykonywane w kolejce, na którą tłumaczona jest kolejka aliasowa lub definicja kolejki zdalnej. Oznacza to, że użytkownik nie potrzebuje uprawnień, aby uzyskać do niego dostęp. Ogranicz uprawnienia do tworzenia kolejek do użytkowników uprzywilejowanych. W przeciwnym razie użytkownicy mogą pominąć zwykłą kontrolę dostępu, tworząc alias.

Aplikacja może jawnie odwoływać się do kolejki zdalnej. Ustawia pola `ObjectName` i `ObjectQMgrName` w deskryptorze obiektu na nazwy kolejki zdalnej i menedżera kolejek zdalnych. Sprawdzenia uprawnień są wykonywane względem kolejki transmisji o takiej samej nazwie jak nazwa zdalnego menedżera kolejek:

- z/OS W systemie z/OSsprawdzenie jest wykonywane w profilu kolejki produktu RACF , który jest zgodny z nazwą zdalnego menedżera kolejek i jest wykonywane niezależnie od tego, czy ta kolejka transmisji jest zdefiniowana lokalnie.
- Multi W systemie Wiele platformsprawdzenie jest wykonywane dla profilu RQMNAME, który jest zgodny z nazwą zdalnego menedżera kolejek, jeśli używane jest łączenie w klastry.

Aplikacja może jawnie odwołać się do kolejki klastra, ustawiając w polu `ObjectName` w deskryptorze obiektu nazwę kolejki klastra. Sprawdzenia uprawnień są wykonywane dla kolejki transmisji klastra, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Uprawnienie do kolejki dynamicznej jest oparte na kolejce modelowej, z której pochodzi, ale nie musi być takie samo; patrz uwaga 1.

Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest uzyskiwany z systemu operacyjnego. Identyfikator użytkownika jest uzyskiwany podczas nawiązywania połączenia przez aplikację z menedżerem kolejek. Odpowiednio autoryzowana aplikacja może wywołać funkcję MQOPEN , określając alternatywny identyfikator użytkownika. Następnie wykonywane są sprawdzenia kontroli dostępu dla alternatywnego identyfikatora użytkownika. Użycie alternatywnego identyfikatora użytkownika nie powoduje zmiany identyfikatora użytkownika powiązanego z aplikacją, tylko tego, który jest używany do sprawdzania kontroli dostępu.

Gdy aplikacja subskrybuje temat za pomocą wywołania MQSUB

Gdy aplikacja subskrybuje temat, określa typ operacji, która ma zostać wykonana. Oznacza to utworzenie subskrypcji, zmianę istniejącej subskrypcji lub wznowienie istniejącej subskrypcji bez jej zmiany. Dla każdego typu operacji menedżer kolejek sprawdza, czy ID użytkownika powiązany z aplikacją ma uprawnienia do wykonania tej operacji.

Gdy aplikacja subskrybuje temat, sprawdzanie uprawnień jest wykonywane względem obiektów tematu, które znajdują się w drzewie tematów. Obiekty tematu znajdują się w lub powyżej punktu w drzewie tematów, w którym zasubskrybowana jest aplikacja. Sprawdzanie uprawnień może obejmować sprawdzanie więcej niż jednego obiektu tematu. Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest uzyskiwany z systemu operacyjnego. Identyfikator użytkownika jest uzyskiwany podczas nawiązywania połączenia przez aplikację z menedżerem kolejek.

Menedżer kolejek sprawdza uprawnienia w kolejkach subskrybentów, ale nie w kolejkach zarządzanych.

Gdy aplikacja usuwa trwałą kolejkę dynamiczną za pomocą wywołania MQCLOSE

Uchwyt obiektu określony w wywołaniu MQCLOSE nie musi być taki sam, jak zwrócony przez wywołanie MQOPEN , które utworzyło trwałą kolejkę dynamiczną. Jeśli jest inny, menedżer kolejek sprawdza ID użytkownika powiązany z aplikacją, która wywołała funkcję MQCLOSE . Sprawdza, czy ID użytkownika jest uprawniony do usunięcia kolejki.

Jeśli aplikacja zamykająca subskrypcję w celu usunięcia jej nie utworzyła, do jej usunięcia wymagane jest odpowiednie uprawnienie.

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, znajduje się w polu UserIdentifier w deskryptorze komunikatu komendy PCF. Ten ID użytkownika musi mieć wymagane uprawnienia w menedżerze kolejek, w którym przetwarzana jest komenda. Równoważna komenda MQSC ujęta 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 101.

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.

Wykonywane są sprawdzenia w celu określenia, czy użytkownik ma uprawnienia do wykonywania operacji na obiekcie IBM MQ powiązanym z komendą. Sprawdzenia są wykonywane, chyba że użytkownik jest członkiem grupy QMQMADM lub ma uprawnienie *ALLOBJ . Wymagane uprawnienia zależą od typu operacji wykonywanej przez komendę na obiekcie. Na przykład komenda **CHGMQMQ**Zmiana kolejki MQM wymaga uprawnienia do zmiany atrybutów kolejki określonej przez komendę. Natomiast komenda **DSPMQMQ**Wyświetlenie kolejki MQM (Display MQM Queue) wymaga uprawnienia do wyświetlania atrybutów kolejki określonej przez komendę.

Wiele komend działa na więcej niż jednym obiekcie. Aby na przykład uruchomić komendę **DLTMQMQ**Usuń 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 do wydania jednej z tych komend wymagane jest tylko uprawnienie IBM i . **STRMQMLSR** Przykładem takiej komendy jest komenda Uruchom program nasłuchujący MQM.

Alternatywne uprawnienia użytkownika

Gdy aplikacja otwiera obiekt lub subskrybuje temat, może podać identyfikator użytkownika w wywołaniu MQOPEN, MQPUT1lub MQSUB. Może on zażądać od menedżera kolejek, aby używał tego identyfikatora użytkownika do sprawdzania uprawnień zamiast tego, który jest powiązany z aplikacją.

Otwarcie obiektu przez aplikację powiedzie się tylko wtedy, gdy spełnione są oba poniższe warunki:

- Identyfikator użytkownika powiązany z aplikacją ma uprawnienia do podawania innego identyfikatora użytkownika na potrzeby sprawdzania uprawnień. Aplikacja ma *alternatywne uprawnienia użytkownika*.
- Identyfikator użytkownika podany przez aplikację ma uprawnienie do otwierania obiektu dla żądanych typów operacji lub do subskrybowania tematu.

Kontekst komunikatu

Informacje *Kontekst komunikatu* umożliwiają aplikacji, która pobiera komunikat, uzyskanie informacji o nadawcy komunikatu. Informacje są przechowywane w polach deskryptora komunikatu, a pola są podzielone na trzy części logiczne.

Są to następujące części:

kontekst tożsamości
Te pola zawierają informacje o użytkowniku aplikacji, który umieścił komunikat w kolejce.

kontekst źródła
Pola te zawierają informacje o samej aplikacji i czasie umieszczenia komunikatu w kolejce.

kontekst użytkownika
Te pola zawierają właściwości komunikatów, które mogą być używane przez aplikacje do wybierania komunikatów, które mają być dostarczane przez menedżer kolejek.

Gdy aplikacja umieszcza komunikat w kolejce, może poprosić menedżera kolejek o wygenerowanie informacji o kontekście w komunikacie. Jest to działanie domyślne. Alternatywnie można określić, że pola kontekstu nie mają zawierać żadnych informacji. ID użytkownika powiązany z aplikacją nie wymaga żadnych specjalnych uprawnień do wykonania żadnej z tych czynności.

Aplikacja może ustawić pola kontekstu tożsamości w komunikacie, umożliwiając menedżerowi kolejek wygenerowanie kontekstu źródłowego, lub może ustawić wszystkie pola kontekstu. Aplikacja może również przekazać pola kontekstu tożsamości z komunikatu, który pobrała, do komunikatu, który umieszcza w kolejce, lub może przekazać wszystkie pola kontekstu. Jednak identyfikator użytkownika powiązany z aplikacją wymaga uprawnień do ustawiania lub przekazywania informacji o kontekście. Aplikacja określa, że zamierza ustawić lub przekazać informacje o kontekście, gdy otworzy kolejkę, w której ma umieścić komunikaty, a jej uprawnienia są sprawdzane w tym momencie.

Poniżej przedstawiono krótki opis każdego z pól kontekstu:

kontekst tożsamości

UserIdentifier
Identyfikator użytkownika powiązany z aplikacją, która umieściła komunikat. Jeśli menedżer kolejek ustawia to pole, jest ono ustawiane na identyfikator użytkownika uzyskany z systemu operacyjnego podczas nawiązywania połączenia przez aplikację z menedżerem kolejek.

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

Dane_tożsamości_aplikacji
Jeśli ID użytkownika powiązany z aplikacją ma uprawnienia do ustawiania pól kontekstu tożsamości lub do ustawiania wszystkich pól kontekstu, aplikacja może ustawić to pole na dowolną wartość związaną z tożsamością. Jeśli menedżer kolejek ustawia to pole, jest ono puste.

Kontekst źródła

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

Nazwa_aplikacji_wstawiającej
Nazwa aplikacji, która umieściła komunikat.

PutDate
Data umieszczenia komunikatu.

PutTime
Czas umieszczenia komunikatu.

Dane_pochodzenia_aplikacji
Jeśli ID użytkownika powiązany z aplikacją ma uprawnienia do ustawiania wszystkich pól kontekstu, aplikacja może ustawić to pole na dowolną wartość związaną z pochodzeniem. Jeśli menedżer kolejek ustawia to pole, jest ono puste.

Kontekst użytkownika

W przypadku systemów **MQINQMP** i **MQSETMP**obsługiwane są następujące wartości:

MQPD_USER _KONTEKST

Właściwość jest powiązana z kontekstem użytkownika.

Aby można było ustawić właściwość powiązaną z kontekstem użytkownika za pomocą 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 zgodnie z opisem dla opcji MQOO_SAVE_ALL_CONTEXT. Wywołanie MQPUT z określoną wartością MQOO_PASS_ALL_CONTEXT powoduje skopiowanie właściwości z zapisanego kontekstu do nowego komunikatu.

MQPD_NO_CONTEXT

Właściwość nie jest powiązana z kontekstem komunikatu.

Nierozpoznana wartość została odrzucona z błędem MQRC_PD_ERROR. Wartością początkową tego pola jest **MQPD_NO_CONTEXT**.

Szczegółowy opis poszczególnych pól kontekstu zawiera sekcja MQMD-deskryptor komunikatu. Więcej informacji na temat używania kontekstu komunikatu zawiera sekcja Kontekst komunikatu.

IBM i ALW *Uprawnienia do pracy z obiektami IBM MQ w systemach IBM i , AIX, Linux, and Windows*

Komponent usługi autoryzacji dostarczany z produktem IBM MQ nosi nazwę *menedżera uprawnień do obiektów* (object authority manager-OAM). Zapewnia on kontrolę dostępu za pośrednictwem kontroli uwierzytelniania i autoryzacji.

AUTHENTICATION.
Sprawdzenie uwierzytelniania wykonywane przez mechanizm OAM dostarczany z produktem IBM MQ jest podstawowe i jest wykonywane tylko w określonych okolicznościach. Nie jest on przeznaczony do spełniania rygorystycznych wymagań oczekiwanych w środowisku o wysokim poziomie bezpieczeństwa.

Moduł OAM wykonuje sprawdzenie uwierzytelniania, gdy aplikacja nawiązuje połączenie z menedżerem kolejek i spełnione są następujące warunki:

- Jeśli struktura MQCSP została dostarczona przez aplikację nawiązującą połączenie i

- Atrybut *AuthenticationType* w strukturze MQCSP ma nadaną wartość MQCSP_AUTH_USER_ID_AND_PWD oraz
- Wartość CHCKLOCL lub CHKCCLNT w skonfigurowanym obiekcie AUTHINFO jest inna niż 'NONE'

Kroki uwierzytelniania w OAM sprawdzają poprawność hasła przy użyciu usług systemu operacyjnego, które mogły zostać skonfigurowane do wykonywania dodatkowych sprawdzeń, takich jak upewnienie się, że nazwa użytkownika nie miała zbyt wielu prób testowania niepoprawnego hasła.

Alternatywne mechanizmy uwierzytelniania mogą być używane po napisaniu nowego komponentu usługi autoryzacji lub uzyskaniu go od dostawcy.

Autoryzacja.
Sprawdzenia autoryzacji są obszerne i mają na celu spełnienie większości normalnych wymagań.

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

W systemach IBM i IBM i i AIX, Linux, and Windows *usługa autoryzacji* zapewnia kontrolę dostępu, gdy aplikacja wysyła wywołanie MQI w celu uzyskania dostępu do obiektu IBM MQ będącego menedżerem kolejek, kolejką, procesem, tematem lub listą nazw. Obejmuje to sprawdzanie alternatywnych uprawnień użytkownika oraz uprawnienia do ustawiania lub przekazywania informacji o kontekście.

Windows W systemie Windows funkcja OAM nadaje członkom grupy Administratorzy uprawnienia do dostępu do wszystkich obiektów IBM MQ , nawet jeśli funkcja UAC jest włączona. Ponadto 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 IBM MQ lub na obiekcie informacji uwierzytelniającej. Równoważna komenda MQSC ujęta w komendzie Escape PCF jest traktowana w ten sam sposób.

IBM i W systemie IBM i , jeśli użytkownik nie jest członkiem grupy QMQMADM lub ma uprawnienie *ALLOBJ, usługa autoryzacji zapewnia również sprawdzanie uprawnień, gdy użytkownik wprowadza komendę CL w grupie 2, która działa na dowolnym z tych obiektów IBM MQ lub na obiekcie informacji uwierzytelniającej.

Usługa autoryzacji jest *instalowalną usługą*, co oznacza, że jest ona implementowana przez co najmniej jeden *instalowalny komponent usługi*. Każdy komponent jest wywoływany za pomocą udokumentowanego interfejsu. Dzięki temu użytkownicy i dostawcy mogą udostępniać komponenty w celu rozszerzania lub zastępowania komponentów udostępnianych przez produkty IBM MQ .

Komponent usługi autoryzacji dostarczany z produktem IBM MQ jest nazywany menedżerem uprawnień do obiektów (object authority manager-OAM). Funkcja OAM jest automatycznie włączana dla każdego utworzonego menedżera kolejek.

OAM utrzymuje listę kontroli dostępu (ACL) dla każdego obiektu IBM MQ , do którego ma dostęp. W systemach AIX and Linux na liście ACL mogą być wyświetlane tylko identyfikatory grup. Oznacza to, że wszyscy członkowie grupy mają takie same uprawnienia. W systemach IBM i IBM i i Windows zarówno identyfikatory użytkowników, jak i identyfikatory grup mogą być wyświetlane na liście ACL. Oznacza to, że uprawnienia mogą być nadawane pojedynczym użytkownikom i grupom.

Ograniczenie do 12 znaków dotyczy zarówno grupy, jak i ID użytkownika. Platformy UNIX zwykle ograniczają długość identyfikatora użytkownika do 12 znaków. Systemy AIX i Linux zwiększyły ten limit, ale system IBM MQ nadal przestrzega ograniczenia 12 znaków na wszystkich platformach UNIX . Jeśli ID użytkownika jest dłuższy niż 12 znaków, IBM MQ zastępuje go wartością "UNKNOWN". Nie należy definiować identyfikatora użytkownika o wartości "UNKNOWN".

OAM może uwierzytelnić użytkownika i zmienić odpowiednie pola kontekstu tożsamości. W tym celu należy określić 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. Jeśli połączenie MQCONNX jest nawiązywane z klienta

IBM MQ , informacje w protokole MQCSP są przekazywane do menedżera kolejek, z którym klient nawiązuje połączenie za pośrednictwem kanału połączenia klienckiego i kanału połączenia serwera. Jeśli wyjścia zabezpieczeń są zdefiniowane w tym kanale, protokół MQCSP jest przekazywany do każdego wyjścia zabezpieczeń i może być modyfikowany przez wyjście. Wyjścia zabezpieczeń mogą również tworzyć protokół MQCSP. Więcej informacji na temat użycia wyjść zabezpieczeń w tym kontekście zawiera sekcja Programy obsługi wyjścia zabezpieczeń kanału.

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 IBM MQOchrona haseł CSP.

W systemach AIX, Linux, and Windows komenda sterująca **setmqaut** nadaje i odbiera uprawnienia oraz 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 , którego właścicielem jest menedżer kolejek JUPITER. Umożliwia on również członkom 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 rozpoczynającej się od znaków `MOON.`. MOON.* jest nazwą profilu ogólnego.*Profil ogólny* umożliwia nadanie uprawnień do zestawu obiektów za pomocą pojedynczej komendy **setmqaut** .

Komenda kontrolna **dspmqaut** jest dostępna do wyświetlania bieżących uprawnień użytkownika lub grupy do określonego obiektu.Dostępna jest także komenda sterująca **dmpmqaut** , która umożliwia wyświetlenie bieżących uprawnień powiązanych z profilami ogólnymi.

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

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

udostępnia tę samą funkcję, co w poprzednim przykładzie komendy **setmqaut** ; umożliwia ona członkom grupy VOYAGER umieszczanie komunikatów w dowolnej kolejce o nazwie rozpoczynającej się od znaków `MOON.`

IBM i Komenda CL DSPMQMAUT wyświetla bieżące uprawnienia użytkownika lub grupy do określonego obiektu. Komendy CL WRKMQMAUT i WRKMQMAUTD są również dostępne do pracy z bieżącymi uprawnieniami powiązanymi z obiektami i profilami ogólnymi.

Jeśli nie chcesz sprawdzać uprawnień, na przykład w środowisku testowym, możesz wyłączyć OAM.

Multi *Korzystanie z PCF w celu uzyskania dostępu do komend OAM*
W systemach IBM ii AIX, Linux, and Windows można użyć komend PCF, aby uzyskać dostęp do komend administracyjnych OAM.

Komendy PCF i odpowiadające im komendy OAM są następujące:

Tabela 8. Komendy PCF i odpowiadające im komendy OAM	
Komenda PCF	**Komenda OAM**
Sprawdź rekordy uprawnień	dmpmqaut,
Sprawdź uprawnienia jednostki	Komenda 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, którym nadano 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 sprawdzania uprawnień powiązanych z wywołaniami interfejsu MQI. Należy zdefiniować niektóre profile RACF i nadać im odpowiednie prawa dostępu. Profil *RESLEVEL* służy do kontrolowania liczby sprawdzanych identyfikatorów użytkowników.

Siedem kategorii sprawdzania uprawnień powiązanych z wywołaniami interfejsu MQI:

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

Bezpieczeństwo kolejki
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja otwiera kolejkę lub usuwa trwałą kolejkę dynamiczną

Zabezpieczenia procesu
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja otwiera obiekt procesu

Zabezpieczenia listy nazw
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja otwiera obiekt listy nazw

alternatywne zabezpieczenie użytkownika
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja żąda alternatywnych uprawnień użytkownika podczas otwierania obiektu

zabezpieczenie kontekstu
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja otwiera kolejkę i określa, że zamierza ustawić lub przekazać informacje o kontekście w komunikatach, które umieszcza w kolejce.

Zabezpieczenia tematu
Sprawdzenia uprawnień, które są wykonywane, gdy aplikacja otwiera temat

Każda kategoria sprawdzania uprawnień jest implementowana w taki sam sposób, jak ochrona komend i ochrona zasobów komend. Należy zdefiniować niektóre profile produktu RACF oraz nadać niezbędne grupy i identyfikatory użytkowników dostęp do tych profili na wymaganych poziomach. W przypadku bezpieczeństwa kolejki poziom dostępu określa typy operacji, które aplikacja może wykonać w kolejce. W przypadku zabezpieczeń kontekstu poziom dostępu określa, czy aplikacja może:

- Przekaż wszystkie pola kontekstu
- Przekaż wszystkie pola kontekstu i ustaw pola kontekstu tożsamości
- Przekaż i ustaw wszystkie pola kontekstu

Każdą kategorię sprawdzania uprawnień można włączyć lub wyłączyć, definiując profile przełączników.

Wszystkie kategorie, z wyjątkiem zabezpieczeń połączeń, są określane zbiorczo jako *ochrona zasobów interfejsu API*.

Domyślnie, gdy w wyniku wywołania MQI z aplikacji korzystającej z połączenia wsadowego wykonywane jest sprawdzenie zabezpieczeń zasobów API, sprawdzany jest tylko jeden identyfikator użytkownika. Jeśli sprawdzenie jest wykonywane w wyniku wywołania MQI z aplikacji CICS lub IMS albo z inicjatora kanału, sprawdzane są dwa identyfikatory użytkowników.

Definiując *profil RESLEVEL*, można jednak określić, czy ma być sprawdzany zero, jeden, czy dwa identyfikatory użytkowników. Liczba sprawdzanych identyfikatorów użytkowników jest określana przez identyfikator użytkownika powiązany z typem połączenia, gdy aplikacja nawiązuje połączenie z menedżerem kolejek i poziomem dostępu, jaki ma ten identyfikator do profilu RESLEVEL. Identyfikator użytkownika powiązany z każdym typem połączenia to:

- Identyfikator użytkownika zadania połączenia dla połączeń wsadowych
- ID użytkownika przestrzeni adresowej CICS dla połączeń CICS
- ID użytkownika przestrzeni adresowej regionu IMS dla połączeń IMS
- ID 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 “Uprawnienia do administrowania systemem IBM MQ w systemie z/OS” na stronie 96.

Zabezpieczenia zdalnego przesyłania komunikatów

W tej sekcji opisano aspekty zabezpieczeń związane ze zdalnym przesyłaniem komunikatów.

Należy zapewnić użytkownikom uprawnienia do korzystania z narzędzi IBM MQ . Jest ona zorganizowana zgodnie z działaniami, które mają być podjęte w odniesieniu do obiektów i definicji. Na przykład:

- Menedżery kolejek mogą być uruchamiane i zatrzymywane przez autoryzowanych użytkowników
- Aplikacje muszą łączyć się z menedżerem kolejek i mieć uprawnienia do używania kolejek
- Kanały komunikatów muszą być tworzone i kontrolowane przez autoryzowanych użytkowników.
- Obiekty są przechowywane w bibliotekach i dostęp do tych bibliotek może być ograniczony

Agent kanału komunikatów w ośrodku zdalnym musi sprawdzić, czy dostarczany komunikat pochodzi od użytkownika z uprawnieniami do wykonania tej czynności w tym ośrodku zdalnym. Ponadto, ponieważ adaptery MCA mogą być uruchamiane zdalnie, może być konieczne sprawdzenie, czy zdalne procesy, które próbują uruchomić te adaptery MCA, są do tego uprawnione. Istnieją cztery możliwe sposoby, aby sobie z tym poradzić:

1. Należy użyć atrybutu PutAuthority definicji kanału RCVR, RQSTR lub CLUSRCVR, aby określić, który użytkownik jest używany do sprawdzania autoryzacji w czasie umieszczania komunikatów przychodzących w kolejkach. Patrz opis komendy DEFINE CHANNEL w publikacji MQSC Command Reference.
2. Zaimplementuj rekordy uwierzytelniania kanału w celu odrzucenia niepotrzebnych prób nawiązania połączenia lub ustawienia wartości MCAUSER w oparciu o następujące informacje: zdalny adres IP, zdalny identyfikator użytkownika, podana nazwa wyróżniająca podmiotu TLS (DN) lub nazwa zdalnego menedżera kolejek.
3. Zaimplementuj sprawdzanie zabezpieczeń *programu użytkownika obsługi wyjścia* , aby upewnić się, że odpowiedni kanał komunikatów jest autoryzowany. Bezpieczeństwo instalacji udostępniającej odpowiedni kanał zapewnia, że wszyscy użytkownicy są odpowiednio autoryzowani, dzięki czemu nie ma potrzeby sprawdzania pojedynczych komunikatów.
4. Zaimplementuj przetwarzanie komunikatów *programu użytkownika obsługi wyjścia* , aby upewnić się, że poszczególne komunikaty są weryfikowane pod kątem autoryzacji.

IBM i *Zabezpieczenia obiektów IBM MQ for IBM i*

W tej sekcji opisano aspekty zabezpieczeń związane ze zdalnym przesyłaniem komunikatów.

Aby korzystać z narzędzi IBM MQ for IBM i , należy udostępnić użytkownikom odpowiednie uprawnienia. To uprawnienie jest zorganizowane zgodnie z działaniami, które mają być podjęte w odniesieniu do obiektów i definicji. Na przykład:

- Menedżery kolejek mogą być uruchamiane i zatrzymywane 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.

Agent kanału komunikatów w ośrodku zdalnym musi sprawdzić, czy dostarczany komunikat pochodzi od użytkownika z uprawnieniami do isue komunikatu w tym ośrodku zdalnym. Ponadto, ponieważ adaptery MCA mogą być uruchamiane zdalnie, może być konieczne sprawdzenie, czy zdalne procesy, które próbują uruchomić te adaptery MCA, są do tego uprawnione. Istnieją cztery możliwe sposoby, aby sobie z tym poradzić:

- Dekret w definicji kanału, że komunikaty muszą zawierać akceptowalne uprawnienie *kontekstowe* , w przeciwnym razie są usuwane.
- Zaimplementuj rekordy uwierzytelniania kanału w celu odrzucenia niepotrzebnych prób nawiązania połączenia lub ustawienia wartości MCAUSER w oparciu o jeden z następujących elementów: zdalny adres IP, zdalny identyfikator użytkownika, podana nazwa wyróżniająca TLS (DN) lub nazwa zdalnego menedżera kolejek.
- Zaimplementuj sprawdzanie zabezpieczeń wyjścia użytkownika, aby upewnić się, że odpowiedni kanał komunikatów jest autoryzowany. Bezpieczeństwo instalacji udostępniającej odpowiedni kanał zapewnia, że wszyscy użytkownicy są odpowiednio autoryzowani, dzięki czemu nie ma potrzeby sprawdzania pojedynczych komunikatów.
- Zaimplementuj przetwarzanie komunikatów wyjścia użytkownika, aby upewnić się, że poszczególne komunikaty są weryfikowane pod kątem autoryzacji.

Poniżej przedstawiono kilka faktów dotyczących sposobu działania produktu IBM MQ for IBM i z zabezpieczeniami:

- 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 AIX *Bezpieczeństwo obiektów w systemie AIX and Linux*

Użytkownicy administracyjni muszą należeć do grupy mqm w systemie (łącznie z użytkownikiem root), jeśli ten identyfikator ma używać komend administracyjnych systemu IBM MQ .

Komendę amqcrsta należy zawsze uruchamiać jako identyfikator użytkownika mqm.

Identyfikatory użytkowników w systemie AIX and Linux

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

Windows *Bezpieczeństwo obiektów w systemach Windows*

Użytkownicy administracyjni muszą należeć zarówno do grupy mqm, jak i do grupy administrators w systemach Windows , jeśli ten identyfikator ma używać komend administracyjnych IBM MQ .

Identyfikatory użytkowników w systemach Windows

W systemach Windows , *jeśli nie zainstalowano wyjścia komunikatów*, menedżer kolejek przekształca wszystkie identyfikatory użytkowników zapisane wielkimi literami lub literami o różnej wielkości w małe litery. Następnie menedżer kolejek wstawia identyfikatory użytkowników do części kontekstu komunikatu lub sprawdza ich autoryzację. Dlatego autoryzacje są oparte tylko na małych identyfikatorach.

Identyfikatory użytkowników w różnych systemach

Platformy inne niż systemy AIX, Linux, and Windows używają w komunikatach wielkich liter w identyfikatorach użytkowników. Aby umożliwić systemom AIX, Linux, and Windows używanie w komunikatach identyfikatorów użytkowników pisanych małymi literami, agent kanału komunikatów (MCA) musi przeprowadzić odpowiednie konwersje znaków alfabetycznych.

Aby umożliwić systemom AIX, Linux, and Windows używanie małych liter w identyfikatorach użytkowników w komunikatach, agent kanału komunikatów (MCA) na tych platformach wykonuje następujące konwersje:

Na końcu wysyłania
Znaki alfabetu we wszystkich identyfikatorach użytkowników są przekształcane na wielkie litery, jeśli nie zainstalowano wyjścia komunikatów.

Po zakończeniu odbioru
Znaki alfabetu we wszystkich identyfikatorach użytkowników są konwertowane na małe litery, jeśli nie zainstalowano wyjścia komunikatów.

Automatyczne konwersje nie są wykonywane, jeśli z jakiegokolwiek innego powodu w systemie AIX, Linux, and Windows zostanie podane wyjście komunikatu.

Korzystanie z niestandardowej usługi autoryzacji

IBM MQ dostarcza instalowalną usługę autoryzacji. Można wybrać instalację alternatywnej usługi.

Komponent usługi autoryzacji dostarczany z produktem IBM MQ nosi nazwę Object Authority Manager (OAM). Jeśli moduł OAM nie dostarcza potrzebnych narzędzi autoryzacji, można napisać własny komponent usługi autoryzacji. Instalowalne funkcje usług, które muszą być zaimplementowane przez komponent usługi autoryzacji, są opisane w sekcji Informacje uzupełniające o interfejsie instalowalnych usług.

Kontrola dostępu dla klientów

Kontrola dostępu jest oparta na identyfikatorach użytkowników. Może istnieć wiele identyfikatorów użytkowników do administrowania, a identyfikatory użytkowników mogą być w różnych formatach. Dla właściwości MCAUSER kanału połączenia z serwerem 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 tworującego wywołania MQI. W przypadku klientów MQI produktu MQ agent MCA połączeń serwera tworzy wywołania MQI w imieniu klientów MQI produktu MQ . Można wybrać alternatywny identyfikator użytkownika dla agenta MCA połączenia z serwerem, który ma być używany do wykonywania wywołań MQI. Alternatywny identyfikator użytkownika może być powiązany albo ze stacją roboczą klienta, albo ze wszystkim, co zostanie wybrane do organizowania i kontrolowania dostępu klientów. Identyfikator użytkownika musi mieć przypisane niezbędne uprawnienia na serwerze, aby można było wykonywać wywołania MQI. Wybór alternatywnego identyfikatora użytkownika jest preferowany w stosunku do umożliwienia klientom wykonywania wywołań MQI z uprawnieniami agenta 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	Używana, chyba że została zablokowana przez regułę **CHLAUTH TYPE(BLOCKUSER)** . Więcej informacji na ten temat zawiera następująca sekcja: “Ustawianie identyfikatora użytkownika w wyjściu zabezpieczeń” na stronie 109 .
Identyfikator użytkownika, który jest ustawiany przez regułę CHLAUTH	Używany, chyba że jest przejeżdżany przez wyjście bezpieczeństwa. Więcej informacji na ten temat zawiera sekcja Rekordy uwierzytelniania kanału .

Tabela 9. Identyfikator użytkownika używany przez kanał połączenia z serwerem (kontynuacja)	
ID użytkownika	**W przypadku użycia**
Identyfikator użytkownika zdefiniowany w atrybucie **MCAUSER** w definicji kanału SVRCONN	Używana, o ile nie została przekroczona przez wyjście zabezpieczeń lub regułę CHLAUTH.
Identyfikator użytkownika, który jest pobierany z komputera klienta	Używana, gdy żaden identyfikator użytkownika nie jest ustawiany w inny sposób.
Identyfikator użytkownika, który uruchomił kanał połączenia z serwerem	Używana, gdy żaden identyfikator użytkownika nie jest ustawiony w inny sposób i nie jest używany żaden identyfikator użytkownika klienta. Więcej informacji na ten temat zawiera następująca sekcja: “Identyfikator użytkownika, który uruchamia program kanału” na stronie 110 .

Ponieważ agent MCA połączenia z serwerem wykonuje wywołania MQI w imieniu użytkowników zdalnych, należy wziąć pod uwagę wpływ na bezpieczeństwo agenta MCA połączenia z serwerem, który wysyła wywołania MQI w imieniu klientów zdalnych, oraz sposób administrowania dostępem potencjalnie dużej liczby użytkowników.

- Jednym z nich jest wydawanie przez agent MCA połączenia z serwerem wywołań MQI z własnym uprawnieniem. Należy jednak mieć na względzie, że zwykle nie jest wskazane, aby agent MCA połączenia z serwerem, z jego potężnymi możliwościami dostępu, wywoływał wywołania MQI w imieniu użytkowników klienta.
- Innym podejściem jest użycie identyfikatora użytkownika, który przepływa z klienta. Agent MCA połączenia z serwerem może wykonywać wywołania MQI przy użyciu możliwości dostępu identyfikatora użytkownika klienta. To podejście przedstawia szereg pytań, które należy rozważyć:
  1. Istnieją różne formaty identyfikatora użytkownika na różnych platformach. Czasami powoduje to problemy, jeśli format identyfikatora użytkownika na kliencie różni się od akceptowalnych formatów na serwerze.
  2. Istnieje potencjalnie wiele klientów z różnymi i zmieniającymi się identyfikatorami użytkowników. Identyfikatory muszą być zdefiniowane i zarządzane na serwerze.
  3. Czy ID użytkownika ma być zaufany? Każdy identyfikator użytkownika może być pobierany z klienta, niekoniecznie musi to być identyfikator zalogowanego użytkownika. Na przykład klient może przepłynąć identyfikator z pełnym uprawnieniem `mqm` , które zostało celowo zdefiniowane na serwerze ze względów bezpieczeństwa.
- Preferowanym podejściem jest zdefiniowanie znaczników identyfikacji klienta na serwerze, a tym samym ograniczenie możliwości aplikacji połączonych z klientem. Zwykle odbywa się to przez ustawienie właściwości MCAUSER kanału połączenia z serwerem na specjalną wartość identyfikatora użytkownika, która ma być używana przez klienty, oraz przez zdefiniowanie kilku identyfikatorów do użycia przez klienty z innym poziomem autoryzacji na serwerze.

Ustawianie identyfikatora użytkownika w wyjściu zabezpieczeń

W przypadku systemu IBM MQ MQI clientsprocesem, który wysyła wywołania MQI, jest agent MCA połączenia z serwerem. Identyfikator użytkownika używany przez agent MCA połączenia serwera jest zawarty w polach `MCAUserIdentifier` lub `LongMCAUserIdentifier` dokumentu MQCD. Zawartość tych pól jest ustawiana przez:

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

Wyjście zabezpieczeń może przesłonić wartości, które są dla niego widoczne, gdy jest wywoływane.

- 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 i od klienta nie został odebrany żaden identyfikator użytkownika, używany jest identyfikator użytkownika, który uruchomił kanał połączenia z serwerem.

Klient IBM MQ nie przepływa potwierdzonego identyfikatora użytkownika do serwera, gdy używane jest wyjście zabezpieczeń po stronie klienta.

Identyfikator użytkownika, który uruchamia program kanału

Jeśli pola ID użytkownika pochodzą z ID użytkownika, który uruchomił kanał połączenia z serwerem, używana jest następująca wartość:

- z/OS W przypadku systemu z/OSjest to identyfikator użytkownika przypisany do uruchomionego zadania inicjatora kanału przez tabelę uruchomionych procedur z/OS .
- W przypadku protokołu TCP/IP (innego niż z/OS) jest to identyfikator użytkownika z pozycji `inetd.conf` lub identyfikator użytkownika, który uruchomił proces nasłuchujący.
- W przypadku architektury SNA (innej niż z/OS) jest to identyfikator użytkownika z pozycji serwera SNA lub (jeśli nie istnieje) przychodzące żądanie przyłączenia lub identyfikator 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 użyć tej definicji kanału do nawiązania połączenia z menedżerem kolejek z uprawnieniami dostępu określonymi przez ID użytkownika podany przez klienta. Może to stanowić zagrożenie dla bezpieczeństwa, jeśli system, w którym działa menedżer kolejek, zezwala na nieautoryzowane połączenia sieciowe. Domyślny kanał połączenia z serwerem IBM MQ (SYSTEM.DEF.SVRCONN) ma atrybut MCAUSER ustawiony na wartość pustą. Aby uniemożliwić dostęp bez uprawnień, należy zaktualizować atrybut MCAUSER definicji domyślnej przy użyciu identyfikatora użytkownika, który nie ma dostępu do obiektów IBM MQ MQ .

Wielkość liter w identyfikatorach użytkowników

Podczas definiowania kanału za pomocą parametru `runmqsc`atrybut MCAUSER jest zmieniany na wielkie litery, chyba że identyfikator użytkownika jest ujęty w pojedynczy cudzysłów.

ALW W przypadku serwerów w systemie AIX, Linux, and Windowszawartość pola `MCAUserIdentifier` odebranego od klienta jest zmieniana na małe litery.

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

Linux AIX W przypadku serwerów w systemach AIX and Linux zawartość pola `LongMCAUserIdentifier` odbieranego od klienta jest zmieniana na małe litery.

Domyślnie identyfikator użytkownika, który jest przekazywany w przypadku używania aplikacji powiązania produktu IBM MQ JMS , jest identyfikatorem użytkownika maszyny JVM, na której działa aplikacja.

Możliwe jest również przekazanie identyfikatora użytkownika za pomocą metody `createQueueConnection` .

Poufność planowania

Zaplanuj sposób zachowania poufności danych.

Poufność można zaimplementować na poziomie aplikacji lub na poziomie łącza. Istnieje możliwość użycia protokołu TLS. W takim przypadku należy zaplanować użycie certyfikatów cyfrowych. Jeśli standardowe narzędzia nie spełniają wymagań, można również użyć programów obsługi wyjścia kanału.

Pojęcia pokrewne

“Porównywanie zabezpieczeń na poziomie łącza i zabezpieczeń na poziomie aplikacji” na stronie 111
Ten temat zawiera informacje o różnych aspektach zabezpieczeń na poziomie łącza i na poziomie aplikacji, a także porównuje dwa poziomy zabezpieczeń.

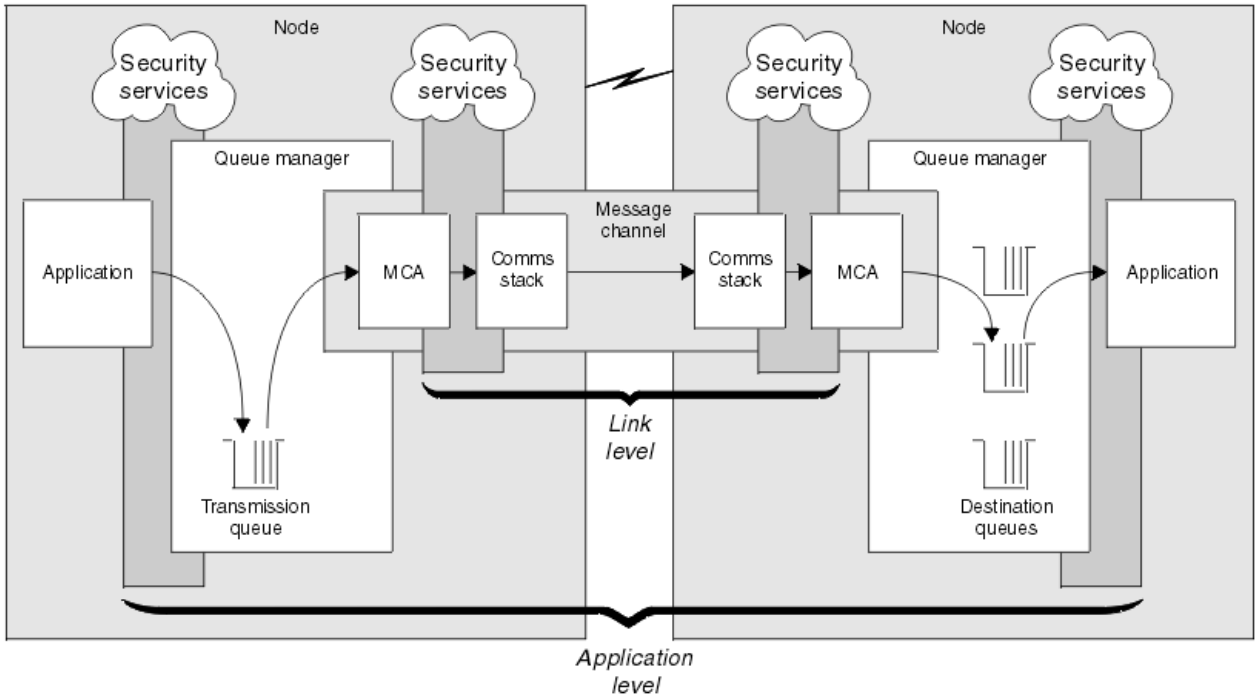
“Programy obsługi wyjścia kanału” na stronie 116
Programy obsługi wyjścia kanału to programy wywoływane w zdefiniowanych miejscach w sekwencji przetwarzania agenta MCA. Użytkownicy i dostawcy mogą tworzyć własne programy obsługi wyjścia kanału. Niektóre są dostarczane przez IBM.

“Zabezpieczanie kanałów za pomocą protokołu SSL/TLS” na stronie 123
Obsługa protokołu TLS w produkcie IBM MQ używa obiektu informacji uwierzytelniającej menedżera kolejek i różnych komend MQSC. Należy również wziąć pod uwagę użycie certyfikatów cyfrowych.

Porównywanie zabezpieczeń na poziomie łącza i zabezpieczeń na poziomie aplikacji

Ten temat zawiera informacje o różnych aspektach zabezpieczeń na poziomie łącza i na poziomie aplikacji, a także porównuje dwa poziomy zabezpieczeń.

Zabezpieczenia na poziomie łącza i na poziomie aplikacji zostały przedstawione w sekcji Rysunek 10 na stronie 111.



Rysunek 10. Zabezpieczenia na poziomie łącza i zabezpieczenia na poziomie aplikacji

Zabezpieczanie komunikatów w kolejkach

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

z/OS Szyfrowanie zestawu danych z/OS może zapewnić pewną ochronę komunikatów przechowywanych w kolejkach, ale tylko dla danych przechowywanych w lokalnym menedżerze kolejek.

Patrz sekcja poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych . :NONE.

Dla porównania zabezpieczenia na poziomie aplikacji mogą chronić komunikaty 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, którą przedstawia Rysunek 10 na stronie 111.

Menedżery kolejek nie działają w środowiskach kontrolowanych i zaufanych

Jeśli menedżer kolejek działa w kontrolowanym i zaufanym środowisku, mechanizmy kontroli dostępu udostępniane przez produkt IBM MQ mogą być uznane za wystarczające do zabezpieczenia komunikatów przechowywanych w jego kolejkach. Jest to szczególnie istotne, jeśli używane jest tylko kolejkowanie lokalne i komunikaty nigdy nie opuszczają menedżera kolejek. W tym przypadku zabezpieczenia na poziomie aplikacji mogą być uznane 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 kontrolowanym i zaufanym środowisku, lub są odbierane z takiego menedżera kolejek. Potrzeba zabezpieczenia na poziomie aplikacji staje się większa, gdy komunikaty są przesyłane do 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 pod względem administracji i wydajności.

Koszt administrowania będzie prawdopodobnie większy, ponieważ potencjalnie istnieje więcej ograniczeń do konfigurowania i obsługi. Na przykład może być konieczne upewnienie się, że określony użytkownik wysyła tylko określone typy komunikatów i wysyła komunikaty tylko do określonych miejsc docelowych. Z drugiej strony może być konieczne zapewnienie, że określony użytkownik otrzyma tylko określone typy komunikatów i otrzyma tylko komunikaty z określonych źródeł. Zamiast zarządzać usługami zabezpieczeń na poziomie łącza w pojedynczym kanale komunikatów, może być konieczne skonfigurowanie i zachowanie reguł dla każdej pary użytkowników, którzy wymieniają komunikaty w tym kanale.

Może to mieć wpływ na wydajność, jeśli usługi zabezpieczeń są wywoływane za każdym razem, gdy aplikacja umieszcza lub pobiera komunikat.

Organizacje zwykle najpierw rozważają bezpieczeństwo na poziomie łącza, ponieważ może być łatwiejsze do zaimplementowania. Biorą pod uwagę zabezpieczenia na poziomie aplikacji, jeśli odkryją, że zabezpieczenia na poziomie łącza nie spełniają wszystkich swoich wymagań.

Dostępność komponentów

Ogólnie rzecz biorąc, w środowisku rozproszonym usługa zabezpieczeń wymaga komponentu w co najmniej dwóch systemach. Na przykład komunikat może być zaszyfrowany w jednym systemie, a zdeszyfrowany w innym. Dotyczy to zarówno zabezpieczeń na poziomie łącza, jak i zabezpieczeń na poziomie aplikacji.

W środowisku heterogenicznym, w którym używane są różne platformy, z których każda ma różne poziomy funkcji zabezpieczeń, wymagane komponenty usługi zabezpieczeń mogą nie być dostępne dla każdej platformy, na której są potrzebne, i w formie, która jest łatwa w użyciu. Jest to prawdopodobnie bardziej istotne w przypadku zabezpieczeń na poziomie aplikacji niż w przypadku zabezpieczeń na poziomie łącza, szczególnie jeśli użytkownik zamierza zapewnić własne zabezpieczenia na poziomie aplikacji, kupując komponenty z różnych źródeł.

Komunikaty w kolejce niedostarczonych komunikatów

Jeśli komunikat jest chroniony przez zabezpieczenia na poziomie aplikacji, może wystąpić problem, jeśli z jakiegoś powodu komunikat nie dociera do miejsca docelowego i jest umieszczany w kolejce niedostarczonych komunikatów. Jeśli nie można określić sposobu przetwarzania komunikatu na

podstawie informacji z deskryptora komunikatu i nagłówka niedostarczonego komunikatu, może być konieczne sprawdzenie treści danych aplikacji. Nie można tego zrobić, jeśli dane aplikacji są zaszyfrowane i tylko odbiorca może je deszyfrować.

Czego nie mogą zrobić zabezpieczenia na poziomie aplikacji

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

- Po uruchomieniu kanału uwierzytelnianie wzajemne dwóch agentów MCA może nadal być wymagane. Może to być wykonane tylko przez usługę zabezpieczeń na poziomie łącza.
- Zabezpieczenia na poziomie aplikacji nie mogą chronić nagłówka kolejki transmisji MQXQH, który zawiera osadzony deskryptor komunikatu. Nie może 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 po stronie serwera kanału MQI, usługi nie mogą chronić parametrów wywołań MQI wysyłanych przez kanał. W szczególności dane aplikacji w wywołaniu MQPUT, MQPUT1lub MQGET są niechronione. W tym przypadku ochrona może być zapewniona tylko przez zabezpieczenia na poziomie łącza.

zabezpieczenia na poziomie łącza

Zabezpieczenia na poziomie łącza odnoszą się do tych usług zabezpieczeń, które są wywoływane bezpośrednio lub pośrednio przez agent MCA, podsystem komunikacyjny lub kombinację tych dwóch działających razem.

Zabezpieczenia na poziomie łącza zostały przedstawione w sekcji Rysunek 10 na stronie 111.

Poniżej przedstawiono kilka przykładów usług zabezpieczeń na poziomie łącza:

- Agent MCA na każdym końcu kanału komunikatów może uwierzytelnić swojego partnera. Jest to wykonywane po uruchomieniu kanału i nawiązaniu połączenia komunikacyjnego, ale przed rozpoczęciem przepływu komunikatów. Jeśli uwierzytelnianie nie powiedzie się na obu końcach, kanał jest zamykany i nie są przesyłane żadne komunikaty. Jest to przykład usługi identyfikacji i uwierzytelniania.
- Komunikat może być szyfrowany na wysyłającym końcu kanału i deszyfrowany na odbierającym końcu. Jest to przykład usługi poufności.
- Komunikat może zostać sprawdzony na odbierającym końcu kanału w celu określenia, czy jego treść została celowo zmodyfikowana podczas przesyłania przez sieć. Jest to przykład usługi integralności danych.

Zabezpieczenia na poziomie łącza udostępniane przez IBM MQ

Podstawowym sposobem zapewnienia poufności i integralności danych w produkcie IBM MQ jest użycie protokołu TLS. Więcej informacji na temat używania protokołu TLS w produkcie IBM MQzawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24. Na potrzeby uwierzytelniania produkt IBM MQ udostępnia narzędzie do korzystania z rekordów uwierzytelniania kanału. Rekordy uwierzytelniania kanału zapewniają precyzyjną kontrolę dostępu do systemów łączących na poziomie poszczególnych kanałów lub grup kanałów. Więcej informacji na ten temat zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.

Zapewnianie własnych zabezpieczeń na poziomie łącza

Użytkownik może udostępnić własne usługi zabezpieczeń na poziomie łącza. Pisanie własnych programów obsługi wyjścia kanału jest głównym sposobem na zapewnienie własnych usług ochrony na poziomie łącza.

Programy obsługi wyjścia kanału zostały wprowadzone w sekcji “Programy obsługi wyjścia kanału” na stronie 116. Ten sam temat zawiera również opis programu obsługi wyjścia kanału, który jest dostarczany z produktem 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 w taki sposób, aby odpowiadał wymaganiom użytkownika. Jeśli ten program obsługi wyjścia kanału lub programy obsługi wyjścia kanału dostępne od innych dostawców nie spełniają wymagań, można zaprojektować i napisać własny. W tym temacie opisano sposoby, w jakie programy obsługi wyjścia kanału mogą udostępniać usługi ochrony. Informacje na temat pisania programu obsługi wyjścia kanału zawiera sekcja Tworzenie programów obsługi wyjścia kanału.

Zabezpieczenia na poziomie łącza przy użyciu wyjścia zabezpieczeń
Wyjścia zabezpieczeń zwykle działają w parach, po jednym na każdym końcu kanału. Są one wywoływane natychmiast po zakończeniu początkowej negocjacji danych podczas uruchamiania kanału.

Wyjścia zabezpieczeń mogą służyć do identyfikacji 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 modyfikować treść komunikatu i zmieniać jego długość.

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

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

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

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

W przypadku kanału komunikatów, jeśli agent MCA musi podzielić komunikat i wysłać go w więcej niż jednym segmencie transmisji, dla każdego segmentu transmisji zawierającego część komunikatu jest wywoływane wyjście wysyłania, a na końcu odbierającym jest wywoływane wyjście odbierania dla każdego segmentu transmisji. To samo występuje w kanale MQI, jeśli parametry wejściowe lub wyjściowe wywołania MQI są zbyt duże, aby można je było wysłać w pojedynczym segmencie transmisji.

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

Gdy wyjście wysyłania jest wywoływane po raz pierwszy w celu uzyskania i zainicjowania potrzebnych zasobów, może zażądać od agenta MCA zarezerwowania określonej ilości miejsca w buforze, w którym znajduje się segment transmisji. Jeśli zostanie wywołana później w celu przetworzenia segmentu transmisji, może na przykład użyć tego obszaru do dodania zaszyfrowanego klucza lub podpisu cyfrowego. Odpowiednie wyjście odbierania na drugim końcu kanału może usunąć dane dodane przez wyjście wysyłania i użyć ich do przetworzenia segmentu transmisji.

Wyjścia nadawcze i odbiorcze najlepiej nadają się do celów, w których nie muszą rozumieć struktury danych, które są przez nie przetwarzane, a zatem mogą traktować każdy segment transmisji jako obiekt binarny.

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

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 w interfejsie między aplikacją a menedżerem kolejek, z którym jest połączona.

Usługi te są wywoływane, gdy aplikacja wysyła wywołania MQI do menedżera kolejek. Usługi mogą być wywoływane, bezpośrednio lub pośrednio, przez aplikację, menedżer kolejek, inny produkt, który obsługuje funkcję IBM MQ, lub przez kombinację tych usług. Zabezpieczenia na poziomie aplikacji są przedstawione w sekcji Rysunek 10 na stronie 111.

Zabezpieczenia na poziomie aplikacji są również określane jako *zabezpieczenia na całej trasie* lub *zabezpieczenia na poziomie komunikatu*.

Poniżej przedstawiono kilka przykładów usług zabezpieczeń na poziomie aplikacji:

- Gdy aplikacja umieszcza komunikat w kolejce, deskryptor komunikatu zawiera identyfikator użytkownika powiązany z aplikacją. Nie ma jednak żadnych danych, takich jak zaszyfrowane hasło, których można użyć do uwierzytelnienia ID użytkownika. Usługa zabezpieczeń może dodać te dane. Po ostatecznym pobraniu komunikatu przez aplikację odbierającą inny komponent usługi może uwierzytelnić identyfikator użytkownika przy użyciu danych, które przeszły z komunikatem. Jest to przykład usługi identyfikacji i uwierzytelniania.
- Komunikat może być szyfrowany, gdy jest umieszczany w kolejce przez aplikację i deszyfrowany, gdy jest pobierany przez aplikację odbierającą.Jest to przykład usługi poufności.
- Komunikat może zostać sprawdzony podczas jego pobierania przez aplikację odbierającą. To sprawdzenie określa, czy jego treść została celowo zmodyfikowana od pierwszego umieszczenia w kolejce przez aplikację wysyłającą.Jest to przykład usługi integralności danych.

Planowanie Advanced Message Security
Advanced Message Security (AMS) jest komponentem produktu IBM MQ , który zapewnia wysoki poziom ochrony danych wrażliwych przepływających przez sieć IBM MQ , nie wpływając jednocześnie na aplikacje końcowe.

W przypadku przenoszenia bardzo wrażliwych lub cennych informacji, w szczególności informacji poufnych lub związanych z płatnościami, takich jak dane pacjentów lub dane karty kredytowej, należy zwrócić szczególną uwagę na bezpieczeństwo informacji. Zapewnienie, że informacje poruszające się w obrębie przedsiębiorstwa zachowują swoją integralność i są chronione przed dostępem bez uprawnień, jest ciągłym wyzwaniem i obowiązkiem. Istnieje również prawdopodobieństwo, że użytkownik będzie zobowiązany do zachowania zgodności z przepisami dotyczącymi bezpieczeństwa, co wiąże się z ryzykiem kar za nieprzestrzeganie tych przepisów.

Użytkownik może utworzyć własne rozszerzenia 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 w przedsiębiorstwie między praktycznie każdym rodzajem komercyjnego systemu informatycznego.

Advanced Message Security rozszerza opcje zabezpieczające produktu IBM MQ w następujący sposób:

- Zapewnia on kompleksową ochronę danych na poziomie aplikacji w infrastrukturze przesyłania komunikatów typu punkt z punktem przy użyciu szyfrowania lub cyfrowego podpisywania komunikatów.
- Zapewnia kompleksową ochronę bez konieczności pisania skomplikowanego kodu bezpieczeństwa lub modyfikowania lub rekompilowania istniejących aplikacji.
- Korzysta z technologii infrastruktury klucza publicznego (Public Key Infrastructure-PKI) w celu zapewnienia usług uwierzytelniania, autoryzacji, poufności i integralności danych dla komunikatów.
- Umożliwia administrowanie strategiami bezpieczeństwa dla serwerów mainframe i serwerów rozproszonych.
- Obsługuje zarówno serwery IBM MQ , jak i klienty.
- Jest on zintegrowany z produktem Managed File Transfer i udostępnia kompleksowe rozwiązanie do bezpiecznego przesyłania komunikatów.

Więcej informacji na ten temat zawiera sekcja “Advanced Message Security” na stronie 652.

Zapewnianie własnych zabezpieczeń na poziomie aplikacji
Istnieje możliwość udostępnienia własnych usług zabezpieczeń na poziomie aplikacji. Aby ułatwić zaimplementowanie zabezpieczeń na poziomie aplikacji, produkt IBM MQ udostępnia dwa wyjścia: wyjście funkcji API i wyjście funkcji API.

Wyjście funkcji API i wyjście funkcji API-crossing mogą zapewnić identyfikację i uwierzytelnianie, kontrolę dostępu, poufność, integralność danych i usługi niezaprzeczalności oraz inne funkcje niezwiązane z bezpieczeństwem.

Jeśli wyjście funkcji API lub wyjście ze skrzyżowania funkcji API nie jest obsługiwane w środowisku systemowym, można rozważyć inne sposoby zapewnienia własnych zabezpieczeń na poziomie aplikacji. Jednym ze sposobów jest utworzenie interfejsu API wyższego poziomu, który hermetyzuje interfejs MQI. Następnie programiści używają tego interfejsu API zamiast interfejsu MQI do pisania aplikacji IBM MQ .

Najczęstszymi przyczynami używania interfejsu API wyższego poziomu są:

- Ukrywanie bardziej zaawansowanych funkcji interfejsu MQI przed programistami.
- Wymuszanie standardów użycia interfejsu MQI.
- Służy do dodawania funkcji do interfejsu MQI. Ta dodatkowa funkcja może być usługą ochrony.

Niektóre produkty dostawców używają 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 zagadnienia dotyczące konwersji danych:

- Jeśli znacznik bezpieczeństwa, taki jak podpis cyfrowy, został dodany do danych aplikacji w komunikacie, każdy kod przeprowadzający konwersję danych musi mieć informacje o obecności tego znacznika.
- Znacznik bezpieczeństwa mógł zostać uzyskany z obrazu binarnego danych aplikacji. Oznacza to, że przed przekształceniem danych należy sprawdzić token.
- Jeśli dane aplikacji w komunikacie zostały zaszyfrowane, muszą zostać zdeszyfrowane przed konwersją danych.

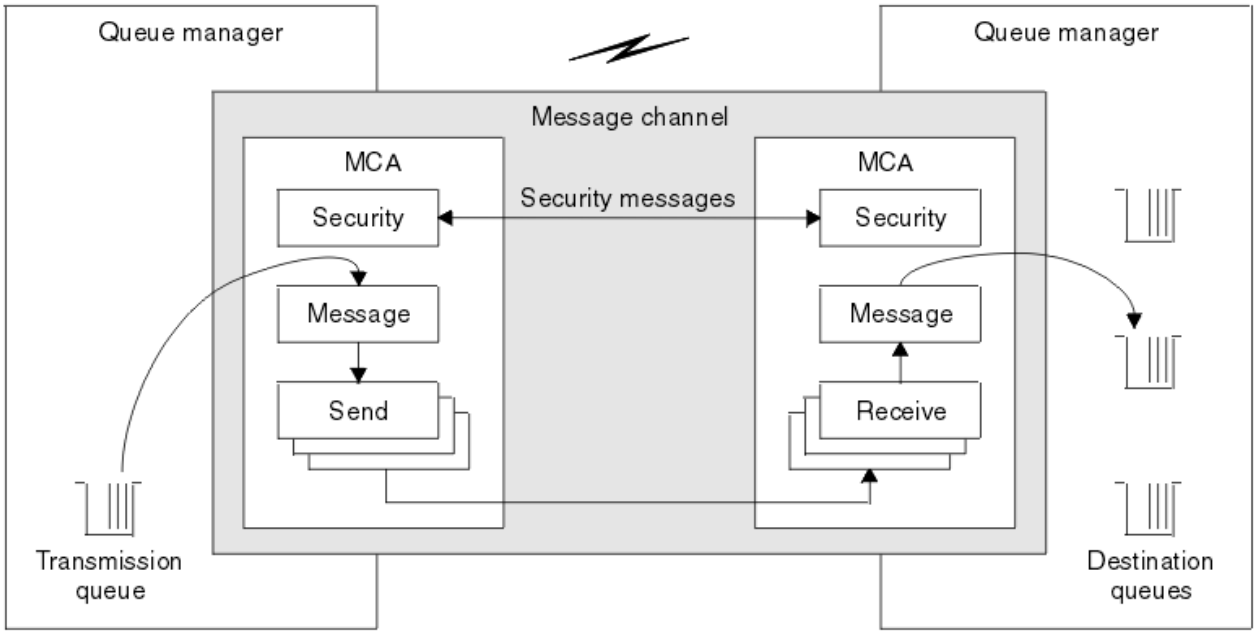
Programy obsługi wyjścia kanału

Programy obsługi wyjścia kanału to programy wywoływane w zdefiniowanych miejscach w sekwencji przetwarzania agenta MCA. Użytkownicy i dostawcy mogą tworzyć własne programy obsługi wyjścia kanału. Niektóre są dostarczane przez IBM.

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

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

Te cztery typy programów obsługi wyjścia kanału zostały zilustrowane w sekcji Rysunek 11 na stronie 117 i opisane w poniższych tematach.



Rysunek 11. Zabezpieczenia, komunikaty, wysyłanie i odbieranie wyjść w kanale komunikatów

Pojęcia pokrewne

Kanał-programy obsługi wyjścia dla kanałów przesyłania komunikatów

Przegląd wyjścia zabezpieczeń

Wyjścia zabezpieczeń zwykle działają w parach. Są one wywoływane przed przepływem komunikatów, a ich celem jest umożliwienie agentowi MCA uwierzytelnienia swojego partnera.

Wyjścia zabezpieczeń zwykle działają w parach, po jednym na każdym końcu kanału. Są one wywoływane natychmiast po zakończeniu początkowej negocjacji danych podczas uruchamiania kanału, ale przed rozpoczęciem przepływu komunikatów. Podstawowym celem wyjścia zabezpieczeń jest włączenie agenta MCA na każdym końcu kanału w celu uwierzytelnienia jego partnera. Nie ma jednak nic, co uniemożliwiłoby wyjściu zabezpieczeń wykonanie innej 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 wyników wymiany komunikatów bezpieczeństwa jest fakt, że jedno z wyjść zabezpieczeń może nie kontynuować działania. W takim przypadku kanał jest zamknięty i komunikaty nie przepływają. Jeśli istnieje wyjście zabezpieczeń tylko na jednym końcu kanału, wyjście jest nadal wywoływane i można wybrać, czy kontynuować, czy zamknąć kanał.

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 114.

Wyjście komunikatu

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

Wyjścia komunikatów na końcach wysyłających i odbierających kanału działają normalnie w parach. Wyjście komunikatu na wysyłającym końcu kanału jest wywoływane po otrzymaniu przez agent MCA komunikatu z kolejki transmisji. Na odbierającym końcu kanału jest wywoływane wyjście komunikatu, zanim agent MCA umieści komunikat w swojej 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

modyfikować treść komunikatu i zmieniać jego długość. Zmiana długości może być wynikiem kompresji, dekompresji, szyfrowania lub deszyfrowania komunikatu. Może to być również wynikiem dodania danych do komunikatu lub usunięcia z niego danych.

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

Wyjście komunikatu może określić, że komunikat, który jest obecnie przetwarzany, nie powinien być dalej przetwarzany w kierunku jego miejsca docelowego. Następnie agent MCA umieszcza komunikat w kolejce niedostarczonych 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 umożliwienie przepływu parametrów wejściowych i wyjściowych wywołań MQI 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 po sobie.

Więcej informacji na temat wyjść komunikatów zawiera sekcja “Zabezpieczenia na poziomie łącza przy użyciu wyjścia komunikatu” na stronie 114.

Wyjścia wysyłania i odbierania

Wyjścia wysyłania i odbierania zwykle działają w parach. Działają one na segmentach transmisji i są najlepiej wykorzystywane, gdy struktura przetwarzanych przez nie danych nie ma znaczenia.

Wyjście wysyłania na jednym końcu kanału i *wyjście odbierania* na drugim końcu normalnie działają w parach. Wyjście wysyłania jest wywoływane tuż przed wysłaniem przez agenta MCA komunikatu komunikacyjnego w celu wysłania danych za pośrednictwem połączenia komunikacyjnego. Wyjście odbierania jest wywoływane tuż po odzyskaniu sterowania przez agent MCA po odebraniu komunikacji i odebraniu danych z połączenia komunikacyjnego. Jeśli używane są konwersacje współużytkowane, w kanale MQI dla każdej konwersacji wywoływana jest inna instancja wyjścia wysyłania i odbierania.

Protokół kanału IBM MQ przepływa między dwiema konsolami HMC w kanale komunikatów zawiera informacje sterujące oraz dane komunikatów. Podobnie w przypadku kanału MQI przepływy zawierają informacje sterujące oraz parametry wywołań MQI. Wyjścia nadawcze i odbiorcze są wywoływane dla wszystkich typów danych.

Dane komunikatu przepływają tylko w jednym kierunku w kanale komunikatów, ale w kanale MQI parametry wejściowe przepływu wywołania MQI w jednym kierunku i parametry wyjściowe w drugim. Zarówno w kanałach komunikatów, jak i MQI, informacje sterujące przepływają w obu kierunkach. W rezultacie wyjścia wysyłania i odbierania mogą być wywoływane na obu końcach kanału.

Jednostka danych przesyłanych w pojedynczym przepływie między dwiema konsolami HMC jest nazywana *segmentem transmisji*. Wyjścia nadawcze i odbiorcze mają dostęp do każdego segmentu transmisji. Mogą modyfikować jego zawartość i zmieniać jego długość. Jednak wyjście wysyłania nie może zmieniać pierwszych 8 bajtów segmentu transmisji. Te 8 bajtów stanowi część nagłówka protokołu kanału IBM MQ . Istnieją również ograniczenia dotyczące stopnia, w jakim wyjście wysyłania może zwiększyć długość segmentu transmisji. W szczególności program obsługi wyjścia wysyłania nie może zwiększyć swojej długości poza maksymalną długość wynegocjowaną między dwiema konsolami MCA podczas uruchamiania kanału.

W przypadku kanału komunikatów, jeśli komunikat jest zbyt duży, aby można go było wysłać w pojedynczym segmencie transmisji, wysyłający agent MCA dzieli komunikat i wysyła go w więcej niż jednym segmencie transmisji. W związku z tym wyjście wysyłania jest wywoływane dla każdego segmentu transmisji zawierającego część komunikatu, a na końcu odbierania jest wywoływane wyjście odbierania dla każdego segmentu transmisji. Odbierający agent MCA ponownie uzgadnia 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 wystąpić na przykład w przypadku wywołania MQPUT, MQPUT1lub MQGET, jeśli dane aplikacji są wystarczająco duże.

Biorąc powyższe pod uwagę, bardziej właściwe jest użycie wyjść wysyłania i odbierania do celów, w których nie muszą one rozumieć struktury danych, które są przez nie przetwarzane, a zatem mogą traktować każdy segment transmisji jako obiekt binarny.

Wyjście wysyłania lub odbierania może zamknąć kanał.

Nazwy wyjścia wysyłania i wyjścia odbierania są określane jako parametry w definicji kanału na każdym końcu kanału. Można również określić listę wyjść wysyłania, które mają być uruchamiane po sobie. Podobnie można określić listę wyjść odbierania.

Więcej informacji na temat wyjść wysyłania i odbierania zawiera sekcja "Zabezpieczenia na poziomie łącza przy użyciu wyjść wysyłania i odbierania" na stronie 114.

Planowanie integralności danych

Zaplanuj sposób zachowania integralności danych.

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

Na poziomie aplikacji można używać programów obsługi wyjścia funkcji API, jeśli standardowe narzędzia nie spełniają wymagań. Do cyfrowego podpisywania komunikatów można używać serwera Advanced Message Security (AMS) w celu ochrony przed nieautoryzowaną modyfikacją.

Na poziomie łącza można wybrać użycie protokołu TLS. W takim przypadku należy zaplanować użycie certyfikatów cyfrowych. Jeśli standardowe narzędzia nie spełniają wymagań, można również użyć programów obsługi wyjścia kanału.

Pojęcia pokrewne

"Zabezpieczanie kanałów za pomocą protokołu SSL/TLS" na stronie 123
Obsługa protokołu TLS w produkcie IBM MQ używa obiektu informacji uwierzytelniającej menedżera kolejek i różnych komend MQSC. Należy również wziąć pod uwagę użycie certyfikatów cyfrowych.

"Integralność danych" na stronie 10
Usługa *integralności danych* wykrywa, czy nastąpiła nieautoryzowana modyfikacja danych.

"Planowanie Advanced Message Security" na stronie 115
Advanced Message Security (AMS) jest komponentem produktu IBM MQ , który zapewnia wysoki poziom ochrony danych wrażliwych przepływających przez sieć IBM MQ , nie wpływając jednocześnie na aplikacje końcowe.

Odsyłacze pokrewne

Odwołanie do wyjścia funkcji API

Wywołania wyjścia kanału i struktury danych

Planowanie kontroli

Zdecyduj, jakie dane mają być kontrolowane, a także w jaki sposób przechwytywać i przetwarzać informacje z kontroli. Należy rozważyć, jak sprawdzić, czy system jest poprawnie skonfigurowany.

Istnieje kilka aspektów monitorowania działań. Aspekty, które należy wziąć pod uwagę, są często definiowane przez wymagania audytora, a te wymagania są często oparte na standardach prawnych, takich jak HIPAA (Health Insurance Portability and Accountability Act) lub SOX (Sarbanes-Oxley). IBM MQ udostępnia funkcje ułatwiające zachowanie zgodności z takimi standardami.

Należy rozważyć, czy użytkownik jest zainteresowany tylko wyjątkami, czy też wszystkimi zachowaniami systemu.

Niektóre aspekty kontroli mogą być również traktowane jako monitorowanie operacyjne; jednym z wyróżnień dla kontroli jest to, że często przeglądane są dane historyczne, a nie tylko alerty w czasie rzeczywistym. Monitorowanie zostało opisane w sekcji Monitorowanie i wydajność.

Jakie dane należy skontrolować

Należy rozważyć, jakie typy danych lub działań mają być kontrolowane, zgodnie z opisem w następujących sekcjach:

Zmiany wprowadzone w pliku IBM MQ za pomocą interfejsów IBM MQ
Skonfiguruj produkt IBM MQ do wywoływania zdarzeń instrumentacji, w szczególności zdarzeń komend i zdarzeń konfiguracji.

Zmiany wprowadzone w pliku IBM MQ poza jego kontrolą
Niektóre zmiany mogą mieć wpływ na zachowanie programu IBM MQ , ale nie mogą być bezpośrednio monitorowane przez program 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 użytkownika obsługi wyjścia, oraz zmiany uprawnień do plików. Aby monitorować te działania, należy użyć narzędzi działających na poziomie systemu operacyjnego. Dostępne są różne narzędzia odpowiednie dla różnych systemów operacyjnych. Dzienniki mogą być również tworzone przez powiązane narzędzia, takie jak *sudo*.

Kontrola operacyjna 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 można skonfigurować do wystawiania zdarzeń instrumentacji.

Działanie aplikacji w produkcie IBM MQ
Aby kontrolować działania aplikacji, na przykład otwieranie kolejek oraz umieszczanie i pobieranie komunikatów, należy skonfigurować produkt IBM MQ do wysyłania odpowiednich zdarzeń.

Alerty intruza
Aby kontrolować próby naruszenia zabezpieczeń, należy skonfigurować system w taki sposób, aby generował zdarzenia autoryzacji. Zdarzenia kanału mogą być również przydatne do wyświetlania aktywności, szczególnie w przypadku nieoczekiwanego zakończenia kanału.

Planowanie przechwytywania, wyświetlania i archiwizowania danych kontroli

Wiele potrzebnych elementów jest raportowanych jako komunikaty zdarzeń IBM MQ . Należy wybrać narzędzia, które mogą odczytywać i formatować te komunikaty. Jeśli użytkownik jest zainteresowany długoterminową pamięcią masową i analizą, musi przenieść je do pomocniczego mechanizmu pamięci masowej, takiego jak baza danych. Jeśli te komunikaty nie zostaną przetworzone, pozostaną w kolejce zdarzeń, prawdopodobnie zapełniając ją. Użytkownik może zdecydować o zaimplementowaniu narzędzia, które automatycznie podejmuje działania w oparciu o niektóre zdarzenia, na przykład w celu wysłania alertu w przypadku wystąpienia awarii zabezpieczeń.

Sprawdzanie, czy system jest poprawnie skonfigurowany

Wraz z produktem IBM MQ Explorerdostarczany jest zestaw testów. Służą one do sprawdzania definicji obiektów pod kątem występowania problemów.

Ponadto należy okresowo sprawdzać, czy konfiguracja systemu jest taka sama, jak oczekiwano. Chociaż zdarzenia komend i konfiguracji mogą zgłaszać zmiany, przydatne jest również wykonanie zrzutu konfiguracji i porównanie jej ze znaną, dobrą kopią.

Planowanie bezpieczeństwa według topologii

W tej sekcji opisano zabezpieczenia w konkretnych sytuacjach, a mianowicie w przypadku kanałów, klastrów menedżera kolejek, aplikacji publikowania/subskrypcji i rozsyłania grupowego oraz 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 IBM MQ . Agenty kanału komunikatów (Message Channel Agents-MCA) to zasadniczo aplikacje IBM MQ , które przenoszą komunikaty między menedżerami kolejek i w związku z tym do poprawnego działania wymagają dostępu do różnych zasobów systemu IBM MQ .

Aby odbierać komunikaty w czasie wykonywania operacji PUT dla agentów MCA, można użyć identyfikatora użytkownika powiązanego z agentem MCA lub identyfikatora użytkownika powiązanego z komunikatem.

W czasie połączenia (CONNECT) można odwzorować sprawdzony identyfikator użytkownika na alternatywnego użytkownika, używając rekordów uwierzytelniania kanału **CHLAUTH** .

W produkcie IBM MQkanały mogą być chronione przez obsługę protokołu TLS.

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

- Identyfikator użytkownika powiązany z kanałem nadawczym wymaga dostępu do menedżera kolejek, kolejki transmisji, kolejki niedostarczonych komunikatów oraz dostępu do wszystkich innych zasobów wymaganych przez wyjścia kanału.
- Identyfikator użytkownika MCAUSER kanału odbiorczego wymaga uprawnienia *+ setall* . Przyczyną jest fakt, że kanał odbiorczy musi utworzyć pełną strukturę MQMD, w tym wszystkie pola kontekstu, przy użyciu danych odebranych ze zdalnego kanału nadawczego. Dlatego menedżer kolejek wymaga, aby użytkownik wykonujący to działanie miał uprawnienie *+ setall* . To uprawnienie *+ setall* musi zostać nadane użytkownikowi dla:
  - 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 nadawca zażądał komunikatu raportu COA, wymaga uprawnienia *+ passid* w kolejce transmisji, która zwraca komunikat raportu. Bez tego uprawnienia rejestrowane są komunikaty o błędach AMQ8077 .
- Korzystając z identyfikatora użytkownika powiązanego z kanałem odbiorczym, można otworzyć kolejki docelowe w celu umieszczenia komunikatów w kolejkach. Dotyczy to interfejsu kolejkowania komunikatów (Message queuing Interface-MQI), dlatego może być konieczne wykonanie dodatkowych sprawdzeń kontroli dostępu, jeśli nie jest używany menedżer IBM MQ Object Authority Manager (OAM). Można określić, czy sprawdzanie autoryzacji ma być wykonywane dla identyfikatora użytkownika powiązanego z agentem MCA (zgodnie z opisem w tym temacie), czy dla identyfikatora użytkownika powiązanego z komunikatem (z pola UserIdentifier MQMD).

  W przypadku typów kanałów, do których ma zastosowanie, parametr **PUTAUT** definicji kanału określa, który ID użytkownika jest używany na potrzeby tych sprawdzeń.
  - Domyślnym ustawieniem kanału jest użycie konta usługi menedżera kolejek, które ma pełne prawa administracyjne i nie wymaga specjalnych autoryzacji.
  - W przypadku kanałów połączenia z serwerem połączenia administracyjne są domyślnie blokowane przez reguły CHLAUTH i wymagają jawnego udostępniania.
  - Kanały typu odbiornik, requester i odbiornik klastra umożliwiają lokalne administrowanie przez dowolny sąsiedni menedżer kolejek, chyba że administrator podejmie kroki w celu ograniczenia tego dostępu.
  - Nie jest konieczne nadawanie uprawnień *dsp* i *ctrlx* dla identyfikatora użytkownika MCAUSER kanału odbiorczego.
  - W przypadku wersji wcześniejszych niż 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 temu identyfikatorowi użytkownika, aby kanał mógł działać.

    W systemie IBM MQ 8.0.0 Fix Pack 4nie są wykonywane żadne sprawdzenia uprawnień, gdy kanał jest resynchronizowany i koryguje numery kolejne.

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

Ostrzeżenie: Jeśli do potwierdzenia zadania wsadowego komunikatu wymagany jest reset kanału, program IBM MQ próbuje wysłać zapytanie do kanału, który wymaga uprawnienia **+dsp** .

- Atrybut MCAUSER nie jest używany dla typu kanału SDR.
- Jeśli używany jest identyfikator użytkownika powiązany z komunikatem, prawdopodobnie pochodzi on z systemu zdalnego. Ten ID użytkownika systemu zdalnego musi być rozpoznawany przez system docelowy. Poniższe komendy są przykładami typów komend, które można wydać w celu nadania uprawnień do ID 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 ID użytkownika do umieszczania komunikatów w kolejce komend lub w innych ważnych kolejkach systemowych.

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

Agent MCA programu wywołującego
Adaptery MCA, które inicjują kanał. Wywołujące adaptery MCA mogą być uruchamiane jako pojedyncze procesy, jako wątki inicjatora kanału lub jako wątki puli procesów. Używany identyfikator użytkownika jest identyfikatorem użytkownika powiązanym z procesem nadrzędnym (inicjatorem kanału) lub identyfikatorem użytkownika powiązanym z procesem, który uruchamia agent MCA.

Agent MCA odpowiadający
Odpowiadające adaptery MCA to adaptery MCA, które są uruchamiane w wyniku żądania przez wywołujący agent MCA. Odpowiadające adaptery MCA mogą być uruchamiane jako pojedyncze procesy, jako wątki procesu nasłuchującego lub jako wątki puli procesów. Identyfikator użytkownika może mieć jeden z następujących typów (w tej kolejności preferencji):

1. W komunikacji APPC wywołujący agent MCA może wskazać identyfikator użytkownika, który ma być używany dla odpowiadającego agenta MCA. Jest to nazywane ID użytkownika sieci i ma zastosowanie tylko do kanałów uruchomionych jako pojedyncze procesy. Ustaw ID użytkownika sieci za pomocą parametru USERID w definicji kanału.
2. Jeśli parametr **USERID** nie jest używany, definicja kanału odpowiadającego agenta MCA może określać identyfikator użytkownika, którego musi używać agent MCA. Identyfikator użytkownika można ustawić za pomocą parametru **MCAUSER** definicji kanału.
3. Jeśli identyfikator użytkownika nie został ustawiony za pomocą żadnej z powyższych (dwóch) metod, używany jest identyfikator użytkownika procesu, który uruchamia agent MCA lub identyfikator użytkownika procesu nadrzędnego (proces nasłuchujący).

Pojęcia pokrewne

“Rekordy uwierzytelniania kanału” na stronie 53
Aby umożliwić bardziej precyzyjną kontrolę na poziomie kanału nad dostępem przydzielonym do systemów, które nawiązują połączenie, można użyć rekordów uwierzytelniania kanału.

Odsyłacze pokrewne

Właściwości rekordu uwierzytelniania kanału

Zabezpieczanie definicji inicjatora kanału
Tylko członkowie grupy mqm mogą manipulować inicjatorami kanału.

IBM MQ inicjatory kanałów 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 ID użytkownika jest członkiem grupy mqm. Jeśli aplikacja wywołuje komendę PCF **StartChannelInitiator**, ID użytkownika określony w deskryptorze komunikatu PCF musi być członkiem grupy mqm w docelowym menedżerze kolejek.

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

Kolejki transmisji
Menedżery kolejek automatycznie umieszczają komunikaty zdalne w kolejce transmisji; w tym celu nie są wymagane żadne uprawnienia specjalne.

Jeśli jednak konieczne jest umieszczenie komunikatu bezpośrednio w kolejce transmisji, wymaga to specjalnej autoryzacji; patrz sekcja Tabela 12 na stronie 141.

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

Więcej informacji na temat wyjść kanałów zawiera sekcja “Programy obsługi wyjścia kanału” na stronie 116 .

Zabezpieczanie kanałów za pomocą protokołu SSL/TLS
Obsługa protokołu TLS w produkcie IBM MQ używa obiektu informacji uwierzytelniającej menedżera kolejek i różnych komend MQSC. Należy również wziąć pod uwagę użycie certyfikatów cyfrowych.

Certyfikaty cyfrowe i repozytoria kluczy

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

Jeśli potrzeba wielu kanałów z certyfikatami, które różnią się od domyślnego zestawu certyfikatów w menedżerze kolejek, należy rozważyć podzielenie kanałów między kilka menedżerów kolejek lub użycie proxy MQIPT przed menedżerem kolejek w celu przedstawienia innego certyfikatu.

Dla każdego kanału można użyć innego certyfikatu, ale jeśli w repozytorium kluczy przechowywanych jest zbyt wiele certyfikatów, uruchomienie kanałów TLS może mieć wpływ na wydajność. Staraj się utrzymać liczbę certyfikatów w repozytorium kluczy poniżej 50 i uznaj 100 za wartość maksymalną, ponieważ wydajność programu IBM Global Security Kit (GSKit) gwałtownie spada w przypadku większych repozytoriów kluczy.

Zezwolenie na wiele certyfikatów w tym samym menedżerze kolejek zwiększa prawdopodobieństwo, że w tym samym menedżerze kolejek zostanie użytych wiele certyfikatów CA. Zwiększa to prawdopodobieństwo konfliktów przestrzeni nazw nazwy wyróżniającej podmiotu certyfikatu dla certyfikatów wydawanych przez osobne ośrodki certyfikacji.

Podczas gdy profesjonalne ośrodki certyfikacji są prawdopodobnie bardziej ostrożne, wewnętrzne ośrodki certyfikacji często nie mają jasnych konwencji nazewnictwa i mogą wystąpić niezamierzone dopasowania między ośrodkiem certyfikacji.

Oprócz nazwy wyróżniającej podmiotu należy sprawdzić nazwę wyróżniającą wystawcy certyfikatu. W tym celu należy użyć rekordu uwierzytelniania kanału SSLPEERMAP i ustawić pola **SSLPEER** i **SSLCERTI** na zgodne odpowiednio z nazwą wyróżniającą podmiotu i nazwą wyróżniającą wystawcy.

Certyfikaty samopodpisane i podpisane przez ośrodek CA

Ważne jest, aby zaplanować wykorzystanie certyfikatów cyfrowych, zarówno podczas tworzenia i testowania aplikacji, jak i do jej wykorzystania w środowisku produkcyjnym. W zależności od użycia menedżerów kolejek i aplikacji klienckich można używać certyfikatów podpisanych przez ośrodek CA lub certyfikatów samopodpisanych.

Certyfikaty podpisane przez ośrodek CA
W przypadku systemów produkcyjnych należy uzyskać certyfikaty od zaufanego ośrodka certyfikacji (CA). Po uzyskaniu certyfikatu z zewnętrznego ośrodka CA należy zapłacić za usługę.

Certyfikaty samopodpisane
Podczas tworzenia aplikacji można używać samopodpisanych certyfikatów lub certyfikatów wydanych przez lokalny ośrodek CA, w zależności od platformy:

W systemach AIX, Linux, and Windows można używać certyfikatów samopodpisanych. Instrukcje znajdują się w sekcji “Tworzenie samopodpisanego certyfikatu osobistego w systemie AIX, Linux, and Windows” na stronie 327.

W systemach IBM i można używać certyfikatów podpisanych przez lokalny ośrodek CA. Instrukcje znajdują się w sekcji “Żądanie certyfikatu serwera w systemie IBM i” na stronie 304 .

W systemie z/OSmożna używać samopodpisanych lub lokalnych certyfikatów podpisanych przez ośrodek CA. Instrukcje znajdują się w sekcji “Tworzenie samopodpisanego certyfikatu osobistego w systemie z/OS” na stronie 356 lub “Żądanie certyfikatu osobistego w systemie z/OS” na stronie 357 .

Certyfikaty samopodpisane nie nadają się do użytku produkcyjnego z następujących powodów:

- Nie można unieważnić samopodpisanych certyfikatów, co może umożliwić atakującemu podszywanie się pod tożsamość po naruszeniu klucza prywatnego. Ośrodki CA mogą unieważnić certyfikat z naruszoną ochroną, co uniemożliwia dalsze korzystanie z niego. Certyfikaty podpisane przez ośrodek CA są zatem bezpieczniejsze w środowisku produkcyjnym, chociaż certyfikaty samopodpisane są wygodniejsze w systemie testowym.
- Certyfikaty samopodpisane 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 związane z faktem, że nie można unieważnić samopodpisanych certyfikatów.
- Certyfikat samopodpisany jest używany zarówno jako certyfikat osobisty, jak i główny (lub zaufany) certyfikat ośrodka CA. Użytkownik z samopodpisanym certyfikatem osobistym może używać go do podpisywania innych certyfikatów osobistych. Ogólnie rzecz biorąc, nie jest to prawdą w przypadku certyfikatów osobistych wystawionych przez ośrodek CA i stanowi znaczące narażenie.

CipherSpecs i certyfikaty cyfrowe

Tylko podzbiór obsługiwanych CipherSpecs może być używany ze wszystkimi obsługiwanymi typami certyfikatów cyfrowych. Dlatego konieczne jest wybranie odpowiedniej CipherSpec dla certyfikatów cyfrowych. Podobnie, jeśli strategia bezpieczeństwa organizacji wymaga użycia konkretnej CipherSpec , należy uzyskać odpowiednie certyfikaty cyfrowe.

Więcej informacji na temat relacji między CipherSpecs i certyfikatami cyfrowymi zawiera sekcja “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48 .

Strategie sprawdzania poprawności certyfikatów

Standard IETF RFC 5280 określa serię reguł sprawdzania poprawności certyfikatów, które muszą zostać zaimplementowane przez zgodne oprogramowanie aplikacji, aby zapobiec atakom personifikacji. Zestaw reguł sprawdzania poprawności certyfikatów jest znany jako strategia sprawdzania poprawności certyfikatów. Więcej informacji na temat strategii sprawdzania poprawności certyfikatów w programie

IBM MQzawiera sekcja “Strategie sprawdzania poprawności certyfikatów w programie IBM MQ” na stronie 46.

Planowanie sprawdzania odwołań certyfikatów

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

W szczególności, jeśli jawnie skonfigurowano użycie serwera odwołań z konkretnego ośrodka CA, na przykład za pomocą obiektu AUTHINFO lub struktury rekordu informacji uwierzytelniającej (MQAIR), sprawdzenie odwołania nie powiedzie się, jeśli zostanie zaprezentowany certyfikat z innego ośrodka CA.

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

Więcej informacji na ten temat zawierają OCSPCheckExtensions i CDPCheckExtensions.

Komendy i atrybuty obsługi protokołu 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 żądanego typu zabezpieczeń, takie jak algorytm szyfrowania, który ma być używany.

- Następujące komendy MQSC obsługują protokół TLS:

  ZMIEŃ INFORMACJE O AUTORYZACJI
  Modyfikuje atrybuty obiektu informacji uwierzytelniającej.

  ZDEFINIUJ INFORMACJE O AUTORYZ.
  Tworzy obiekt informacji uwierzytelniającej.

  USUŃ INFORMACJE O AUTORYZ
  Usuwa obiekt informacji uwierzytelniającej.

  WYŚWIETL INFORMACJE O AUTORYZ
  Wyświetla atrybuty konkretnego obiektu informacji uwierzytelniającej.

- Następujące parametry menedżera kolejek obsługują protokół TLS:

  CERTLABL
  Definiuje etykietę certyfikatu osobistego, która ma być używana.

  V 9.3.0 V 9.3.0 **PPWD KLUCZA**
  W systemach AIX, Linux, and Windows definiuje hasło używane przez program IBM MQ do uzyskania dostępu do repozytorium kluczy. To pole jest szyfrowane przy użyciu systemu zabezpieczania hasłem.

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

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

  SSLEV
  Określa, czy komunikat zdarzenia TLS jest zgłaszany, jeśli kanał korzystający z protokołu TLS nie może nawiązać połączenia TLS.

  SSLFIPS
  Określa, czy mają być używane tylko algorytmy z certyfikatem FIPS, jeśli szyfrowanie jest wykonywane w produkcie IBM MQ , a nie w sprzęcie szyfrującym. Jeśli sprzęt szyfrujący jest

skonfigurowany, używane są moduły szyfrujące udostępniane przez produkt sprzętowy, które mogą mieć certyfikat FIPS na określonym poziomie. Zależy to od używanego produktu sprzętowego.

SSLKEYR
W systemach AIX, Linux, and Windows wiąże repozytorium kluczy z menedżerem kolejek. GSKit umożliwia korzystanie z zabezpieczeń TLS w systemach AIX, Linux, and Windows .

SSLRKEYC
Liczba bajtów do wysłania i odebrania 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 program IBM MQ wymaga i sprawdza poprawność certyfikatu pochodzącego od klienta TLS.

SSLCIPH
Określa siłę i funkcję szyfrowania (CipherSpec), na przykład TLS_RSA_WITH_AES_128_CBC_SHA. Wartość CipherSpec musi być zgodna na obu końcach kanału.

SSLPEER
Określa nazwę wyróżniającą (unikalny identyfikator) dozwolonych partnerów.

W tej sekcji opisano komendy **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg**i **dspmqfls** służące do obsługi obiektu informacji uwierzytelniającej. Opisano także komendy **runmqckm** (iKeycmd) i **runmqakm** służące do zarządzania certyfikatami w systemie AIX, Linux, and Windows. Patrz następujące sekcje:

- setmqaut (setmqaut)
- dspmqaut
- dmpmqaut (dmpmqaut)
- rcrmqobj (obiekt Rcrmqobj)
- rcdmqimg
- dspmqfls (komenda dspmqfls)
- Zarządzanie kluczami i certyfikatami

Przegląd zabezpieczeń kanału przy użyciu protokołu TLS znajduje się w sekcji

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

Szczegółowe informacje na temat komend MQSC powiązanych z protokołem TLS zawiera sekcja

- ZMIEŃ INFORMACJE AUTORYZ.
- DEFINIOWANIE INFORMACJI O AUTORYZ
- USUŃ INFORMACJE O AUTORYZ.
- WYŚWIETL INFORMACJE O AUTORYZ

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

Kanał SVRCONN systemu IBM MQ for z/OS nie jest zabezpieczony bez zaimplementowania uwierzytelniania kanału lub dodania wyjścia zabezpieczeń przy użyciu protokołu TLS. Kanały SVRCONN nie mają domyślnie zdefiniowanego wyjścia zabezpieczeń.

Zagadnienia związane z bezpieczeństwem

Kanały SVRCONN nie są chronione zgodnie z początkowym definicją, SYSTEM.DEF.SVRCONN . Aby zabezpieczyć kanał SVRCONN, należy skonfigurować uwierzytelnianie kanału za pomocą komendy SET CHLAUTH lub zainstalować wyjście zabezpieczeń i zaimplementować protokół TLS.

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

Dostępnych jest kilka przykładów, których można użyć jako dobrego punktu początkowego do napisania własnego wyjścia zabezpieczeń kanału SVRCONN.

W systemie IBM MQ for z/OSpodzbiór CSQ4BCX3 w bibliotece hlq.SCSQC37S jest przykładem wyjścia zabezpieczeń napisanym w języku C. Przykładowy plik CSQ4BCX3 jest również dostarczany wstępnie skompilowany w bibliotece hlq.SCSQAUTH .

Przykładowe wyjście CSQ4BCX3 można zaimplementować, kopiując skompilowany podzbiór hlq.SCSQAUTH(CSQ4BCX3) do biblioteki ładowania, która jest przydzielona do definicji danych CSQXLIB w procesie CHIN. Należy zauważyć, że CHIN wymaga, aby biblioteka ładowania była ustawiona jako "sterowana przez program".

Zmień kanał SVRCONN, aby ustawić CSQ4BCX3 jako wyjście zabezpieczeń.

Gdy klient łączy się przy użyciu tego kanału SVRCONN, CSQ4BCX3 uwierzytelnia się przy użyciu pary **RemoteUserIdentifier** i **RemotePassword** z MQCD lub, z IBM MQ for z/OS 9.1.4, pary **CSPUserIdPtr** i **CSPPasswordPtr** z MQCSP. Jeśli uwierzytelnianie zakończy się pomyślnie, program **RemoteUserIdentifier** zostanie skopiowany do katalogu **MCAUserIdentifier**, co spowoduje zmianę kontekstu tożsamości wątku.

W systemach Long Term Support i Continuous Delivery przed IBM MQ for z/OS 9.1.4, gdy klient łączy się przy użyciu tego kanału SVRCONN, CSQ4BCX3 uwierzytelni się przy użyciu pary **RemoteUserIdentifier** i **RemotePassword** z MQCD. Jeśli uwierzytelnianie zakończy się pomyślnie, program **RemoteUserIdentifier** zostanie skopiowany do katalogu **MCAUserIdentifier**, co spowoduje zmianę kontekstu tożsamości wątku.

W przypadku pisania klienta IBM MQ Java można użyć okien wywoływanych, aby wysłać zapytanie do użytkownika i ustawić wartości MQEnvironment.userID i MQEnvironment.password. Te wartości zostaną przekazane po nawiązaniu połączenia.

Teraz, gdy istnieje funkcjonalne wyjście zabezpieczeń, istnieje dodatkowa obawa, że identyfikator użytkownika i hasło są przesyłane w postaci jawnego tekstu przez sieć podczas nawiązywania połączenia, podobnie jak treść kolejnych komunikatów IBM MQ . Za pomocą protokołu TLS można zaszyfrować te początkowe informacje o połączeniu, a także treść dowolnych komunikatów IBM MQ .

Przykład

Aby zabezpieczyć IBM MQ Explorer kanał SVRCONN SYSTEM.ADMIN.SVRCONN wykonaj następujące kroki:

1. Skopiuj plik hlq.SCSQAUTH(CSQ4BCX3) do biblioteki ładowania, która jest przydzielona do definicji danych CSQXLIB w procesie CHINIT.
2. Sprawdź, czy biblioteka ładowania jest sterowana przez program.
3. Zmień wartość systemową ADMIN.SVRCONN , aby użyć wyjścia zabezpieczeń CSQ4BCX3.
4. W programie IBM MQ Explorerkliknij prawym przyciskiem myszy nazwę menedżera kolejek z/OS , wybierz opcję **Szczegóły połączenia** > **Właściwości** > **ID użytkownika** i wprowadź ID użytkownika z/OS .
5. Połącz się z menedżerem kolejek z/OS , wprowadzając hasło.

Dodatkowe informacje

Aby wyjść z programu CSQ4BCX3 w celu uruchomienia w środowisku sterowanym przez program, wszystkie elementy załadowane do przestrzeni adresowej CHIN muszą być załadowane z biblioteki

sterowanej przez program, na przykład wszystkie biblioteki w bibliotece STEPLIB i wszystkie biblioteki wymienione w definicji danych CSQXLIB. Aby ustawić bibliotekę ładowania jako komendy RACF sterowane przez program (Program Controlled). W poniższym przykładzie nazwa biblioteki ładowania to 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 systemu 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 kanałów zawiera sekcja “Programy obsługi wyjścia kanału” na stronie 116 .

Zadania pokrewne

Pisanie programów obsługi wyjścia kanału w systemie z/OS

Usługi ochrony SNA LU 6.2

Jednostka logiczna SNA 6.2 obsługuje 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 SNA (Systems Network Architecture). Inna dokumentacja, o której mowa w niniejszej sekcji, zawiera krótkie wprowadzenie do odpowiednich pojęć i terminologii. Jeśli wymagane jest bardziej obszerne wprowadzenie techniczne do architektury SNA, należy zapoznać się z publikacją *Systems Network Architecture Technical Overview*(Przegląd techniczny architektury systemów sieciowych), GC30-3073.

Jednostka logiczna SNA 6.2 udostępnia trzy usługi ochrony:

- Szyfrowanie na poziomie sesji
- Uwierzytelnianie na poziomie sesji
- Uwierzytelnianie na poziomie konwersacji

Do szyfrowania na poziomie sesji i uwierzytelniania na poziomie sesji SNA używa 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.

Szyfrowanie na poziomie sesji
Szyfrowanie na poziomie sesji szyfruje i deszyfruje dane sesji przy użyciu algorytmu DES. Można go zatem użyć do zapewnienia usługi poufności na poziomie łącza w kanałach SNA LU 6.2 .

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

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

W *sesji szyfrowania selektywnego*jednostka logiczna szyfruje tylko jednostki żądań danych określone przez wysyłający program transakcyjny (TP). Wysyłająca jednostka logiczna sygnalizuje, że dane są szyfrowane przez ustawienie indykatora w nagłówku żądania. Zaznaczając ten indykator, odbierająca jednostka logiczna może określić, które jednostki żądań mają zostać zdeszyfrowane przed przekazaniem ich do odbierającego programu transakcyjnego.

W sieci SNA IBM MQ MCA są programami transakcyjnymi. Adaptery MCA nie żądają szyfrowania wysyłanych przez nie danych. Selektywne szyfrowanie danych nie jest więc dostępne; w sesji możliwe jest tylko obowiązkowe szyfrowanie danych lub nie jest możliwe żadne szyfrowanie danych.

Informacje na temat implementowania obowiązkowego szyfrowania danych zawiera dokumentacja podsystemu SNA. Zapoznaj się z tą samą dokumentacją, aby uzyskać informacje na temat silniejszych form szyfrowania, które mogą być używane na danej platformie, takich jak 24-bajtowe szyfrowanie Triple DES w systemie z/OS.

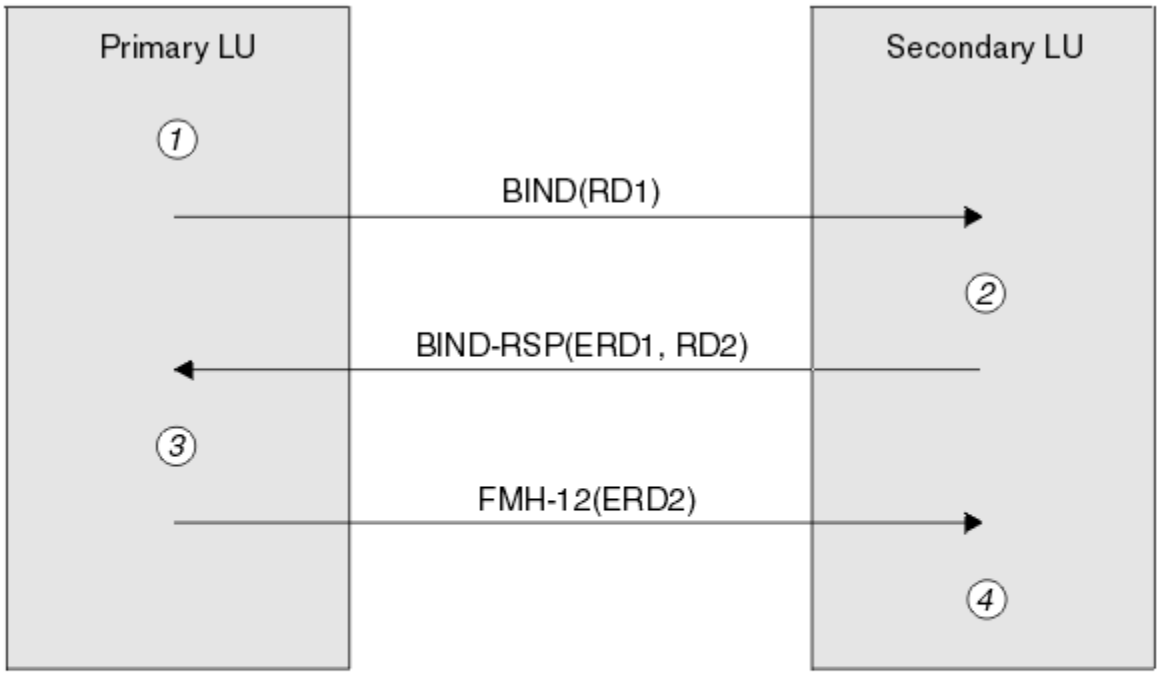
Więcej ogólnych informacji na temat szyfrowania na poziomie sesji zawiera sekcja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Uwierzytelnianie na poziomie sesji
Uwierzytelnianie na poziomie sesji jest protokołem bezpieczeństwa na poziomie sesji, który umożliwia dwóm jednostom logicznym uwierzytelnianie się podczas aktywowania sesji. Jest ona również nazywana *weryfikacją LU-LU*.

Ponieważ jednostka logiczna jest w rzeczywistości "bramą" do systemu z sieci, można uznać ten poziom uwierzytelniania za 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 na zaufanie tożsamości pozostałych komponentów systemu zdalnego po uwierzytelnieniu jednostki logicznej.

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

Rysunek 12 na stronie 129 przedstawia przepływy dla 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 uwierzytelniania na poziomie sesji jest następujący. Liczby w procedurze odpowiadają liczbie podanej w sekcji Rysunek 12 na stronie 129.

1. Podstawowa jednostka logiczna generuje losową wartość danych (RD1) i wysyła ją do wtórnej jednostki logicznej w żądaniu BIND.
2. Gdy drugorzędna jednostka logiczna otrzymuje żądanie BIND z danymi losowymi, szyfruje dane przy użyciu algorytmu DES z kopią hasła LU-LU jako klucza. Następnie wtórna jednostka logiczna generuje drugą losową wartość danych (RD2) i wysyła ją z zaszyfrowanymi danymi (ERD1) do podstawowej jednostki logicznej w odpowiedzi BIND.
3. Gdy podstawowa jednostka logiczna otrzymuje odpowiedź BIND, oblicza własną wersję zaszyfrowanych danych na podstawie pierwotnie wygenerowanych danych losowych. W tym celu należy użyć algorytmu DES z kopią hasła LU-LU jako klucza. Następnie porównuje swoją wersję z zaszyfrowanymi danymi odebranymi w odpowiedzi BIND. Jeśli te dwie wartości są takie same, podstawowa jednostka logiczna wie, że drugorzędna jednostka logiczna ma takie samo hasło, a dodatkowa jednostka logiczna jest uwierzytelniona. Jeśli dwie wartości nie są zgodne, podstawowa jednostka logiczna kończy sesję.

   Następnie podstawowa jednostka logiczna szyfruje dane losowe odebrane w odpowiedzi BIND i wysyła zaszyfrowane dane (ERD2) do wtórnej jednostki logicznej w nagłówku 12 zarządzania funkcjami (FMH-12).
4. Gdy drugorzędna jednostka logiczna otrzyma FMH-12, oblicza własną wersję zaszyfrowanych danych na podstawie wygenerowanych danych losowych. Następnie porównuje swoją wersję z zaszyfrowanymi danymi odebranymi w modelu FMH-12. Jeśli te dwie wartości są takie same, podstawowa jednostka logiczna jest uwierzytelniana. Jeśli te dwie wartości nie są zgodne, dodatkowa jednostka logiczna kończy sesję.

W rozszerzonej wersji protokołu, która zapewnia lepszą ochronę przed atakami człowieka w środku, dodatkowa jednostka logiczna oblicza kod uwierzytelniania komunikatu DES (MAC) z RD1, RD2i pełną nazwę drugorzędnej jednostki logicznej, używając jako klucza kopii hasła LU-LU. Drugorzędna jednostka logiczna wysyła kod MAC do podstawowej jednostki logicznej w odpowiedzi BIND zamiast ERD1.

Podstawowa jednostka logiczna uwierzytelnia dodatkową jednostkę logiczną, obliczając własną wersję kodu MAC, którą porównuje z kodem MAC odebranym w odpowiedzi BIND. Następnie podstawowa jednostka logiczna oblicza drugi kod MAC z systemu RD1 i RD2, a następnie wysyła kod MAC do drugorzędnej jednostki logicznej w FMH-12 zamiast ERD2.

Dodatkowa jednostka logiczna uwierzytelnia podstawową jednostkę logiczną, obliczając własną wersję drugiego kodu MAC, którą porównuje z kodem MAC odebranym w FMH-12.

Informacje na temat konfigurowania uwierzytelniania na poziomie sesji zawiera dokumentacja podsystemu SNA. Więcej ogólnych informacji na temat uwierzytelniania na poziomie sesji zawiera publikacja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Uwierzytelnianie na poziomie konwersacji
Gdy lokalny program transakcyjny próbuje przydzielić konwersację z partnerskim programem transakcyjnym, lokalna jednostka logiczna wysyła żądanie przyłączenia do partnerskiej jednostki logicznej, prosząc ją o przyłączenie partnerskiego programu transakcyjnego. W pewnych okolicznościach żądanie przyłączenia może zawierać informacje o ochronie, które mogą być używane przez partnerską jednostkę logiczną do uwierzytelniania lokalnego programu TP. Jest to nazywane *uwierzytelnianiem na poziomie konwersacji*lub *weryfikacją użytkownika końcowego*.

W poniższych tematach opisano, w jaki sposób produkt IBM MQ zapewnia obsługę uwierzytelniania na poziomie konwersacji.

Więcej informacji na temat uwierzytelniania na poziomie konwersacji zawiera publikacja *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Informacje specyficzne dla systemu z/OSmożna znaleźć w sekcji z/OS MVS Planning: APPC/MVS Management(Planowanie systemu MVS: Zarządzanie systemem APPC/MVS).

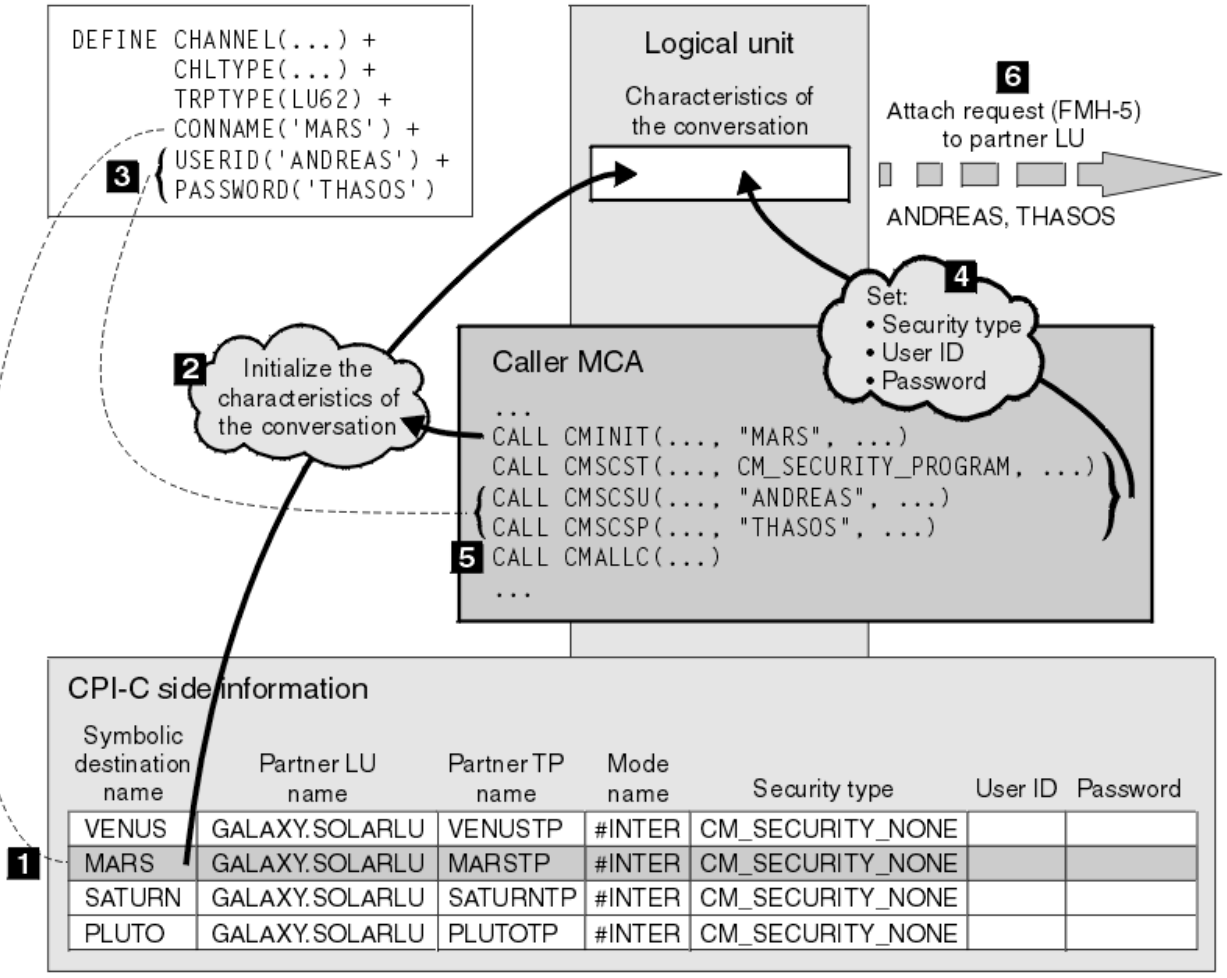
Więcej informacji na temat interfejsu CPI-C zawiera sekcja Korzystanie z komunikacji CPI.

Więcej informacji na temat usług APPC/MVS TP Conversation Callable Services zawiera sekcja APPC/MVS TP Conversation Callable Services.

Multi *Obsługa uwierzytelniania na poziomie konwersacji na wielu platformach*

Ten temat zawiera przegląd sposobu działania uwierzytelniania na poziomie konwersacji w systemie wieloplatformowym.

Obsługa uwierzytelniania na poziomie konwersacji w środowisku wieloplatformowym została zilustrowana w sekcji Rysunek 13 na stronie 131. Liczby na diagramie odpowiadają numerom w poniższym opisie.



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 systemie IBM MQ

W środowisku wieloplatformowym agent MCA używa wywołań Common Programming Interface Communications (CPI-C) do komunikacji 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 ubocznych CPI-C (1). Ta pozycja określa:

- Nazwa partnerskiej jednostki logicznej
- Nazwa partnerskiego programu TP, który jest odpowiadającym agentem MCA
- Nazwa trybu, który ma być używany dla konwersacji

Wpis informacji ubocznych może również określać następujące informacje o ochronie:

- 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.

Wywołujący agent MCA przygotowuje się do przydzielenia konwersacji z odpowiadającym agentem MCA przez wywołanie CPI-C CMINIT przy użyciu wartości CONNAME jako jednego z parametrów wywołania. Wywołanie CMINIT identyfikuje, z korzyścią dla lokalnej jednostki logicznej, pozycję informacji ubocznych, której agent MCA zamierza użyć na potrzeby konwersacji. Lokalna jednostka logiczna używa wartości z tej pozycji do inicjowania parametrów konwersacji (2).

Następnie wywołujący agent MCA sprawdza wartości parametrów USERID i PASSWORD w definicji kanału (3). Jeśli parametr USERID jest ustawiony, wywołujący agent MCA wysyła następujące wywołania CPI-C (4):

- CMSCST, aby ustawić typ zabezpieczeń dla konwersacji na CM_SECURITY_PROGRAM.
- CMSCSU, aby ustawić identyfikator użytkownika dla konwersacji na wartość USERID.
- CMSCSP, aby ustawić hasło dla konwersacji na wartość PASSWORD. 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 ubocznych.

Następnie wywołujący agent MCA 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 zaakceptuje ID użytkownika i hasło, wartości USERID i PASSWORD zostaną uwzględnione w żądaniu przyłączenia. Jeśli stowarzyszona jednostka logiczna nie akceptuje identyfikatora użytkownika i hasła, wartości nie są uwzględniane w żądaniu przyłączenia. Lokalna jednostka logiczna wykrywa, czy stowarzyszona jednostka logiczna będzie akceptować ID użytkownika i hasło w ramach wymiany informacji, gdy jednostki logiczne zostaną powiązane w celu utworzenia sesji.

W późniejszej wersji żądania przyłączenia substytut hasła może przepływać między jednostkami logicznymi zamiast jawnego hasła. Substytut hasła to kod uwierzytelniania komunikatu DES (MAC) lub skrót komunikatu SHA-1 utworzony na podstawie hasła. Zastępców haseł można używać tylko wtedy, gdy obsługują je obie jednostki logiczne.

Gdy stowarzyszona jednostka logiczna otrzyma przychodzące żądanie przyłączenia zawierające identyfikator użytkownika i hasło, może użyć tego identyfikatora użytkownika i hasła do celów identyfikacji i uwierzytelniania. Odwołując się do list kontroli dostępu, stowarzyszona jednostka logiczna może również określić, czy identyfikator użytkownika ma uprawnienie do przydzielania konwersacji i przyłączania odpowiadającego agenta MCA.

Ponadto agent MCA odpowiadający może działać z identyfikatorem użytkownika uwzględnionym w żądaniu przyłączenia. W takim przypadku identyfikator użytkownika staje się domyślnym identyfikatorem odpowiadającego agenta MCA i jest używany do sprawdzania uprawnień, gdy agent MCA próbuje nawiązać połączenie z menedżerem kolejek. Może być również używana 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, jest zależny od implementacji. Informacje specyficzne dla podsystemu SNA można znaleźć w odpowiedniej dokumentacji.

Jeśli USERID nie jest ustawiony, wywołujący agent MCA nie wywoła CMSCST, CMSCSU i CMSCSP. W takim przypadku informacje o zabezpieczeniach, które przepływają w żądaniu przyłączenia, są określane wyłącznie przez informacje określone w pozycji informacji ubocznych i przez informacje akceptowane przez partnerską jednostkę logiczną.

Uwierzytelnianie na poziomie konwersacji i IBM MQ for z/OS
Ten temat zawiera przegląd sposobu działania uwierzytelniania na poziomie konwersacji w systemie z/OS.

W systemie IBM MQ for z/OSadaptery MCA nie używają interfejsu CPI-C. Zamiast tego korzystają z usług APPC/MVS TP Conversation Callable Services, implementacji zaawansowanej komunikacji program-program (APPC), która ma pewne funkcje CPI-C. Gdy agent MCA programu wywołującego przydziela konwersację, w wywołaniu określany jest typ zabezpieczeń SAME. Dlatego, 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 zaakceptuje już zweryfikowany identyfikator użytkownika, jednostka logiczna APPC/MVS wysyła żądanie przyłączenia zawierające:
  - ID użytkownika przestrzeni adresowej inicjatora kanału
  - Nazwa profilu zabezpieczeń, która, jeśli używana jest wartość RACF , jest nazwą bieżącej grupy połączeń dla ID użytkownika przestrzeni adresowej inicjatora kanału.
  - Już zweryfikowany indykator
- Jeśli stowarzyszona jednostka logiczna nie ufa jednostce logicznej APPC/MVS i nie zaakceptuje już zweryfikowanego identyfikatora użytkownika, jednostka logiczna APPC/MVS wysyła żądanie przyłączenia bez informacji o ochronie.

W systemie IBM MQ for z/OSparametry USERID i PASSWORD komendy DEFINE CHANNEL nie mogą być używane dla kanału komunikatów i są poprawne tylko na końcu połączenia klienckiego kanału MQI. Dlatego żądanie przyłączenia z jednostki logicznej APPC/MVS nigdy nie zawiera wartości określonych przez te parametry.

Zabezpieczenia klastrów menedżera kolejek

Mimo że klastry menedżera kolejek mogą być wygodne w użyciu, należy zwrócić szczególną uwagę na ich bezpieczeństwo.

Klaster menedżerów kolejek jest siecią menedżerów kolejek, które są powiązane logicznie w pewien sposób. Menedżer kolejek będący elementem klastra jest nazywany *menedżerem kolejek klastra*.

Kolejka należąca do menedżera kolejek klastra może być znana innym menedżerom kolejek w klastrze. Taka kolejka jest nazywana *kolejką klastrową*. Każdy menedżer kolejek w klastrze może wysyłać komunikaty do kolejek klastra bez konieczności wykonywania następujących czynności:

- Jawna definicja kolejki zdalnej dla każdej kolejki klastra
- Jawnie zdefiniowane kanały do i z każdego zdalnego menedżera kolejek
- Oddzielna kolejka transmisji dla każdego kanału wychodzącego

Można utworzyć klaster, w którym co najmniej dwa menedżery kolejek są klonami. Oznacza to, że mają one instancje tych samych kolejek lokalnych, w tym wszystkie kolejki lokalne zadeklarowane jako kolejki klastra, i mogą obsługiwać instancje tych samych aplikacji serwera.

Gdy aplikacja połączona z menedżerem kolejek klastra wysyła komunikat do kolejki klastra, która ma instancję w każdym ze sklonowanych menedżerów kolejek, program IBM MQ decyduje, do którego menedżera kolejek ma go wysłać. Gdy wiele aplikacji wysyła komunikaty do kolejki klastra, program IBM MQ równoważy obciążenie między poszczególnymi menedżerami kolejek, które mają instancję kolejki. Jeśli jeden z systemów udostępniających sklonowany menedżer kolejek nie powiedzie się, program IBM MQ kontynuuje równoważenie obciążenia pozostałych menedżerów kolejek do momentu zrestartowania systemu, który uległ awarii.

Jeśli używane są klastry menedżera kolejek, należy wziąć pod uwagę następujące problemy z bezpieczeństwem:

- 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 uwagi są istotne nawet wtedy, gdy nie są używane klastry, ale stają się ważniejsze w przypadku korzystania z klastrów.

Jeśli aplikacja może wysyłać komunikaty do jednej kolejki klastra, może wysyłać komunikaty do dowolnej innej kolejki klastra bez konieczności stosowania dodatkowych definicji kolejek zdalnych, kolejek transmisji lub kanałów. Dlatego ważniejsze staje się rozważenie, czy konieczne jest ograniczenie dostępu do kolejek klastra w menedżerze kolejek oraz ograniczenie kolejek klastra, do których aplikacje mogą wysyłać komunikaty.

Istnieją pewne dodatkowe zagadnienia dotyczące zabezpieczeń, które mają zastosowanie tylko w przypadku używania klastrów menedżera kolejek:

- Zezwalanie na dołączanie do klastra tylko wybranych menedżerów kolejek
- Wymuszanie opuszczenia klastra przez niechciane menedżery kolejek

Więcej informacji na ten temat zawiera sekcja Utrzymywanie bezpieczeństwa klastrów. z/OS Uwagi dotyczące systemu IBM MQ for z/OSmożna znaleźć w sekcji “Zabezpieczenia w klastrach menedżera kolejek w systemie z/OS” na stronie 280.

Zadania pokrewne

“Blokowanie odbierania komunikatów przez menedżery kolejek” na stronie 530
Można uniemożliwić menedżerowi kolejek klastra odbieranie komunikatów, które nie są autoryzowane do odbierania, za pomocą programów obsługi wyjścia.

Zabezpieczenia mechanizmu publikowania/subskrypcji produktu IBM MQ

Jeśli używane jest publikowanie/subskrypcja produktu IBM MQ , należy wziąć pod uwagę dodatkowe zagadnienia dotyczące zabezpieczeń.

W systemie publikowania/subskrypcji istnieją dwa typy aplikacji: publikator i subskrybent. *Publikatory* dostarczają informacji w postaci komunikatów IBM MQ . Gdy publikator publikuje komunikat, określa *temat*, który identyfikuje temat informacji w komunikacie.

Subskrybenty są konsumentami publikowanych informacji. Subskrybent określa interesujące go tematy, subskrybując je.

Menedżer kolejek jest aplikacją dostarczaną z funkcją publikowania/subskrypcji produktu IBM MQ . Odbiera on opublikowane komunikaty od publikatorów i żądania subskrypcji od subskrybentów, a następnie kieruje opublikowane komunikaty do subskrybentów. Subskrybent otrzymuje komunikaty tylko w tych tematach, które zasubskrybował.

Więcej informacji na ten temat zawiera sekcja Zabezpieczenia publikowania/subskrypcji.

Ochrona rozsyłania grupowego

Te informacje umożliwiają zrozumienie, dlaczego w przypadku rozsyłania grupowego produktu IBM MQ mogą być potrzebne procesy zabezpieczeń.

Funkcja rozsyłania grupowego produktu IBM MQ nie ma wbudowanych zabezpieczeń. Sprawdzenia zabezpieczeń są obsługiwane w menedżerze kolejek w czasie 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 Współdziałanie rozsyłania grupowego z funkcją przesyłania komunikatów o małym opóźnieniu (IBM MQ Low Latency Messaging)), dlatego może być konieczne zaimplementowanie własnych procedur bezpieczeństwa, ponieważ aplikacje odbierające nie mogą mieć pewności co do poprawności pól kontekstu.

Istnieją trzy procesy bezpieczeństwa, które należy wziąć pod uwagę:

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 108.

Zabezpieczenia sieci

Odizolowana sieć może być realną opcją zabezpieczającą przed fałszywymi wiadomościami. Aplikacja na adresie grupy rozsyłania grupowego może publikować szkodliwe komunikaty przy użyciu rodzimych funkcji komunikacyjnych, których nie można odróżnić od komunikatów produktu MQ , ponieważ pochodzą one z aplikacji na tym samym adresie grupy rozsyłania grupowego.

Możliwe jest również, aby klient na adresie grupy rozsyłania otrzymywał komunikaty, które były przeznaczone dla innych klientów na tym samym adresie grupy rozsyłania.

Izolowanie sieci rozsyłania grupowego zapewnia dostęp tylko do poprawnych klientów i aplikacji. Ten środek ostrożności może zapobiec przedostawaniu się złośliwych komunikatów i ujawnieniu poufnych informacji.

Informacje na temat adresów sieciowych grupy rozsyłania grupowego zawiera sekcja Ustawianie odpowiedniego ruchu w sieci dla rozsyłania grupowego .

Podpisy cyfrowe

Podpis cyfrowy jest tworzony przez szyfrowanie reprezentacji komunikatu. Szyfrowanie wykorzystuje klucz prywatny sygnatariusza i ze względu na wydajność zwykle działa na streszczonym komunikacie, a nie na samym komunikacie. Cyfrowe podpisywanie komunikatu przed wykonaniem operacji MQPUT stanowi dobry środek ostrożności, ale ten proces może mieć negatywny wpływ na wydajność w przypadku dużej liczby komunikatów.

Podpisy cyfrowe różnią się w zależności od podpisywanych danych. Jeśli dwie różne wiadomości są podpisane cyfrowo przez tę samą jednostkę, obie podpisy różnią się, ale można je zweryfikować przy użyciu tego samego klucza publicznego, czyli klucza publicznego jednostki, która podpisała wiadomości.

Jak wspomniano wcześniej w tej sekcji, aplikacja na adresie grupy rozsyłania może publikować szkodliwe komunikaty przy użyciu rodzimych funkcji komunikacyjnych, których nie można odróżnić od komunikatów produktu MQ . Podpisy cyfrowe stanowią dowód pochodzenia i tylko nadawca zna klucz prywatny, który stanowi mocny dowód na to, że nadawca jest inicjatorem wiadomości.

Więcej informacji na ten temat zawiera sekcja “Pojęcia związane z szyfrowaniem” na stronie 11.

Zapory firewall i Internet pass-thru

Zwykle należy użyć firewalla, aby uniemożliwić dostęp z wrogich adresów IP, na przykład w przypadku ataku polegającego na spowodowaniu odmowy usługi. Jednak może być konieczne tymczasowe zablokowanie adresów IP w programie IBM MQ, na przykład podczas oczekiwania na aktualizację reguł firewalla przez administratora bezpieczeństwa.

Aby zablokować jeden lub więcej adresów IP, utwórz rekord uwierzytelniania kanału typu BLOCKADDR lub ADDRESSMAP. Więcej informacji na ten temat zawiera sekcja “Blokowanie konkretnych adresów IP” na stronie 429.

zabezpieczenia dlaIBM MQ Internet Pass-Thru

IBM MQ Internet Pass-Thru może uprościć komunikację za pośrednictwem firewalla, ale ma to wpływ na bezpieczeństwo.

IBM MQ Internet Pass-Thru (MQIPT) to opcjonalny komponent produktu IBM MQ , który może być używany do implementowania rozwiązań przesyłania komunikatów między ośrodkami zdalnymi w Internecie.

Produkt MQIPT umożliwia wymianę komunikatów między dwoma menedżerami kolejek lub nawiązywanie przez aplikację kliencką IBM MQ połączenia z menedżerem kolejek przez Internet bez konieczności nawiązywania bezpośredniego połączenia TCP/IP. Jest to przydatne, jeśli firewall uniemożliwia bezpośrednie połączenie TCP/IP między dwoma systemami. Dzięki temu przepływanie przez protokół kanału IBM MQ do i z firewalla jest prostsze i łatwiejsze w zarządzaniu przez tunelowanie przepływów wewnątrz protokołu HTTP lub przez działanie jako serwer proxy. Za pomocą protokołu TLS (Transport Layer Security) można go również używać do szyfrowania i deszyfrowania wiadomości wysyłanych przez Internet.

Gdy system IBM MQ komunikuje się z serwerem MQIPT, o ile nie jest używany tryb proxy SSL w produkcie MQIPT, należy upewnić się, że specyfikacja CipherSpec używana przez produkt IBM MQ jest zgodna z pakietem CipherSuite używanym przez produkt MQIPT:

- Jeśli produkt MQIPT działa jako serwer TLS, a produkt IBM MQ łączy się jako klient TLS, wartość CipherSpec używana przez produkt IBM MQ musi odpowiadać wartości CipherSuite włączonej w odpowiednim pliku kluczy MQIPT .

- Jeśli produkt MQIPT działa jako klient TLS i łączy się z serwerem IBM MQ TLS, pakiet MQIPT CipherSuite musi być zgodny z wartością CipherSpec zdefiniowaną w odbierającym kanale IBM MQ .

W przypadku migracji z produktu MQIPT do zintegrowanej obsługi protokołu TLS produktu IBM MQ należy przesłać certyfikaty cyfrowe z pliku kluczy MQIPT za pomocą systemu **mqiptKeyman** lub **mqiptKeycmd**.

Więcej informacji na ten temat zawiera sekcja IBM MQ Internet Pass-Thru.

z/OS Lista kontrolna implementacji zabezpieczeń systemu IBM MQ for z/OS

W tym temacie przedstawiono procedurę krok po kroku, której można użyć do określenia i zdefiniowania implementacji zabezpieczeń dla każdego menedżera kolejek produktu IBM MQ .

RACF udostępnia definicje klas zabezpieczeń 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 są one aktywowane zgodnie z opisem w sekcji “Klasy zabezpieczeń systemu RACF” na stronie 196.

Szczegółowe informacje na ten temat można znaleźć w innych sekcjach, w szczególności w sekcji “Profile używane do sterowania dostępem do zasobów IBM MQ” na stronie 207.

Jeśli wymagane jest sprawdzanie bezpieczeństwa, należy użyć poniższej listy kontrolnej, aby je zaimplementować:

1. Aktywuj klasę RACF MQADMIN (profile pisane wielkimi literami) lub MXADMIN (profile z mieszaną wielkością liter).
   - Czy zabezpieczenia mają być dostępne na poziomie grupy współużytkowania kolejek, na poziomie menedżera kolejek lub w kombinacji obu tych elementów?

     Patrz “Profile sterujące grupą współużytkowania kolejek lub zabezpieczeniami na poziomie menedżera kolejek” na stronie 201.
2. Czy potrzebujesz ochrony połączenia?
   - **Tak**: Aktywuj klasę 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: Tylko użytkownicy żądania interfejsu API `MQCONN` lub identyfikatorów użytkowników przestrzeni adresowej CICS lub IMS muszą mieć dostęp do odpowiedniego profilu połączenia.
   - **Nie**: zdefiniuj wartość hlq.NO.CONNECT.CHECKS na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
3. Czy wymagane jest sprawdzanie bezpieczeństwa komend?
   - **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 samego menedżera kolejek i inicjatora kanału. Patrz sekcja “Konfigurowanie ochrony zasobów IBM MQ for z/OS” na stronie 271.
   - **Nie**: zdefiniuj wartość hlq.NO.CMD.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
4. Czy potrzebna jest ochrona zasobów używanych w komendach?
   - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj odpowiednie profile w celu ochrony zasobów w 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 komendzie CSQ6SYSP na domyślny ID użytkownika, który ma być używany do sprawdzania bezpieczeństwa komend.

Jeśli używana jest grupa współużytkowania kolejek, może być konieczne dołączenie identyfikatorów użytkowników używanych przez samego menedżera kolejek i inicjatora kanału. Patrz sekcja “Konfigurowanie ochrony zasobów IBM MQ for z/OS” na stronie 271.

- **Nie**: zdefiniuj wartość hlq.NO.CMD.RESC.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.

5. Czy potrzebujesz ochrony 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**: zdefiniuj wartość hlq.NO.QUEUE.CHECKS 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 odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: zdefiniuj wartość hlq.NO.PROCESS.CHECKS dla odpowiedniego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
7. Czy potrzebna jest ochrona listy nazw?
   - **Tak**: Aktywuj klasę 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**: zdefiniuj wartość hlq.NO.NLIST.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
8. Czy potrzebujesz ochrony tematu?
   - **Tak**: Aktywuj klasę MXTOPIC. Zdefiniuj odpowiednie profile tematów na poziomie menedżera kolejek lub na poziomie grupy współużytkowania kolejek w klasie MXTOPIC. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: zdefiniuj wartość hlq.NO.TOPIC.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
9. Czy użytkownicy muszą chronić użycie opcji `MQOPEN` lub `MQPUT1` związanych z używaniem kontekstu?
   - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj profile hlq.CONTEXT.queuename na poziomie kolejki, menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN. Następnie należy zezwolić odpowiednim użytkownikom lub grupom na dostęp do tych profili.
   - **Nie**: zdefiniuj wartość hlq.NO.CONTEXT.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
10. Czy należy chronić użycie alternatywnych identyfikatorów użytkowników?
    - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj odpowiednią wartość hlq.ALTERNATE.USER. Profile produktu *alternateuserid* dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek i zezwalanie wymaganym użytkownikom lub grupom na dostęp do tych profili.
    - **Nie**: zdefiniuj profil hlq.NO.ALTERNATE.USER.CHECKS dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN.
11. Czy należy dostosować identyfikatory użytkowników, które mają być używane do sprawdzania bezpieczeństwa zasobów za pomocą opcji RESLEVEL?
    - **Tak**: upewnij się, że klasa MQADMIN lub MXADMIN jest aktywna. Zdefiniuj profil hlq.RESLEVEL na poziomie menedżera kolejek lub grupy współużytkowania kolejek w klasie MQADMIN lub MXADMIN. Następnie należy zezwolić wymaganym użytkownikom lub grupom na dostęp do profilu.

- **Nie**: Upewnij się, że w klasie MQADMIN lub MXADMIN nie istnieją żadne profile ogólne, które mogą mieć zastosowanie do hlq.RESLEVEL. Zdefiniuj profil hlq.RESLEVEL dla wymaganego menedżera kolejek lub grupy współużytkowania kolejek i upewnij się, że żaden użytkownik ani żadna grupa nie ma do niego dostępu.

12. Czy konieczne jest przekroczenie limitu czasu dla nieużywanych identyfikatorów użytkowników z produktu IBM MQ ?

    - **Tak**: Określ wartości limitu czasu, które mają zostać użyte, i wydaj komendę MQSC ALTER SECURITY, aby zmienić parametry TIMEOUT i INTERVAL.
    - **Nie**: wywołaj komendę MQSC ALTER SECURITY, aby ustawić wartość INTERVAL na zero.

    Uwaga: Zaktualizuj zestaw danych wejściowych inicjowania CSQINP1 używany przez podsystem, tak aby komenda MQSC ALTER SECURITY była wydawana automatycznie po uruchomieniu menedżera kolejek.

13. Czy używane jest rozproszone kolejkowanie?

    - **Tak**: użyj rekordów uwierzytelniania kanału. Więcej informacji na ten temat zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.
    - Można również określić odpowiednią wartość atrybutu MCAUSER dla każdego kanału lub udostępnić 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 swoją infrastrukturę TLS. Zainstaluj opcję System SSL produktu z/OS. W programie RACFnależy skonfigurować filtry nazw certyfikatów (CNF), jeśli są one używane, oraz certyfikaty cyfrowe. Skonfiguruj plik kluczy SSL. Upewnij się, że atrybut SSLKEYR menedżera kolejek nie jest pusty i wskazuje na plik kluczy SSL. Upewnij się również, że wartość parametru SSLTASKS wynosi co najmniej 2.
    - **Nie**: upewnij się, że pole SSLKEYR jest puste, a pole SSLTASKS ma wartość zero.

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

15. Czy używasz klientów?

    - **Tak**: użyj rekordów uwierzytelniania kanału.
    - Można również określić odpowiednią wartość atrybutu MCAUSER dla każdego kanału połączenia z serwerem lub w razie potrzeby udostępnić odpowiednie wyjścia zabezpieczeń kanału.

16. Sprawdź ustawienia przełącznika.

    Program IBM MQ wysyła komunikaty po uruchomieniu menedżera kolejek, które wyświetlają ustawienia zabezpieczeń. Te komunikaty umożliwiają określenie, czy przełączniki są poprawnie ustawione.

17. Czy hasła są wysyłane z aplikacji klienckich?

    - **Tak**: Upewnij się, że opcja z/OS jest zainstalowana i że narzędzie ICSF (Integrated Cryptographic Service Facility) zostało uruchomione w celu zapewnienia najlepszej ochrony.
    - **Nie**: można zignorować komunikat o błędzie informujący, że narzędzie ICSF nie zostało uruchomione.

    Więcej informacji na temat ICSF można znaleźć pod adresem “Korzystanie z narzędzia ICSF (Integrated Cryptographic Service Facility)” na stronie 280

Konfigurowanie zabezpieczeń

Ta kolekcja tematów zawiera informacje dotyczące różnych systemów operacyjnych i korzystania z klientów.

ALW Konfigurowanie zabezpieczeń w systemie AIX, Linux, and Windows

Zagadnienia dotyczące zabezpieczeń specyficzne dla systemów AIX, Linux, and Windows .

Menedżery kolejek produktu IBM MQ przesyłają informacje, które są potencjalnie cenne, dlatego należy użyć systemu uprawnień, aby zapewnić, że nieautoryzowani użytkownicy nie będą mieli dostępu do menedżerów kolejek. Należy wziąć pod uwagę następujące typy zabezpieczeń:

Kto może administrować programem IBM MQ
Istnieje możliwość zdefiniowania zestawu użytkowników, którzy mogą wydawać komendy w celu administrowania produktem IBM MQ.

Kto może używać obiektów IBM MQ
Można zdefiniować, którzy użytkownicy (zwykle aplikacje) mogą używać wywołań MQI i komend PCF do wykonywania następujących czynności:

- Kto może nawiązać połączenie z menedżerem kolejek.
- Kto może uzyskiwać dostęp do obiektów (kolejek, definicji procesów, list nazw, kanałów, kanałów połączeń klienta, obiektów nasłuchiwania, usług i informacji uwierzytelniających) oraz jaki typ dostępu ma do tych obiektów.
- Kto może uzyskać dostęp do komunikatów IBM MQ .
- Kto może uzyskać dostęp do informacji o kontekście powiązanych z komunikatem.

Zabezpieczenia kanału
Należy upewnić się, że kanały używane do wysyłania komunikatów do systemów zdalnych mają dostęp do wymaganych zasobów.

Dostęp do bibliotek programów, bibliotek łączy MQI i komend można uzyskać za pomocą standardowych narzędzi operacyjnych. Jednak katalog zawierający kolejki i inne dane menedżera kolejek jest prywatny dla produktu IBM MQ. W celu nadania lub odebrania autoryzacji do zasobów MQI nie należy używać standardowych komend systemu operacyjnego.

ALW Sposób działania autoryzacji w systemie AIX, Linux, and Windows

Tabele specyfikacji autoryzacji w tematach tej sekcji dokładnie definiują sposób działania autoryzacji i stosowane ograniczenia.

Tabele dotyczą następujących sytuacji:

- Aplikacje wywołujące wywołania MQI
- Programy administracyjne, które wywołują komendy MQSC jako poprawki PCFs o zmienionym znaczeniu
- Programy administracyjne wydające komendy PCF

W tej sekcji przedstawiono informacje w postaci zestawu 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 uwierzytelniające, kanał, kanał połączenia klienckiego, program nasłuchujący lub usługa.

Wymagane uprawnienia
Wyrażona jako stała MQZAO_.

W tabelach stałe poprzedzone przedrostkiem MQZAO_ odpowiadają słowom kluczowym na liście autoryzacji dla komendy `setmqaut` dla konkretnej jednostki. Na przykład parametr MQZAO_BROWSE odpowiada słowu kluczowemu `+browse`, parametr MQZAO_SET_ALL_CONTEXT odpowiada słowu

kluczowemu +setallitd. Stałe te są zdefiniowane w pliku nagłówkowym cmqzc.hdostarczanym z produktem.

ALW *Autoryzacje dla wywołań MQI*

MQCONN, **MQOPEN**, **MQPUT1**i **MQCLOSE** mogą wymagać sprawdzenia autoryzacji. Tabele w tym temacie zawierają podsumowanie autoryzacji wymaganych dla każdego wywołania.

Aplikacja może wydawać konkretne wywołania MQI i opcje tylko wtedy, gdy identyfikator użytkownika, pod którym jest uruchomiona (lub którego autoryzacje może przyjąć), otrzymał odpowiednią autoryzację.

Cztery wywołania MQI mogą wymagać sprawdzenia autoryzacji: **MQCONN**, **MQOPEN**, **MQPUT1**i **MQCLOSE**.

W systemach **MQOPEN** i **MQPUT1**sprawdzanie uprawnień jest wykonywane dla nazwy otwieranego obiektu, a nie dla nazwy lub nazw, które powstały po przetłumaczeniu nazwy. Na przykład aplikacji może zostać nadane uprawnienie do otwierania kolejki aliasowej bez uprawnienia do otwierania kolejki podstawowej, na którą alias jest tłumaczony. Reguła polega na tym, że sprawdzanie jest wykonywane dla pierwszej definicji napotkanej podczas procesu tłumaczenia nazwy, która nie jest aliasem menedżera kolejek, chyba że definicja aliasu menedżera kolejek jest otwierana bezpośrednio, co oznacza, że jej nazwa jest wyświetlana w polu *ObjectName* deskryptora obiektu. Uprawnienia do otwieranego obiektu są zawsze wymagane. W niektórych przypadkach wymagane jest dodatkowe uprawnienie niezależne od kolejki, uzyskane przez autoryzację dla obiektu menedżera kolejek.

Tabela 10 na stronie 140, Tabela 11 na stronie 140, Tabela 12 na stronie 141i Tabela 13 na stronie 142 zawierają podsumowanie autoryzacji wymaganych dla każdego wywołania. W tabelach *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie jest istotne dla tej operacji; *Bez sprawdzania* oznacza, że sprawdzanie autoryzacji nie jest wykonywane.

Uwaga: W tych tabelach nie ma wzmianki o listach nazw, kanałach, kanałach połączeń klienckich, programach nasłuchujących, usługach ani obiektach informacji uwierzytelniającej. Dzieje się tak, ponieważ żadna autoryzacja nie ma zastosowania do tych obiektów, z wyjątkiem MQOO_INQUIRE, dla których obowiązują takie same autoryzacje, jak dla innych obiektów.

Autoryzacja specjalna MQZAO_ALL_MQI obejmuje wszystkie autoryzacje w tabelach, które są istotne dla typu obiektu, z wyjątkiem MQZAO_DELETE i MQZAO_DISPLAY, które są klasyfikowane jako autoryzacje administracyjne.

Aby zmodyfikować dowolną z opcji kontekstu komunikatu, należy mieć odpowiednie autoryzacje do wywołania. Aby na przykład użyć komendy MQOO_SET_IDENTITY_CONTEXT lub MQPMO_SET_IDENTITY_CONTEXT, należy mieć uprawnienie +setid .

Tabela 10. Autoryzacja zabezpieczeń wymagana dla wywołań MQCONN

Autoryzacja wymagana dla:	**Obiekt kolejki (“1” na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCONN	Nie dotyczy	Nie dotyczy	MQZAO_CONNECT

Tabela 11. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN

Autoryzacja wymagana dla:	**Obiekt kolejki (“1” na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_INQUIRE	MQZAO_INQUIRE,	MQZAO_INQUIRE,	MQZAO_INQUIRE,
MQOO_BROWSE,	MQZAO_BROWSE,	Nie dotyczy	Nie sprawdzaj
MQOO_INPUT_ *	MQZAO_INPUT	Nie dotyczy	Nie sprawdzaj
MQOO_SAVE_ ALL_CONTEXT **(“2” na stronie 142)**	MQZAO_INPUT	Nie dotyczy	Nie dotyczy

Tabela 11. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN (kontynuacja)			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_OUTPUT (kolejka normalna) **("3" na stronie 142)**	MQZAO_WYNIK	Nie dotyczy	Nie dotyczy
MQOO_PASS_ IDENTY_CONTEXT **("4" na stronie 142)**	MQZAO_PASS_ KONTEKST_TOŻSAMOŚCI	Nie dotyczy	Nie sprawdzaj
MQOO_PASS_ALL_ CONTEXT **("4" na stronie 142, "5" na stronie 142)**	MQZAO_PASS _ALL_CONTEXT	Nie dotyczy	Nie sprawdzaj
MQOO_SET_ IDENTITY_CONTEXT **("4" na stronie 142, "5" na stronie 142)**	MQZAO_SET_IDENTITY_C ONTEXT (MQZAO_SET_IDENTITY_ CONTEXT)	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stronie 142)**
MQOO_SET_ ALL_CONTEXT **("4" na stronie 142, "7" na stronie 142)**	MQZAO_SET_ ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 142)**
MQOO_OUTPUT (kolejka transmisji) **("8" na stronie 142)**	MQZAO_SET_ ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 142)**
MQOO_SET	MQZAO_SET	Nie dotyczy	Nie sprawdzaj
MQOO_ALTERNATE_ UPRAWNIENIE_UŻYTKO WNIKA	**("9" na stronie 142)**	**("9" na stronie 142)**	MQZAO_ALTERNATE_ USER_AUTHORITY **("9" na stronie 142, "10" na stronie 142)**

Tabela 12. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_IDENTITY _CONTEXT (KONTEKST TOŻSAMOŚCI MQPMO_PASS_)	MQZAO_PASS_ TOŻSAMOŚCI_KONTEKST **("11" na stronie 142)**	Nie dotyczy	Nie sprawdzaj
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **("11" na stronie 142)**	Nie dotyczy	Nie sprawdzaj
MQPMO_SET_ KONTEKST_TOŻSAMOŚCI	MQZAO_SET_ IDENTITY_CONTEXT **("11" na stronie 142)**	Nie dotyczy	MQZAO_SET_ IDENTITY_CONTEXT **("6" na stronie 142)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **("11" na stronie 142)**	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 142)**
(Kolejka transmisji) **("8" na stronie 142)**	MQZAO_SET_ ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ ALL_CONTEXT **("6" na stronie 142)**

Tabela 12. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1 (kontynuacja)			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_ALTERNATE_UPRAWNIENIE_UŻYTKOWNIKA	**("12" na stronie 142)**	Nie dotyczy	MQZAO_ALTERNATE_USER_AUTHORITY **("10" na stronie 142)**

Tabela 13. Autoryzacja zabezpieczeń wymagana dla wywołań MQCLOSE			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 142)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCO_DELETE	MQZAO_DELETE **("13" na stronie 143)**	Nie dotyczy	Nie dotyczy
MQCO_DELETE-OPRÓŻNIONE	MQZAO_DELETE **("13" na stronie 143)**	Nie dotyczy	Nie dotyczy

Uwagi dotyczące tabel:

1. W przypadku otwierania kolejki modelowej:
   - Uprawnienie MQZAO_DISPLAY jest wymagane dla kolejki modelowej, oprócz uprawnienia do otwarcia kolejki modelowej dla typu dostępu, dla którego otwierany jest użytkownik.
   - Uprawnienie MQZAO_CREATE nie jest wymagane do utworzenia kolejki dynamicznej.
   - Identyfikator użytkownika używany do otwierania kolejki modelowej jest automatycznie nadawany wszystkim uprawnieniom specyficznym dla kolejki (równoważnym uprawnieniom MQZAO_ALL) dla tworzonej kolejki dynamicznej.
2. Należy również podać wartość MQOO_INPUT_ *. Dotyczy to kolejki lokalnej, kolejki modelowej lub kolejki aliasowej.
3. To sprawdzenie jest wykonywane dla wszystkich przypadków wyjściowych, z wyjątkiem kolejek transmisji (patrz uwaga "8" na stronie 142).
4. Należy również określić parametr MQOO_OUTPUT.
5. Opcja ta zakłada również wartość MQOO_PASS_IDENTITY_CONTEXT.
6. Uprawnienie to jest wymagane zarówno dla obiektu menedżera kolejek, jak i dla konkretnej kolejki.
7. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT i MQOO_SET_IDENTITY_CONTEXT są również implikowane przez tę opcję.
8. To sprawdzenie jest wykonywane dla kolejki lokalnej lub modelowej, która ma atrybut kolejki *Użycie* o wartości MQUS_TRANSMISSION i jest otwierana bezpośrednio dla danych wyjściowych. Nie ma zastosowania, jeśli otwierana jest kolejka zdalna (przez określenie nazw menedżera kolejek zdalnych i kolejki zdalnej lub przez określenie nazwy lokalnej definicji kolejki zdalnej).
9. Należy również określić co najmniej jeden z następujących typów obiektów: MQOO_INQUIRE (dla dowolnego typu obiektu) lub MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET (dla kolejek). Przeprowadzone sprawdzenie jest takie samo jak w przypadku innych określonych opcji, przy użyciu podanego alternatywnego identyfikatora użytkownika dla konkretnego uprawnienia do obiektu o określonej nazwie i bieżącego uprawnienia do aplikacji dla sprawdzenia MQZAO_ALTERNATE_USER_IDENTIFIER.
10. Ta autoryzacja umożliwia podanie dowolnego identyfikatora *AlternateUserId* .
11. Sprawdzenie MQZAO_OUTPUT jest również wykonywane, jeśli kolejka nie ma atrybutu kolejki *Użycie* o wartości MQUS_TRANSMISSION.
12. Przeprowadzone sprawdzenie jest takie samo jak w przypadku innych określonych opcji, przy użyciu podanego alternatywnego identyfikatora użytkownika dla uprawnienia kolejki o określonej nazwie i bieżącego uprawnienia aplikacji dla sprawdzenia MQZAO_ALTERNATE_USER_IDENTIFIER.

13. Kontrola jest przeprowadzana tylko wtedy, gdy spełnione są oba poniższe warunki:
    - Trwała kolejka dynamiczna jest zamykana i usuwana.
    - Kolejka nie została utworzona przez wywołanie MQOPEN , które zwróciło używany uchwyt obiektu.

    W przeciwnym razie nie jest sprawdzana.

ALW *Autoryzacje dla komend MQSC w systemach CF o zmienionym znaczeniu*

Informacje te zawierają podsumowanie autoryzacji wymaganych dla każdej komendy MQSC zawartej w pliku Escape PCF.

Nie dotyczy oznacza, że ta operacja nie dotyczy tego typu obiektu.

ID użytkownika, pod którym działa program wprowadzający 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 wywoływania komendy MQSC w tekście komendy Escape PCF

ALTER *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	MQZAO_CHANGE
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE
Informacje o komunikacji	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

Obiekt	Wymagane uprawnienia
Usługa	Nie dotyczy
Informacje o komunikacji	Nie dotyczy

DEFINE *obiekt* NOREPLACE (“1” na stronie 148)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Temat	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Proces	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Informacje uwierzytelniające	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Kanał	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Kanał połączenia klienta	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Program nasłuchujący	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Usługa	MQZAO_CREATE **(w systemie “2” na stronie 148)**
Informacje o komunikacji	MQZAO_CREATE **(w systemie “2” na stronie 148)**

DEFINE *obiekt* REPLACE (“1” na stronie 148, “3” na stronie 148)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE
Informacje o komunikacji	MQZAO_CHANGE

DELETE *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_USUŃ
Temat	MQZAO_USUŃ
Proces	MQZAO_USUŃ
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_USUŃ
Informacje uwierzytelniające	MQZAO_USUŃ
Kanał	MQZAO_USUŃ
Kanał połączenia klienta	MQZAO_USUŃ
Program nasłuchujący	MQZAO_USUŃ
Usługa	MQZAO_USUŃ
Informacje o komunikacji	MQZAO_USUŃ

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

Obiekt	Wymagane uprawnienia
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

STOP *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	MQZAO_CONTROL
Usługa	MQZAO_CONTROL
Informacje o komunikacji	Nie dotyczy

Komendy kanałów

Komenda	Obiekt	Wymagane uprawnienia
WYKONAJ KOMENDĘ PING DLA KANAŁU	Kanał	MQZAO_CONTROL
Resetuj kanał	Kanał	MQZAO_CONTROL_EXTENDED,
Rozstrzyganie kanału	Kanał	MQZAO_CONTROL_EXTENDED,

Komendy dotyczące subskrypcji

Komenda	Obiekt	Wymagane uprawnienia
ZMIEŃ 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	MQZAO_CHANGE
USUŃ AUTORA	Menedżer kolejek	MQZAO_CHANGE
WYŚWIETL AUTORYZ.	Menedżer kolejek	MQZAO_DISPLAY

Komenda	Obiekt	Wymagane uprawnienia
WYŚWIETL AUTHSERV	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL ENTAUTH	Menedżer kolejek	MQZAO_DISPLAY
USTAW CHLAURA	Menedżer kolejek	MQZAO_CHANGE
WYŚWIETL CHLAURA	Menedżer kolejek	MQZAO_DISPLAY
REFRESH SECURITY	Menedżer kolejek	MQZAO_CHANGE

Ekrany statusu

Komenda	Obiekt	Wymagane uprawnienia
WYŚWIETLENIE STATUSU CHSTATUS	Menedżer kolejek	MQZAO_DISPLAY Należy zauważyć, że uprawnienie `+inq` (lub równoważne uprawnienie MQZAO_INQUIRE) jest wymagane w kolejce transmisji, jeśli kanał jest typu CLUSSDR.
WYŚWIETL STATUS LSSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL PUBSUB	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL STATUS SBSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETL STATUS SYSTEMU SVSTATUS	Menedżer kolejek	MQZAO_DISPLAY
WYŚWIETLENIE STATUSU TPSTATUS	Menedżer kolejek	MQZAO_DISPLAY

Komendy klastrów

Komenda	Obiekt	Wymagane uprawnienia
WYŚWIETL LISTĘ CLUSQMGR	Menedżer kolejek	MQZAO_DISPLAY
ODŚWIEŻ KLASTER	Wymagane przypisanie do grupy mqm	
Resetowanie klastra	Wymagane przypisanie do grupy mqm	
Menedżer kolejki zawieszony	Wymagane przypisanie do grupy mqm	
WZNOWIENIE MENEDŻERA KOLEJEK	Wymagane przypisanie do grupy mqm	

Inne komendy administracyjne

Komenda	Obiekt	Wymagane uprawnienia
PING QMGR	Menedżer kolejek	MQZAO_DISPLAY
ODŚWIEŻ MENEDŻERA KOLEJEK	Menedżer kolejek	MQZAO_CHANGE
RESETUJ MENEDŻER KOLEJEK	Menedżer kolejek	MQZAO_CHANGE
WYŚWIETL KONN	Menedżer kolejek	MQZAO_DISPLAY
ZATRZYMAJ KONN	Menedżer kolejek	MQZAO_CHANGE

Uwaga:

1. W przypadku komend DEFINE uprawnienie MQZAO_DISPLAY jest również wymagane dla obiektu LIKE, jeśli zostało określone, lub dla odpowiedniego systemu SYSTEM.DEFAULT.xxx DEFAULT.xxx, jeśli pominięto LIKE.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane wszystkim obiektom dla określonego menedżera kolejek przez określenie typu obiektu QMGR w komendzie `setmqaut` .
3. Ma to zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli nie, sprawdzanie jest takie samo jak w przypadku opcji DEFINE *obiekt* NOREPLACE.

Informacje pokrewne

Technologia klastrowa: sprawdzone procedury użycia komendy REFRESH CLUSTER

ALW *Autoryzacje dla komend PCF*

Ta sekcja zawiera podsumowanie autoryzacji wymaganych dla każdej komendy PCF.

Bez sprawdzania oznacza, że nie jest wykonywane sprawdzanie autoryzacji; *Nie dotyczy* oznacza, że ta operacja nie jest odpowiednia dla tego typu obiektu.

ID użytkownika, pod którym działa program wprowadzający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie MQZAO_DISPLAY w menedżerze kolejek w celu wykonania komend PCF

Autoryzacja specjalna MQZAO_ALL_ADMIN obejmuje wszystkie autoryzacje z poniższej listy, które są istotne dla typu obiektu, z wyjątkiem MQZAO_CREATE, która nie jest specyficzna dla konkretnego obiektu lub typu obiektu.

Zmień *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
menedżer kolejek	MQZAO_CHANGE
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE
Informacje o komunikacji	MQZAO_CHANGE

Wyczyść *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CLEAR,
Temat	MQZAO_CLEAR,
Proces	Nie dotyczy

Obiekt	Wymagane uprawnienia
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	Nie dotyczy
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy
Informacje o komunikacji	Nie dotyczy

Skopiuj *obiekt* (bez zastępowania) (1)

Obiekt	Wymagane uprawnienia
Kolejka	Komenda MQZAO_CREATE **(2)**
Temat	Komenda MQZAO_CREATE **(2)**
Proces	Komenda MQZAO_CREATE **(2)**
Menedżer kolejek	Nie dotyczy
Lista nazw	Komenda MQZAO_CREATE **(2)**
Informacje uwierzytelniające	Komenda MQZAO_CREATE **(2)**
Kanał	Komenda MQZAO_CREATE **(2)**
Kanał połączenia klienta	Komenda MQZAO_CREATE **(2)**
Program nasłuchujący	Komenda MQZAO_CREATE **(2)**
Usługa	Komenda MQZAO_CREATE **(2)**
Informacje o komunikacji	MQZAO_CREATE **(w systemie "2" na stronie 154)**

Skopiuj *obiekt* (z zastępowaniem) (1, 4)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE
Informacje o komunikacji	MQZAO_CHANGE

Utwórz *obiekt* (bez zastępowania) (3)

Obiekt	Wymagane uprawnienia
Kolejka	Komenda MQZAO_CREATE **(2)**
Temat	Komenda MQZAO_CREATE **(2)**
Proces	Komenda MQZAO_CREATE **(2)**
Menedżer kolejek	Nie dotyczy
Lista nazw	Komenda MQZAO_CREATE **(2)**
Informacje uwierzytelniające	Komenda MQZAO_CREATE **(2)**
Kanał	Komenda MQZAO_CREATE **(2)**
Kanał połączenia klienta	Komenda MQZAO_CREATE **(2)**
Program nasłuchujący	Komenda MQZAO_CREATE **(2)**
Usługa	Komenda MQZAO_CREATE **(2)**
Informacje o komunikacji	Komenda MQZAO_CREATE **(2)**

Utwórz *obiekt* (z zastępowaniem) (3, 4)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE
Informacje o komunikacji	MQZAO_CHANGE

Usuń *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_USUŃ
Temat	MQZAO_USUŃ
Proces	MQZAO_USUŃ
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_USUŃ
Informacje uwierzytelniające	MQZAO_USUŃ
Kanał	MQZAO_USUŃ

Obiekt	Wymagane uprawnienia
Kanał połączenia klienta	MQZAO_USUŃ
Program nasłuchujący	MQZAO_USUŃ
Usługa	MQZAO_USUŃ
Informacje o komunikacji	MQZAO_USUŃ

Sprawdź *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

Sprawdź nazwy *obiektów*

Obiekt	Wymagane uprawnienia
Kolejka	Nie sprawdzaj
Temat	Nie sprawdzaj
Proces	Nie sprawdzaj
Menedżer kolejek	Nie sprawdzaj
Lista nazw	Nie sprawdzaj
Informacje uwierzytelniające	Nie sprawdzaj
Kanał	Nie sprawdzaj
Kanał połączenia klienta	Nie sprawdzaj
Program nasłuchujący	Nie sprawdzaj
Usługa	Nie sprawdzaj
Informacje o komunikacji	Nie sprawdzaj

Uruchom *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

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
Uzyskiwanie informacji o subskrypcji	Temat	MQZAO_DISPLAY

Komendy ochrony

Komenda	Obiekt	Wymagane uprawnienia
Ustaw rekord uprawnień	Menedżer kolejek	MQZAO_CHANGE
Usuń rekord uprawnień	Menedżer kolejek	MQZAO_CHANGE
Zapytanie o rekordy uprawnień	Menedżer kolejek	MQZAO_DISPLAY
Usługa sprawdzania uprawnień	Menedżer kolejek	MQZAO_DISPLAY
Inquire Entity Authority (zapytanie o uprawnienie jednostki)	Menedżer kolejek	MQZAO_DISPLAY
Ustawianie rekordu uwierzytelniania kanału	Menedżer kolejek	MQZAO_CHANGE
Zapytanie o rekordy uwierzytelniania kanału	Menedżer kolejek	MQZAO_DISPLAY
Odśwież zabezpieczenia	Menedżer kolejek	MQZAO_CHANGE

Ekrany statusu

Komenda	Obiekt	Wymagane uprawnienia
Zapytanie o status kanału	Menedżer kolejek	MQZAO_DISPLAY Należy zauważyć, że uprawnienie `+inq` (lub równoważne uprawnienie MQZAO_INQUIRE) jest wymagane w kolejce transmisji, jeśli kanał jest typu CLUSSDR.
Zapytanie o status programu nasłuchującego kanału	Menedżer kolejek	MQZAO_DISPLAY
Status publikowania/ subskrypcji zapytania	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status subskrypcji	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status usługi	Menedżer kolejek	MQZAO_DISPLAY
Zapytanie o status tematu	Menedżer kolejek	MQZAO_DISPLAY

Komendy klastrów

Komenda	Obiekt	Wymagane uprawnienia
Uzyskiwanie informacji o menedżerze kolejek klastra	Menedżer kolejek	MQZAO_DISPLAY
Odśwież klaster	Wymagane przypisanie do grupy mqm	Wymagane przypisanie do grupy mqm
Resetowanie klastra	Wymagane przypisanie do grupy mqm	Wymagane przypisanie do grupy mqm
Zawieś klaster menedżera kolejek	Wymagane przypisanie do grupy mqm	Wymagane przypisanie do grupy mqm

Komenda	Obiekt	Wymagane uprawnienia
Wznów klaster menedżera kolejek	Wymagane przypisanie do grupy mqm	Wymagane przypisanie do grupy mqm

Inne komendy administracyjne

Komenda	Obiekt	Wymagane uprawnienia
Menedżer kolejek ping	Menedżer kolejek	MQZAO_DISPLAY
Odśwież menedżera kolejek	Menedżer kolejek	MQZAO_CHANGE
Resetuj menedżer kolejek	Menedżer kolejek	MQZAO_CHANGE
Resetuj statystyki kolejki	Kolejka	MQZAO_DISPLAY i MQZAO_CHANGE
Zapytanie o połączenie	Menedżer kolejek	MQZAO_DISPLAY
Zatrzymaj połączenie	Menedżer kolejek	MQZAO_CHANGE

Uwaga:

1. W przypadku komend kopiowania wymagane jest również uprawnienie MQZAO_DISPLAY dla obiektu źródłowego.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane wszystkim obiektom dla określonego menedżera kolejek przez określenie typu obiektu QMGR w komendzie `setmqaut` .
3. W przypadku komend tworzenia wymagane jest również uprawnienie MQZAO_DISPLAY dla odpowiedniego systemu SYSTEM.DEFAULT.* .
4. Ma to zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli nie, sprawdzanie jest takie samo jak w przypadku opcji Kopiuj lub Utwórz bez zastępowania.

AIX Tworzenie grup i zarządzanie nimi w systemie AIX

W systemie AIX, jeśli nie używasz NIS ani NIS +, użyj programu SMITTY do pracy z grupami.

O tym zadaniu

W systemie AIXmożna użyć programu SMITTY do utworzenia grupy, dodania użytkownika do grupy, wyświetlenia listy użytkowników należących do grupy i usunięcia użytkownika z grupy.

Procedura

1. W programie 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 zostać dodani do grupy, rozdzielając je przecinkami.

d) Naciśnij klawisz Enter, aby dodać nazwy do grupy.

5. Aby wyświetlić osoby należące 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.
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 nazwę użytkownika, którego chcesz usunąć z grupy.
   d) Naciśnij klawisz Enter, aby usunąć nazwę z grupy.

Linux Tworzenie grup i zarządzanie nimi w systemie Linux

W systemie Linux, jeśli nie używasz NIS lub NIS +, użyj pliku `/etc/group` do pracy z grupami.

O tym zadaniu

W systemie Linuxinformacje o grupie są przechowywane w pliku `/etc/group` . Za pomocą komend można utworzyć grupę, dodać użytkownika do grupy, wyświetlić listę użytkowników należących do grupy i usunąć użytkownika z grupy.

Procedura

1. Aby utworzyć nową grupę, należy użyć komendy **groupadd** .
   Wywołaj następującą komendę:
   ```
   groupadd -g group-ID group-name
   ```
   gdzie *ID_grupy* jest liczbowym identyfikatorem grupy, a *nazwa_grupy* jest nazwą grupy.
2. Aby dodać członka do grupy uzupełniającej, należy użyć komendy **usermod** w celu wyświetlenia grup uzupełniających, do których użytkownik jest obecnie członkiem, oraz grup uzupełniających, do których użytkownik ma należeć.
   Jeśli na przykład użytkownik jest już członkiem grupy `groupa`i ma zostać członkiem grupy `groupb`, należy użyć następującej komendy:
   ```
   usermod -G groupa,groupb user-name
   ```
   gdzie *nazwa-użytkownika* jest nazwą użytkownika.
3. Aby wyświetlić członków 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 listy grup uzupełniających, do których użytkownik ma pozostać członkiem.
   Na przykład, jeśli podstawową grupą użytkownika jest `users` , a użytkownik jest również 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 Windowsdo administrowania grupami na stacji roboczej lub serwerze składowym służy opcja Zarządzanie komputerem.

O tym zadaniu

W przypadku kontrolerów domeny użytkownicy i grupy są administrowane za pomocą usługi Active Directory. Więcej informacji na temat korzystania z usługi Active Directory zawierają odpowiednie instrukcje dla systemu operacyjnego.

Wszelkie zmiany wprowadzone w przypisaniu do grupy użytkownika nie są rozpoznawane, dopóki menedżer kolejek nie zostanie zrestartowany lub nie zostanie wywołana komenda MQSC **REFRESH SECURITY** (lub odpowiednik PCF).

Panel Windows Zarządzanie komputerem służy do pracy z użytkownikami i grupami. Wszelkie zmiany wprowadzone w aktualnie zalogowanym użytkowniku mogą nie zostać uwzględnione do momentu ponownego zalogowania się użytkownika.

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**i 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 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. Na 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 żądana grupa nie jest widoczna:
   a) Kliknij przycisk **Dodaj**.
      Zostanie wyświetlony panel Wybierz grupy.
   b) Kliknij opcję **Lokalizacje ...**.
      Zostanie wyświetlony panel Lokalizacje.
   c) Wybierz z listy położenie grupy, do której chcesz dodać użytkownika, i kliknij przycisk **OK**.
   d) W udostępnionym polu wpisz nazwę grupy.

Można również kliknąć opcję **Zaawansowane ...** a następnie **Znajdź teraz** , aby wyświetlić grupy dostępne w aktualnie wybranym położeniu. W tym miejscu wybierz grupę, do której chcesz dodać użytkownika, i kliknij przycisk **OK**.

e) Kliknij przycisk **OK**.

Zostanie wyświetlony panel właściwości użytkownika zawierający dodaną grupę.

f) Wybierz grupę.

9. Kliknij przycisk **OK**.

Zostanie wyświetlony panel Zarządzanie komputerem.

Windows *Wyświetlanie osób należących do grupy w systemie Windows*

Wyświetl członków 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. Na 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*

Usuwanie 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. Na 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 bezpieczeństwa w systemie Windows

Niektóre funkcje zabezpieczeń zachowują się inaczej w różnych wersjach systemu Windows.

Bezpieczeństwo systemu IBM MQ opiera się na wywołaniach interfejsu API systemu operacyjnego w celu uzyskania informacji o autoryzacjach użytkowników i przynależności do grup. Niektóre funkcje nie zachowują się identycznie w systemach Windows . Ta kolekcja tematów zawiera opisy wpływu tych różnic na bezpieczeństwo systemu IBM MQ podczas uruchamiania systemu IBM MQ w środowisku Windows .

Windows *Konta użytkowników lokalnych i domenowych 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, które może być używane przez program IBM MQ do wysyłania zapytań o informacje o każdym użytkowniku, który próbuje uzyskać taki dostęp.

- “Konfigurowanie specjalnych kont użytkowników za pomocą programu Prepare IBM MQ Wizard” na stronie 158
- “Używanie systemu IBM MQ z usługą Active Directory” na stronie 159
- “Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows” na stronie 159

Konfigurowanie specjalnych kont użytkowników za pomocą programu Prepare IBM MQ Wizard

Prepare IBM MQ Wizard tworzy specjalne konto użytkownika, dzięki czemu usługa Windows może być współużytkowana przez procesy, które z niej korzystają (patrz sekcja Konfigurowanie produktu IBM MQ z produktem PPrepare IBM MQ Wizard).

Usługa systemu Windows jest współużytkowana przez procesy klienta w ramach instalacji produktu IBM MQ . Dla każdej instalacji tworzona jest jedna usługa. Każda usługa ma nazwę `MQ_`*`InstallationName`*i nazwę wyświetlaną `IBM MQ(`*`InstallationName`*`)`.

Ponieważ każda usługa musi być współużytkowana przez nieinteraktywne i interaktywne sesje logowania, należy uruchomić każdą z nich przy użyciu specjalnego konta użytkownika. Można użyć jednego specjalnego konta użytkownika dla wszystkich usług lub utworzyć inne specjalne konta użytkownika. Każde specjalne konto użytkownika musi mieć uprawnienie do `logowania jako usługa`. Więcej informacji na ten temat zawiera sekcja Tabela 14 na stronie 159. Jeśli identyfikator użytkownika nie ma uprawnień do uruchomienia usługi, usługa nie zostanie uruchomiona i zwróci błąd w dzienniku zdarzeń systemu Windows . Zwykle należy uruchomić plik Prepare IBM MQ Wizardi poprawnie skonfigurować identyfikator użytkownika. Jeśli jednak identyfikator użytkownika został skonfigurowany ręcznie, może wystąpić problem, który należy rozwiązać.

Po pierwszym zainstalowaniu produktu IBM MQ i uruchomieniu programu Prepare IBM MQ Wizard tworzone jest lokalne konto użytkownika dla usługi o nazwie MUSR_MQADMIN z wymaganymi ustawieniami i uprawnieniami, w tym `Logowanie w trybie usługi`.

W przypadku kolejnych instalacji Prepare IBM MQ Wizard tworzy konto użytkownika o nazwie MUSR_MQADMIN*x*, gdzie *x* jest następnym dostępnym numerem reprezentującym identyfikator użytkownika, który nie istnieje. Hasło dla użytkownika MUSR_MQADMIN*x* jest generowane losowo podczas tworzenia konta i używane do konfigurowania środowiska logowania dla usługi. Wygenerowane hasło nie traci ważności.

Na to konto IBM MQ nie mają wpływu żadne strategie kont skonfigurowane w systemie, które wymagają, aby hasła kont były zmieniane po upływie określonego czasu.

Hasło nie jest znane poza tym jednorazowym przetwarzaniem i jest przechowywane przez system operacyjny Windows w bezpiecznej części rejestru.

Używanie systemu IBM MQ z usługą Active Directory

W niektórych konfiguracjach sieciowych, w których konta użytkowników są zdefiniowane w kontrolerach domeny korzystających z usługi katalogowej Active Directory , lokalne konto użytkownika, w ramach którego działa program IBM MQ , może nie mieć uprawnień wymaganych do wysyłania zapytań o członkostwo w grupie innych kont użytkowników domeny. Podczas instalowania produktu IBM MQ Prepare IBM MQ Wizard określa, czy tak jest, przeprowadzając testy i zadając pytania dotyczące konfiguracji sieci.

Jeśli konto użytkownika lokalnego, w ramach którego działa program IBM MQ , nie ma wymaganych uprawnień, program Prepare IBM MQ Wizard wyświetli zapytanie o szczegóły konta użytkownika domeny z konkretnymi uprawnieniami. Informacje na temat tworzenia i konfigurowania konta domeny Windows zawiera sekcja Tworzenie i konfigurowanie kont domeny Windows dla produktu IBM MQ. Informacje na temat uprawnień wymaganych przez konto użytkownika domeny zawiera sekcja Tabela 14 na stronie 159.

Po wprowadzeniu poprawnych szczegółów konta dla konta użytkownika domeny w programie Prepare IBM MQ Wizardkreator skonfiguruje usługę IBM MQ Windows , która ma być uruchamiana z nowym kontem. Szczegóły konta są przechowywane w bezpiecznej części rejestru i nie mogą być odczytywane przez użytkowników.

Gdy usługa jest uruchomiona, uruchamiana jest usługa IBM MQ Windows , która pozostaje uruchomiona tak długo, jak długo jest ona uruchomiona. Administrator systemu IBM MQ , który loguje się do serwera po uruchomieniu usługi Windows , może użyć programu IBM MQ Explorer do administrowania menedżerami kolejek na serwerze. Spowoduje to połączenie procesu IBM MQ Explorer z istniejącym procesem usługi Windows . Te dwa działania wymagają różnych poziomów uprawnień, zanim będą mogły działać:

- Proces uruchamiania wymaga uprawnienia do uruchamiania.
- Administrator IBM MQ wymaga uprawnień dostępu.

Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows

Poniższa tabela zawiera listę uprawnień użytkownika wymaganych dla lokalnych i domenowych kont użytkowników, w ramach których uruchamiana jest usługa Windows dla instalacji IBM MQ .

Tabela 14. Uprawnienia użytkownika wymagane dla usługi systemu Windows produktu IBM MQ

Uprawnienie	**Opis**
Zaloguj się jako zadanie wsadowe	Umożliwia uruchomienie usługi IBM MQ Windows z tym kontem 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 to skonfigurowane, gdy odtwarzanie usługi nie powiedzie się.
zwiększanie limitu miejsca na dysku	Wymagane dla wywołania systemu operacyjnego `CreateProcessAsUser` .
działanie jako część systemu operacyjnego	Wymagane dla wywołania `LogonUser` systemu operacyjnego.
Pomiń sprawdzanie przechodzenia	Wymagane dla wywołania `LogonUser` systemu operacyjnego.
zamiana znacznika poziomu procesu	Wymagane dla wywołania `LogonUser` systemu operacyjnego.

Uwaga: Prawa do debugowania programów mogą być wymagane w środowiskach, w których działają aplikacje ASP i IIS.

Konto użytkownika domeny musi mieć te prawa użytkownika Windows ustawione jako obowiązujące 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 zabezpieczeń domeny.

Windows *Uprawnienia zabezpieczeń serwera Windows*
Instalacja produktu IBM MQ działa inaczej na serwerze Windows Server, w zależności od tego, czy instalację przeprowadza użytkownik lokalny, czy użytkownik domeny.

Jeśli *lokalny* użytkownik zainstaluje IBM MQ, Prepare IBM MQ Wizard wykryje, że lokalny użytkownik utworzony dla usługi IBM MQ Windows może pobrać informacje o członkostwie w grupie użytkownika instalującego. Prepare IBM MQ Wizard zadaje użytkownikowi pytania dotyczące konfiguracji sieci w celu określenia, czy istnieją inne konta użytkowników zdefiniowane w kontrolerach domeny działających w systemie Windows 2000 lub nowszym. Jeśli tak, usługa IBM MQ Windows musi działać z użyciem konta użytkownika domeny z określonymi ustawieniami i uprawnieniami. Prepare IBM MQ Wizard pyta użytkownika o szczegóły konta tego użytkownika zgodnie z opisem w sekcji Konfigurowanie produktu IBM MQ z Prepare IBM MQ Wizard.

Jeśli użytkownik *domeny* zainstaluje IBM MQ, Prepare IBM MQ Wizard wykryje, że lokalny użytkownik utworzony dla usługi IBM MQ Windows nie może pobrać informacji o członkostwie w grupie użytkownika instalującego. W takim przypadku Prepare IBM MQ Wizard zawsze pyta użytkownika o szczegóły konta użytkownika domeny, które ma być używane przez usługę IBM MQ Windows .

Jeśli usługa IBM MQ Windows wymaga użycia konta użytkownika należącego do domeny, produkt IBM MQ nie może działać poprawnie, dopóki nie zostanie on skonfigurowany przy użyciu pliku Prepare IBM MQ Wizard. Prepare IBM MQ Wizard nie zezwala użytkownikowi na kontynuowanie 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*
Można zmienić nazwę użytkownika powiązaną z usługą IBM MQ , tworząc nowe konto i wprowadzając jego szczegóły za pomocą programu Prepare IBM MQ Wizard.

O tym zadaniu

Po pierwszym zainstalowaniu produktu IBM MQ i uruchomieniu programu Prepare IBM MQ Wizard tworzone jest lokalne konto użytkownika dla usługi o nazwie MUSR_MQADMIN. W przypadku kolejnych instalacji Prepare IBM MQ Wizard tworzy konto użytkownika o nazwie MUSR_MQADMIN*x*, gdzie *x* jest następnym dostępnym numerem reprezentującym identyfikator użytkownika, który nie istnieje.

Może być konieczna zmiana nazwy użytkownika powiązanej z usługą IBM MQ z 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 dłuższych 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 z produktem Prepare IBM MQ Wizard

Windows *Zmiana hasła do lokalnego konta użytkownika usługi IBM MQ Windows*
Hasło do lokalnego konta użytkownika usługi IBM MQ Windows można zmienić za pomocą panelu Zarządzanie komputerem.

O tym zadaniu

Aby zmienić hasło lokalnego konta użytkownika usługi IBM MQ Windows , wykonaj następujące kroki:

Procedura

1. Zidentyfikuj użytkownika, dla którego działa usługa.
2. Zatrzymaj usługę IBM MQ na panelu Zarządzanie komputerem.
3. Zmień wymagane hasło w taki sam sposób, jak hasło osoby.
4. W panelu Zarządzanie komputerem przejdź do właściwości usługi IBM MQ .
5. Wybierz stronę **Logowanie** .
6. Potwierdź, że podana nazwa konta jest zgodna z nazwą użytkownika, dla którego zmodyfikowano hasło.
7. Wpisz hasło w polu **Hasło** i **Potwierdź hasło** , a następnie kliknij przycisk **OK**.

Windows *Zmiana hasła dla usługi IBM MQ Windows dla instalacji działającej na koncie użytkownika domeny*

Zamiast używać programu Prepare IBM MQ Wizard do wprowadzania szczegółów konta użytkownika domeny, można użyć panelu Zarządzanie komputerem, aby zmienić szczegóły **Logowanie** dla usługi IBM MQ specyficznej dla instalacji.

O tym zadaniu

Jeśli usługa IBM MQ Windows dla instalacji jest uruchomiona z konta użytkownika należącego do domeny, można zmienić hasło dla tego konta w następujący sposób:

Procedura

1. Zmień hasło dla konta domeny w kontrolerze domeny. Może być konieczne poproście o to administratora domeny.
2. Wykonaj następujące czynności, aby zmodyfikować stronę **Logowanie** dla usługi IBM MQ .
   a) Zidentyfikuj użytkownika, który uruchomiła usługę.
   b) Zatrzymaj usługę IBM MQ na panelu Zarządzanie komputerem.
   c) Zmień wymagane hasło w taki sam sposób, jak hasło osoby.
   d) W panelu Zarządzanie komputerem przejdź do właściwości usługi IBM MQ .
   e) Wybierz stronę **Logowanie** .
   f) Potwierdź, że podana nazwa konta jest zgodna z nazwą użytkownika, dla którego zmodyfikowano hasło.
   g) Wpisz hasło w polu **Hasło** i **Potwierdź hasło** , a następnie kliknij przycisk **OK**.

   Konto użytkownika, w ramach którego działa usługa IBM MQ Windows , wykonuje wszystkie komendy MQSC wydawane przez aplikacje interfejsu użytkownika lub wykonywane automatycznie podczas uruchamiania systemu, zamykania systemu lub odtwarzania usługi. Z tego powodu to konto użytkownika musi mieć uprawnienia administracyjne IBM MQ . Domyślnie jest on dodawany do lokalnej grupy mqm na serwerze. Jeśli to przypisanie zostanie usunięte, usługa IBM MQ Windows nie będzie działać. Więcej informacji na temat uprawnień użytkownika zawiera sekcja “Wymagane prawa użytkownika dla usługi IBM MQ w systemie Windows” na stronie 159.

   Jeśli wystąpi problem z bezpieczeństwem związany z kontem użytkownika, w ramach którego działa usługa IBM MQ Windows , w dzienniku zdarzeń systemu pojawią się komunikaty o błędach i opisy.

Zadania pokrewne

Konfigurowanie produktu IBM MQ z produktem Prepare IBM MQ Wizard

Windows *Uwagi dotyczące awansowania serwerów Windows do kontrolerów domeny*

Podczas awansowania serwera Windows do kontrolera domeny należy rozważyć, czy ustawienie zabezpieczeń dotyczące uprawnień użytkowników i grup jest odpowiednie. Podczas zmiany stanu komputera z systemem Windows między serwerem a kontrolerem domeny należy wziąć pod uwagę, że może to mieć wpływ na działanie systemu IBM MQ , ponieważ produkt IBM MQ używa lokalnie zdefiniowanej grupy mqm.

Ustawienia zabezpieczeń dotyczące uprawnień użytkownika i grupy domeny

IBM MQ korzysta z informacji o członkostwie w grupach w celu zaimplementowania swojej strategii bezpieczeństwa, co oznacza, że ważne jest, aby ID użytkownika wykonującego operacje IBM MQ mógł określić przynależność do grup innych użytkowników.

Podczas awansowania serwera Windows do kontrolera domeny wyświetlana jest opcja ustawień zabezpieczeń dotyczących uprawnień użytkowników i grup. Ta opcja określa, czy dowolni użytkownicy mogą pobierać przypisania do grup z katalogu aktywnego. Jeśli kontroler domeny jest skonfigurowany w taki sposób, że konta lokalne mają uprawnienia do wysyłania zapytań o przynależność do grup kont użytkowników domeny, domyślny identyfikator użytkownika utworzony przez program IBM MQ podczas procesu instalacji może uzyskać przynależność do grup dla innych użytkowników zgodnie z wymaganiami. Jeśli jednak kontroler domeny jest skonfigurowany w taki sposób, że konta lokalne nie mają uprawnień do wysyłania zapytań o członkostwo w grupie kont użytkowników domeny, uniemożliwia to produktowi IBM MQ zakończenie sprawdzania, czy użytkownicy zdefiniowani w domenie mają uprawnienia dostępu do menedżerów kolejek lub kolejek, a dostęp kończy się niepowodzeniem. Jeśli produkt Windows jest używany na kontrolerze domeny, który został skonfigurowany w ten sposób, należy użyć specjalnego konta użytkownika domeny z wymaganymi uprawnieniami.

W takim przypadku należy wiedzieć:

- Sposób zachowania uprawnień zabezpieczeń dla danej wersji produktu Windows .
- W tej sekcji opisano, w jaki sposób zezwolić członkom grupy domeny mqm na odczytywanie przypisania do grupy.
- W tej sekcji opisano sposób konfigurowania usługi produktu IBM MQ Windows do uruchamiania przez użytkownika należącego do domeny.

Więcej informacji na ten temat zawiera sekcja Konfigurowanie kont użytkowników dla produktu IBM MQ.

Dostęp produktu IBM MQ do lokalnej grupy mqm

Gdy serwery Windows są awansowane do kontrolerów domeny lub z nich degradowane, produkt IBM MQ traci dostęp do lokalnej grupy mqm.

Gdy serwer jest promowany jako kontroler domeny, zasięg zmienia się z lokalnego na lokalny. Po zdegradowaniu komputera do serwera usuwane są wszystkie lokalne grupy domeny. Oznacza to, że zmiana komputera z serwera na kontroler domeny i z powrotem na serwer powoduje utratę dostępu do lokalnej grupy mqm. Objawem jest błąd wskazujący na brak lokalnej grupy mqm, na przykład:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

Aby rozwiązać ten problem, 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 IBM MQ w nowo utworzonej lokalnej grupie mqm. Jeśli komputer jest członkiem domeny, należy również dodać grupę domain mqm do lokalnej grupy mqm, aby nadać uprawnionym identyfikatorom użytkowników domeny uprzywilejowanej IBM MQ wymagany poziom uprawnień.

Windows *Ograniczenia dotyczące grup zagnieżdżonych w systemie Windows*

Istnieją ograniczenia dotyczące używania grup zagnieżdżonych. Wynikają one częściowo z poziomu funkcjonalnego domeny, a częściowo z ograniczeń systemu IBM MQ .

Active Directory może obsługiwać różne typy grup w kontekście domeny w zależności od poziomu funkcjonalnego domeny. Domyślnie domeny Windows 2003 znajdują się w katalogu " 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 dozwolone podczas konfigurowania identyfikatorów użytkowników w środowisku domeny. Szczegółowe informacje na temat zasięgu grupy i kryteriów włączania można znaleźć w dokumentacji usługi Active Directory .

Oprócz wymagań Active Directory , dodatkowe ograniczenia są nakładane na identyfikatory używane przez produkt IBM MQ. Sieciowe interfejsy API używane przez produkt IBM MQ nie obsługują wszystkich konfiguracji, które są obsługiwane przez poziom funkcjonalny domeny. W wyniku tego program IBM MQ nie może wysłać zapytań o przynależność do grup dla 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. Obsługiwane są jednak natychmiast zagnieżdżone grupy globalne lub uniwersalne.

Windows *Autoryzowanie użytkowników do zdalnego korzystania z produktu IBM MQ*

Jeśli konieczne jest utworzenie i uruchomienie menedżerów kolejek po nawiązaniu zdalnego połączenia z programem IBM MQ , należy mieć dostęp na poziomie użytkownika `Utwórz obiekty globalne` .

O tym zadaniu

Uwaga: Administratorzy mają domyślnie dostęp na poziomie `Utwórz obiekty globalne` , dlatego administrator może tworzyć i uruchamiać menedżery kolejek w przypadku połączenia zdalnego bez zmiany uprawnień użytkownika.

Jeśli połączenie z komputerem z systemem Windows jest nawiązywane przy użyciu usług terminalowych lub połączenia pulpitu zdalnego i występują problemy z tworzeniem, uruchamianiem lub usuwaniem menedżera kolejek, może to być spowodowane brakiem dostępu użytkownika do opcji `Utwórz obiekty globalne`.

Dostęp użytkownika `Utwórz obiekty globalne` ogranicza uprawnienia użytkowników do tworzenia obiektów w globalnej przestrzeni nazw. Aby aplikacja mogła utworzyć obiekt globalny, musi być uruchomiona w globalnej przestrzeni nazw lub użytkownik, który uruchomił aplikację, musi mieć zastosowany dostęp użytkownika `Utwórz obiekty globalne` .

Jeśli połączenie zdalne z komputerem z systemem Windows jest nawiązywane przy użyciu usług terminalowych lub połączenia z pulpitem zdalnym, aplikacje działają we własnej lokalnej przestrzeni nazw. Próba utworzenia lub usunięcia menedżera kolejek za pomocą komendy IBM MQ Explorer , **`crtmqm`** lub **`dltmqm`** albo uruchomienia menedżera kolejek za pomocą komendy **`strmqm`** spowoduje niepowodzenie autoryzacji. Spowoduje to utworzenie IBM MQ FDC z ID sondy XY132002.

Uruchomienie menedżera kolejek za pomocą programu IBM MQ Explorerlub komendy **`amqmdain qmgr start`** działa poprawnie, ponieważ te komendy 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 produktem IBM MQ nie działają podczas korzystania z usług terminalowych, należy spróbować ustawić uprawnienie 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 **Panelu sterowania** > **System i konserwacja** > **Narzędzia administracyjne**.

   Windows 8.1
   Dostęp do tego panelu można uzyskać za pomocą **narzędzi administracyjnych** > **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 nową grupę do strategii `Utwórz obiekty globalne` .

Windows *Program obsługi wyjścia kanału SSPI w systemie Windows*

Produkt IBM MQ for Windows dostarcza program obsługi wyjścia zabezpieczeń, który może być używany zarówno w kanałach komunikatów, jak i MQI. Wyjście jest dostarczane jako kod źródłowy i kod obiektu oraz udostępnia uwierzytelnianie jednokierunkowe i dwukierunkowe.

Wyjście zabezpieczeń używa interfejsu SSPI (Security Support Provider Interface), który udostępnia zintegrowane zabezpieczenia platform Windows .

Wyjście zabezpieczeń udostępnia następujące usługi identyfikacji i uwierzytelniania:

uwierzytelnianie jednokierunkowe
W tym celu używana jest obsługa uwierzytelniania Windows NT LAN Manager (NTLM). Protokół NTLM umożliwia serwerom uwierzytelnianie klientów. Nie pozwala on klientowi na uwierzytelnienie serwera lub jednemu serwerowi na uwierzytelnienie innego. Protokół NTLM został zaprojektowany dla środowiska sieciowego, w którym zakłada się, że serwery są oryginalne. Protokół NTLM jest obsługiwany na wszystkich platformach Windows , które są obsługiwane przez system IBM WebSphere MQ 7.0.

Ta usługa jest zwykle używana w kanale MQI w celu umożliwienia menedżerowi kolejek serwera uwierzytelniania aplikacji IBM MQ MQI client . Aplikacja kliencka jest identyfikowana przez identyfikator użytkownika powiązany z uruchomionym procesem.

Aby przeprowadzić uwierzytelnianie, wyjście zabezpieczeń na końcu kanału po stronie klienta uzyskuje znacznik uwierzytelniania z protokołu NTLM i wysyła znacznik w komunikacie bezpieczeństwa do swojego partnera na drugim końcu kanału. Wyjście zabezpieczeń partnera przekazuje znacznik do protokołu NTLM, który sprawdza, czy znacznik jest autentyczny. Jeśli wyjście zabezpieczeń partnera nie jest zadowalające z powodu autentyczności tokenu, agent MCA zamyka kanał.

Uwierzytelnianie dwukierunkowe (wzajemne)
Używane są usługi uwierzytelniania Kerberos . Protokół Kerberos nie zakłada, że serwery w środowisku sieciowym są autentyczne. Serwery mogą uwierzytelniać klientów i inne serwery, a klienty mogą uwierzytelniać serwery. Protokół Kerberos jest obsługiwany na wszystkich platformach Windows , które są obsługiwane przez system 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 wzajemne uwierzytelnianie menedżera kolejek serwera i aplikacji IBM MQ MQI client . Menedżer kolejek jest identyfikowany przez nazwę poprzedzoną łańcuchem `ibmMQSeries/`. Aplikacja kliencka jest identyfikowana przez identyfikator użytkownika powiązany z uruchomionym procesem.

Aby przeprowadzić uwierzytelnianie wzajemne, inicjujące wyjście zabezpieczeń uzyskuje znacznik uwierzytelniania z serwera zabezpieczeń Kerberos i wysyła znacznik w komunikacie bezpieczeństwa do swojego partnera. Wyjście zabezpieczeń partnera przekazuje znacznik do serwera Kerberos , który sprawdza jego autentyczność. Serwer zabezpieczeń Kerberos generuje drugi znacznik, który partner wysyła w komunikacie bezpieczeństwa do inicjującego wyjścia zabezpieczeń. Następnie inicjujące wyjście zabezpieczeń prosi serwer Kerberos o sprawdzenie, czy drugi token jest autentyczny. Podczas tej wymiany, jeśli jedno z wyjść zabezpieczeń nie jest spełnione z uwierzytelnieniem tokenu wysłanego przez drugie, wysyła do agenta MCA instrukcję zamknięcia kanału.

Wyjście zabezpieczeń jest dostarczane zarówno w formacie źródłowym, jak i w formacie obiektu. Można użyć kodu źródłowego jako punktu początkowego do pisania własnych programów obsługi wyjścia kanału lub użyć dostarczonego modułu wynikowego. Moduł obiektu ma dwa punkty wejścia, jeden dla uwierzytelniania jednokierunkowego przy użyciu obsługi uwierzytelniania NTLM, a drugi dla uwierzytelniania dwukierunkowego przy użyciu usług uwierzytelniania Kerberos .

Więcej informacji na temat działania programu obsługi wyjścia kanału SSPI oraz instrukcje dotyczące sposobu jego implementacji 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 zastosowane do plików i katalogów IBM MQ . Jeśli używany jest wysoce bezpieczny szablon, należy go zastosować przed zainstalowaniem produktu IBM MQ.

Produkt Windows obsługuje tekstowe pliki szablonów zabezpieczeń, których można użyć do zastosowania jednolitych ustawień zabezpieczeń na jednym lub wielu komputerach z przystawką Konfiguracja zabezpieczeń i analiza MMC. W szczególności produkt Windows udostępnia kilka szablonów, które obejmują szereg ustawień zabezpieczeń w celu zapewnienia konkretnych poziomów zabezpieczeń. Do tych szablonów należą: Zgodne, Bezpieczne i Wysokich zabezpieczeń.

Zastosowanie jednego z tych szablonów może mieć wpływ na ustawienia zabezpieczeń stosowane do plików i katalogów IBM MQ . Jeśli ma być używany szablon Highly Secure, należy skonfigurować komputer przed zainstalowaniem produktu IBM MQ.

Jeśli szablon o wysokim poziomie bezpieczeństwa zostanie zastosowany na komputerze, na którym jest już zainstalowany produkt IBM MQ , wszystkie uprawnienia ustawione dla plików i katalogów IBM MQ zostaną usunięte. Ponieważ te uprawnienia zostały usunięte, użytkownik traci dostęp do grupy *Administrator*, *mqm*oraz, jeśli ma to zastosowanie, do grupy *Wszyscy* z poziomu katalogów błędów.

Windows *Konfigurowanie dodatkowych uprawnień dla aplikacji Windows łączących się z serwerem IBM MQ*

Konto, z którego uruchamiane są procesy IBM MQ , może wymagać dodatkowej autoryzacji, zanim będzie można nadać dostęp SYNCHRONIZE do procesów aplikacji.

O tym zadaniu

Mogą wystąpić problemy w przypadku aplikacji Windows , na przykład stron ASP, łączących się z serwerem IBM MQ , które są skonfigurowane do działania na wyższym niż zwykle poziomie bezpieczeństwa.

Produkt IBM MQ wymaga dostępu do procesów aplikacji za pomocą opcji SYNCHRONIZE w celu koordynowania pewnych działań. Gdy aplikacja serwera po raz pierwszy próbuje nawiązać połączenie z menedżerem kolejek IBM MQ modyfikuje proces, nadając uprawnienie SYNCHRONIZE administratorom produktu IBM MQ . Jednak konto, z którego uruchamiane są procesy IBM MQ , może wymagać dodatkowej autoryzacji przed nadaniem żądanego dostępu.

Aby skonfigurować dodatkowe uprawnienia dla ID użytkownika, dla którego są uruchomione procesy IBM MQ , wykonaj następujące kroki:

Procedura

1. Uruchom narzędzie Zasady zabezpieczeń lokalnych, kliknij opcję **Ustawienia zabezpieczeń**->**Zasady lokalne**->**Przypisania praw użytkownika**, a następnie kliknij opcję **Debuguj programy**.
2. Kliknij dwukrotnie opcję **Debuguj programy**, a następnie dodaj ID użytkownika IBM MQ do listy.

   Jeśli system znajduje się w domenie Windows , a obowiązujące ustawienie strategii nadal nie jest ustawione, nawet jeśli lokalne ustawienie strategii jest ustawione, identyfikator użytkownika musi być autoryzowany w ten sam sposób na poziomie domeny za pomocą narzędzia strategii bezpieczeństwa domeny.

IBM i Konfigurowanie zabezpieczeń w systemie IBM i

Zabezpieczenia w systemie IBM i są implementowane przy użyciu menedżera OAM (IBM MQ Object Authority Manager) i zabezpieczeń na poziomie obiektu systemu IBM i .

Zagadnienia dotyczące bezpieczeństwa, które muszą być uwzględnione podczas określania uprawnień dostępu do obiektów IBM MQ .

Podczas konfigurowania uprawnień dla użytkowników w przedsiębiorstwie należy wziąć pod uwagę następujące kwestie:

1. Nadaj i odbierz uprawnienia do komend IBM MQ for IBM i za pomocą komend IBM i GRTOBJAUT i RVKOBJAUT .

   W bibliotece QMQM niektóre obiekty niebędące komendami (* cmd) mają uprawnienie ***PUBLIC** do pliku ***USE**. Nie należy zmieniać uprawnień do tych obiektów ani używać listy autoryzacji do udostępniania uprawnień. Niepoprawne uprawnienia mogą naruszyć funkcjonalność produktu IBM MQ .
2. Podczas instalacji systemu IBM MQ for IBM itworzone są następujące specjalne profile użytkowników:

   QMQM,
   Jest używany głównie do wewnętrznych funkcji produktu. Można go jednak użyć do uruchamiania zaufanych aplikacji przy użyciu powiązań MQCNO_FASTPATH_BINDINGS. Patrz sekcja Nawiązywanie połączenia z menedżerem kolejek za pomocą wywołania MQCONNX.

   QMQMADM,
   Jest używany jako profil grupowy dla administratorów produktu IBM MQ. Profil grupowy zapewnia dostęp do komend CL i zasobów IBM MQ .

   Jeśli komenda SBMJOB jest używana do wprowadzania programów wywołujących komendy systemu IBM MQ , parametr USER nie może być jawnie ustawiony na wartość QMQMADM. Zamiast tego należy ustawić wartość USER na QMQM lub inny profil użytkownika, dla którego określono grupę QMQMADM.
3. Jeśli komendy kanału są wysyłane do zdalnych menedżerów kolejek, upewnij się, że profil użytkownika należy do grupy QMQMADM w systemie docelowym. Listę komend PCF i kanału MQSC zawiera sekcja Komendy CLIBM MQ for IBM i.
4. Zestaw grup powiązany z użytkownikiem jest buforowany, gdy autoryzacje grup są obliczane przez system OAM.

   Wszelkie zmiany wprowadzone w przypisaniach do grup użytkownika po buforowaniu 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. Komendy te obejmują:
   - 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 specjalnych rozważań. Szczegółowe informacje na temat wyjść zabezpieczeń zawiera sekcja “Przegląd wyjścia zabezpieczeń” na stronie 117.
7. Można zastąpić programy wyjścia kanału i monitora wyzwalacza. Odpowiedzialność za bezpieczeństwo takich wymian ponosi programista.

IBM i Menedżer uprawnień do obiektów w systemie IBM i

Menedżer uprawnień do obiektów (object authority manager-OAM) zarządza autoryzacjami użytkowników do manipulowania obiektami IBM MQ , w tym kolejkami i definicjami procesów. Udostępnia także interfejs komend, za pomocą którego można nadać lub odebrać uprawnienia dostępu do obiektu określonej grupie użytkowników. Decyzja o zezwoleniu na dostęp do zasobu jest podejmowana przez menedżera OAM,

a menedżer kolejek postępuje zgodnie z tą decyzją. Jeśli mechanizm OAM nie może podjąć decyzji, menedżer kolejek uniemożliwia dostęp do tego zasobu.

Za pomocą OAM można kontrolować:

- Dostęp do obiektów IBM MQ za pośrednictwem interfejsu MQI. Gdy aplikacja próbuje uzyskać dostęp do obiektu, OAM sprawdza, czy profil użytkownika wysyłający żądanie ma uprawnienia do żądanej operacji.

  W szczególności oznacza to, że kolejki i 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 wykonywać zarówno operacje umieszczania, jak i pobierania; inna grupa może tylko przeglądać kolejkę (MQGET z opcją przeglądania). Podobnie, niektóre grupy mogą mieć uprawnienie do pobierania i umieszczania w kolejce, 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 , użytkownik musi mieć uprawnienia do wywoływania komendy i uzyskiwania dostępu do obiektu, do którego następuje odwołanie. Administratorzy mają dostęp do wszystkich zasobów IBM MQ .

Dostęp do obiektów 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 IBM MQ for IBM i są dostarczane z właścicielem QMQM, a profil administracyjny (QMQMADM) ma uprawnienia *USE z dostępem *PUBLIC ustawionym na *EXCLUDE.

Uwaga: Program QSRDUPER jest używany przez instalator programu licencjonowanego IBM MQ for IBM i do duplikowania obiektów komendy (*CMD) w bibliotece QSYS. W systemie IBM i V5R4 i nowszych program QSRDUPER został zmieniony w taki sposób, że domyślnym działaniem jest utworzenie komendy proxy, a nie duplikowanie oryginalnej komendy. Komenda proxy przekierowuje wykonanie komendy do innej komendy i ma atrybut PRX. Jeśli komenda proxy o takiej samej nazwie jak kopiowana komenda istnieje w bibliotece QSYS, uprawnienia prywatne do komendy proxy nie są nadawane komendzie w bibliotece produktu. Próbuje wyświetlić lub uruchomić komendę proxy w QSYS, sprawdź uprawnienia komendy docelowej w bibliotece produktu. Wszelkie zmiany uprawnień do obiektów *CMD muszą być wykonane w bibliotece produktu (QMQM), a zmiany 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 umożliwiają publiczne użycie tych komend, jeśli użytkownik ma wymagane uprawnienie OAM do obiektów IBM MQ , aby wprowadzić te zmiany.

Aby być administratorem produktu IBM MQ w systemie IBM i, należy być członkiem *grupy QMQMADM*. Ta grupa ma właściwości podobne do właściwości grupy mqm z systemów AIX, Linux, and Windows . W szczególności grupa QMQMADM jest tworzona podczas instalowania produktu IBM MQ for IBM i, a członkowie grupy QMQMADM mają dostęp do wszystkich zasobów produktu IBM MQ w systemie. Użytkownik ma również dostęp do wszystkich zasobów systemu IBM MQ , jeśli ma uprawnienia *ALLOBJ.

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

Pojęcia pokrewne

“Uprawnienia do administrowania systemem IBM MQ w systemie IBM i” na stronie 95

IBM i *Uprawnienia dostępu do obiektów IBM MQ w systemie IBM i*

Uprawnienia dostępu wymagane do uruchamiania komend CL systemu IBM MQ .

IBM MQ for IBM i dzieli komendy CL produktu na dwie grupy:

Grupa 1

Aby przetwarzać te komendy, użytkownicy muszą należeć do grupy użytkowników QMQMADM lub mieć uprawnienie *ALLOBJ. Użytkownicy posiadający jedno z tych uprawnień mogą przetwarzać wszystkie komendy we wszystkich kategoriach bez konieczności posiadania dodatkowych uprawnień.

Uwaga: Te uprawnienia przesłaniają uprawnienia OAM.

Komendy te można pogrupować w następujący sposób:

- Komendy serwera komend
  - ENDMQMCSVR, Zakończenie działania serwera komend IBM MQ
  - STRMQMCSVR, Uruchomienie serwera komend IBM MQ
- Komenda programu obsługi kolejki niedostarczonych komunikatów
  - STRMQMDLQ, Uruchamianie programu obsługi kolejki niedostarczonych komunikatów IBM MQ
- Komenda nasłuchiwania
  - ENDMQMLSR, zakończenie programu nasłuchującego IBM MQ
  - STRMQMLSR, Uruchamianie nasłuchiwania obiektów innych niż obiekty
- Komendy odtwarzania
  - RCDMQMIMG, rejestrowanie obrazu obiektu IBM MQ
  - RCRMQMOBJ, Ponowne 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 (End Message Queue Manager)
  - STRMQM, Uruchomienie menedżera kolejek komunikatów
- Komendy ochrony
  - GRTMQMAUT, Nadawanie uprawnień do obiektu IBM MQ
  - RVKMQMAUT, Odwołanie Uprawnienia Do Obiektu IBM MQ
- Komenda śledzenia
  - TRCMQM, Śledzenie Zadania IBM MQ
- Komendy transakcji
  - RSVMQMTRN, rozstrzyganie transakcji IBM MQ
- Komendy monitora wyzwalacza
  - STRMQMTRM, Uruchomienie monitora wyzwalacza
- Komendy systemu IBM MQSC
  - RUNMQSC, Uruchom Komendy IBM MQSC
  - STRMQMMQSC, Komendy Uruchomienie IBM MQSC

Grupa 2

Pozostałe komendy, dla których wymagane są dwa poziomy uprawnień:

1. Uprawnienie IBM i do uruchomienia komendy. Administrator systemu IBM MQ ustawia tę wartość 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, dające poprawne uprawnienie IBM i w kroku 1.

   Uprawnienie to jest kontrolowane przez użytkownika posiadającego odpowiednie uprawnienie OAM dla wymaganego działania, ustawione 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 * connect do menedżera kolejek i uprawnienia * admchg do kanału.
  - CPYMQMCHL, Kopiowanie kanału IBM MQ

    Wymaga to uprawnienia * connect i * admcrt do menedżera kolejek, uprawnienia * admdsp do domyślnego typu kanału, który ma zostać 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 uprawnienia * connect i * admcrt dla menedżera kolejek, uprawnienia * admdsp dla domyślnego typu kanału do utworzenia i uprawnienia * admcrt dla klasy obiektu kanału.

    Na przykład utworzenie kanału nadawczego wymaga uprawnienia * admdsp do systemu SYSTEM.DEF.SENDER
  - DLTMQMCHL, Usunięcie kanału IBM MQ

    Wymaga to uprawnienia * connect do menedżera kolejek i uprawnienia * admdlt do kanału.
  - RSVMQMCHL, rozstrzyganie kanału IBM MQ

    Wymaga to uprawnienia * connect do menedżera kolejek i uprawnienia * ctrlx do kanału.
- Wyświetl komendy

  Aby przetworzyć komendy DSP, należy nadać użytkownikowi uprawnienia `*connect` i `*admdsp` do menedżera kolejek wraz z dowolną z wymienionych opcji:
  - DSPMQM, Wyświetlenie menedżera kolejek komunikatów
  - DSPMQMAUT, Wyświetlenie uprawnień do obiektu IBM MQ
  - DSPMQMAUTI, Wyświetlenie IBM MQ informacji uwierzytelniającej- `*admdsp` dla obiektu informacji uwierzytelniającej
  - DSPMQMCHL, wyświetlenie IBM MQ kanału- `*admdsp` dla kanału
  - DSPMQMCSVR, Wyświetlenie serwera komend IBM MQ
  - DSPMQMNL, Wyświetl IBM MQ Lista nazw- `*admdsp` na liście nazw
  - DSPMQMOBJN, Wyświetlenie nazw obiektów IBM MQ

  - DSPMQMPRC, wyświetl IBM MQ proces- *admdsp dla procesu
  - DSPMQMQ, wyświetlenie IBM MQ kolejki- *admdsp dla kolejki
  - DSPMQMTOP, wyświetl IBM MQ Temat- *admdsp dla tematu
- Praca z komendami

  Aby przetworzyć komendy WRK i wyświetlić panel opcji, należy nadać użytkownikowi uprawnienia *connect i *admdsp do menedżera kolejek wraz z każdą wymienioną opcją:

  - WRKMQM, Praca z menedżerami kolejek komunikatów
  - WRKMQMAUT, Praca z uprawnieniami do obiektów IBM MQ
  - WRKMQMAUTD, Praca z danymi uprawnień do obiektu IBM MQ
  - WRKMQMAUTI, Praca z informacjami uwierzytelniającymi systemu IBM MQ
    - *admchg dla komendy Zmiana obiektu informacji uwierzytelniającej systemu IBM MQ (Change Authentication Information Object).
    - *admcrt dla komendy tworzenia i kopiowania obiektu informacji uwierzytelniającej systemu IBM MQ .
    - *admdlt dla komendy Usunięcie obiektu informacji uwierzytelniającej (Delete IBM MQ Authentication Information Object).
    - *admdsp dla komendy Wyświetlenie obiektu informacji uwierzytelniającej (Display IBM MQ Authentication Information Object).
  - WRKMQMCHL, Praca z kanałem IBM MQ

    Wymaga to następujących uprawnień:

    - *admchg dla komendy Zmiana kanału (Change IBM MQ Channel).
    - *admclr dla komendy Clear IBM MQ Channel.
    - *admcrt dla komendy tworzenia i kopiowania kanału IBM MQ .
    - *admdlt dla komendy Usunięcie kanału (Delete IBM MQ Channel).
    - *admdsp dla komendy Wyświetlenie kanału (Display IBM MQ Channel).
    - *ctrl dla komendy Uruchomienie kanału (Start IBM MQ Channel).
    - *ctrl dla komendy End IBM MQ Channel.
    - *ctrl dla komendy Ping w kanale IBM MQ .
    - *ctrlx dla komendy resetowania kanału IBM MQ .
    - *ctrlx dla komendy Resolve IBM MQ Channel.
  - 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 systemu IBM MQ

    Wymaga to następujących uprawnień:

    - *admchg dla komendy Change IBM MQ Namelist.
    - *admcrt dla komendy Create i Copy IBM MQ Namelist.
    - *admdlt dla komendy Delete IBM MQ Namelist.

- *admdsp dla komendy Wyświetlenie listy nazw (Display IBM MQ Namelist).

– WRKMQMPRC, praca z procesami IBM MQ

  Wymaga to następujących uprawnień:

  - *admchg dla komendy Change IBM MQ Process.
  - *admcrt dla komendy tworzenia i kopiowania procesu IBM MQ .
  - *admdlt dla komendy Delete IBM MQ Process.
  - *admdsp dla komendy wyświetlania procesu IBM MQ .

– WRKMQMQ, Praca z kolejkami IBM MQ

  Wymaga to następujących uprawnień:

  - *admchg dla komendy Zmiana kolejki (Change IBM MQ Queue).
  - *admclr dla komendy Usuwanie zawartości kolejki (Clear IBM MQ Queue).
  - *admcrt dla komendy tworzenia i kopiowania kolejki IBM MQ .
  - *admdlt dla komendy Usunięcie kolejki (Delete IBM MQ Queue).
  - *admdsp dla komendy Wyświetlenie kolejki (Display IBM MQ Queue).

– WRKMQMQSTS, praca ze statusem kolejki IBM MQ

– WRKMQMTOP, Praca z tematami IBM MQ

  Wymaga to następujących uprawnień:

  - *admchg dla komendy Change IBM MQ Topic.
  - *admcrt dla komendy tworzenia i kopiowania tematu IBM MQ .
  - *admdlt dla komendy Delete IBM MQ Topic.
  - *admdsp dla komendy wyświetlania tematu IBM MQ .

– WRKMQMSUB, Praca z subskrypcjami IBM MQ

• Inne komendy kanału

  Aby przetworzyć komendy kanału, należy nadać użytkownikowi wymienione uprawnienia szczegółowe:

  – ENDMQMCHL, zakończenie kanału 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, Ping dla kanału IBM MQ

    Wymaga to uprawnienia *connect i *inq do menedżera kolejek oraz 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 oraz uprawnienia *allmqi do kolejki inicjującej powiązanej z kolejką transmisji kanału.

  – STRMQMLSR, Uruchamianie programu nasłuchującego IBM MQ

Wymaga to uprawnienia * connect do menedżera kolejek i uprawnienia * ctrl do nazwanego obiektu nasłuchiwania.

- Inne komendy:

  Aby przetworzyć następujące komendy, należy nadać użytkownikowi wymienione uprawnienia szczegółowe:

  – CCTMQM, połączenie z menedżerem kolejek komunikatów

    Nie wymaga to uprawnień do obiektu IBM MQ .

  – CHGMQM, Zmiana menedżera kolejek komunikatów

    Wymaga to uprawnień `*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 uwierzytelniającej.

  – 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, Usuwanie zawartości kolejki IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admclr` do kolejki.

  – CPYMQMAUTI, Kopiowanie Informacji Uwierzytelniania IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admdsp` do obiektu informacji uwierzytelniającej oraz uprawnienia `*admcrt` do klasy obiektu informacji uwierzytelniającej.

  – CPYMQMNL, Kopiowanie listy nazw IBM MQ

    Wymaga to uprawnień `*connect` i `*admcrt` do menedżera kolejek.

  – CPYMQMPRC, kopiowanie procesu IBM MQ

    Wymaga to uprawnień `*connect` i `*admcrt` do menedżera kolejek.

  – CPYMQMQ, Kopiowanie Kolejki IBM MQ (Copy Queue)

    Wymaga to uprawnień `*connect` i `*admcrt` do menedżera kolejek.

  – CRTMQMAUTI, Tworzenie Informacji Uwierzytelniającej IBM MQ

    Wymaga to uprawnienia `*connect` do menedżera kolejek i uprawnienia `*admdsp` do obiektu informacji uwierzytelniającej oraz uprawnienia `*admcrt` do klasy obiektu informacji uwierzytelniającej.

  – CRTMQMNL, Tworzenie IBM MQ listy nazw

    Wymaga to uprawnienia `*connect` i `*admcrt` do menedżera kolejek oraz uprawnienia `*admdsp` do domyślnej listy nazw.

  – CRTMQMPRC, Tworzenie procesu IBM MQ

    Wymaga to uprawnień `*connect` i `*admcrt` do menedżera kolejek oraz uprawnienia `*admdsp` do procesu domyślnego.

  – CRTMQMQ, Tworzenie kolejki IBM MQ

    Wymaga to uprawnień `*connect` i `*admcrt` do menedżera kolejek oraz uprawnienia `*admdsp` do kolejki domyślnej.

  – CVTMQMDTA, Komenda Konwersja Typu 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 uwierzytelniającej.

– 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, rozłączenie z menedżerem kolejek komunikatów

  Nie wymaga to uprawnień do obiektu IBM MQ .

– RFRMQMAUT, odświeżanie zabezpieczeń

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

– RFRMQMCL, Odświeżanie klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

– RSMMQMCLQM, wznawianie menedżera kolejek klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

– RSTMQMCL, Resetowanie klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

– SPDMQMCLQM, Zawieszenie menedżera kolejek klastra

  Wymaga to uprawnienia `*connect` do menedżera kolejek.

IBM i *Autoryzacje dostępu w systemie IBM i*

W tej sekcji zamieszczono informacje na temat komend autoryzacji dostępu.

Autoryzacje zdefiniowane przez słowo kluczowe AUT w komendach GRTMQMAUT i RVKMQMAUT można podzielić na następujące kategorie:

- Autoryzacje związane z wywołaniami MQI
- Komendy administracyjne związane z autoryzacją
- Autoryzacje kontekstowe
- Autoryzacje ogólne, to jest dla wywołań MQI, dla komend lub dla obu

W poniższych tabelach przedstawiono różne uprawnienia, używając parametru AUT dla wywołań MQI, wywołań kontekstowych, komend MQSC i PCF oraz operacji ogólnych.

Tabela 15. Autoryzacje dla wywołań MQI

Testowana aplikacja	**Opis**
*ALTUSR	Zezwalaj na używanie uprawnień innego użytkownika dla wywołań MQOPEN i MQPUT1 .
*BROWSE	Pobranie komunikatu z kolejki za pomocą wywołania MQGET z opcją BROWSE.
*CONNECT	Połącz aplikację z określonym menedżerem kolejek, wywołując wywołanie MQCONN.
*GET	Pobranie komunikatu z kolejki za pomocą wywołania MQGET.

Tabela 15. Autoryzacje dla wywołań MQI (kontynuacja)	
Testowana aplikacja	**Opis**
*INQ	Utwórz zapytanie dotyczące konkretnej kolejki, wywołując wywołanie MQINQ.
*PUB	Otwórz temat, aby opublikować komunikat przy użyciu wywołania MQPUT.
*PUT	Umieść komunikat w konkretnej kolejce, wywołując wywołanie MQPUT.
*WZNOWIENIE	Wznawianie subskrypcji przy użyciu wywołania MQSUB.
*SET	Ustawianie atrybutów kolejki z interfejsu MQI za pomocą wywołania MQSET. Jeśli otwierasz kolejkę dla wielu opcji, musisz być autoryzowany dla każdej z nich.
*SUB	Tworzenie, zmiana lub wznawianie subskrypcji tematu przy użyciu wywołania MQSUB.

Tabela 16. Autoryzacje dla wywołań kontekstowych	
Testowana aplikacja	**Opis**
*PASSALL	Przekaż cały kontekst w określonej kolejce. Wszystkie pola kontekstu są kopiowane z oryginalnego żądania.
*PASSID	Przekaż kontekst tożsamości w określonej kolejce. Kontekst tożsamości jest taki sam, jak kontekst żądania.
*SETALL	Ustawia cały kontekst w określonej kolejce. Jest ona używana przez specjalne programy narzędziowe systemu.
*SETID	Ustaw kontekst tożsamości w określonej kolejce. Jest ona używana przez specjalne programy narzędziowe systemu.

Tabela 17. Autoryzacje dla wywołań MQSC i PCF	
Testowana aplikacja	**Opis**
*ADMCHG	Zmień atrybuty określonego obiektu.
*ADMCLR	Wyczyść określony obiekt (tylko komenda PCF Clear object).
*ADMCRT	Utwórz obiekty określonego typu.
*ADMDLT	Usuń określony obiekt.
*ADMDSP	Wyświetla atrybuty określonego obiektu.

Tabela 18. Autoryzacje dla operacji ogólnych	
Testowana aplikacja	**Opis**
*ALL	Użyj wszystkich operacji mających zastosowanie do obiektu. Uprawnienie `all` jest równoważne unii uprawnień `alladm`, `allmqii` `system` odpowiednich dla danego typu obiektu.
*ALLADM	Wykonaj wszystkie operacje administracyjne mające zastosowanie do obiektu.
*ALLMQI	Użyj wszystkich wywołań MQI mających zastosowanie do obiektu.

Tabela 18. Autoryzacje dla operacji ogólnych (kontynuacja)	
Testowana aplikacja	**Opis**
*CTRL	Sterowanie uruchamianiem i zamykaniem kanałów, programów nasłuchujących i usług.
*CTRLX	Zresetuj numer kolejny i rozstrzygnij wątpliwe kanały.

IBM i *Korzystanie z komend autoryzacji dostępu w systemie IBM i*

Poniższe informacje umożliwiają zapoznanie się z komendami autoryzacji dostępu i zawierają przykłady tych komend.

Korzystanie z komendy GRTMQMAUT

Jeśli użytkownik ma wymagane uprawnienia, może użyć komendy GRTMQMAUT , aby nadać uprawnienie dostępu do określonego obiektu profilowi użytkownika lub grupie użytkowników. Poniższe przykłady ilustrują 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 jest nazwą profilu użytkownika w systemie, dla którego mają zostać zmienione autoryzacje. Ten profil może być używany jako profil grupowy dla innych użytkowników.
   - *BROWSE i *PUT to autoryzacje nadawane określonej kolejce.

     Produkt *BROWSE dodaje autoryzację do przeglądania komunikatów w kolejce (w celu wywołania MQGET z opcją przeglądania).

     Produkt *PUT dodaje autoryzację do umieszczania komunikatów (MQPUT) w kolejce.
   - saturn.queue.manager jest nazwą menedżera kolejek.
2. Poniższa 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. Poniższa komenda nadaje użytkownikowi GEORGE uprawnienie 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 użytkownik ma wymagane uprawnienia, może użyć komendy RVKMQMAUT , aby usunąć uprzednio nadane uprawnienia profilu użytkownika lub grupy użytkowników w celu uzyskania dostępu do określonego obiektu. Poniższe przykłady ilustrują sposób użycia komendy RVKMQMAUT :

1. ```
   RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
   AUT(*PUT) MQMNAME('saturn.queue.manager')
   ```

Uprawnienie do umieszczania komunikatów w określonej kolejce, które zostało nadane w poprzednim przykładzie, jest usuwane dla GROUPA.

2.
```
RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
MQMNAME(PAYROLLQM)
```

Uprawnienie do pobierania komunikatów z dowolnej kolejki o nazwie rozpoczynającej się znakami PAY, której właścicielem jest menedżer kolejek PAYROLLQM, jest usuwane ze wszystkich użytkowników systemu, chyba że oni lub grupa, do której należą, zostały autoryzowane oddzielnie.

Korzystanie z komendy DSPMQMAUT

Wyświetlenie uprawnień MQM (Display MQM authority- DSPMQMAUT) Komenda wyświetla dla określonego obiektu i użytkownika listę autoryzacji, które użytkownik ma dla obiektu. Poniższy przykład ilustruje sposób użycia komendy:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

Korzystanie z komendy RFRMQMAUT

Odświeżenie zabezpieczeń MQM (RFRMQMAUT) Komenda umożliwia natychmiastowe zaktualizowanie informacji o grupie autoryzacji OAM, odzwierciedlając zmiany wprowadzone na poziomie systemu operacyjnego, bez konieczności zatrzymywania i restartowania menedżera kolejek. Poniższy przykład ilustruje sposób użycia komendy:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i Tabele specyfikacji autoryzacji w systemie IBM i

Za pomocą tych informacji można określić, jaka autoryzacja jest wymagana do użycia konkretnych wywołań API i konkretnych opcji tych wywołań w obiektach kolejki, obiektach procesu i obiektach menedżera kolejek.

Tabele specyfikacji autoryzacji rozpoczynające się od Tabela 19 na stronie 177 dokładnie definiują sposób działania autoryzacji i stosowane ograniczenia. Tabele dotyczą następujących sytuacji:

- Aplikacje wywołujące wywołania MQI
- Programy administracyjne, które wywołują komendy MQSC jako poprawki PCFs o zmienionym znaczeniu
- Programy administracyjne wydające komendy PCF

W tej sekcji przedstawiono informacje w postaci zestawu 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 klienckiego, proces nasłuchujący, usługa lub obiekt informacji uwierzytelniającej.

Wymagane uprawnienia
Wyrażona jako stała MQZAO_.

W tabelach stałe poprzedzone przedrostkiem MQZAO_ odpowiadają słowom kluczowym na liście autoryzacji dla komend **GRTMQMAUT** i **RVKMQMAUT** dla konkretnej jednostki. Na przykład wartość MQZAO_BROWSE odpowiada słowu kluczowemu *BROWSE . Podobnie słowo kluczowe MQZAO_SET_ALL_CONTEXT odpowiada słowu kluczowemu *SETALLitd. Stałe te są zdefiniowane w pliku nagłówkowym cmqzc.h, który jest dostarczany z produktem.

Autoryzacje MQI

Aplikacja może wydawać konkretne wywołania MQI i opcje tylko wtedy, gdy identyfikator użytkownika, pod którym jest uruchomiona (lub którego autoryzacje może przyjąć), otrzymał odpowiednią autoryzację.

Cztery wywołania MQI wymagają sprawdzenia autoryzacji: MQCONN, MQOPEN, MQPUT1i MQCLOSE.

W przypadku wywołań MQOPEN i MQPUT1sprawdzanie uprawnień jest wykonywane dla nazwy otwieranego obiektu, a nie dla nazwy lub nazw, które powstały po przetłumaczeniu nazwy. Na przykład aplikacji można nadać uprawnienie do otwierania kolejki aliasowej bez uprawnienia do otwierania kolejki podstawowej, na którą alias jest tłumaczony. Reguła polega na tym, że sprawdzanie jest wykonywane dla pierwszej definicji napotkanej podczas procesu tłumaczenia nazw, która nie jest aliasem menedżera kolejek, chyba że definicja aliasu menedżera kolejek jest otwierana bezpośrednio, czyli jej nazwa jest wyświetlana w polu *ObjectName* deskryptora obiektu. Uprawnienie jest zawsze wymagane dla konkretnego otwieranego obiektu; w niektórych przypadkach wymagane jest dodatkowe uprawnienie niezależne od kolejki, uzyskane przez autoryzację dla obiektu menedżera kolejek.

Tabela 19 na stronie 177, Tabela 20 na stronie 177, Tabela 21 na stronie 178i Tabela 22 na stronie 179 zawierają podsumowanie autoryzacji wymaganych dla każdego wywołania.

Uwaga: W tych tabelach nie są wymieniane listy nazw, kanały, kanały połączeń klienta, programy nasłuchujące, usługi ani obiekty informacji uwierzytelniającej. Dzieje się tak, ponieważ żadna autoryzacja nie ma zastosowania do tych obiektów, z wyjątkiem MQOO_INQUIRE, dla których obowiązują takie same autoryzacje, jak dla innych obiektów.

Tabela 19. Autoryzacja zabezpieczeń wymagana dla wywołań MQCONN

Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 179)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
Opcja MQCONN	Nie dotyczy	Nie dotyczy	MQZAO_CONNECT

Tabela 20. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN

Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 179)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_INQUIRE	MQZAO_INQUIRE **("2" na stronie 179)**	MQZAO_INQUIRE **("2" na stronie 179)**	MQZAO_INQUIRE **("2" na stronie 179)**
MQOO_BROWSE,	MQZAO_BROWSE,	Nie dotyczy	Nie sprawdzaj
MQOO_INPUT_ *	MQZAO_INPUT	Nie dotyczy	Nie sprawdzaj
MQOO_SAVE_ ALL_CONTEXT **("3" na stronie 179)**	MQZAO_INPUT	Nie dotyczy	Nie dotyczy
MQOO_OUTPUT (kolejka normalna) **("4" na stronie 179)**	MQZAO_WYNIK	Nie dotyczy	Nie dotyczy
MQOO_PASS_ IDENTY_CONTEXT **("5" na stronie 179)**	MQZAO_PASS_ KONTEKST_TOŻSAMOŚCI	Nie dotyczy	Nie sprawdzaj
MQOO_PASS_ALL_ CONTEXT **("5" na stronie 179, "6" na stronie 179)**	MQZAO_PASS _ALL_CONTEXT	Nie dotyczy	Nie sprawdzaj

Tabela 20. Autoryzacja zabezpieczeń wymagana dla wywołań MQOPEN (kontynuacja)			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 179)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQOO_SET_IDENTITY_CONTEXT **("5" na stronie 179, "6" na stronie 179)**	MQZAO_SET_IDENTITY_CONTEXT (MQZAO_SET_IDENTITY_CONTEXT)	Nie dotyczy	MQZAO_SET_IDENTITY_CONTEXT **("7" na stronie 179)**
MQOO_SET_ALL_CONTEXT **("5" na stronie 179, "8" na stronie 179)**	MQZAO_SET_ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ALL_CONTEXT **("7" na stronie 179)**
MQOO_OUTPUT (kolejka transmisji) **("9" na stronie 179)**	MQZAO_SET_ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ALL_CONTEXT **("7" na stronie 179)**
MQOO_SET	MQZAO_SET	Nie dotyczy	Nie sprawdzaj
MQOO_ALTERNATE_UPRAWNIENIE_UŻYTKOWNIKA	**("10" na stronie 179)**	**("10" na stronie 179)**	MQZAO_ALTERNATE_USER_AUTHORITY **("10" na stronie 179, "11" na stronie 179)**

Tabela 21. Autoryzacja zabezpieczeń wymagana dla wywołań MQPUT1			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 179)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQPMO_PASS_IDENTITY_CONTEXT (KONTEKST TOŻSAMOŚCI MQPMO_PASS_)	MQZAO_PASS_TOŻSAMOŚCI_KONTEKST **("12" na stronie 179)**	Nie dotyczy	Nie sprawdzaj
MQPMO_PASS_ALL_CONTEXT	MQZAO_PASS_ALL_CONTEXT **("12" na stronie 179)**	Nie dotyczy	Nie sprawdzaj
MQPMO_SET_KONTEKST_TOŻSAMOŚCI	MQZAO_SET_IDENTITY_CONTEXT **("12" na stronie 179)**	Nie dotyczy	MQZAO_SET_IDENTITY_CONTEXT **("7" na stronie 179)**
MQPMO_SET_ALL_CONTEXT	MQZAO_SET_ALL_CONTEXT **("12" na stronie 179)**	Nie dotyczy	MQZAO_SET_ALL_CONTEXT **("7" na stronie 179)**
(Kolejka transmisji) **("9" na stronie 179)**	MQZAO_SET_ALL_CONTEXT (ZESTAW MQZAO_ALL_CONTEXT)	Nie dotyczy	MQZAO_SET_ALL_CONTEXT **("7" na stronie 179)**
MQPMO_ALTERNATE_UPRAWNIENIE_UŻYTKOWNIKA	**("13" na stronie 179)**	Nie dotyczy	MQZAO_ALTERNATE_USER_AUTHORITY **("11" na stronie 179)**

Tabela 22. Autoryzacja zabezpieczeń wymagana dla wywołań MQCLOSE			
Autoryzacja wymagana dla:	**Obiekt kolejki ("1" na stronie 179)**	**Obiekt procesu**	**Obiekt menedżera kolejek**
MQCO_DELETE	MQZAO_DELETE **("14" na stronie 179)**	Nie dotyczy	Nie dotyczy
MQCO_DELETE-OPRÓŻNIONE	MQZAO_DELETE **("14" na stronie 179)**	Nie dotyczy	Nie dotyczy

Uwagi dotyczące tabel:

1. Jeśli kolejka modelowa jest otwierana:
   - Uprawnienie MQZAO_DISPLAY jest wymagane dla kolejki modelowej, oprócz uprawnienia do otwarcia kolejki modelowej dla typu dostępu, dla którego otwierany jest użytkownik.
   - Uprawnienie MQZAO_CREATE nie jest wymagane do utworzenia kolejki dynamicznej.
   - Identyfikator użytkownika używany do otwierania kolejki modelowej jest automatycznie nadawany wszystkim uprawnieniom specyficznym dla kolejki (równoważnym uprawnieniom MQZAO_ALL) dla tworzonej kolejki dynamicznej.
2. W zależności od typu otwieranego obiektu sprawdzana jest kolejka, proces, lista nazw lub obiekt menedżera kolejek.
3. Należy również podać wartość MQOO_INPUT_ *. Ta opcja jest poprawna dla kolejki lokalnej, modelowej lub kolejki aliasowej.
4. To sprawdzenie jest wykonywane dla wszystkich obserwacji wyjściowych, z wyjątkiem obserwacji określonych w uwadze "9" na stronie 179.
5. Należy również określić parametr MQOO_OUTPUT.
6. Opcja ta zakłada również wartość MQOO_PASS_IDENTITY_CONTEXT.
7. Uprawnienie to jest wymagane zarówno dla obiektu menedżera kolejek, jak i dla konkretnej kolejki.
8. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT i MQOO_SET_IDENTITY_CONTEXT są również implikowane przez tę opcję.
9. To sprawdzenie jest wykonywane dla kolejki lokalnej lub modelowej, która ma atrybut kolejki *Użycie* o wartości MQUS_TRANSMISSION i jest otwierana bezpośrednio dla danych wyjściowych. Nie ma zastosowania, jeśli otwierana jest kolejka zdalna (przez określenie nazw menedżera kolejek zdalnych i kolejki zdalnej lub przez określenie nazwy lokalnej definicji kolejki zdalnej).
10. Należy również określić co najmniej jedną z wartości MQOO_INQUIRE (dla dowolnego typu obiektu) lub (dla kolejek) MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET. Przeprowadzone sprawdzenie jest takie samo jak w przypadku innych określonych opcji, przy użyciu podanego alternatywnego identyfikatora użytkownika dla konkretnego uprawnienia do obiektu o określonej nazwie i bieżącego uprawnienia do aplikacji dla sprawdzenia MQZAO_ALTERNATE_USER_IDENTIFIER.
11. Ta autoryzacja umożliwia podanie dowolnego identyfikatora *AlternateUserId* .
12. Sprawdzenie MQZAO_OUTPUT jest również wykonywane, jeśli kolejka nie ma atrybutu kolejki *Użycie* o wartości MQUS_TRANSMISSION.
13. Przeprowadzone sprawdzanie jest takie samo jak w przypadku innych określonych opcji, przy użyciu podanego alternatywnego identyfikatora użytkownika dla uprawnienia kolejki o określonej nazwie i bieżącego uprawnienia aplikacji dla sprawdzenia MQZAO_ALTERNATE_USER_IDENTIFIER.
14. Kontrola jest przeprowadzana tylko wtedy, gdy spełnione są oba poniższe warunki:
    - Trwała kolejka dynamiczna jest zamykana i usuwana.
    - Kolejka nie została utworzona przez program MQOPEN, który zwrócił używany uchwyt obiektu.

    W przeciwnym razie nie jest sprawdzana.

Uwagi ogólne:

1. Autoryzacja specjalna MQZAO_ALL_MQI obejmuje wszystkie następujące autoryzacje istotne dla typu obiektu:
   - MQZAO_CONNECT
   - MQZAO_INQUIRE,
   - MQZAO_SET
   - MQZAO_BROWSE,
   - MQZAO_INPUT
   - MQZAO_WYNIK
   - MQZAO_PASS_IDENTITY_CONTEXT,
   - MQZAO_PASS_ALL_CONTEXT (mqzao_pass_all)
   - MQZAO_SET_IDENTITY_CONTEXT,
   - MQZAO_SET_ALL_CONTEXT (mqzao_set_all)
   - MQZAO_ALTERNATE_USER_AUTHORITY (uprawnienie użytkownika na przemian)
2. MQZAO_DELETE (patrz uwaga "14" na stronie 179) i MQZAO_DISPLAY są klasyfikowane jako autoryzacje administracyjne. Dlatego nie są one uwzględniane w MQZAO_ALL_MQI.
3. *Bez sprawdzania* oznacza, że nie jest przeprowadzane sprawdzanie autoryzacji.
4. *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie jest istotne dla tej operacji. Na przykład nie można wywołać wywołania MQPUT dla obiektu procesu.

IBM i *Autoryzacje dla komend MQSC w systemach CF o zmienionym znaczeniu w systemie IBM i*

Te autoryzacje umożliwiają użytkownikowi wydawanie komend administracyjnych jako komunikat o przedwczesnym zakończeniu PCF. Te metody umożliwiają programowi wysłanie komendy administracyjnej jako komunikatu do menedżera kolejek w celu wykonania w imieniu tego użytkownika.

W tej sekcji przedstawiono podsumowanie autoryzacji wymaganych dla każdej komendy MQSC zawartej w pliku Escape PCF.

Nie dotyczy oznacza, że sprawdzanie autoryzacji nie jest istotne dla tej operacji.

ID użytkownika, pod którym działa program wprowadzający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie DISPLAY do menedżera kolejek w celu wykonania komend PCF
- Uprawnienie do wywoływania komend MQSC w tekście komendy Escape PCF

ALTER *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	MQZAO_CHANGE
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE

Obiekt	Wymagane uprawnienia
Usługa	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 184)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Temat	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Proces	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Informacje uwierzytelniające	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Kanał	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Kanał połączenia klienta	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Program nasłuchujący	MQZAO_CREATE **(w systemie “2” na stronie 184)**
Usługa	MQZAO_CREATE **(w systemie “2” na stronie 184)**

DEFINE *obiekt* REPLACE (“1” na stronie 184, “3” na stronie 184)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE

Obiekt	Wymagane uprawnienia
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE

DELETE *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_USUŃ
Temat	MQZAO_USUŃ
Proces	MQZAO_USUŃ
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_USUŃ
Informacje uwierzytelniające	MQZAO_USUŃ
Kanał	MQZAO_USUŃ
Kanał połączenia klienta	MQZAO_USUŃ
Program nasłuchujący	MQZAO_USUŃ
Usługa	MQZAO_USUŃ

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	
Usługa	

WYKONAJ KOMENDĘ PING DLA 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
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
Lista nazw	Nie dotyczy
Informacje uwierzytelniające	Nie dotyczy
Kanał	MQZAO_CONTROL_EXTENDED,
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy

Obiekt	Wymagane uprawnienia
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 uprawnienie MQZAO_DISPLAY jest również wymagane dla obiektu LIKE, jeśli zostało określone, lub dla odpowiedniego systemu SYSTEM.DEFAULT.xxx DEFAULT.xxx, jeśli pominięto LIKE.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane wszystkim obiektom dla określonego menedżera kolejek przez określenie typu obiektu QMGR w komendzie GRTMQMAUT .
3. Ta opcja ma zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli nie, sprawdzanie jest takie samo 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. Te metody umożliwiają programowi wysłanie komendy administracyjnej jako komunikatu do menedżera kolejek w celu wykonania w imieniu tego użytkownika.

Ta sekcja zawiera podsumowanie autoryzacji wymaganych dla każdej komendy PCF.

Bez sprawdzania oznacza, że nie jest wykonywane sprawdzanie autoryzacji; *Nie dotyczy* oznacza, że sprawdzanie autoryzacji nie jest istotne dla tej operacji.

ID użytkownika, pod którym działa program wprowadzający komendę, musi mieć również następujące uprawnienia:

- Uprawnienie MQZAO_CONNECT do menedżera kolejek
- Uprawnienie DISPLAY do menedżera kolejek w celu wykonania komend PCF

Autoryzacja specjalna MQZAO_ALL_ADMIN obejmuje następujące autoryzacje:

- MQZAO_CHANGE
- MQZAO_CLEAR,
- MQZAO_USUŃ
- MQZAO_DISPLAY
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED,

Instrukcja MQZAO_CREATE nie jest uwzględniana, ponieważ nie jest specyficzna dla konkretnego obiektu lub typu obiektu

Zmień *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	MQZAO_CHANGE
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE

Wyczyść *obiekt*

Obiekt	**Wymagane uprawnienia**
Kolejka	MQZAO_CLEAR,
Temat	MQZAO_CLEAR,
Proces	Nie dotyczy
Menedżer kolejek	Nie dotyczy
Lista nazw	Nie dotyczy

Obiekt	Wymagane uprawnienia
Informacje uwierzytelniające	Nie dotyczy
Kanał	Nie dotyczy
Kanał połączenia klienta	Nie dotyczy
Program nasłuchujący	Nie dotyczy
Usługa	Nie dotyczy

Skopiuj *obiekt* (bez zastępowania) (“1” na stronie 191)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Temat	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Proces	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Menedżer kolejek	Nie dotyczy
Lista nazw MQZAO_CREATE	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Informacje uwierzytelniające	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Kanał	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Kanał połączenia klienta	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Program nasłuchujący	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Usługa	MQZAO_CREATE **(w systemie “2” na stronie 191)**

Skopiuj *obiekt* (z zastępowaniem) (“1” na stronie 191, “4” na stronie 191)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE

Utwórz *obiekt* (bez zastępowania) (“3” na stronie 191)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Temat	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Proces	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Informacje uwierzytelniające	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Kanał	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Kanał połączenia klienta	MQZAO_CREATE **(w systemie “2” na stronie 191)**
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE

Utwórz *obiekt* (z zastępowaniem) (“3” na stronie 191, “4” na stronie 191)

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_CHANGE
Temat	MQZAO_CHANGE
Proces	MQZAO_CHANGE
Menedżer kolejek	Nie dotyczy
Lista nazw	MQZAO_CHANGE
Informacje uwierzytelniające	MQZAO_CHANGE
Kanał	MQZAO_CHANGE
Kanał połączenia klienta	MQZAO_CHANGE
Program nasłuchujący	MQZAO_CHANGE
Usługa	MQZAO_CHANGE

Usuń *obiekt*

Obiekt	Wymagane uprawnienia
Kolejka	MQZAO_USUŃ
Temat	MQZAO_USUŃ
Proces	MQZAO_USUŃ
Menedżer kolejek	MQZAO_USUŃ
Lista nazw	MQZAO_USUŃ

Obiekt	Wymagane uprawnienia
Informacje uwierzytelniające	MQZAO_USUŃ
Kanał	MQZAO_USUŃ
Kanał połączenia klienta	MQZAO_USUŃ
Program nasłuchujący	MQZAO_USUŃ
Usługa	MQZAO_USUŃ

Sprawdź *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 *obiektów*

Obiekt	Wymagane uprawnienia
Kolejka	Nie sprawdzaj
Temat	Nie sprawdzaj
Proces	Nie sprawdzaj
Menedżer kolejek	Nie sprawdzaj
Lista nazw	Nie sprawdzaj
Informacje uwierzytelniające	Nie sprawdzaj
Kanał	Nie sprawdzaj
Kanał połączenia klienta	Nie sprawdzaj
Program nasłuchujący	Nie sprawdzaj
Usługa	Nie sprawdzaj

Wyślij ping do kanału

Obiekt	Wymagane uprawnienia
Kolejka	Nie dotyczy
Temat	Nie dotyczy
Proces	Nie dotyczy

Obiekt	Wymagane uprawnienia
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

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

Obiekt	Wymagane uprawnienia
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

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 kopiowania wymagane jest również uprawnienie MQZAO_DISPLAY dla obiektu źródłowego.
2. Uprawnienie MQZAO_CREATE nie jest specyficzne dla konkretnego obiektu lub typu obiektu. Uprawnienie do tworzenia jest nadawane wszystkim obiektom dla określonego menedżera kolejek przez określenie typu obiektu QMGR w komendzie GRTMQMAUT .
3. W przypadku komend tworzenia wymagane jest również uprawnienie MQZAO_DISPLAY dla odpowiedniego systemu SYSTEM.DEFAULT.* .
4. Ta opcja ma zastosowanie, jeśli obiekt, który ma zostać zastąpiony, już istnieje. Jeśli nie, sprawdzanie jest takie samo jak w przypadku opcji Kopiuj lub Utwórz bez zastępowania.

IBM i Ogólne profile OAM w systemie IBM i

Profile ogólne menedżera uprawnień do obiektów (OAM) umożliwiają ustawienie uprawnień użytkownika do wielu obiektów jednocześnie, bez konieczności wydawania oddzielnych komend **GRTMQMAUT** dla każdego tworzonego obiektu. Użycie profili ogólnych w komendzie **GRTMQMAUT** umożliwia ustawienie uprawnień ogólnych dla wszystkich tworzonych w przyszłości obiektów, które są zgodne z tym profilem.

W dalszej części tej sekcji opisano bardziej szczegółowo użycie profili ogólnych:

- "Korzystanie ze znaków wieloznacznych" na stronie 191
- "Priorytety profilu" na stronie 192

Korzystanie ze znaków wieloznacznych

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 utworzonych z nazwami 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 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 ma zastosowanie do 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 ma zastosowanie do obiektów ABC.DE.JKL, ABC.DEF.JKLi ABC.DEGH.JKL.

******

Użyj podwójnej gwiazdki (**) ***jeden raz*** w nazwie profilu jako:

- Cała nazwa profilu, która ma być zgodna ze wszystkimi nazwami obiektów. Jeśli na przykład do identyfikowania procesów używane jest słowo kluczowe OBJTYPE (*PRC), a następnie jako nazwy profilu używane jest słowo kluczowe **, należy zmienić autoryzacje dla wszystkich procesów.
- 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.

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:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

Pierwsza nadaje uprawnienie do umieszczania (put) wszystkim kolejkom 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 można zastosować komendę GRTMQMAUT do tej kolejki. 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 konkretne**. 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. Tak więc w poprzednim przykładzie była 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. **

IBM i Określanie usługi autoryzacji zainstalowanej w systemie IBM i

Można określić, który komponent usługi autoryzacji ma być używany.

Parametr **`Service Component name`** w systemach **GRTMQMAUT** i **RVKMQMAUT** umożliwia określenie nazwy zainstalowanego komponentu usługi autoryzacji.

Wybranie opcji **F24** w panelu początkowym, po którym następuje **F9=All parameters** w następnym panelu dowolnej komendy, umożliwia określenie zainstalowanego komponentu autoryzacji (*DFT) lub nazwy wymaganego komponentu usługi autoryzacji określonego w sekcji Service pliku qm.ini menedżera kolejek.

DSPMQMAUT ma również ten dodatkowy parametr. Ten parametr umożliwia wyszukiwanie wszystkich zainstalowanych komponentów autoryzacji (*DFT) lub określonej nazwy komponentu usługi autoryzacji dla podanej nazwy obiektu, typu obiektu i użytkownika.

IBM i Praca z profilami uprawnień i bez nich w systemie IBM i

Sekcja zawiera informacje na temat pracy z profilami uprawnień i pracy bez profili uprawnień.

Można pracować z profilami uprawnień, zgodnie z opisem w sekcji “Praca z profilami uprawnień” na stronie 192, lub bez nich, zgodnie z opisem w tej sekcji:

Aby pracować bez profili uprawnień, należy użyć parametru *NONE jako parametru uprawnień w systemie **GRTMQMAUT** w celu utworzenia profili bez uprawnień. Spowoduje to pozostawienie istniejących profili bez zmian.

W systemie **RVKMQMAUT**należy użyć parametru *REMOVE jako parametru uprawnień, aby usunąć istniejący profil uprawnień.

Praca z profilami uprawnień

Istnieją dwie komendy powiązane z profilowaniem uprawnień:

- **WRKMQMAUT**
- **WRKMQMAUTD**

Dostęp do tych komend można uzyskać bezpośrednio z wiersza komend lub z panelu WRKMQM:

1. Wpisz nazwę menedżera kolejek i naciśnij klawisz `Enter` , aby uzyskać dostęp do panelu wyników programu **WRKMQM** .
2. Na tym panelu wybierz opcję `F23=More options` .

Opcja 24 powoduje wybranie panelu wyników dla **WRKMQMAUT** komendy , a opcja 25 powoduje wybranie komendy **WRKMQMAUTI** , która jest używana z warstwą powiązań SSL.

WRKMQMAUT

Ta komenda umożliwia pracę z danymi uprawnień przechowywanymi w kolejce uprawnień.

Uwaga: Aby uruchomić tę komendę, użytkownik musi mieć uprawnienia `*connect` i `*admdsp` do menedżera kolejek. Jednak do utworzenia lub usunięcia profilu wymagane jest uprawnienie QMQMADM.

Jeśli informacje zostaną wyświetlone na ekranie, zostanie wyświetlona lista nazw profili uprawnień wraz z ich typami. Jeśli wydrukujesz dane wyjściowe, otrzymasz szczegółową listę wszystkich danych uprawnień, zarejestrowanych użytkowników i ich uprawnień.

Wprowadzenie nazwy obiektu lub profilu w tym panelu i naciśnięcie klawisza ENTER spowoduje przejście do panelu wyników programu **WRKMQMAUT** .

Jeśli zostanie wybrana opcja `4=Delete`, zostanie wyświetlony nowy panel, w którym można potwierdzić zamiar usunięcia wszystkich nazw użytkowników zarejestrowanych w określonym profilu uprawnień ogólnych. Ta opcja powoduje uruchomienie komendy **RVKMQMAUT** z opcją *REMOVE dla wszystkich użytkowników i stosuje się **tylko** do nazw profili ogólnych.

Po wybraniu opcji `12=Work with profile` należy przejść do panelu wyników komendy **WRKMQMAUTD** , zgodnie z opisem w sekcji “WRKMQMAUTD” na stronie 193.

WRKMQMAUTD

Ta komenda umożliwia wyświetlenie wszystkich użytkowników zarejestrowanych z określoną nazwą profilu uprawnień i typem obiektu. Aby uruchomić tę komendę, użytkownik musi mieć uprawnienia `*connect` i `*admdsp` do menedżera kolejek. Jednak w celu nadania, uruchomienia, utworzenia lub usunięcia profilu wymagane jest uprawnienie QMQMADM.

Po wybraniu opcji `F24=More keys` z początkowego panelu wejściowego, po której następuje opcja `F9=All Parameters` , wyświetlana jest nazwa komponentu usługi, na przykład **GRTMQMAUT** i **RVKMQMAUT**.

Uwaga: Klawisz `F11=Display Object Authorizations` przełącza między następującymi typami uprawnień:

- Autoryzacje obiektów
- Autoryzacje kontekstowe
- Autoryzacje MQI

Na ekranie dostępne są następujące opcje:

2=Grant
Powoduje przejście do panelu **GRTMQMAUT** w celu dodania do bieżących uprawnień.

3=Revoke
Powoduje przejście do panelu **RVKMQMAUT** w celu usunięcia niektórych bieżących definicji.

4=Delete
Powoduje przejście do panelu, który umożliwia usunięcie danych uprawnień dla określonych użytkowników. Spowoduje to uruchomienie komendy **RVKMQMAUT** z opcją *REMOVE.

5=Display
Powoduje przejście 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-deskryptor komunikatu.

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 120.

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

Zagadnienia dotyczące zabezpieczeń specyficzne dla produktu z/OS.

Bezpieczeństwo w systemie IBM MQ for z/OS jest kontrolowane za pomocą programu RACF lub równoważnego zewnętrznego menedżera zabezpieczeń (ESM).

W poniższych instrukcjach przyjęto założenie, że używana jest baza danych RACF.

Pojęcia pokrewne
Scenariusz zabezpieczeń: dwa menedżery kolejek w systemie z/OS
Scenariusz zabezpieczeń: grupa współużytkowania kolejek w systemie z/OS

z/OS Klasy zabezpieczeń systemu RACF

Klasy RACF są używane do przechowywania profili wymaganych do sprawdzania zabezpieczeń systemu IBM MQ . Wiele klas składowych ma równoważne klasy grupowe. Należy aktywować klasy i umożliwić im akceptowanie profili ogólnych.

Każda klasa RACF zawiera jeden lub więcej profili używanych w pewnym momencie w kolejności sprawdzania, jak to pokazano na rysunku (Tabela 23 na stronie 196).

Tabela 23. Klasy RACF używane przez IBM MQ

Klasa składowa	Klasa grupy	Spis treści
MQADMIN	GMQADMIN,	Profile, które są używane głównie na potrzeby funkcji administracyjnych. Na przykład: • Profile dla przełączników zabezpieczeń IBM MQ . • Profil zabezpieczeń RESLEVEL. • Profile dla alternatywnych zabezpieczeń użytkownika. • Profile zabezpieczeń kontekstu. • Profile dla ochrony zasobów komend. Ta klasa może zawierać tylko profile RACF pisane wielkimi literami.

Tabela 23. Klasy RACF używane przez IBM MQ (kontynuacja)

Klasa składowa	Klasa grupy	Spis treści
MXADMIN	GMXADMIN,	Profile, które są używane głównie na potrzeby funkcji administracyjnych. Na przykład: • Profile dla przełączników zabezpieczeń IBM MQ . • Profil zabezpieczeń RESLEVEL. • Profile dla alternatywnych zabezpieczeń użytkownika. • Profile zabezpieczeń kontekstu. • Profile dla ochrony zasobów komend. Ta klasa może zawierać zarówno wielkie litery, jak i profile RACF z literami o różnej wielkości.
ZMQCONN		Profile używane na potrzeby ochrony połączenia.
MQCMDS		Profile używane na potrzeby ochrony komend.
MQQUEUE	KOLEJKA GMQQUEUE	Profile pisane wielkimi literami używane w zabezpieczeniach zasobów kolejki.
MXQUEUE	GMXQUEUE	Profile z literami o różnej wielkości i wielkimi literami używane w zabezpieczeniach zasobów kolejki.
MQPROC	Komenda GMQPROC	Profile pisane wielkimi literami używane w zabezpieczeniach zasobów procesu.
MXPROC	GMXPROC	Profile z literami o różnej wielkości i wielkimi literami używane w zabezpieczeniach zasobów procesu.
MQNLIST	LISTA GMQN	Profile pisane wielkimi literami używane w zabezpieczeniach zasobów listy nazw.
MXNLIST	GMXNLISTA	Profile z literami o różnej wielkości i wielkimi literami używane w zabezpieczeniach zasobów listy nazw.
MXTOPIC	ZAGADNIENIENIE GMXTOPIC	Profile z literami o różnej wielkości i wielkimi literami używane w zabezpieczeniach tematu.

Niektóre klasy mają powiązaną *klasę grupy* , która umożliwia tworzenie grup zasobów o podobnych wymaganiach dostępu. Szczegółowe informacje na temat różnic między klasami elementów i grup oraz na temat tego, kiedy należy używać klasy elementów lub grup, zawiera publikacja z/OS Security Server RACF Security Administrator's Guide.

Klasy muszą być aktywowane przed wykonaniem kontroli bezpieczeństwa. Aby aktywować wszystkie klasy 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 klasy zostały skonfigurowane tak, aby mogły akceptować profile ogólne. Można to również wykonać za pomocą komendy RACF **SETROPTS**, 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 kolejek. Należy zachować ostrożność, gdy znak procentu jest używany jako znak wieloznaczny.

Wszystkie profile RACF używane przez IBM MQ zawierają przedrostek. W przypadku zabezpieczeń na poziomie grupy współużytkowania kolejki jest to nazwa grupy współużytkowania kolejki. W przypadku zabezpieczeń na poziomie menedżera kolejek przedrostkiem jest nazwa menedżera kolejek. Jeśli używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, profile będą używane z obydwoma typami przedrostków. Grupy współużytkowania kolejek i zabezpieczenia na poziomie menedżera kolejek są opisane w sekcji Zabezpieczenia i opcje w produkcie IBM MQ for z/OS.

Na przykład, aby chronić kolejkę o nazwie QUEUE_FOR_SUBSCRIBER_LIST w grupie współużytkowania kolejek QSG1 na poziomie grupy współużytkowania kolejek, odpowiedni profil zostanie zdefiniowany w pliku RACF jako:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Aby chronić kolejkę o nazwie QUEUE_FOR_LOST_CARD_LIST, która należy do menedżera kolejek STCD na poziomie menedżera kolejek, odpowiedni profil zostanie zdefiniowany w pliku 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 jednocześnie mieć różne opcje zabezpieczeń.

Nie należy używać ogólnych nazw menedżerów kolejek w profilach, aby uniknąć nieprzewidzianego dostępu użytkowników.

IBM MQ zezwala na użycie znaku procentu (%) w nazwach obiektów. Jednak RACF używa znaku% jako znaku wieloznacznego zastępującego jeden znak. Oznacza to, że podczas definiowania nazwy obiektu ze znakiem% w nazwie, należy wziąć to pod uwagę podczas definiowania odpowiedniego profilu.

For example, for the queue CREDIT_CARD_%_RATE_INQUIRY, on queue manager CRDP, the profile would be defined to RACF as follows:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Ta kolejka nie może być chroniona przez profil ogólny, taki jak CRDP. * *.

IBM MQ umożliwia stosowanie w nazwach obiektów znaków mieszanych. Obiekty te można chronić, definiując:

1. Profile o różnej wielkości liter w odpowiednich klasach RACF o różnej wielkości liter, lub
2. Profile ogólne w odpowiednich klasach RACF pisane wielkimi literami.

Aby użyć profili z mieszaną wielkością liter i klas RACF z mieszaną wielkością liter, należy wykonać kroki opisane w sekcji “Migrowanie menedżera kolejek systemu z/OS do zabezpieczeń z mieszaną wielkością liter” na stronie 285.

Niektóre profile (lub ich części) pozostają tylko wielkimi literami, ponieważ wartości są udostępniane przez produkt IBM MQ. Są to:

- Przełącz profile.
- Wszystkie kwalifikatory wysokiego poziomu (HLQ), w tym identyfikatory podsystemów i grup współużytkowania kolejek.
- Profile dla obiektów SYSTEM.

- Profile dla obiektów domyślnych.
- Klasa **MQCMDS** , więc wszystkie profile komend są tylko pisane wielkimi literami.
- Klasa **MQCONN** , więc wszystkie profile połączeń są tylko pisane wielkimi literami.
- Profile **RESLEVEL** .
- Kwalifikacja `'object'` w profilach zasobów komend, na przykład `hlq.QUEUE.queuename`. Nazwa zasobu zawiera tylko wielkie i małe litery.
- Dynamiczne profile kolejek `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*`i `CSQXCMD.*`.
- Część `'CONTEXT'` pliku `hlq.CONTEXT.resourcename`.
- Część `'ALTERNATE.USER'` pliku `hlq.ALTERNATE.USER.userid`.

Na przykład można zdefiniować profil w celu nadania dostępu do kolejki o nazwie `PAYROLL.Dept1` w menedżerze kolejek `QM01` w jeden z następujących sposobów.

- Jeśli używane są profile z mieszanymi przypadkami, można zdefiniować profil w klasie IBM MQ RACF MXQUEUE za pomocą następującej komendy:

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Jeśli używane są profile pisane wielkimi literami, można zdefiniować profil w klasie IBM MQ RACF MQQUEUE za pomocą następującej komendy:

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

Pierwszy przykład, w którym używane są profile o różnej wielkości liter, daje bardziej szczegółową kontrolę nad nadawaniem uprawnień dostępu do zasobu.

z/OS Przełącz profile

Aby kontrolować sprawdzanie zabezpieczeń wykonywane przez system IBM MQ, należy użyć *profili przełącznika*. Profil przełącznika to normalny profil systemu RACF , który ma specjalne znaczenie dla systemu IBM MQ. Lista dostępu w profilach przełącznika nie jest używana przez produkt IBM MQ.

IBM MQ utrzymuje przełącznik wewnętrzny dla każdego typu przełącznika przedstawionego w tabelach Przełączanie profili dla zabezpieczeń na poziomie podsystemu, Przełączanie profili dla zabezpieczeń na poziomie grupy współużytkowania kolejek lub menedżera kolejeki Przełączanie profili dla sprawdzania zasobów. Profile przełączników mogą być obsługiwane na poziomie grupy współużytkowania kolejek, na poziomie menedżera kolejek lub na obu tych poziomach. Używając pojedynczego zestawu profili przełączników zabezpieczeń grupy współużytkowania kolejek, można sterować bezpieczeństwem wszystkich menedżerów kolejek w grupie współużytkowania kolejek.

Gdy przełącznik bezpieczeństwa jest włączony, wykonywane są sprawdzenia bezpieczeństwa powiązane z przełącznikiem. Gdy przełącznik bezpieczeństwa jest wyłączony, kontrole bezpieczeństwa powiązane z przełącznikiem są pomijane. Domyślnie włączone są wszystkie przełączniki zabezpieczeń.

z/OS *Przełączniki i klasy*

Po uruchomieniu menedżera kolejek lub odświeżeniu zabezpieczeń program IBM MQ przełącza się zgodnie ze stanem różnych klas RACF .

Po uruchomieniu menedżera kolejek (lub po odświeżeniu klasy MQADMIN lub MXADMIN za pomocą komendy IBM MQ REFRESH SECURITY) program IBM MQ najpierw sprawdza status RACF i odpowiednią klasę:

- Klasa MQADMIN, jeśli używane są profile pisane wielkimi literami
- Klasa MXADMIN, jeśli używany jest profil z mieszaną wielkością liter.

Powoduje wyłączenie przełącznika bezpieczeństwa podsystemu, jeśli spełniony jest dowolny z następujących warunków:

- Program RACF jest nieaktywny lub nie jest zainstalowany.
- Klasa MQADMIN lub MXADMIN nie jest zdefiniowana (te klasy są zawsze zdefiniowane dla RACF , ponieważ są uwzględnione w tabeli deskryptorów klas (CDT)).
- Klasa MQADMIN lub MXADMIN nie została aktywowana.

Jeśli zarówno RACF , jak i klasa MQADMIN lub MXADMIN są aktywne, produkt IBM MQ sprawdza klasę MQADMIN lub MXADMIN, aby sprawdzić, czy został zdefiniowany jakikolwiek profil przełącznika. Najpierw sprawdzane są profile opisane w sekcji "Profile do sterowania bezpieczeństwem podsystemu" na stronie 201. Jeśli zabezpieczenia podsystemu nie są wymagane, program IBM MQ wyłącza wewnętrzne zabezpieczenia podsystemu i nie wykonuje dalszych sprawdzeń.

Profile określają, czy odpowiedni przełącznik IBM MQ jest włączony, czy wyłączony.

- Jeśli przełącznik jest wyłączony, ten typ zabezpieczeń jest dezaktywowany.
- Jeśli przełącznik IBM MQ jest włączony, produkt IBM MQ sprawdza status klasy RACF powiązanej z typem zabezpieczeń odpowiadającym przełącznikowi IBM MQ . Jeśli klasa nie jest zainstalowana lub nie jest aktywna, przełącznik IBM MQ jest wyłączony. Na przykład sprawdzanie zabezpieczeń procesu nie jest wykonywane, jeśli klasa MQPROC lub MXPROC nie została aktywowana. Klasa, która nie jest aktywna, jest równoważna definiowaniu wartości NO.PROCESS.CHECKS dla każdego menedżera kolejek i grupy współużytkowania kolejek, które używają tej bazy danych RACF .

z/OS *Jak działają przełączniki*

Aby wyłączyć przełącznik zabezpieczeń, należy zdefiniować parametr NO.* Profil przełącznika dla niego. Można przesłonić wartość NO.* profil ustawiony na poziomie grupy współużytkowania kolejki przez zdefiniowanie YES.* profil dla menedżera kolejek.

Aby wyłączyć przełącznik bezpieczeństwa, należy zdefiniować NO.* Profil przełącznika dla niego. Istnienie NO.* Profil oznacza, że sprawdzanie zabezpieczeń **nie** jest wykonywane dla tego typu zasobu, chyba że zostanie wybrane nadpisanie ustawienia na poziomie grupy współużytkowania kolejek w konkretnym menedżerze kolejek. Zostało to opisane w sekcji "Nadpisywanie ustawień na poziomie grupy współużytkowania kolejek" na stronie 200.

Jeśli menedżer kolejek nie jest elementem grupy współużytkowania kolejek, nie trzeba definiować żadnych profili na poziomie grupy współużytkowania kolejek ani żadnych profili przesłaniania. Należy jednak pamiętać o zdefiniowaniu tych profili, jeśli menedżer kolejek dołączy do grupy współużytkowania kolejek w późniejszym terminie.

Każde NO.* Profil przełącznika, który program IBM MQ wykrywa, wyłącza sprawdzanie dla tego typu zasobu. Profile przełączników są aktywowane podczas uruchamiania menedżera kolejek. Jeśli profile przełącznika zostaną zmienione podczas działania menedżerów kolejek, których to dotyczy, program IBM MQ może rozpoznać wprowadzone zmiany, wprowadzając komendę IBM MQ REFRESH SECURITY.

Profile przełącznika muszą być zawsze zdefiniowane w klasie MQADMIN lub MXADMIN. Nie definiuj ich w klasie GMQADMIN ani GMXADMIN. W tabelach Przełączanie profili dla bezpieczeństwa na poziomie podsystemu i Przełączanie profili dla sprawdzania zasobów wyświetlane są poprawne profile przełącznika i typ zabezpieczeń, którym sterują.

Nadpisywanie ustawień na poziomie grupy współużytkowania kolejek

Ustawienia zabezpieczeń na poziomie grupy współużytkowania kolejki można przesłonić dla konkretnego menedżera kolejek, który jest członkiem tej grupy. Aby wykonać sprawdzenia menedżera kolejek dla pojedynczego menedżera kolejek, które nie są wykonywane dla innych menedżerów kolejek w grupie, należy użyć wartości (qmgr-name.YES. *) profile przełączników.

I odwrotnie, jeśli nie ma być wykonywane określone sprawdzenie dla jednego 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. (Program IBM MQ sprawdza profil na poziomie grupy współużytkowania kolejek tylko wtedy, gdy nie znajdzie profilu na poziomie menedżera kolejek).

z/OS *Profile do sterowania bezpieczeństwem podsystemu*

Program IBM MQ sprawdza, czy dla podsystemu, menedżera kolejek i grupy współużytkowania kolejek wymagane są sprawdzenia zabezpieczeń podsystemu.

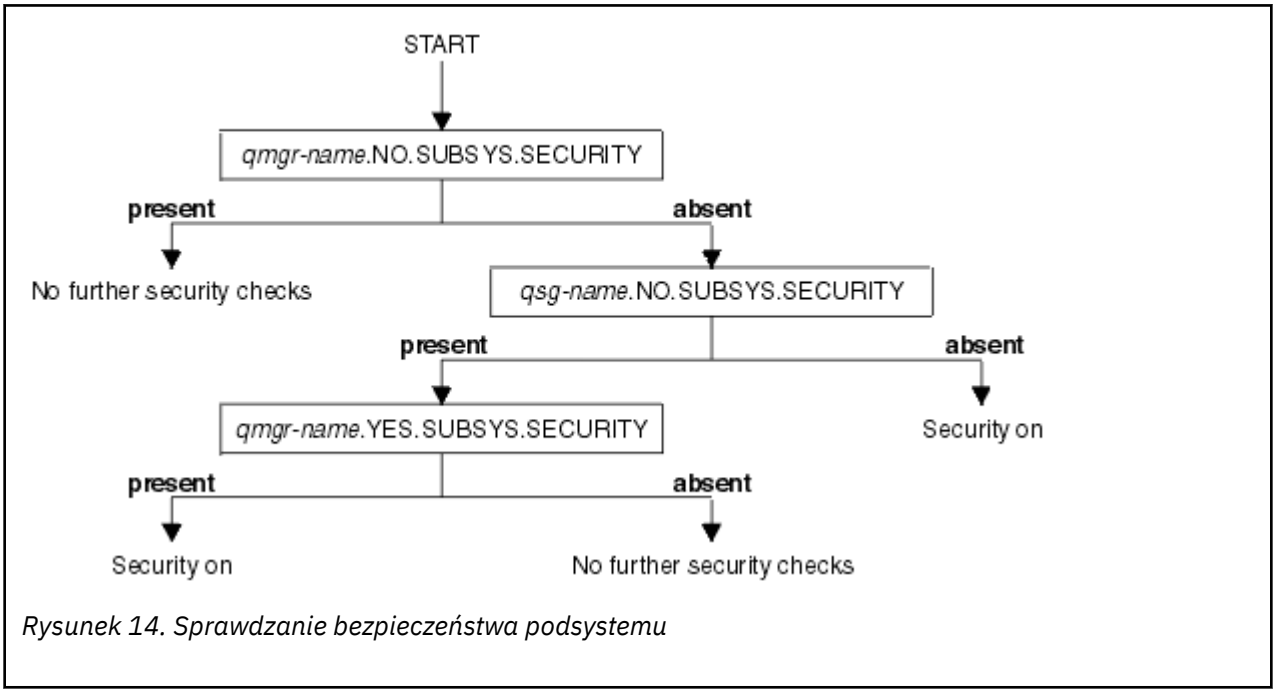
Pierwsza kontrola bezpieczeństwa wykonana przez IBM MQ jest używana do określenia, czy kontrole bezpieczeństwa są wymagane dla całego podsystemu IBM MQ . Jeśli określono, że zabezpieczenia podsystemu nie mają być stosowane, nie są wykonywane dalsze sprawdzenia.

Następujące profile przełączników są sprawdzane w celu określenia, czy wymagana jest ochrona podsystemu. Rysunek 14 na stronie 201 przedstawia kolejność, w jakiej są sprawdzane.

Tabela 24. Profile przełączników dla bezpieczeństwa na poziomie podsystemu

Nazwa profilu przełącznika	**Typ kontrolowanego zasobu lub sprawdzania**
qmgr-name.NO.SUBSYS.SECURITY	Zabezpieczenia podsystemu dla tego menedżera kolejek
qsg-name.NO.SUBSYS.SECURITY	Bezpieczeństwo podsystemu dla tej grupy współużytkowania kolejek
qmgr-name.YES.SUBSYS.SECURITY	Przesłonięcie zabezpieczeń podsystemu dla tego menedżera kolejek

Jeśli menedżer kolejek nie jest elementem grupy współużytkowania kolejek, program IBM MQ sprawdza tylko profil przełącznika qmgr-name.NO.SUBSYS.SECURITY .



Rysunek 14. Sprawdzanie bezpieczeństwa podsystemu

z/OS *Profile sterujące grupą współużytkowania kolejek lub zabezpieczeniami na poziomie menedżera kolejek*

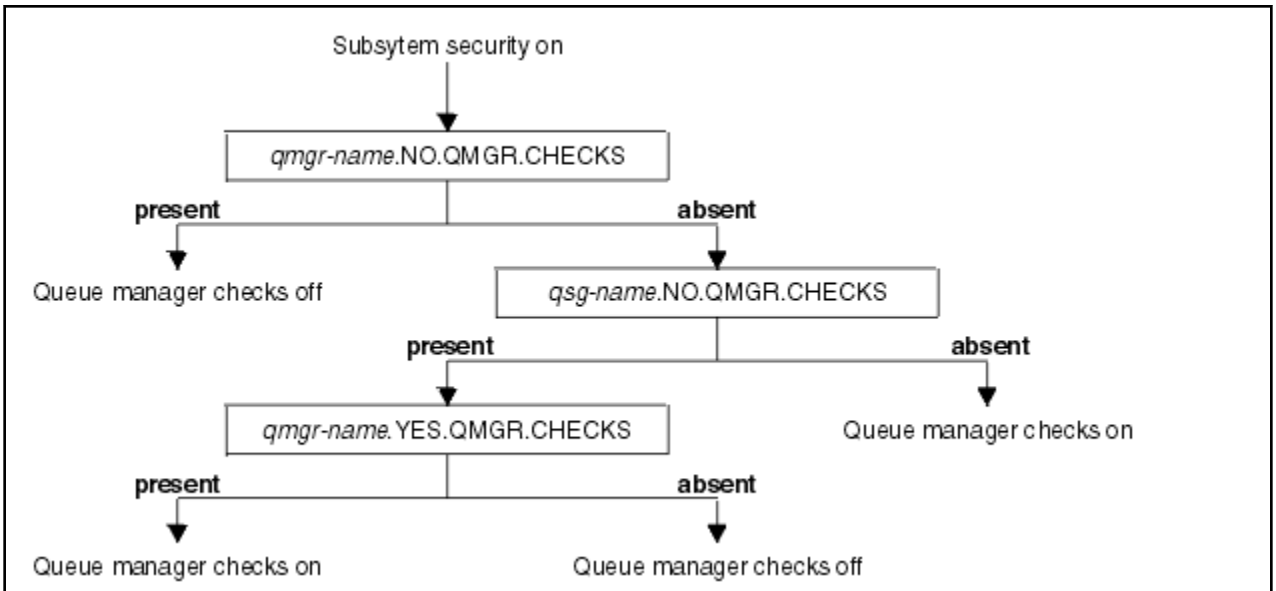
Jeśli sprawdzanie zabezpieczeń podsystemu jest wymagane, program IBM MQ sprawdza, czy sprawdzanie zabezpieczeń jest wymagane na poziomie grupy współużytkowania kolejek lub menedżera kolejek.

Jeśli program IBM MQ określił, że sprawdzanie zabezpieczeń jest wymagane, określa on, czy sprawdzanie jest wymagane na poziomie grupy współużytkowania kolejek i/lub menedżera kolejek. Te sprawdzenia nie są wykonywane, jeśli menedżer kolejek nie jest elementem grupy współużytkowania kolejek.

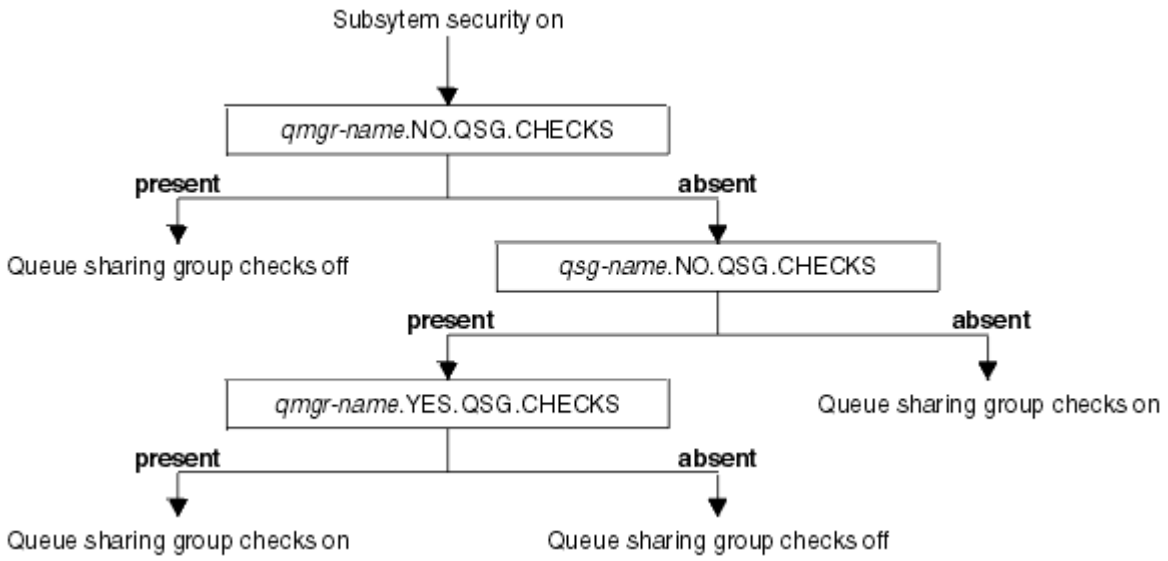
Następujące profile przełączników są sprawdzane w celu określenia wymaganego poziomu. Rysunek 15 na stronie 202 i Rysunek 16 na stronie 203 wyświetlają kolejność, w jakiej są sprawdzane.

Tabela 25. Przełącz profile dla grupy współużytkowania kolejek lub zabezpieczeń na poziomie menedżera kolejek	
Nazwa profilu przełącznika	**Typ kontrolowanego zasobu lub sprawdzania**
qmgr-name.NO.QMGR.CHECKS	Brak sprawdzania na poziomie menedżera kolejek dla tego menedżera kolejek
qsg-name.NO.QMGR.CHECKS	Brak sprawdzania na poziomie menedżera kolejek dla tej grupy współużytkowania kolejek
qmgr-name.YES.QMGR.CHECKS	Nadpisanie sprawdzeń na poziomie menedżera kolejek dla tego menedżera kolejek
qmgr-name.NO.QSG.CHECKS	Brak sprawdzania na poziomie grupy współużytkowania kolejki dla tego menedżera kolejek
qsg-name.NO.QSG.CHECKS	Brak sprawdzania na poziomie grupy współużytkowania kolejki dla tej grupy współużytkowania kolejki
qmgr-name.YES.QSG.CHECKS	Nadpisanie sprawdzeń na poziomie grupy współużytkowania kolejki dla tego menedżera kolejek

Jeśli zabezpieczenia podsystemu są aktywne, nie można wyłączyć zarówno zabezpieczeń na poziomie grupy współużytkowania kolejek, jak i zabezpieczeń na poziomie menedżera kolejek. Jeśli zostanie podjęta taka próba, program IBM MQ ustawi sprawdzanie zabezpieczeń na obu poziomach.



Rysunek 15. Sprawdzanie zabezpieczeń na poziomie menedżera kolejek



Rysunek 16. Sprawdzanie zabezpieczeń na poziomie grupy współużytkowania kolejek

z/OS *Poprawne kombinacje przełączników zabezpieczeń*

Poprawne są tylko niektóre kombinacje przełączników. Jeśli używana jest kombinacja niepoprawnych ustawień przełącznika, generowany jest komunikat CSQH026I , a sprawdzanie zabezpieczeń jest ustawiane zarówno na poziomie grupy współużytkowania kolejek, jak i na poziomie menedżera kolejek.

Tabela 26 na stronie 203, Tabela 27 na stronie 203, Tabela 28 na stronie 204i Tabela 29 na stronie 204 przedstawiają zestawy kombinacji ustawień przełącznika, które są poprawne dla każdego typu poziomu zabezpieczeń.

Tabela 26. Poprawne kombinacje przełączników zabezpieczeń dla zabezpieczeń na poziomie 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 kolejki

Kombinacje
qmgr-name.NO.QMGR.CHECKS
qsg-name.NO.QMGR.CHECKS

Tabela 27. Poprawne kombinacje przełączników zabezpieczeń dla zabezpieczeń na poziomie grupy współużytkowania kolejki (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 Brak QSG.* zdefiniowane profile
Brak 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 z przełączników

*Tabela 29. Inne poprawne kombinacje przełączników zabezpieczeń, które przełączają oba poziomy sprawdzania **w**.*
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 używana jest pewna liczba profili przełączników. Niektóre operacje sprawdzania są wykonywane na menedżerze kolejek lub grupie współużytkowania kolejek. Mogą one zostać przesłonięte przez profile, które umożliwiają sprawdzanie konkretnych menedżerów kolejek.

Tabela 30 na stronie 205 przedstawia profile przełączników używane do sterowania dostępem do zasobów IBM MQ .

Jeśli menedżer kolejek jest częścią grupy współużytkowania kolejek i aktywne są zarówno zabezpieczenia menedżera kolejek, jak i grupy współużytkowania kolejek, można użyć wartości YES.* Przełączenie profilu w celu przesłonięcia profili na poziomie grupy współużytkowania kolejek i włączenia zabezpieczeń dla konkretnego menedżera kolejek.

Niektóre profile mają zastosowanie zarówno do menedżerów kolejek, jak i grup współużytkowania kolejek. Są one poprzedzone łańcuchem *hlq* i należy zastąpić nazwę grupy współużytkowania kolejek lub menedżera kolejek, jeśli ma to zastosowanie. Nazwy profili wyświetlane z przedrostkiem *qmgr-name* są profilami przesłonięcia menedżera kolejek. Należy zastąpić nazwę menedżera kolejek.

Tabela 30. Profile przełączników na potrzeby sprawdzania zasobów

Typ kontrolowanego sprawdzania zasobów	**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
Ochrona zasobów komend	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
Zabezpieczenia tematu	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Uwaga: Ogólne profile przełączników, takie jak hlq.NO. * * są ignorowane przez IBM MQ		

Aby na przykład wykonywać sprawdzenia zabezpieczeń procesu w menedżerze kolejek QM01, który jest elementem grupy współużytkowania kolejek QSG3 , ale nie wykonywać sprawdzania zabezpieczeń procesu w żadnym innym menedżerze kolejek w grupie, należy zdefiniować następujące profile przełączników:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Aby wszystkie menedżery kolejek w grupie współużytkowania kolejek z wyjątkiem QM02były sprawdzane pod kątem bezpieczeństwa, należy zdefiniować następujący profil przełącznika:

```
QM02.NO.QUEUE.CHECKS
```

(Nie ma potrzeby definiowania profilu dla grupy współużytkowania kolejek, ponieważ sprawdzanie jest automatycznie włączane, jeśli nie ma zdefiniowanego profilu).

z/OS *Przykład definiowania przełączników*

Różne podsystemy IBM MQ mają różne wymagania dotyczące bezpieczeństwa, które można zaimplementować przy użyciu różnych profili przełączników.

Zdefiniowano cztery podsystemy IBM MQ :

- MQP1 (system produkcyjny)
- MQP2 (system produkcyjny)
- MQD1 (system programistyczny)
- MQT1 (system testowy)

Wszystkie cztery menedżery kolejek są elementami grupy współużytkowania kolejek QS01. Wszystkie klasy IBM MQ RACF zostały zdefiniowane i aktywowane.

Te podsystemy mają różne wymagania dotyczące bezpieczeństwa:

- Systemy produkcyjne wymagają pełnego sprawdzania zabezpieczeń IBM MQ , aby były aktywne na poziomie grupy współużytkowania kolejek w obu systemach.

  W tym celu należy określić następujący profil:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Powoduje to ustawienie sprawdzania na poziomie grupy współużytkowania kolejki dla wszystkich menedżerów kolejek w grupie współużytkowania kolejki. Nie ma potrzeby definiowania żadnych innych profili przełączników dla menedżerów kolejek produkcyjnych, ponieważ mają być sprawdzane wszystkie elementy dla tych systemów.
- Testowanie menedżera kolejek MQT1 również wymaga pełnego sprawdzania zabezpieczeń. Jednak ze względu na to, że może być to konieczne później, zabezpieczenia można zdefiniować na poziomie menedżera kolejek, aby można było zmienić ustawienia zabezpieczeń dla tego menedżera kolejek bez wpływu na inne elementy grupy współużytkowania kolejek.

  W tym celu należy zdefiniować wartość NO.QSG.CHECKS dla produktu MQT1 można wykonać w następujący sposób:

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```
- Programistyczny menedżer kolejek MQD1 ma inne wymagania dotyczące zabezpieczeń niż reszta grupy współużytkowania kolejek. Wymaga, aby aktywne były tylko zabezpieczenia połączenia i kolejki.

  W tym celu należy zdefiniować profil `MQD1.YES.QMGR.CHECKS` dla tego menedżera kolejek, a następnie zdefiniować następujące profile, aby wyłączyć sprawdzanie 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.

Ustawienia przełącznika można również zmienić podczas działania menedżera kolejek, definiując lub usuwając odpowiedni profil przełącznika w klasie MQADMIN. Aby aktywować zmiany w ustawieniach przełącznika, należy wprowadzić komendę REFRESH SECURITY dla klasy MQADMIN.

Więcej informacji na temat używania komend DISPLAY SECURITY and REFRESH SECURITY zawiera sekcja “Odświeżanie zabezpieczeń menedżera kolejek w systemie z/OS” na stronie 265 .

z/OS Profile używane do sterowania dostępem do zasobów IBM MQ

Oprócz profili przełącznika, które mogły zostać zdefiniowane, należy zdefiniować profile RACF , aby kontrolować dostęp do zasobów IBM MQ . Ta kolekcja tematów zawiera informacje o profilach RACF dla różnych typów zasobów IBM MQ .

Jeśli profil zasobu nie jest zdefiniowany dla konkretnego sprawdzenia zabezpieczeń, a użytkownik wysyła żądanie, które wymagałoby tego sprawdzenia, program IBM MQ odmawia dostępu. Nie ma potrzeby definiowania profili dla typów zabezpieczeń związanych z przełącznikami zabezpieczeń, które zostały zdezaktywowane.

z/OS *Profile zabezpieczeń połączenia*

Jeśli zabezpieczenia połączenia są aktywne, należy zdefiniować profile w klasie MQCONN i zezwolić na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili, aby mogły one łączyć się z produktem IBM MQ.

Aby umożliwić nawiązywanie połączenia, należy nadać użytkownikom dostęp do odczytu (RACF READ) do odpowiedniego profilu. (Jeśli nie istnieje profil na poziomie menedżera kolejek, a menedżer kolejek jest elementem grupy współużytkowania kolejek, można sprawdzić profile na poziomie grupy współużytkowania kolejek, jeśli w tym celu skonfigurowano zabezpieczenia).

Profil połączenia kwalifikowany nazwą menedżera kolejek steruje dostępem do konkretnego menedżera kolejek, a użytkownicy mający dostęp do tego profilu mogą nawiązywać połączenie z tym menedżerem kolejek. Profil połączenia kwalifikowany nazwą grupy współużytkowania kolejek steruje dostępem do wszystkich menedżerów kolejek w grupie 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 na poziomie menedżera kolejek.

Uwaga:

1. Informacje na temat identyfikatorów użytkowników sprawdzanych dla różnych żądań zabezpieczeń zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253.
2. Sprawdzanie zabezpieczeń na poziomie zasobów (RESLEVEL) jest również wykonywane w czasie połączenia. Szczegółowe informacje na ten temat zawiera sekcja “Profil zabezpieczeń RESLEVEL” na stronie 246.

Zabezpieczenia systemu IBM MQ rozpoznają następujące różne typy połączeń:

- Połączenia wsadowe (i typu wsadowego), obejmują:
  - z/OS Zadania wsadowe
  - Aplikacje TSO
  - z/OS UNIX System Services znaki
  - Db2Procedury składowane
- Połączenia serwera CICS
- Połączenia IMS z regionów sterowania i przetwarzania aplikacji
- Inicjator kanału IBM MQ

z/OS *Profile zabezpieczeń połączeń dla połączeń wsadowych*

Profile do sprawdzania połączeń typu wsadowego składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *BATCH*. Nadaj ID użytkownika powiązanego z łączącą przestrzenią adresową prawo do odczytu profilu połączenia.

Profile do sprawdzania połączeń wsadowych i wsadowych przybierają następującą formę:

```
hlq.BATCH
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza, czy istnieje profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek. Jeśli znalezienie jednego z tych profili nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączenia typu wsadowego lub wsadowego należy zezwolić identyfikatorowi użytkownika, który jest powiązany z łączącą przestrzenią adresową, na dostęp do profilu połączenia. Na przykład poniższa komenda RACF umożliwia użytkownikom z grupy CONNTQM1 nawiązanie połączenia z menedżerem kolejek TQM1; użytkownicy ci będą mogli używać dowolnego połączenia wsadowego lub wsadowego.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS *Korzystanie z programu **CHCKLOCL** w aplikacjach powiązanych lokalnie*

CHCKLOCL ma zastosowanie tylko do połączeń nawiązywanych za pomocą połączeń BATCH i nie ma zastosowania do połączeń nawiązywanych z systemu CICS lub IMS. Połączenia nawiązywane za pośrednictwem inicjatora kanału są sterowane przez program **CHCKCLNT**.

Przegląd

Aby skonfigurować menedżer kolejek systemu z/OS do sprawdzania identyfikatora użytkownika i hasła dla niektórych, ale nie wszystkich, aplikacji powiązanych lokalnie, należy wykonać dodatkowe czynności konfiguracyjne.

Wynika to z tego, że po skonfigurowaniu produktu **CHCKLOCL** (*REQUIRED*) wcześniejsze aplikacje wsadowe używające wywołania API MQCONN nie będą mogły nawiązać połączenia z menedżerem kolejek.

Tylko w systemie z/OS : do przejścia na starszą wersję globalnej konfiguracji CHCKLOCL (REQUIRED) do CHCKLOCL (OPTIONAL) dla specjalnie zdefiniowanych identyfikatorów użytkowników można użyć bardziej szczegółowego mechanizmu opartego na zabezpieczeniach połączenia przestrzeni adresowej. Użyty mechanizm jest opisany w poniższym tekście wraz z przykładem.

Aby zezwolić na większą granulację w systemie **CHCKLOCL** (*REQUIRED*) niż w przypadku wszystkich, należy zmodyfikować plik **CHCKLOCL** w taki sam sposób, w jaki modyfikowany jest poziom dostępu ID użytkownika powiązanego z przestrzenią adresową połączenia z profilami połączeń `hlq.batch` w klasie MQCONN.

Jeśli ID użytkownika przestrzeni adresowej ma tylko prawo do odczytu (READ), co jest wartością minimalną wymaganą do nawiązania połączenia w ogóle, konfiguracja **CHCKLOCL** ma zastosowanie w takiej postaci, w jakiej została zapisana.

Jeśli ID użytkownika przestrzeni adresowej ma dostęp UPDATE (lub wyższy), konfiguracja **CHCKLOCL** działa w trybie *OPTIONAL* . Oznacza to, że nie trzeba podawać identyfikatora użytkownika i hasła, ale w takim przypadku identyfikator użytkownika i hasło muszą być poprawną parą.

Zabezpieczenia połączenia zostały już skonfigurowane dla menedżera kolejek produktu z/OS

Jeśli dla menedżera kolejek produktu z/OS skonfigurowano zabezpieczenia połączenia i chcesz, aby produkt **CHCKLOCL** (*REQUIRED*) miał zastosowanie do aplikacji serwera WAS powiązanych lokalnie, a nie do innych aplikacji, wykonaj następujące kroki:

1. Rozpocznij od **CHCKLOCL** (*OPTIONAL*) jako konfiguracji. Oznacza to, że wszystkie podane ID użytkownika i hasła są sprawdzane pod kątem poprawności, 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 powoduje wyświetlenie 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 do odczytu (READ), zmień dostęp na

```
UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

4. Zaktualizuj konfigurację IBM MQ do **CHCKLOCL** (*REQUIRED*).

   Kombinacja dostępu UPDATE do MQ23.BATCH i bieżącego ustawienia oznacza, że używany jest program **CHCKLOCL** (*OPTIONAL*).

5. Teraz zastosuj zachowanie **CHCKLOCL** (*REQUIRED*) do jednego konkretnego ID użytkownika, na przykład WASUSER, aby wszystkie połączenia przychodzące z tego regionu musiały podać ID użytkownika i hasło.

   W tym celu należy wycofać wprowadzone wcześniej zmiany, wprowadzając 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 połączeń dla produktu hlq.BATCH w klasie MQCONN, wprowadzając komendę:

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. Autoryzuj wszystkie identyfikatory użytkowników, które tworzą połączenia wsadowe z menedżerem kolejek, tak aby miały dostęp do aktualizacji (UPDATE) do tego profilu. Powoduje to pominięcie wymagania **CHCKLOCL** (*REQUIRED*) dotyczącego identyfikatora i hasła użytkownika w czasie nawiązywania połączenia.

   W tym celu należy wydać komendę:

```
PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
```

   Są to między innymi identyfikatory użytkowników:

   a. Używany dla paneli CSQUTIL, ISPF i innych lokalnie powiązanych narzędzi.

   b. Powiązane z połączeniem wsadowym podobnym do połączeń z menedżerem kolejek. Na przykład: Advanced Message Security, IBM Integration Bus, procedury składowane Db2 , użytkownicy z/OS UNIX System Services i TSO oraz aplikacje Java .

3. Usuń profil przełącznika dla menedżera kolejek, wprowadzając komendę:

```
hlq.NO.CONNECT.CHECKS
```

4. Teraz zastosuj zachowanie **CHCKLOCL** (*REQUIRED*) do jednego konkretnego ID użytkownika, na przykład WASUSER, aby wszystkie połączenia przychodzące z tego regionu musiały podać ID użytkownika i hasło.

   W tym celu należy wycofać wprowadzone wcześniej zmiany, wprowadzając komendę:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS *Profile zabezpieczeń połączeń dla połączeń CICS*

Profile do sprawdzania połączeń CICS składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *CICS* . Nadaj ID użytkownika powiązany z przestrzenią adresową CICS prawo do odczytu profilu połączenia.

Profile służące do sprawdzania połączeń z produktu CICS przyjmują następującą postać:

```
hlq.CICS
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza, czy istnieje profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek. Jeśli znalezienie jednego z tych profili nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączenia kierowanych przez CICSnależy zezwolić na dostęp do profilu połączenia tylko identyfikatorowi użytkownika przestrzeni adresowej CICS .

Na przykład następujące komendy RACF umożliwiają ID użytkownika przestrzeni adresowej CICS KCBCICS 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 połączeń dla połączeń IMS*

Profile do sprawdzania połączeń IMS składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *IMS* . Nadaj identyfikatorom użytkowników regionu sterującego IMS i regionu zależnego prawo do odczytu profilu połączenia.

Profile służące do sprawdzania połączeń z produktu IMS przyjmują następującą postać:

```
hlq.IMS
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza, czy istnieje profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek. Jeśli znalezienie jednego z tych profili nie powiedzie się, żądanie połączenia nie powiedzie się.

W przypadku żądań połączeń wysyłanych przez IMSnależy zezwolić na dostęp do profilu połączenia dla identyfikatorów użytkowników regionu sterującego i regionu zależnego produktu IMS .

Na przykład następujące komendy RACF umożliwiają:

- ID użytkownika regionu IMS , IMSREG, do połączenia z menedżerem kolejek TQM1.
- Użytkownicy w grupie BMPGRP przesyłają zadania 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 sprawdzania połączeń z inicjatora kanału składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *CHIN*. Nadaj ID użytkownika używany przez przestrzeń adresową uruchomionego zadania inicjatora kanału prawo do odczytu profilu połączenia.

Profile służące do sprawdzania połączeń z inicjatora kanału przyjmują następującą formę:

```
hlq.CHIN
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek). Jeśli używany jest zarówno menedżer kolejek, jak i zabezpieczenia na poziomie grupy współużytkowania kolejek, produkt IBM MQ sprawdza, czy istnieje profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek. Jeśli znalezienie jednego z tych profili nie powiedzie się, żądanie połączenia nie powiedzie się.

Dla żądań połączenia inicjatora kanału należy zdefiniować dostęp do profilu połączenia dla ID użytkownika używanego przez przestrzeń adresową uruchomionego zadania inicjatora kanału.

Na przykład następujące komendy systemu RACF umożliwiają przestrzeni adresowej inicjatora kanału uruchomionego z identyfikatorem użytkownika DQCTRL nawiązanie połączenia z menedżerem kolejek TQM1:

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS *Profile zabezpieczeń kolejki*

Jeśli zabezpieczenia kolejki są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili. Profile zabezpieczeń kolejki mają nazwy zgodne z nazwą menedżera kolejek lub grupy współużytkowania kolejek oraz z nazwą kolejki, która ma zostać otwarta.

Jeśli zabezpieczenia kolejki są aktywne, należy:

- Zdefiniuj profile w klasach **MQQUEUE** lub **GMQQUEUE** , jeśli używane są profile pisane wielkimi literami.
- Zdefiniuj profile w klasach **MXQUEUE** lub **GMXQUEUE** , jeśli używane są profile z mieszaną wielkością liter.
- Należy zezwolić grupom lub identyfikatorom użytkowników na dostęp do tych profili, aby mogły one wysyłać żądania API IBM MQ , które korzystają z kolejek.

Profile zabezpieczeń kolejki przyjmują następującą formę:

```
hlq.queuename
```

gdzie `hlq` może mieć wartość `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `queuename` jest nazwą otwieranej kolejki, zgodnie z określeniem w deskryptorze obiektu w wywołaniu `MQOPEN` lub `MQPUT1` .

Profil poprzedzony nazwą menedżera kolejek steruje dostępem do pojedynczej kolejki w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek steruje dostępem do jednej lub większej liczby kolejek o tej nazwie we wszystkich menedżerach kolejek w grupie współużytkowania kolejek lub dostępem do kolejki współużytkowanej przez dowolny menedżer kolejek w grupie. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tej kolejki w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

Jeśli używane są kolejki współużytkowane, zalecane jest użycie zabezpieczeń na poziomie grupy współużytkowania kolejek.

Szczegółowe informacje na temat sposobu działania zabezpieczeń kolejki, gdy nazwa kolejki jest nazwą kolejki aliasowej lub kolejki modelowej, znajdują się w sekcji “Uwagi dotyczące kolejek aliasowych” na stronie 213 i “Uwagi dotyczące kolejek modelowych” na stronie 214 .

Dostęp RACF wymagany do otwarcia kolejki zależy od określonych opcji MQOPEN lub MQPUT1 . Jeśli kodowana jest więcej niż jedna z opcji MQOO_ * i MQPMO_ *, sprawdzanie zabezpieczeń kolejki jest wykonywane dla najwyższego wymaganego uprawnienia RACF .

Tabela 31. Poziomy dostępu dla zabezpieczeń kolejki przy użyciu wywołań MQOPEN lub MQPUT1

Opcja MQOPEN lub MQPUT1	**RACF poziom dostępu wymagany dla 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 lub umieszczania komunikatów we wszystkich kolejkach o nazwach zaczynających się od łańcucha PAY. Można to zrobić za pomocą następujących komend 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 przyznając 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 poziom dostępu RACF , jaki aplikacja ma dla profilu zabezpieczeń kolejki, zostanie zmieniony, zmiany odniosą skutek tylko w przypadku wszystkich nowych uchwytów obiektów uzyskanych dla tej kolejki (czyli nowych uchwytów MQOPEN). Uchwyty te istnieją już w momencie zmiany i zachowują istniejący dostęp do kolejki. Jeśli aplikacja musi użyć zmienionego poziomu dostępu do kolejki, a nie istniejącego poziomu dostępu, musi zamknąć i ponownie otworzyć kolejkę dla każdego uchwytu obiektu, który wymaga zmiany.
2. W tym przykładzie nazwa menedżera kolejek QM77 może być również nazwą grupy współużytkowania kolejek.

W czasie otwierania kolejki mogą również wystąpić inne rodzaje sprawdzania zabezpieczeń, w zależności od określonych opcji otwierania i typów zabezpieczeń, które są aktywne. Patrz także “Profile zabezpieczeń kontekstu” na stronie 230 i “Profile dla alternatywnych zabezpieczeń użytkownika” na stronie 228. Tabela podsumowania przedstawiająca opcje otwierania i autoryzację zabezpieczeń, która jest wymagana, gdy wszystkie zabezpieczenia kolejki, kontekstu i alternatywnego użytkownika są aktywne, znajduje się w sekcji Tabela 36 na stronie 220.

W przypadku korzystania z funkcji publikowania/subskrypcji należy wziąć pod uwagę następujące kwestie. Podczas przetwarzania żądania MQSUB wykonywane jest sprawdzenie zabezpieczeń w celu upewnienia się, że ID użytkownika wysyłającego żądanie ma dostęp wymagany do umieszczania komunikatów w docelowej kolejce IBM MQ oraz dostęp wymagany do subskrybowania tematu IBM MQ .

Tabela 32. Poziomy dostępu dla zabezpieczeń kolejki przy użyciu wywołania MQSUB

Opcja MQSUB	**RACF poziom dostępu wymagany dla 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 tworzonej kolejki zarządzanej i kolejki dynamicznej.
2. Takiej techniki można użyć dla kolejki docelowej, która została określona w wywołaniu funkcji API MQSUB, aby odróżnić użytkowników dokonujących subskrypcji od użytkowników pobierających publikacje z kolejki docelowej.

z/OS *Uwagi dotyczące kolejek aliasowych*

Po wywołaniu wywołania MQOPEN lub MQPUT1 dla kolejki aliasowej program IBM MQ sprawdza zasób względem nazwy kolejki określonej w deskryptorze obiektu (MQOD) w wywołaniu. Nie sprawdza, czy użytkownik ma dostęp do nazwy kolejki docelowej.

Na przykład kolejka aliasowa o nazwie PAYROLL.REQUEST jest tłumaczona na kolejkę docelową PAY.REQUEST. Jeśli ochrona kolejki jest aktywna, użytkownik musi mieć tylko uprawnienia dostępu do kolejki PAYROLL.REQUEST. Nie jest wykonywane sprawdzanie, czy masz uprawnienia 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 mieć możliwość otwarcia zarówno samej kolejki modelowej, jak i kolejki dynamicznej, na którą jest rozstrzygana. Zdefiniuj ogólne profile RACF dla kolejek dynamicznych, w tym kolejek dynamicznych używanych przez programy narzędziowe IBM MQ .

Po otwarciu kolejki modelowej zabezpieczenia produktu IBM MQ przeprowadzają dwa sprawdzenia bezpieczeństwa kolejki:

1. Czy masz uprawnienia dostępu do kolejki modelowej?
2. Czy masz uprawnienia dostępu do kolejki dynamicznej, na którą rozstrzygana jest kolejka modelowa?

Jeśli nazwa kolejki dynamicznej zawiera końcowy znak gwiazdki (*), ten znak * jest zastępowany przez łańcuch znaków wygenerowany przez IBM MQ, aby utworzyć kolejkę dynamiczną o unikalnej nazwie. Ponieważ jednak do sprawdzania uprawnień używana jest cała nazwa, w tym wygenerowany łańcuch, należy zdefiniować profile ogólne dla tych kolejek.

Na przykład wywołanie MQOPEN używa nazwy kolejki modelowej CREDIT.CHECK.REPLY.MODEL i nazwa kolejki dynamicznej CREDIT.REPLY.* w menedżerze kolejek (lub grupie współużytkowania kolejek) Usługa MQSP.

W tym celu należy wydać następujące komendy RACF , aby zdefiniować niezbędne profile kolejek:

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Należy również wydać odpowiednie komendy RACF PERMIT, aby umożliwić użytkownikowi dostęp do tych profili.

Typowa nazwa kolejki dynamicznej utworzonej przez komendę MQOPEN jest podobna do nazwy CREDIT.REPLY.A346EF00367849A0. Dokładna wartość ostatniego kwalifikatora jest nieprzewidywalna; dlatego dla takich nazw kolejek należy używać profili ogólnych.

Liczba programów narzędziowych IBM MQ umieszczających komunikaty w kolejkach dynamicznych. Należy zdefiniować profile dla następujących nazw kolejek dynamicznych i zapewnić dostęp do odpowiednich identyfikatorów użytkowników za pomocą instrukcji RACF UPDATE (poprawne identyfikatory użytkowników można znaleźć w sekcji “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253):

```
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 sterującego używaniem nazwy kolejki dynamicznej, która jest domyślnie używana w elementach kopii programowania aplikacji. Struktury copybook dostarczone z produktem IBM MQzawierają domyślny plik *DynamicQName*, którym jest CSQ. *. Umożliwia to ustanowienie odpowiedniego profilu RACF .

Uwaga: Nie należy zezwalać programistom aplikacji na określanie pojedynczej gwiazdki (*) dla nazwy kolejki dynamicznej. W przeciwnym razie należy zdefiniować hlq. * * profil w klasie MQQUEUE i należy nadać mu szeroki zakres dostępu. Oznacza to, że ten profil może być również używany dla innych kolejek innych niż dynamiczne, które nie mają bardziej konkretnego profilu RACF . Użytkownicy mogą więc uzyskać dostęp do kolejek, do których nie powinni mieć dostępu.

z/OS *Opcje zamykania w trwałych kolejkach 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 operacji stosowane są dodatkowe sprawdzenia zabezpieczeń.

Tabela 33. Poziomy dostępu dla opcji zamykania w trwałych kolejkach dynamicznych

Opcja MQCLOSE	**RACF poziom dostępu wymagany dla hlq.queuename**
MQCO_DELETE	Zmień
MQCO_DELETE_PURGE	Zmień

z/OS *Bezpieczeństwo i kolejki zdalne*

Jeśli komunikat jest umieszczany w kolejce zdalnej, zabezpieczenia kolejki implementowane przez menedżer kolejek lokalnych zależą od sposobu określenia kolejki zdalnej podczas jej otwierania.

Stosowane są następujące reguły:

1. Jeśli kolejka zdalna została zdefiniowana w menedżerze kolejek lokalnych za pomocą komendy IBM MQ DEFINE QREMOTE, sprawdzana kolejka jest nazwą kolejki zdalnej. Jeśli na przykład kolejka zdalna jest zdefiniowana w menedżerze kolejek MQS1 , wykonaj następujące czynności:

   ```
   DEFINE QREMOTE(BANK7.CREDIT.REFERENCE)
          RNAME(CREDIT.SCORING.REQUEST)
          RQMNAME(BNK7)
          XMITQ(BANK1.TO.BANK7)
   ```

   W tym przypadku jest to profil dla BANK7.CREDIT.REFERENCE musi być zdefiniowana w klasie MQQUEUE.
2. Jeśli nazwa menedżera kolejek *ObjectQMgr* dla żądania nie zostanie przetłumaczona na lokalny menedżer kolejek, zostanie wykonane sprawdzenie zabezpieczeń względem przetłumaczonych (zdalnych) nazw menedżera kolejek, z wyjątkiem kolejki klastra, w której wykonywane jest sprawdzenie nazwy kolejki klastra.

   Na przykład kolejka transmisji BANK1.TO.BANK7 jest zdefiniowany w menedżerze kolejek MQS1. Następnie w programie MQS1 jest wysyłane żądanie MQPUT1 z parametrem *ObjectName* na wartość BANK1.INTERBANK.TRANSFERS oraz *ObjectQMgrNazwa* banku BANK1.TO.BANK7. W takim przypadku użytkownik wykonujący żądanie musi mieć dostęp do konta BANK1.TO.BANK7.
3. Jeśli do kolejki zostanie wysłane żądanie MQPUT i zostanie podana wartość *ObjectQMgrName* jako nazwa aliasu lokalnego menedżera kolejek, tylko nazwa kolejki zostanie sprawdzona pod kątem bezpieczeństwa, a nie menedżera kolejek.

Po przesłaniu komunikatu do zdalnego menedżera kolejek może on podlegać dodatkowemu przetwarzaniu zabezpieczeń. Więcej informacji na ten temat zawiera “Zabezpieczenia zdalnego przesyłania komunikatów” na stronie 106.

z/OS *Bezpieczeństwo kolejki niedostarczonych komunikatów*

Do kolejki niedostarczonych komunikatów mają zastosowanie specjalne uwagi, ponieważ wielu użytkowników musi mieć możliwość umieszczania w niej komunikatów, ale dostęp do pobierania komunikatów musi być ściśle ograniczony. Można to osiągnąć, stosując różne uprawnienia RACF do kolejki niedostarczonych komunikatów i kolejki aliasowej.

Niedostarczone komunikaty można umieścić w specjalnej kolejce nazywanej kolejką niedostarczonych komunikatów. Jeśli istnieją dane poufne, które mogą znajdować się w tej kolejce, należy wziąć pod uwagę wpływ tej sytuacji na bezpieczeństwo, ponieważ nieautoryzowani użytkownicy nie powinni pobierać tych danych.

Każdy z poniższych elementów musi mieć możliwość umieszczania komunikatów w kolejce niedostarczonych komunikatów:

- Programy użytkowe.
- Przestrzeń adresowa inicjatora kanału i identyfikatory użytkowników MCA. (Jeśli profil RESLEVEL nie istnieje lub jest zdefiniowany w taki sposób, że identyfikatory użytkowników kanału są sprawdzane, identyfikator użytkownika kanału wymaga również uprawnień do umieszczania komunikatów w kolejce niedostarczonych komunikatów).
- CKTI, CICSdostarczony CICS inicjator zadania.
- CSQQTRMN, monitor wyzwalacza IBM MQdostarczony IMS .

Jedyną aplikacją, która może pobierać komunikaty z kolejki niedostarczonych komunikatów, powinna być aplikacja specjalna, która przetwarza te komunikaty. Jednak w przypadku nadania aplikacjom uprawnienia RACF UPDATE do kolejki niedostarczonych komunikatów dla MQPUT , ponieważ mogą one automatycznie pobierać komunikaty z kolejki za pomocą wywołań MQGET . Nie można wyłączyć kolejki

niedostarczonych komunikatów dla operacji pobierania, ponieważ nawet aplikacje specjalne nie mogą pobierać komunikatów.

Jednym z rozwiązań tego problemu jest skonfigurowanie dwupoziomowego dostępu do kolejki niedostarczonych komunikatów. CKTI, transakcje agenta kanału komunikatów lub przestrzeń adresowa inicjatora kanału i aplikacje specjalne mają bezpośredni dostęp. Inne aplikacje mogą uzyskać dostęp do kolejki niedostarczonych komunikatów tylko za pośrednictwem kolejki aliasowej. Ten alias jest zdefiniowany, aby umożliwić aplikacjom umieszczanie komunikatów w kolejce niedostarczonych komunikatów, ale nie w celu pobierania z niej komunikatów.

Tak to może działać:

1. Zdefiniuj rzeczywistą kolejkę niedostarczonych komunikatów z atrybutami PUT (ENABLED) i GET (ENABLED), jak pokazano w przykładzie thlqual.SCSQPROC(CSQ4INYG).
2. Nadaj uprawnienie RACF UPDATE do kolejki niedostarczonych komunikatów następującym identyfikatorom użytkowników:
   - Identyfikatory użytkowników, w których działają CKTI i MCA lub przestrzeń adresowa inicjatora kanału.
   - Identyfikatory użytkowników powiązane ze specjalną aplikacją przetwarzającą kolejkę niedostarczonych komunikatów.
3. Zdefiniuj kolejkę aliasową, która jest tłumaczona na rzeczywistą kolejkę niedostarczonych komunikatów, ale nadaj tej kolejce aliasowej następujące atrybuty: PUT (ENABLED) i GET (DISABLED). Nadaj kolejce aliasowej nazwę z tym samym rdzeniem co nazwa kolejki niedostarczonych komunikatów, ale dołącz do niej znaki ". PUT". Na przykład, jeśli nazwa kolejki niedostarczonych komunikatów to hlq.DEAD.QUEUEnazwą kolejki aliasowej będzie hlq.DEAD.QUEUE.PUT.
4. Aby umieścić komunikat w kolejce niedostarczonych komunikatów, aplikacja używa kolejki aliasowej. To jest to, co aplikacja musi zrobić:
   - Pobieranie nazwy rzeczywistej kolejki niedostarczonych komunikatów. W tym celu otwiera obiekt menedżera kolejek za pomocą komendy `MQOPEN` , a następnie wysyła komendę `MQINQ` w celu pobrania nazwy kolejki niedostarczonych komunikatów.
   - Zbuduj kolejkę aliasową, dodając do niej znaki '.PUT', w tym przypadku hlq.DEAD.QUEUE.PUT.
   - Otwórz kolejkę aliasową hlq.DEAD.QUEUE.PUT.
   - Umieść komunikat w rzeczywistej kolejce niedostarczonych komunikatów, wysyłając komendę `MQPUT` dla kolejki aliasowej.
5. Nadaj identyfikatorowi użytkownika powiązani z aplikacją uprawnienie RACF UPDATE do aliasu, ale bez 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 dla operacji pobierania.

   Aplikacja nie może pobrać żadnych komunikatów z rzeczywistej kolejki niedostarczonych komunikatów, ponieważ ma odpowiednie uprawnienie RACF .

Tabela 34 na stronie 217 zawiera podsumowanie uprawnień RACF wymaganych 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 aliasów (hlq.DEAD.QUEUE.PUT)**
Przestrzeń adresowa MCA lub inicjatora kanału i CKTI	TEMPERATURY	Brak

Tabela 34. Uprawnienie RACF do kolejki niedostarczonych komunikatów i jej aliasu (kontynuacja)		
Powiązane identyfikatory użytkowników	**Rzeczywista kolejka niedostarczonych komunikatów (hlq.DEAD.QUEUE)**	**Kolejka niedostarczonych komunikatów aliasów (hlq.DEAD.QUEUE.PUT)**
'Specjalna' aplikacja (do przetwarzania kolejki niedostarczonych komunikatów)	TEMPERATURY	Brak
Identyfikatory użytkowników aplikacji zapisane przez użytkownika	Brak	TEMPERATURY

W przypadku użycia tej metody aplikacja nie może określić maksymalnej długości komunikatu (MAXMSGL) dla kolejki niedostarczonych komunikatów. Jest to spowodowane tym, że nie można pobrać atrybutu MAXMSGL z kolejki aliasowej. Dlatego aplikacja powinna przyjąć, że maksymalna długość komunikatu wynosi 100 MB (maksymalna wielkość obsługiwana przez IBM MQ for z/OS). Rzeczywista kolejka niedostarczonych komunikatów powinna być również zdefiniowana z atrybutem MAXMSGL o wartości 100 MB.

Uwaga: Aplikacje 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*

Należy skonfigurować dostęp do systemu RACF , aby umożliwić niektórym identyfikatorom użytkowników dostęp do określonych kolejek systemowych.

Wiele kolejek systemowych jest dostępnych dla dodatkowych części systemu IBM MQ:

- Program narzędziowy CSQUTIL
- Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL)
- Operacje i panele sterowania
- Przestrzeń adresowa inicjatora kanału (w tym umieszczony w kolejce demon publikowania/subskrypcji)
- Serwer mqweb używany przez IBM MQ Console i REST API.

Identyfikatory użytkowników, dla których są one uruchamiane, muszą mieć dostęp do tych kolejek na poziomie RACF , jak to pokazano na rysunku (Tabela 35 na stronie 218).

Tabela 35. Dostęp wymagany przez program IBM MQ do kolejek SYSTEM					
Kolejka systemowa	**CSQUTIL**	**CSQ0UTIL**	**Serwer mqweb**	**Obsługa i panele sterowania**	**Inicjator kanału dla rozproszonego kolejkowania**
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	TEMPERATURY
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	TEMPERATURY	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	Zmień
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	Zmień
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	Zmień
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	TEMPERATURY

Tabela 35. Dostęp wymagany przez program IBM MQ do kolejek SYSTEM (kontynuacja)

Kolejka systemowa	CSQUTIL	CSQ0UTIL	Serwer mqweb	Obsługa i panele sterowania	Inicjator kanału dla rozproszonego kolejkowania
SYSTEM.CHANNEL.INITQ	-	-	-	-	TEMPERATURY
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	TEMPERATURY
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	Zmień
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	TEMPERATURY
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	Zmień
SYSTEM.COMMAND.INPUT	TEMPERATURY	-	-	TEMPERATURY	TEMPERATURY
SYSTEM.COMMAND.REPLY.*	-	-	-	-	TEMPERATURY
SYSTEM.COMMAND.REPLY.MODEL	TEMPERATURY	-	-	TEMPERATURY	TEMPERATURY
SYSTEM.CSQOREXX.*	-	-	-	TEMPERATURY	-
SYSTEM.CSQUTIL.*	TEMPERATURY	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	TEMPERATURY
SYSTEM.HIERARCHY.STATE	-	-	-	-	TEMPERATURY
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	TEMPERATURY
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	TEMPERATURY
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	TEMPERATURY
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	TEMPERATURY
SYSTEM.PROTECTION.POLICY.QUEUE	-	Aktualizacja“1” na stronie 220	-	-	ODCZYT
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	TEMPERATURY
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	TEMPERATURY

Tabela 35. Dostęp wymagany przez program IBM MQ do kolejek SYSTEM (kontynuacja)					
Kolejka systemowa	**CSQUTIL**	**CSQ0UTIL**	**Serwer mqweb**	**Obsługa i panele sterowania**	**Inicjator kanału dla rozproszonego kolejkowania**
SYSTEM.REST.REPLY.QUEUE	-	-	TEMPERATURY	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	TEMPERATURY

Uwagi:

1. Użytkownik przestrzeni adresowej Advanced Message Security musi mieć również dostęp do tej kolejki z prawem do odczytu (READ).

z/OS *Krótki przegląd informacji o zabezpieczeniach zasobów interfejsu API*

Podsumowanie opcji **MQOPEN**, **MQPUT1**, **MQSUB**i **MQCLOSE** oraz dostęp wymagany przez różne typy zabezpieczeń zasobów.

Tabela 36. Opcje MQOPEN, MQPUT1, MQSUB i MQCLOSE oraz wymagana autoryzacja zabezpieczeń. Objaśnienia przedstawione w ten sposób **(1)** znajdują się w uwagach poniżej tej tabeli.				
	Wymagany 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		PRZECZYTAJ **(5)**	Nie sprawdzaj	Nie sprawdzaj
MQOO_BROWSE,		ODCZYT	Nie sprawdzaj	Nie sprawdzaj
MQOO_INPUT_ *		TEMPERATURY	Nie sprawdzaj	Nie sprawdzaj
MQOO_SAVE_ALL_CONTEXT **(6)**		TEMPERATURY	Nie sprawdzaj	Nie sprawdzaj
MQOO_OUTPUT (USAGE = NORMALNY) **(7)**		TEMPERATURY	Nie sprawdzaj	Nie sprawdzaj
MQOO_PASS_IDENTITY_CONTEXT **(8)**		TEMPERATURY	ODCZYT	Nie sprawdzaj
MQOO_PASS_ALL_CONTEXT **(8) (9)**		TEMPERATURY	ODCZYT	Nie sprawdzaj
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		TEMPERATURY	TEMPERATURY	Nie sprawdzaj
MQOO_SET_ALL_CONTEXT **(8) (10)**		TEMPERATURY	CONTROL	Nie sprawdzaj
MQOO_OUTPUT (USAGE (XMITQ) **(11)**		TEMPERATURY	CONTROL	Nie sprawdzaj

Tabela 36. Opcje MQOPEN, MQPUT1, MQSUB i MQCLOSE oraz wymagana autoryzacja zabezpieczeń. Objaśnienia przedstawione w ten sposób **(1)** znajdują się w uwagach poniżej tej tabeli. *(kontynuacja)*

	Wymagany 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)**
MQOO_OUTPUT (obiekt tematu)	AKTUALIZUJ **(16)**			
MQOO_OUTPUT (kolejka aliasowa do obiektu tematu)	AKTUALIZUJ **(16)**	TEMPERATUR Y		
MQOO_SET		Zmień	Nie sprawdzaj	Nie sprawdzaj
MQOO_ALTERNATE_USER_AUTHORITY (uprawnienie użytkownika na przemian)		**(12)**	**(12)**	TEMPERATUR Y
Opcja MQPUT1				
Umieszczenie w normalnej kolejce **(7)**		TEMPERATUR Y	Nie sprawdzaj	Nie sprawdzaj
MQPMO_PASS_IDENTITY_CONTEXT,		TEMPERATUR Y	ODCZYT	Nie sprawdzaj
MQPMO_PASS_ALL_CONTEXT		TEMPERATUR Y	ODCZYT	Nie sprawdzaj
MQPMO_SET_IDENTITY_CONTEXT,		TEMPERATUR Y	TEMPERATUR Y	Nie sprawdzaj
MQPMO_SET_ALL_CONTEXT		TEMPERATUR Y	CONTROL	Nie sprawdzaj
MQOO_OUTPUT Umieszczenie w kolejce transmisji **(11)**		TEMPERATUR Y	CONTROL	Nie sprawdzaj
MQOO_OUTPUT (obiekt tematu)	AKTUALIZUJ **(16)**			
MQOO_OUTPUT (kolejka aliasowa do obiektu tematu)	AKTUALIZUJ **(16)**	TEMPERATUR Y		
MQPMO_ALTERNATE_UPRAWNIENIA_UŻYTKOWNIKA		**(13)**	**(13)**	TEMPERATUR Y
Opcja MQCLOSE				
MQCO_DELETE **(14)**		Zmień	Nie sprawdzaj	Nie sprawdzaj
MQCO_DELETE_PURGE **(14)**		Zmień	Nie sprawdzaj	Nie sprawdzaj
MQCO_REMOVE_SUB	ALTER **(15)**			
Opcja MQSUB				
MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER (zmiana MQSO)	ALTER **(15)**	**(17)**	**(18)**	

Tabela 36. Opcje MQOPEN, MQPUT1, MQSUB i MQCLOSE oraz wymagana autoryzacja zabezpieczeń. Objaśnienia przedstawione w ten sposób **(1)** znajdują się w uwagach poniżej tej tabeli. *(kontynuacja)*

	Wymagany 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)**
MQSO_RESUME	PRZECZYTAJ **(15)**	**(17)**	Nie sprawdzaj	
MQSO_ALTERNATE_UPRAWNIENIA_UŻYTKOWNIKA				TEMPERATURY
MQSO_SET_IDENTITY_CONTEXT,			**(18)**	

Uwaga:

1. Ta opcja nie jest ograniczona do kolejek. Użyj klasy MQNLIST lub MXNLIST dla list nazw oraz 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 zauważyć, że do tego sprawdzenia używane jest maksymalnie 12 znaków pola *`AlternateUserId`* , w przeciwieństwie do innych sprawdzeń, w których używane jest tylko 8 pierwszych znaków identyfikatora użytkownika.
5. Podczas otwierania menedżera kolejek dla zapytań nie jest wykonywane żadne sprawdzenie.
6. Należy także podać wartość MQOO_INPUT_ *. Dotyczy to kolejki lokalnej, kolejki modelowej lub kolejki aliasowej.
7. To sprawdzenie jest wykonywane dla kolejki lokalnej lub modelowej, która ma atrybut kolejki **Usage** o wartości MQUS_NORMAL, a także dla kolejki aliasowej lub zdalnej (zdefiniowanej dla połączonego menedżera kolejek). Jeśli kolejka jest kolejką zdalną, która została otwarta jawnie, określając parametr *`ObjectQMgrName`* (a nie nazwę połączonego menedżera kolejek), sprawdzenie jest wykonywane względem kolejki o takiej samej nazwie jak parametr *`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 również implikowana przez tę opcję.
10. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT i MQOO_SET_IDENTITY_CONTEXT są również implikowane przez tę opcję.
11. To sprawdzenie jest wykonywane dla kolejki lokalnej lub modelowej, która ma atrybut kolejki **Usage** o wartości MQUS_TRANSMISSION i jest otwierana bezpośrednio na potrzeby danych wyjściowych. Nie ma zastosowania, jeśli otwierana jest kolejka zdalna.
12. Musi być określona co najmniej jedna z następujących wartości: MQOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT lub MQOO_SET. Przeprowadzona kontrola jest taka sama jak w przypadku innych określonych opcji.
13. Przeprowadzona kontrola jest taka sama jak w przypadku innych określonych opcji.
14. Dotyczy to tylko trwałych kolejek dynamicznych, które zostały otwarte bezpośrednio, czyli nie zostały otwarte za pomocą kolejki modelowej. Do usunięcia tymczasowej kolejki dynamicznej nie są 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, do której mają zostać wysłane publikacje, wykonywane jest sprawdzenie bezpieczeństwa dla tej kolejki, aby upewnić się, że użytkownik ma uprawnienia do tej kolejki.
18. Jeśli w żądaniu MQSUB z określonymi opcjami MQSO_CREATE lub MQSO_ALTER mają zostać ustawione dowolne pola kontekstu tożsamości w strukturze MQSD, należy również określić opcję MQSO_SET_IDENTITY_CONTEXT oraz odpowiednie uprawnienia do profilu kontekstu dla kolejki docelowej.

z/OS *Profile zabezpieczeń tematu*

Jeśli zabezpieczenia tematu są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili.

Pojęcie zabezpieczeń tematu w drzewie tematów zostało opisane w sekcji Zabezpieczenia publikowania/subskrypcji.

Jeśli zabezpieczenia tematu są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach **MXTOPIC** lub **GMXTOPIC** .
- Zezwól na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili, aby mogły one wysyłać żądania interfejsu API IBM MQ , które korzystają z tematów.

Profile zabezpieczeń tematów przyjmują następującą postać:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

where

- Parametr `hlq` ma wartość `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek).
- `topicname` jest nazwą węzła administracyjnego tematu w drzewie tematów, powiązanego z tematem zasubskrybowanym za pośrednictwem wywołania MQSUB lub opublikowanego za pośrednictwem wywołania MQOPEN.

Profil poprzedzony nazwą menedżera kolejek steruje dostępem do pojedynczego tematu w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek steruje dostępem do jednego lub większej liczby tematów o tej nazwie we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tego tematu w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

Subskrybowanie

Aby zasubskrybować temat, należy mieć dostęp zarówno do tematu, który ma zostać zasubskrybowany, jak i do kolejki docelowej publikacji.

Podczas wysyłania 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 do subskrybowania przez zabezpieczenia tematu	
Opcja MQSUB	**Dostęp RACF wymagany do profilu `hlq.SUBSCRIBE.topicname` w klasie MXTOPIC**
MQSO_CREATE i MQSO_ALTER	Zmień
MQSO_RESUME	ODCZYT

Tabela 38. Dodatkowe uprawnienie wymagane do subskrybowania przy użyciu niezarządzanej kolejki docelowej	
Opcja MQSUB	**Wymagany dostęp RACF do profilu `hlq.CONTEXT.queuename` w klasie MQADMIN lub MXADMIN**
MQSO_CREATE, MQSO_ALTER i MQSO_RESUME	TEMPERATURY
	RACF wymagany dostęp do profilu `hlq.queuename` w klasie MQQUEUE lub MXQUEUE
MQSO_CREATE i MQSO_ALTER	TEMPERATURY
	RACF dostęp wymagany do profilu `hlq.ALTERNATE.USER.alternateuserid` w klasie MQADMIN lub MXADMIN
MQSO_ALTERNATE_UPRAWNIENIA_UŻYTKOWNIKA	TEMPERATURY

Uwagi dotyczące kolejek zarządzanych dla subskrypcji

Zostanie przeprowadzone sprawdzenie zabezpieczeń w celu sprawdzenia, czy użytkownik ma uprawnienia do subskrybowania tematu. Jednak podczas tworzenia kolejki zarządzanej lub w celu określenia, czy użytkownik ma dostęp do umieszczania komunikatów w tej kolejce docelowej, nie są wykonywane żadne sprawdzenia zabezpieczeń.

Nie można zamknąć kolejki zarządzanej.

Używane są następujące kolejki modelowe: `SYSTEM.DURABLE.MODEL.QUEUE` i `SYSTEM.NDURABLE.MODEL.QUEUE`.

Kolejki zarządzane utworzone na podstawie tych kolejek modelowych mają postać `SYSTEM.MANAGED.DURABLE.A346EF00367849A0` i `SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0` , gdzie ostatni kwalifikator jest nieprzewidywalny.

Nie należy nadawać użytkownikom dostępu do tych kolejek. Kolejki mogą być chronione przy użyciu profili ogólnych w postaci `SYSTEM.MANAGED.DURABLE.*` i `SYSTEM.MANAGED.NDURABLE.*` bez nadanych uprawnień.

Komunikaty mogą być pobierane z tych kolejek za pomocą uchwytu zwróconego w żądaniu MQSUB.

Jeśli jawnie zostanie wykonane wywołanie MQCLOSE dla subskrypcji z określoną opcją `MQCO_REMOVE_SUB` , a subskrypcja zamykana pod tym uchwytem nie została utworzona, w momencie zamknięcia wykonywane jest sprawdzenie zabezpieczeń w celu upewnienia się, że użytkownik ma odpowiednie uprawnienia do wykonania operacji.

Tabela 39. Poziom dostępu wymagany dla profili na potrzeby zabezpieczeń tematu na potrzeby zamykania operacji subskrybowania	
Opcja MQCLOSE	**Dostęp RACF wymagany do profilu `hlq.SUBSCRIBE.topicname` w klasie MXTOPIC**
MQCO_REMOVE_SUB	Zmień

Publikowanie

Aby publikować w temacie, wymagany jest dostęp do tematu oraz, jeśli używane są kolejki aliasowe, do kolejki aliasowej.

Tabela 40. Poziom dostępu wymagany do publikowania przez zabezpieczenia tematu	
Opcja MQOPEN lub MQPUT1	**Dostęp RACF wymagany do profilu `hlq.PUBLISH.topicname` w klasie MXTOPIC**
MQOO_OUTPUT lub MQPUT1	TEMPERATURY

Tabela 41. Poziom dostępu wymagany do otwarcia kolejki aliasowej, która jest tłumaczona na temat	
Opcja MQOPEN lub MQPUT1	**Wymagany dostęp RACF do profilu `hlq.queuename` w klasie MQQUEUE lub MXQUEUE dla kolejki aliasowej**
MQOO_OUTPUT lub MQPUT1	TEMPERATURY

Szczegółowe informacje na temat działania zabezpieczeń tematu w przypadku otwarcia kolejki aliasowej, która jest tłumaczona na nazwę tematu, można znaleźć w sekcji “Uwagi dotyczące kolejek aliasowych, które są rozstrzygane na tematy dla operacji publikowania” na stronie 225.

Podczas uwzględniania kolejek aliasowych używanych dla kolejek docelowych w ograniczeniach PUT i GET należy zapoznać się z sekcją “Uwagi dotyczące kolejek aliasowych” na stronie 213.

Jeśli poziom dostępu aplikacji RACF do profilu zabezpieczeń tematu zostanie zmieniony, zmiany odniosą skutek tylko w przypadku wszystkich uzyskanych nowych uchwytów obiektów (czyli nowych uchwytów MQSUB lub MQOPEN) dla tego tematu. Uchwyty te już istnieją w momencie zmiany, zachowując istniejący dostęp do tematu. Ponadto istniejący subskrybenci zachowują dostęp do wszystkich subskrypcji, które już dokonali.

Uwagi dotyczące kolejek aliasowych, które są rozstrzygane na tematy dla operacji publikowania

Po wywołaniu komendy MQOPEN lub MQPUT1 dla kolejki aliasowej, która jest tłumaczona na temat, program IBM MQ sprawdza dwa zasoby:

- Pierwsza nazwa kolejki aliasowej określona w deskryptorze obiektu (MQOD) w wywołaniu MQOPEN lub MQPUT1 .
- Drugi względem tematu, na który rozstrzygana jest kolejka aliasowa

Należy pamiętać, że to zachowanie różni się od zachowania, które jest uzyskiwane, gdy kolejki aliasowe są tłumaczone na inne kolejki. Aby działanie publikowania było kontynuowane, należy mieć poprawny dostęp do obu profili.

Bezpieczeństwo tematu systemowego

Przestrzeń adresowa inicjatora kanału ma dostęp do następujących tematów systemowych.

Identyfikatory użytkowników, dla których ta komenda jest uruchamiana, muszą mieć dostęp do tych kolejek na poziomie RACF , jak to pokazano na rysunku (Tabela 42 na stronie 226).

Tabela 42. Wymagany dostęp do tematów SYSTEM		
SYSTEM, temat	**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 niezbędnych grup lub identyfikatorów użytkowników do tych profili.

Jeśli zabezpieczenia procesu są aktywne, należy:

- Zdefiniuj profile w klasach **MQPROC** lub **GMQPROC** , jeśli używane są profile pisane wielkimi literami.
- Zdefiniuj profile w klasach **MXPROC** lub **GMXPROC** , jeśli używane są profile z mieszaną wielkością liter.
- Zezwól na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili, aby mogły one wysyłać żądania interfejsu API IBM MQ , które korzystają z procesów.

Profile dla procesów przyjmują formę:

```
hlq.processname
```

gdzie `hlq` może mieć wartość `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `processname` jest nazwą otwieranego procesu.

Profil poprzedzony nazwą menedżera kolejek steruje dostępem do pojedynczej definicji procesu w tym menedżerze kolejek. Profil z przedrostkiem nazwy grupy współużytkowania kolejek 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 pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tej definicji procesu w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

W poniższej tabeli przedstawiono dostęp wymagany do otwarcia procesu.

Tabela 43. Poziomy dostępu dla bezpieczeństwa procesu	
Opcja MQOPEN	**RACF poziom dostępu wymagany dla hlq.processname**
MQOO_INQUIRE	ODCZYT

Na przykład w menedżerze kolejek MQS9grupa RACF INQVPRC musi mieć możliwość wykonania zapytania (`MQINQ`). na wszystkich procesach rozpoczynających się od litery V. Definicje RACF dla tej opcji są następujące:

```
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 opcji otwierania 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 dostęp do tych profili.

Jeśli zabezpieczenia listy nazw są aktywne, należy:

- Zdefiniuj profile w klasach **MQNLIST** lub **GMQNLIST** , jeśli używane są profile pisane wielkimi literami.
- Zdefiniuj profile w klasach **MXNLIST** lub **GMXNLIST** , jeśli używane są profile z mieszaną wielkością liter.
- Zezwól na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili.

Profile dla list nazw przyjmują formę:

```
hlq.namelistname
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `namelistname` jest nazwą otwieranej listy nazw.

Profil poprzedzony nazwą menedżera kolejek steruje dostępem do pojedynczej listy nazw w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek steruje dostępem do co najmniej jednej listy nazw o tej nazwie we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tej listy nazw w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

W poniższej tabeli przedstawiono dostęp wymagany do otwarcia listy nazw.

Tabela 44. Poziomy dostępu dla zabezpieczeń listy nazw

Opcja MQOPEN	**RACF poziom dostępu wymagany dla hlq.namelistname**
MQOO_INQUIRE	ODCZYT

Na przykład w menedżerze kolejek (lub grupie współużytkowania kolejek) PQM3grupa RACF DEPT571 musi mieć możliwość wykonania zapytania (`MQINQ`). na tych listach nazw:

- Wszystkie listy nazw rozpoczynające się od "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/ŻĄDANIE/KOLEJKI
- WAREHOUSE.BROADCAST

Aby to zrobić, należy wykonać następujące definicje RACF :

```
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.

Bezpieczeństwo listy nazw systemu

Wiele list nazw systemów jest dostępnych w dodatkowych częściach systemu IBM MQ:

- Program narzędziowy CSQUTIL
- Operacje i panele sterowania
- Przestrzeń adresowa inicjatora kanału (w tym umieszczony w kolejce demon publikowania/subskrypcji)

Identyfikatory użytkowników, dla których są one uruchamiane, muszą mieć dostęp RACF do tych list nazw, jak to pokazano w sekcji Tabela 45 na stronie 228.

Tabela 45. Dostęp wymagany przez IBM MQ do list nazw SYSTEM

Lista nazw SYSTEM	CSQUTIL	Obsługa i panele sterowania	Inicjator kanału dla rozproszonego kolejkowania
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	ODCZYT
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	ODCZYT

z/OS *Profile dla alternatywnych zabezpieczeń użytkownika*

Jeśli alternatywne zabezpieczenia użytkowników są aktywne, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili.

Więcej informacji na temat komendy *AlternateUserId*zawiera sekcja AlternateUserID (MQCHAR12).

Jeśli alternatywne zabezpieczenia użytkownika są aktywne, należy wykonać następujące czynności:

- Zdefiniuj profile w klasach MQADMIN lub GMQADMIN, jeśli używane są profile pisane wielkimi literami.
- Zdefiniuj profile w klasach MXADMIN lub GMXADMIN, jeśli używane są profile z mieszaną wielkością liter.

Zezwól na dostęp niezbędnych grup lub identyfikatorów użytkowników do tych profili, aby mogły one używać opcji ALTERNATE_USER_AUTHORITY podczas otwierania obiektu.

Profile dla alternatywnych zabezpieczeń użytkownika mogą być określone na poziomie podsystemu lub na poziomie grupy współużytkowania kolejki i mają następującą postać:

```
hlq.ALTERNATE.USER.alternateuserid
```

Gdzie `hlq` może mieć wartość `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), a `alternateuserid` jest wartością pola *AlternateUserId* w deskryptorze obiektu.

Profil poprzedzony nazwą menedżera kolejek steruje użyciem alternatywnego identyfikatora użytkownika w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek 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 grupie współużytkowania kolejek przez użytkownika, który ma odpowiednie prawa dostępu. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tego alternatywnego identyfikatora użytkownika w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

W poniższej tabeli przedstawiono dostęp podczas określania alternatywnej opcji użytkownika.

Tabela 46. Poziomy dostępu dla alternatywnych zabezpieczeń użytkownika	
Opcja MQOPEN, MQSUB lub MQPUT1	**Wymagany poziom dostępu RACF**
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	TEMPERATURY

Oprócz alternatywnych sprawdzeń bezpieczeństwa użytkownika można również wykonywać inne sprawdzenia bezpieczeństwa kolejki, procesu, listy nazw i kontekstu. Alternatywny identyfikator użytkownika, jeśli został podany, jest używany tylko na potrzeby sprawdzania zabezpieczeń w zasobach kolejki, definicji procesu lub listy nazw. W przypadku alternatywnych sprawdzeń bezpieczeństwa użytkowników i kontekstu, identyfikator użytkownika żądającego sprawdzenia jest używany. Szczegółowe informacje na temat obsługi identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253. Tabela podsumowania przedstawiająca opcje otwierania i sprawdzania zabezpieczeń wymagane, gdy wszystkie zabezpieczenia kolejki, kontekstu i alternatywnego użytkownika są aktywne, znajduje się w sekcji Tabela 36 na stronie 220.

Alternatywny profil użytkownika daje żądającemu ID użytkownika dostęp do zasobów powiązanych z ID użytkownika określonym w alternatywnym ID użytkownika. Na przykład serwer listy płac uruchomiony z identyfikatorem 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 listy płac będzie wykonywana z identyfikatorem użytkownika zgłaszającego żądanie, używane są alternatywne uprawnienia użytkownika. Serwer listy płac wie, który identyfikator użytkownika należy określić jako alternatywny identyfikator użytkownika, ponieważ programy żądające generują komunikaty przy użyciu opcji umieszczania komunikatu MQPMO_DEFAULT_CONTEXT. Więcej informacji na temat uzyskiwania alternatywnych identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253 .

Następujące przykładowe definicje RACF umożliwiają programowi serwera określenie alternatywnych identyfikatorów użytkowników rozpoczynających się 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. Wszystkie 12 bajtów jest używanych podczas sprawdzania profilu, ale tylko 8 pierwszych bajtów jest używanych jako ID użytkownika przez IBM MQ. Jeśli obcięcie identyfikatora użytkownika nie jest pożądane, aplikacje wysyłające żądanie muszą przetłumaczyć dowolny alternatywny identyfikator użytkownika na więcej niż 8 bajtów.
2. Jeśli określono opcję MQOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY lub MQPMO_ALTERNATE_USER_AUTHORITY, a nie określono pola *AlternateUserId* w deskryptorze obiektu, używany jest identyfikator użytkownika pusty. Na potrzeby zabezpieczeń alternatywnych należy sprawdzić, czy identyfikator użytkownika używany dla kwalifikatora *AlternateUserId* to -BLANK-. Na przykład `RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-`.

   Jeśli użytkownik ma dostęp do tego profilu, wszystkie dalsze sprawdzenia są wykonywane przy użyciu identyfikatora użytkownika o wartości pustej. Szczegółowe informacje na temat pustych identyfikatorów użytkowników zawiera sekcja “Puste identyfikatory użytkowników i poziomy UACC” na stronie 262.

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 funkcji RACF RACVAR. Szczegółowe informacje na temat używania komendy RACVAR zawiera dokumentacja produktu z/OS Security Server RACF .

Gdy komunikat jest umieszczany w kolejce, która została otwarta z alternatywnymi uprawnieniami użytkownika, a kontekst komunikatu został wygenerowany przez menedżer kolejek, pole MQMD_USER_IDENTIFIER jest ustawiane na alternatywny identyfikator użytkownika.

z/OS *Profile zabezpieczeń kontekstu*

Jeśli zabezpieczenia kontekstu są aktywne, aby kontrolować dostęp do informacji o kontekście komunikatu, należy zdefiniować profile w odpowiednich klasach i zezwolić na dostęp do tych profili niezbędnych grup lub identyfikatorów użytkowników. Kontekst komunikatu jest zawarty w deskryptorze komunikatu (MQMD).

Korzystanie z profili na potrzeby zabezpieczeń kontekstu

Jeśli zabezpieczenia kontekstu są aktywne, aby umożliwić użytkownikom dostęp do informacji o kontekście dla komunikatów w konkretnej kolejce lub podczas publikowania w konkretnym temacie, należy zdefiniować profil w jednej z następujących klas:

- Klasa `MQADMIN` , jeśli używane są profile pisane wielkimi literami.
- Klasa `MXADMIN` , jeśli używane są profile z mieszanymi wielkami liter.

Profile zabezpieczeń kontekstu mogą być określone na poziomie podsystemu lub na poziomie grupy współużytkowania kolejki i mają następującą postać:

```
hlq.CONTEXT.queuename
hlq.CONTEXT.topicname
```

gdzie *hlq* może być nazwą menedżera kolejek lub nazwą grupy współużytkowania kolejek, a *queuename* i *topicname* może być pełną lub ogólną nazwą kolejki lub tematu, dla którego ma zostać zdefiniowany profil kontekstu.

Profil z przedrostkiem nazwy menedżera kolejek i wartością ** określoną jako nazwa kolejki lub tematu umożliwia sterowanie zabezpieczeniami kontekstu we wszystkich kolejkach i tematach należących do tego menedżera kolejek. Można to przesłonić w pojedynczej kolejce lub temacie, definiując konkretny profil dla kontekstu w tej kolejce lub temacie.

Profil z przedrostkiem nazwy grupy współużytkowania kolejek i wartością ** określoną jako nazwa kolejki lub tematu umożliwia sterowanie kontekstem we wszystkich kolejkach i tematach należących do menedżerów kolejek w grupie współużytkowania kolejek. Można to przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla kontekstu w tym menedżerze kolejek, określając profil z przedrostkiem w postaci nazwy menedżera kolejek. Można ją także przesłonić w pojedynczej kolejce lub temacie, określając profil z dołączonym przyrostkiem nazwy kolejki lub tematu.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

Należy zezwolić na dostęp niezbędnych grup lub identyfikatorów użytkowników do tego profilu. W poniższej tabeli przedstawiono wymagany poziom dostępu, w zależności od specyfikacji opcji kontekstu podczas otwierania kolejki.

Tabela 47. Poziomy dostępu dla zabezpieczeń kontekstu

Opcja MQOPEN lub MQPUT1	**RACF poziom dostępu wymagany do 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

Tabela 47. Poziomy dostępu dla zabezpieczeń kontekstu (kontynuacja)	
Opcja MQOPEN lub MQPUT1	**RACF poziom dostępu wymagany do hlq.CONTEXT.queuename lub hlq.CONTEXT.topicname**
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
Opcja MQSUB	
MQSO_SET_IDENTITY_CONTEXT **(Uwaga 2)**	TEMPERATURY

Uwaga:

1. Identyfikatory użytkowników używane do kolejkowania rozproszonego wymagają `KONTROLI` dostępu do `hlq.CONTEXT.queuename` w celu umieszczenia komunikatów w kolejce docelowej. Więcej informacji na temat używanych identyfikatorów użytkowników zawiera sekcja “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 256 .
2. Jeśli w żądaniu MQSUB z określonymi opcjami `MQSO_CREATE` lub `MQSO_ALTER` ma zostać ustawione dowolne pole kontekstu tożsamości w strukturze MQSD, należy określić opcję `MQSO_SET_IDENTITY_CONTEXT` . Wymagane są również odpowiednie uprawnienia do profilu kontekstu dla kolejki docelowej.

Jeśli komendy są umieszczane w kolejce wejściowej komend systemowych, należy użyć opcji umieszczania kontekstu domyślnego, aby powiązać poprawny ID użytkownika z komendą.

Na przykład do przenoszenia i przeładowywania komunikatów w kolejkach można użyć dostarczonego przez IBM MQprogramu narzędziowego CSQUTIL. Gdy przenoszone komunikaty są odtwarzane do kolejki, program narzędziowy CSQUTIL używa opcji `MQOO_SET_ALL_CONTEXT` do przywrócenia pierwotnego stanu komunikatów. Oprócz zabezpieczeń kolejki wymaganych przez tę opcję otwierania wymagane jest również uprawnienie kontekstowe. Jeśli na przykład to uprawnienie jest wymagane przez grupę BACKGRP w menedżerze kolejek MQS1, będzie ono definiowane przez:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

W zależności od określonych opcji i typów wykonywanych zabezpieczeń, podczas otwierania kolejki mogą również wystąpić inne typy sprawdzania zabezpieczeń. Są to między innymi zabezpieczenia kolejki (patrz sekcja “Profile zabezpieczeń kolejki” na stronie 211) i alternatywne zabezpieczenia użytkownika (patrz sekcja “Profile dla alternatywnych zabezpieczeń użytkownika” na stronie 228). Tabela podsumowania przedstawiająca opcje otwierania i sprawdzania zabezpieczeń wymagane, gdy wszystkie zabezpieczenia kolejki, kontekstu i alternatywnego użytkownika są aktywne, znajduje się w sekcji Tabela 36 na stronie 220.

Bezpieczeństwo kontekstu kolejki systemowej

Wiele kolejek systemowych jest dostępnych w dodatkowych częściach systemu IBM MQ, na przykład w przestrzeni adresowej inicjatora kanału oraz na serwerze mqweb używanym przez IBM MQ Console i REST API.

Identyfikatory użytkowników, dla których są one uruchamiane, muszą mieć dostęp do tych kolejek na poziomie RACF , jak to pokazano na rysunku (Tabela 48 na stronie 232).

Tabela 48. Dostęp wymagany do kolejek SYSTEM dla operacji kontekstowych

Kolejka systemowa	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 dla ochrony komend*

Aby włączyć sprawdzanie zabezpieczeń dla komend, należy dodać profile do klasy MQCMDS. Nazwy profili są oparte na komendach MQSC, ale sterują komendami MQSC i PCF. Profile mogą mieć zastosowanie do menedżera kolejek lub grupy współużytkowania kolejek.

Aby sprawdzić bezpieczeństwo komend (dlatego nie zdefiniowano profilu przełącznika bezpieczeństwa komendy hlq.NO.CMD.CHECKS) należy dodać profile do klasy MQCMDS.

Te same profile zabezpieczeń sterują komendami MQSC i PCF. Nazwy profili RACF na potrzeby sprawdzania zabezpieczeń komend są oparte na samych nazwach komend MQSC. Profile te mają następującą postać:

```
hlq.verb.pkw
```

Gdzie `hlq` może mieć wartość `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek), `verb` jest częścią komendy komendy, na przykład ALTER, a `pkw` jest typem obiektu, na przykład QLOCAL w przypadku kolejki lokalnej.

Dlatego nazwa profilu dla komendy ALTER QLOCAL w podsystemie CSQ1 jest następująca:

```
CSQ1.ALTER.QLOCAL
```

Profili ogólnych można używać do ochrony zestawów komend, aby zmniejszyć liczbę profili do obsługi, a tym samym zmniejszyć liczbę list dostępu. Należy rozważyć utworzenie profilu ogólnego, który ma zastosowanie do wszystkich komend niechronionych przez bardziej szczegółowy profil. Zdefiniuj ten profil z dostawcą UACC (NONE) i nadaj dostęp typu ALTER tylko grupom RACF zawierającym administratorów. Następnie można utworzyć profil ogólny, który będzie miał zastosowanie do wszystkich komend DISPLAY i nadać mu szeroki dostęp. Między tymi skrajnościami można zidentyfikować grupy użytkowników, którzy potrzebują dostępu do pewnych zestawów komend. W takim przypadku można utworzyć profile dla tych zestawów i nadać dostęp grupom RACF reprezentującym 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 nazwą menedżera kolejek steruje użyciem komendy w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek steruje użyciem komendy we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tej komendy w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i na poziomie grupy współużytkowania kolejek,

program IBM MQ sprawdza, czy istnieje profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

Ustawiając profile komend na poziomie menedżera kolejek, użytkownik może zostać ograniczony do wydawania komend w konkretnym menedżerze kolejek. Alternatywnie można zdefiniować jeden profil dla grupy współużytkowania kolejek dla każdej komendy, a wszystkie sprawdzenia zabezpieczeń będą wykonywane dla tego profilu zamiast dla poszczególnych menedżerów kolejek.

Jeśli zarówno zabezpieczenia podsystemu, jak i zabezpieczenia grupy współużytkowania kolejek są aktywne, a profil lokalny nie został znaleziony, wykonywane jest sprawdzenie bezpieczeństwa komendy w celu sprawdzenia, czy użytkownik ma dostęp do profilu grupy współużytkowania kolejek.

Jeśli atrybut CMDSCOPE jest używany do kierowania komendy do innych menedżerów kolejek w grupie współużytkowania kolejek, zabezpieczenia są sprawdzane w każdym menedżerze kolejek, w którym uruchomiono komendę, ale niekoniecznie w menedżerze kolejek, w którym wprowadzono komendę.

Tabela 49 na stronie 233 przedstawia dla każdej komendy MQSC IBM MQ profile wymagane do sprawdzania zabezpieczeń komend oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

Tabela 50 na stronie 239 przedstawia dla każdej komendy PCF systemu IBM MQ profile wymagane do przeprowadzenia sprawdzania bezpieczeństwa komendy oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu

Komenda	**Profil komendy MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla MQADMIN lub MXADMIN**	**Poziom dostępu dla MQADMIN lub MXADMIN**
ZMIEŃ INFORMACJE O AUTORYZACJI	hlq.ALTER.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
ZMIEŃ BUFFPOOL	hlq.ALTER.BUFFPOOL	Zmień	Nie sprawdzaj	-
ALTER CFSTRUCT,	hlq.ALTER.CFSTRUCT	Zmień	Nie sprawdzaj	-
ZMIEŃ KANAŁ	hlq.ALTER.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
ZMIEŃ NAZWĘ	hlq.ALTER.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
ZMIEŃ PROCES	hlq.ALTER.PROCESS	Zmień	hlq.PROCESS.process	Zmień
ZMIEŃ PSID	hlq.ALTER.PSID	Zmień	Nie sprawdzaj	-
ZMIEŃ QALIAS	hlq.ALTER.QALIAS	Zmień	hlq.QUEUE.queue	Zmień
ALTER QLOCAL,“5” na stronie 239	hlq.ALTER.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
ALTER QMGR (Zmiana menedżera kolejek)	hlq.ALTER.QMGR	Zmień	Nie sprawdzaj	-
ZMIEŃ QMODEL“5” na stronie 239	hlq.ALTER.QMODEL	Zmień	hlq.QUEUE.queue	Zmień
ZMIEŃ QREMOTE	hlq.ALTER.QREMOTE	Zmień	hlq.QUEUE.queue	Zmień
ZMIEŃ ZABEZPIECZENIA	hlq.ALTER.SECURITY	Zmień	Nie sprawdzaj	-
MODYFIKUJ SMDS	hlq.ALTER.SMDS	Zmień	Nie sprawdzaj	-
ZMIEŃ KLASĘ STGCLASS	hlq.ALTER.STGCLASS	Zmień	Nie sprawdzaj	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
ZMIEŃ SUB	hlq.ALTER.SUB	Zmień	Nie sprawdzaj	-
ALTER TOPIC	hlq.ALTER.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
MODYFIKUJ ŚLEDZENIE	hlq.ALTER.TRACE	Zmień	Nie sprawdzaj	-
DZIENNIK ARCHIWUM	hlq.ARCHIVE.LOG	CONTROL	Nie sprawdzaj	-
KOPIA ZAPASOWA CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROL	Nie sprawdzaj	-
WYCZYŚĆ QLOCAL	hlq.CLEAR.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
WYCZYŚĆ POLE WYBORU “3” na stronie 239	hlq.CLEAR.TOPICSTR	Zmień	hlq.TOPIC.topic	Zmień
ZDEFINIUJ INFORMACJE O AUTORYZ.	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
DEFINIUJ PULĘ BUFORÓW	hlq.DEFINE.BUFFPOOL	Zmień	Nie sprawdzaj	-
ZDEFINIUJ CFSTRUCT	hlq.DEFINE.CFSTRUCT	Zmień	Nie sprawdzaj	-
Zdefiniowanie kanału	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
ZDEFINIUJ DZIENNIK	hlq.DEFINE.LOG	Zmień	Nie sprawdzaj	-
ZDEFINIUJ MAXSMSGS	hlq.DEFINE.MAXSMSGS	Zmień	Nie sprawdzaj	-
DEFINIUJ LISTĘ NAZW	hlq.DEFINE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
ZDEFINIUJ PROCES	hlq.DEFINE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
ZDEFINIUJ PID	hlq.DEFINE.PSID	Zmień	Nie sprawdzaj	-
ZDEFINIUJ QALIAS	hlq.DEFINE.QALIAS	Zmień	hlq.QUEUE.queue	Zmień
ZDEFINIUJ QLOCAL“5” na stronie 239	hlq.DEFINE.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
ZDEFINIUJ QMODEL“5” na stronie 239	hlq.DEFINE.QMODEL	Zmień	hlq.QUEUE.queue	Zmień
DEFINIUJ QREMOTE	hlq.DEFINE.QREMOTE	Zmień	hlq.QUEUE.queue	Zmień
ZDEFINIUJ KLASĘ STGCLASS	hlq.DEFINE.STGCLASS	Zmień	Nie sprawdzaj	-
DEFINE SUB	hlq.DEFINE.SUB	Zmień	Nie sprawdzaj	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
ZDEFINIUJ TEMAT	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
USUŃ INFORMACJE O AUTORYZ	hlq.DELETE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
USUŃ BUFFPOOL	hlq.DELETE.BUFFPOOL	Zmień	Nie sprawdzaj	-
USUŃ CFSTRUCT	hlq.DELETE.CFSTRUCT	Zmień	Nie sprawdzaj	-
Usuń kanał	hlq.DELETE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
USUŃ NAZWĘ	hlq.DELETE.NAMELIST	Zmień	hlq.NAMELIST.namelist	Zmień
Usuń proces	hlq.DELETE.PROCESS	Zmień	hlq.PROCESS.process	Zmień
USUŃ PSID	hlq.DELETE.PSID	Zmień	Nie sprawdzaj	-
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 STG	hlq.DELETE.STGCLASS	Zmień	Nie sprawdzaj	-
USUŃ SUB	hlq.DELETE.SUB	Zmień	Nie sprawdzaj	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
WYŚWIETL ARCHIWUM “1” na stronie 238	hlq.DISPLAY.ARCHIVE	ODCZYT	Nie sprawdzaj	-
WYŚWIETL INFORMACJE O AUTORYZ	hlq.DISPLAY.AUTHINFO	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE STATUSU CFSTATUS	hlq.DISPLAY.CFSTATUS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL CFSTRUCT	hlq.DISPLAY.CFSTRUCT	ODCZYT	Nie sprawdzaj	-
WYŚWIETL KANAŁ	hlq.DISPLAY.CHANNEL	ODCZYT	Nie sprawdzaj	-
WYŚWIETL CHINIT	hlq.DISPLAY.CHINIT	ODCZYT	Nie sprawdzaj	-
WYŚWIETL CHLAURA	hlq.DISPLAY.CHLAUTH	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE STATUSU CHSTATUS	hlq.DISPLAY.CHSTATUS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL LISTĘ CLUSQMGR	hlq.DISPLAY.CLUSQMGR	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE CMDSERV	hlq.DISPLAY.CMDSERV	ODCZYT	Nie sprawdzaj	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
WYŚWIETL KONN “1” na stronie 238	hlq.DISPLAY.CONN	ODCZYT	Nie sprawdzaj	-
GRUPA WYŚWIETLANIA	hlq.DISPLAY.GROUP	ODCZYT	Nie sprawdzaj	-
WYŚWIETL DZIENNIK “1” na stronie 238	hlq.DISPLAY.LOG	ODCZYT	Nie sprawdzaj	-
WYŚWIETL MAXSMSGS	hlq.DISPLAY.MAXSMSGS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL LISTĘ NAZW	hlq.DISPLAY.NAMELIST	ODCZYT	Nie sprawdzaj	-
WYŚWIETL PROCES	hlq.DISPLAY.PROCESS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL PUBSUB	hlq.DISPLAY.PUBSUB	ODCZYT	Nie sprawdzaj	-
WYŚWIETL QALIAS	hlq.DISPLAY.QALIAS	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE KLASTRA (DISPLAY QCLUSTER)	hlq.DISPLAY.QCLUSTER	ODCZYT	Nie sprawdzaj	-
WYŚWIETL QLOCAL	hlq.DISPLAY.QLOCAL	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE QMGR	hlq.DISPLAY.QMGR	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE QMODEL	hlq.DISPLAY.QMODEL	ODCZYT	Nie sprawdzaj	-
WYŚWIETL QREMOTE	hlq.DISPLAY.QREMOTE	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE STATUSU QSTATUS	hlq.DISPLAY.QSTATUS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL KOLEJKĘ	hlq.DISPLAY.QUEUE	ODCZYT	Nie sprawdzaj	-
WYŚWIETL STATUS SBSTATUS	hlq.DISPLAY.SBSTATUS	ODCZYT	Nie sprawdzaj	-
Wyświetlanie zestawu SMDS	hlq.DISPLAY.SMDS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL SMDSCONN	hlq.DISPLAY.SMDSCONN	ODCZYT	Nie sprawdzaj	-
WYŚWIETL SUB	hlq.DISPLAY.SUB	ODCZYT	Nie sprawdzaj	-
WYŚWIETL ZABEZPIECZENIA	hlq.DISPLAY.SECURITY	ODCZYT	Nie sprawdzaj	-
WYŚWIETL KLASĘ STGCLASS	hlq.DISPLAY.STGCLASS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL SYSTEM “1” na stronie 238	hlq.DISPLAY.SYSTEM	ODCZYT	Nie sprawdzaj	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
WYŚWIETL WĄTEK	hlq.DISPLAY.THREAD	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE STATUSU TPSTATUS	hlq.DISPLAY.TPSTATUS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL TEMAT	hlq.DISPLAY.TOPIC	ODCZYT	Nie sprawdzaj	-
WYŚWIETLENIE STATUSU TPSTATUS	hlq.DISPLAY.TPSTATUS	ODCZYT	Nie sprawdzaj	-
WYŚWIETL ŚLEDZENIE	hlq.DISPLAY.TRACE	ODCZYT	Nie sprawdzaj	-
WYŚWIETL UŻYCIE “1” na stronie 238	hlq.DISPLAY.USAGE	ODCZYT	Nie sprawdzaj	-
PRZENIEŚ QLOCAL	hlq.MOVE.QLOCAL	Zmień	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	Zmień
WYKONAJ KOMENDĘ PING DLA KANAŁU	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ODTWÓRZ BSDS	hlq.RECOVER.BSDS	CONTROL	Nie sprawdzaj	-
ODZYSKIWANIE CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROL	Nie sprawdzaj	-
ODŚWIEŻ KLASTER	hlq.REFRESH.CLUSTER	Zmień	Nie sprawdzaj	-
ODŚWIEŻ MENEDŻERA KOLEJEK	hlq.REFRESH.QMGR	Zmień	Nie sprawdzaj	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	Zmień	Nie sprawdzaj	-
RESETUJ CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROL	Nie sprawdzaj	-
Resetuj kanał	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Resetowanie klastra	hlq.RESET.CLUSTER	CONTROL	Nie sprawdzaj	-
RESETUJ MENEDŻER KOLEJEK	hlq.RESET.QMGR	CONTROL	Nie sprawdzaj	-
ZRESETUJ QSTATS	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
ZRESETUJ SMDS	hlq.RESET.SMDS	CONTROL	Nie sprawdzaj	-
WYCZYŚĆ POTOK TPIPE	hlq.RESET.TPIPE	CONTROL	Nie sprawdzaj	-
Rozstrzyganie kanału	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ROZSTRZYGNIJ WĄTPLIWE	hlq.RESOLVE.INDOUBT	CONTROL	Nie sprawdzaj	-
WZNOWIENIE MENEDŻERA KOLEJEK	hlq.RESUME.QMGR	CONTROL	Nie sprawdzaj	-

Tabela 49. Komendy MQSC, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
RVERIFY-BEZPIECZEŃSTWO	hlq.RVERIFY.SECURITY	Zmień	Nie sprawdzaj	-
USTAW ARCHIWUM	hlq.SET.ARCHIVE	CONTROL	Nie sprawdzaj	-
USTAW CHLAURA	hlq.SET.CHLAUTH	CONTROL	Nie sprawdzaj	-
USTAW DZIENNIK	hlq.SET.LOG	CONTROL	Nie sprawdzaj	-
USTAW SYSTEM	hlq.SET.SYSTEM	CONTROL	Nie sprawdzaj	-
URUCHOM KANAŁ	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
URUCHOM CHINIT “4” na stronie 239	hlq.START.CHINIT	CONTROL	Nie sprawdzaj	-
URUCHOM CMDSERV	hlq.START.CMDSERV	CONTROL	Nie sprawdzaj	-
Uruchom proces nasłuchujący	hlq.START.LISTENER	CONTROL	Nie sprawdzaj	-
URUCHOM QMGR	Brak“2” na stronie 238	-	-	-
URUCHOM SMDSCONN	hlq.START.SMDSCONN	CONTROL	Nie sprawdzaj	-
URUCHOM ŚLEDZENIE	hlq.START.TRACE	CONTROL	Nie sprawdzaj	-
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
ZATRZYMAJ CHINIT	hlq.STOP.CHINIT	CONTROL	Nie sprawdzaj	-
ZATRZYMAJ CMDSERV	hlq.STOP.CMDSERV	CONTROL	Nie sprawdzaj	-
Zatrzymaj proces nasłuchujący	hlq.STOP.LISTENER	CONTROL	Nie sprawdzaj	-
ZATRZYMAJ QMGR	hlq.STOP.QMGR	CONTROL	Nie sprawdzaj	-
ZATRZYMAJ SMDSCONN	hlq.STOP.SMDSCONN	CONTROL	Nie sprawdzaj	-
ZATRZYMAJ ŚLEDZENIE	hlq.STOP.TRACE	CONTROL	Nie sprawdzaj	-
Menedżer kolejki zawieszony	hlq.SUSPEND.QMGR	CONTROL	Nie sprawdzaj	-

Uwagi:

1. Komendy te mogą być wydawane wewnętrznie przez menedżer kolejek; w takich przypadkach nie jest sprawdzane żadne uprawnienie.
2. IBM MQ nie sprawdza uprawnień użytkownika, który wydał komendę START QMGR. Jednak dostęp do komendy START xxxxMSTR wywołanej w wyniku wykonania komendy START QMGR można kontrolować za pomocą programu RACFlub alternatywnych narzędzi bezpieczeństwa.

W tym celu należy kontrolować dostęp do profilu MVS.START.STC.xxxxMSTR w klasie komend operatora RACF (OPERCMDS). Szczegółowe informacje na temat tej procedury zawiera sekcja Nadawanie użytkownikowi dostępu do klasy RACF OPERCMDS w podręczniku *z/OS MVS Planning: Operations*. Jeśli ta technika zostanie użyta, a nieautoryzowany użytkownik podejmie próbę uruchomienia menedżera kolejek, zostanie on zakończony z kodem przyczyny 00F30216.

3. Zasób **hlq.TOPIC.topic** odwołuje się do obiektu Topic pochodzącego z TOPICSTR. Więcej informacji na ten temat zawiera sekcja "Zabezpieczenia publikowania/subskrypcji" na stronie 533
4. W języku IBM MQ for z/OS: nazwa zasobu MVS.START.STC.CSQ1CHIN dołączany jest dodatkowy kwalifikator JOBNAME. Może to powodować problemy podczas uruchamiania inicjatora kanału.

   Aby rozwiązać ten problem, zastąp MVS.START.STC. *ssid* CHIN z profilem dla zasobu o nazwie MVS.START.STC. *ssid* WEJŚCIE **.*** lub MVS.START.STC. *ssid* CHIN. *ssid* CHIN, gdzie *ssid* jest identyfikatorem podsystemu menedżera kolejek. Wymaga to uprawnienia RACF UPDATE. Więcej informacji na ten temat zawiera sekcja MVS Commands, RACF Access Authorities, and Resource Names (Komendy, uprawnienia dostępu i nazwy zasobów) w podręczniku *z/OS MVS Planning: Operations*(Planowanie: operacje).

   START dla *ssid* MSTR nie zawiera parametru JOBNAME=. W celu zachowania spójności można zaktualizować profil dla MVS.START.STC.ssidMSTR na MVS.START.STC.ssidMSTR. *.

5. V 9.3.0 Ustawienie niepustej wartości atrybutu STREAMQ kolejki wymaga również ustawienia poziomu dostępu ALTER na wartość MQADMIN lub MXADMIN na wartość `hlq.ALTER.streamQ`.

Tabela 50. Komendy PCF, profile i ich poziomy dostępu

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
Zapasowa struktura CF	hlq.BACKUP.CFSTRUCT	CONTROL	Nie sprawdzaj	-
Zmień obiekt informacji uwierzytelniającej	hlq.ALTER.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Zmień strukturę CF	hlq.ALTER.CFSTRUCT	Zmień	Nie sprawdzaj	-
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
Zmień kolejkę"2" na stronie 243	hlq.ALTER.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Zmiana menedżera kolejek	hlq.ALTER.QMGR	Zmień	Nie sprawdzaj	-
Zmiana zabezpieczeń	hlq.ALTER.SECURITY	Zmień	Nie sprawdzaj	-
Zmień SMDS	hlq.ALTER.SMDS	Zmień	Nie sprawdzaj	-
Zmień klasę pamięci masowej	hlq.ALTER.STGCLASS	Zmień	Nie sprawdzaj	-
Zmień subskrypcję	hlq.ALTER.SUB	Zmień	Nie sprawdzaj	-
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 243	hlq.CLEAR.TOPICSTR	Zmień	hlq.TOPIC.topic	Zmień

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
Kopiowanie obiektu informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Kopiuj strukturę CF	hlq.DEFINE.CFSTRUCT	Zmień	Nie sprawdzaj	-
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	Nie sprawdzaj	-
Kopiuj klasę pamięci masowej	hlq.DEFINE.STGCLASS	Zmień	Nie sprawdzaj	-
Kopiuj temat	hlq.DEFINE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Utwórz obiekt informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Utwórz strukturę CF	hlq.DEFINE.CFSTRUCT	Zmień	Nie sprawdzaj	-
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“2” na stronie 243	hlq.DEFINE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Utwórz klasę pamięci masowej	hlq.DEFINE.STGCLASS	Zmień	Nie sprawdzaj	-
Utwórz subskrypcję	hlq.DEFINE.SUB	Zmień	Nie sprawdzaj	-
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	Nie sprawdzaj	-
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	Nie sprawdzaj	-
Usuń subskrypcję	hlq.DELETE.SUB	Zmień	Nie sprawdzaj	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Sprawdź archiwum	hlq.DISPLAY.ARCHIVE	ODCZYT	Nie sprawdzaj	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
Sprawdź obiekt informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy obiektów informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	ODCZYT	Nie sprawdzaj	-
Sprawdź strukturę CF	hlq.DISPLAY.CFSTRUCT	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy struktur CF	hlq.DISPLAY.CFSTRUCT	ODCZYT	Nie sprawdzaj	-
Sprawdź status struktury CF	hlq.DISPLAY.CFSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź kanał	hlq.DISPLAY.CHANNEL	ODCZYT	Nie sprawdzaj	-
Sprawdź rekordy uwierzytelniania kanału	hlq.DISPLAY.CHLAUTH	ODCZYT	Nie sprawdzaj	-
Sprawdź inicjatora kanału	hlq.DISPLAY.CHINIT	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy kanałów	hlq.DISPLAY.CHANNEL	ODCZYT	Nie sprawdzaj	-
Sprawdź status kanału	hlq.DISPLAY.CHSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź menedżera kolejek klastra	hlq.DISPLAY.CLUSQMGR	ODCZYT	Nie sprawdzaj	-
Sprawdź połączenie	hlq.DISPLAY.CONNPCF	ODCZYT	Nie sprawdzaj	-
Sprawdź grupę	hlq.DISPLAY.GROUP	ODCZYT	Nie sprawdzaj	-
Sprawdź dziennik	hlq.DISPLAY.LOG	ODCZYT	Nie sprawdzaj	-
Sprawdź listę nazw	hlq.DISPLAY.NAMELIST	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy list nazw	hlq.DISPLAY.NAMELIST	ODCZYT	Nie sprawdzaj	-
Sprawdź proces	hlq.DISPLAY.PROCESS	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy procesów	hlq.DISPLAY.PROCESS	ODCZYT	Nie sprawdzaj	-
Sprawdź status publikowania/ subskrypcji	hlq.DISPLAY.PUBSUB	ODCZYT	Nie sprawdzaj	-
Sprawdź kolejkę	hlq.DISPLAY.QUEUE	ODCZYT	Nie sprawdzaj	-
Sprawdź menedżera kolejek	hlq.DISPLAY.QMGR	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy kolejek	hlq.DISPLAY.QUEUE	ODCZYT	Nie sprawdzaj	-
Sprawdź status kolejki	hlq.DISPLAY.QSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź zabezpieczenia	hlq.DISPLAY.SECURITY	ODCZYT	Nie sprawdzaj	-
Sprawdź SMDS	hlq.DISPLAY.SMDS	ODCZYT	Nie sprawdzaj	-
Sprawdź SMDSCONN	hlq.DISPLAY.SMDSCONN	ODCZYT	Nie sprawdzaj	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla MQADMIN lub MXADMIN
Sprawdź klasę pamięci masowej	hlq.DISPLAY.STGCLASS	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy klas pamięci masowej	hlq.DISPLAY.STGCLASS	ODCZYT	Nie sprawdzaj	-
Sprawdź subskrypcję	hlq.INQUIRE.SUB	ODCZYT	Nie sprawdzaj	-
Sprawdź status subskrypcji	hlq.INQUIRE.SBSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź system	hlq.DISPLAY.SYSTEM	ODCZYT	Nie sprawdzaj	-
Sprawdź temat	hlq.DISPLAY.TOPIC	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy tematów	hlq.DISPLAY.TOPIC	ODCZYT	Nie sprawdzaj	-
Sprawdź status tematu	hlq.DISPLAY.TPSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź użycie	hlq.DISPLAY.USAGE	ODCZYT	Nie sprawdzaj	-
Przenieś kolejkę	hlq.MOVE.QLOCAL	Zmień	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	Zmień
Wyślij ping do kanału	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Odtwórz strukturę CF	hlq.RECOVER.CFSTRUCT	CONTROL	Nie sprawdzaj	-
Odśwież klaster	hlq.REFRESH.CLUSTER	Zmień	Nie sprawdzaj	-
Odśwież menedżera kolejek	hlq.REFRESH.QMGR	Zmień	Nie sprawdzaj	-
Odśwież zabezpieczenia	hlq.REFRESH.SECURITY	Zmień	Nie sprawdzaj	-
Resetuj strukturę CF	hlq.RESET.CFSTRUCT	CONTROL	Nie sprawdzaj	-
Resetowanie kanału	hlq.RESET.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Resetowanie klastra	hlq.RESET.CLUSTER	CONTROL	Nie sprawdzaj	-
Resetuj menedżer kolejek	hlq.RESET.QMGR	CONTROL	Nie sprawdzaj	-
Resetuj statystyki kolejki	hlq.RESET.QSTATS	CONTROL	hlq.QUEUE.queue	CONTROL
Zresetuj SMDS	hlq.RESET.SMDS	CONTROL	Nie sprawdzaj	-
Rozstrzyganie kanału	hlq.RESOLVE.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Wznów menedżera kolejek	hlq.RESUME.QMGR	CONTROL	Nie sprawdzaj	-
Wznawianie klastra menedżera kolejek	hlq.RESUME.QMGR	CONTROL	Nie sprawdzaj	-
Zweryfikuj ponownie zabezpieczenia	hlq.RVERIFY.SECURITY	Zmień	Nie sprawdzaj	-
Ustaw archiwum	hlq.SET.ARCHIVE	CONTROL	Nie sprawdzaj	-
Ustaw rekord uwierzytelniania kanału	hlq.SET.CHLAUTH	CONTROL	Nie sprawdzaj	-
Ustaw dziennik	hlq.SET.LOG	CONTROL	Nie sprawdzaj	-

Tabela 50. Komendy PCF, profile i ich poziomy dostępu (kontynuacja)				
Komenda	**Profil komendy MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla MQADMIN lub MXADMIN**	**Poziom dostępu dla MQADMIN lub MXADMIN**
Ustaw system	hlq.SET.SYSTEM	CONTROL	Nie sprawdzaj	-
Uruchom kanał	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Uruchom inicjatora kanału	hlq.START.CHINIT	CONTROL	Nie sprawdzaj	-
Uruchom program nasłuchujący kanału	hlq.START.LISTENER	CONTROL	Nie sprawdzaj	-
Uruchom połączenie SMDS	hlq.START.SMDSCONN	CONTROL	Nie sprawdzaj	-
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Zatrzymaj inicjatora kanału	hlq.STOP.CHINIT	CONTROL	Nie sprawdzaj	-
Zatrzymaj program nasłuchujący kanału	hlq.STOP.LISTENER	CONTROL	Nie sprawdzaj	-
Zatrzymaj połączenie SMDS	hlq.STOP.SMDSCONN	CONTROL	Nie sprawdzaj	-
Menedżer kolejki - SUSPEND	hlq.SUSPEND.QMGR	CONTROL	Nie sprawdzaj	-
Zawieś klaster menedżera kolejek	hlq.SUSPEND.QMGR	CONTROL	Nie sprawdzaj	-

Uwagi:

1. Zasób **`hlq.TOPIC.topic`** odwołuje się do obiektu Topic pochodzącego z TOPICSTR. Więcej informacji na ten temat zawiera sekcja “Zabezpieczenia publikowania/subskrypcji” na stronie 533
2. V 9.3.0 Ustawienie niepustej wartości atrybutu STREAMQ kolejki wymaga również ustawienia poziomu dostępu ALTER na wartość MQADMIN lub MXADMIN na wartość `hlq.ALTER.streamQ`.

Szczegółowe informacje na temat wymaganych profili PCF IBM MQ podczas korzystania z IBM MQ Consolezawiera sekcja “IBM MQ Console -wymagane profile zabezpieczeń komend” na stronie 243 .

z/OS *IBM MQ Console -wymagane profile zabezpieczeń komend*

Operacje wykonywane w produkcie IBM MQ Console przez użytkownika w roli `MQWebAdmin`lub `MQWebAdminRO`są wykonywane w kontekście zabezpieczeń identyfikatora użytkownika uruchomionego zadania serwera mqweb. Jeśli ma być używany plik IBM MQ Console, identyfikator użytkownika uruchomionego zadania serwera mqweb musi mieć uprawnienia do wydawania określonych komend PCF.

Tabela 51 na stronie 244 przedstawia dla każdej komendy PCF systemu IBM MQ wymagane profile zabezpieczeń komend oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS wymaganej przez IBM MQ Console.

Tabela 51. Komendy PCF IBM MQ Console , profile i ich poziomy dostępu

Komenda	Profil komendy MQCMDS	Poziom dostępu dla MQCMDS	Profil zasobu komendy dla MQADMIN lub MXADMIN	Poziom dostępu dla 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
Zmień kolejkę	hlq.ALTER.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Zmiana menedżera kolejek	hlq.ALTER.QMGR	Zmień	Nie sprawdzaj	-
Zmień temat	hlq.ALTER.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Wyczyść kolejkę	hlq.CLEAR.QLOCAL	Zmień	hlq.QUEUE.queue	Zmień
Utwórz obiekt informacji uwierzytelniającej	hlq.DEFINE.AUTHINFO	Zmień	hlq.AUTHINFO.resourcename	Zmień
Utwórz kanał	hlq.DEFINE.CHANNEL	Zmień	hlq.CHANNEL.channel	Zmień
Utwórz kolejkę	hlq.DEFINE.QUEUE	Zmień	hlq.QUEUE.queue	Zmień
Utwórz subskrypcję	hlq.DEFINE.SUB	Zmień	Nie sprawdzaj	-
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	Nie sprawdzaj	-
Usuń temat	hlq.DELETE.TOPIC	Zmień	hlq.TOPIC.topic	Zmień
Sprawdź obiekt informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy obiektów informacji uwierzytelniającej	hlq.DISPLAY.AUTHINFO	ODCZYT	Nie sprawdzaj	-
Sprawdź kanał	hlq.DISPLAY.CHANNEL	ODCZYT	Nie sprawdzaj	-
Sprawdź rekordy uwierzytelniania kanału	hlq.DISPLAY.CHLAUTH	ODCZYT	Nie sprawdzaj	-
Sprawdź inicjatora kanału	hlq.DISPLAY.CHINIT	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy kanałów	hlq.DISPLAY.CHANNEL	ODCZYT	Nie sprawdzaj	-
Sprawdź status kanału	hlq.DISPLAY.CHSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź kolejkę	hlq.DISPLAY.QUEUE	ODCZYT	Nie sprawdzaj	-
Sprawdź menedżera kolejek	hlq.DISPLAY.QMGR	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy kolejek	hlq.DISPLAY.QUEUE	ODCZYT	Nie sprawdzaj	-
Sprawdź status kolejki	hlq.DISPLAY.QSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź subskrypcję	hlq.INQUIRE.SUB	ODCZYT	Nie sprawdzaj	-

Tabela 51. Komendy PCF IBM MQ Console , profile i ich poziomy dostępu (kontynuacja)				
Komenda	**Profil komendy MQCMDS**	**Poziom dostępu dla MQCMDS**	**Profil zasobu komendy dla MQADMIN lub MXADMIN**	**Poziom dostępu dla MQADMIN lub MXADMIN**
Sprawdź status subskrypcji	hlq.INQUIRE.SBSTATUS	ODCZYT	Nie sprawdzaj	-
Sprawdź temat	hlq.DISPLAY.TOPIC	ODCZYT	Nie sprawdzaj	-
Sprawdź nazwy tematów	hlq.DISPLAY.TOPIC	ODCZYT	Nie sprawdzaj	-
Sprawdź status tematu	hlq.DISPLAY.TPSTATUS	ODCZYT	Nie sprawdzaj	-
Wyślij ping do kanału	hlq.PING.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Odśwież klaster	hlq.REFRESH.CLUSTER	Zmień	Nie sprawdzaj	-
Odśwież zabezpieczenia	hlq.REFRESH.SECURITY	Zmień	Nie sprawdzaj	-
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	Nie sprawdzaj	-
Uruchom kanał	hlq.START.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL
Zamknij kanał	hlq.STOP.CHANNEL	CONTROL	hlq.CHANNEL.channel	CONTROL

z/OS *Profile dla ochrony zasobów komend*

Jeśli nie zdefiniowano profilu przełącznika bezpieczeństwa zasobów komendy, aby sprawdzić bezpieczeństwo zasobów powiązanych z komendami, należy dodać profile zasobów dla każdego zasobu do odpowiedniej klasy. Te same profile zabezpieczeń sterują komendami MQSC i PCF.

Jeśli nie zdefiniowano profilu przełącznika bezpieczeństwa zasobów komendy (`hlq.NO.CMD.RESC.CHECKS`), aby sprawdzić bezpieczeństwo zasobów powiązanych z komendami, należy wykonać następujące czynności:

- Dodaj profil zasobu w klasie **MQADMIN** , jeśli używane są profile pisane wielkimi literami, dla każdego zasobu.
- Dodaj profil zasobu w klasie **MXADMIN** , jeśli używane są profile z mieszaną wielkością liter, dla każdego zasobu.

Te same profile zabezpieczeń sterują komendami MQSC i PCF.

Profile sprawdzania ochrony zasobów komend przyjmują następującą formę:

```
hlq.type.resourcename
```

gdzie `hlq` może być `qmgr-name` (nazwa menedżera kolejek) lub `qsg-name` (nazwa grupy współużytkowania kolejek).

Profil poprzedzony nazwą menedżera kolejek steruje dostępem do zasobów powiązanych z komendami w tym menedżerze kolejek. Profil poprzedzony nazwą grupy współużytkowania kolejek steruje dostępem do zasobów powiązanych z komendami we wszystkich menedżerach kolejek w grupie współużytkowania kolejek. Ten dostęp można przesłonić w pojedynczym menedżerze kolejek, definiując profil na poziomie menedżera kolejek dla tego zasobu komendy w tym menedżerze kolejek.

Jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek i używane są zarówno zabezpieczenia na poziomie menedżera kolejek, jak i grupy współużytkowania kolejek, program IBM MQ

najpierw sprawdza profil z przedrostkiem w postaci nazwy menedżera kolejek. Jeśli go nie znajdzie, szuka profilu poprzedzonego nazwą grupy współużytkowania kolejek.

Na przykład nazwa profilu RACF na potrzeby sprawdzania bezpieczeństwa zasobów komend 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, część "type" nazwy profilu jest wymagana w profilu w celu odróżnienia zasobów różnych typów, które mają taką samą nazwę. Częścią typu nazwy profilu może być CHANNEL, QUEUE, TOPIC, PROCESS lub NAMELIST. Na przykład użytkownik może mieć uprawnienia do definiowania kolejki hlq.QUEUE programu hlq.QUEUE.PAYROLL.ONE, ale nie ma uprawnień do zdefiniowania procesu hlq.PROCESS.PAYROLL.ONE

Jeśli typem zasobu jest kolejka, a profil jest profilem na poziomie grupy współużytkowania kolejek, steruje on dostępem do co najmniej jednej kolejki lokalnej w grupie współużytkowania kolejek lub dostępem do pojedynczej kolejki współużytkowanej z dowolnego menedżera kolejek w grupie współużytkowania kolejek.

W sekcji Komendy MQSC, profile i ich poziomy dostępu dla każdej komendy IBM MQ MQSC wyświetlane są profile wymagane do przeprowadzenia sprawdzania zabezpieczeń komend oraz odpowiednie poziomy dostępu dla każdego profilu w klasie MQCMDS.

Komendy PCF, profile i ich poziomy dostępu -dla każdej komendy IBM MQ PCF-przedstawiają profile wymagane do przeprowadzenia sprawdzania bezpieczeństwa komendy oraz odpowiedni poziom dostępu dla każdego profilu w klasie MQCMDS.

z/OS *Sprawdzanie bezpieczeństwa zasobów komend dla kolejek aliasowych i kolejek zdalnych*
Zarówno kolejka aliasowa, jak i kolejka zdalna udostępniają kierunek do innej kolejki. Dodatkowe punkty mają zastosowanie, gdy rozważa się sprawdzanie bezpieczeństwa dla tych kolejek.

Kolejki aliasowe

Podczas definiowania kolejki aliasowej sprawdzanie zabezpieczeń zasobów komend jest wykonywane tylko dla nazwy kolejki aliasowej, a nie dla nazwy kolejki docelowej, na którą alias jest tłumaczony.

Kolejki aliasowe mogą być tłumaczone zarówno na kolejki lokalne, jak i zdalne. Aby nie zezwalać użytkownikom na dostęp do określonych kolejek lokalnych lub zdalnych, należy wykonać obie poniższe czynności:

1. Nie zezwalaj użytkownikom na dostęp do tych kolejek lokalnych i zdalnych.
2. Ogranicz użytkownikom możliwość definiowania aliasów dla tych kolejek. Oznacza to, że należy uniemożliwić im wydawanie komend DEFINE QALIAS i ALTER QALIAS.

Kolejki zdalne

Podczas definiowania kolejki zdalnej sprawdzanie bezpieczeństwa zasobów komend jest wykonywane tylko dla nazwy kolejki zdalnej. Nie są wykonywane żadne sprawdzenia nazw kolejek określonych w atrybutach RNAME lub XMITQ w definicji obiektu kolejki zdalnej.

z/OS Profil zabezpieczeń RESLEVEL

Istnieje możliwość zdefiniowania specjalnego profilu w klasie MQADMIN lub MXADMIN w celu kontrolowania liczby identyfikatorów użytkowników sprawdzanych pod kątem zabezpieczeń zasobów API. Ten profil jest nazywany profilem RESLEVEL. Wpływ tego profilu na bezpieczeństwo zasobów interfejsu API zależy od sposobu dostępu do produktu IBM MQ.

Gdy aplikacja próbuje połączyć się z produktem IBM MQ, produkt IBM MQ sprawdza dostęp, jaki ma ID użytkownika powiązany z połączeniem do profilu w klasie MQADMIN lub MXADMIN o nazwie:

```
hlq.RESLEVEL
```

Gdzie `hlq` może mieć wartość `ssid` (ID podsystemu) lub `qsg` (ID grupy współużytkowania kolejek).

Identyfikatory użytkowników powiązane z każdym typem połączenia są następujące:

- Identyfikator użytkownika zadania połączenia dla połączeń wsadowych
- ID użytkownika przestrzeni adresowej CICS dla połączeń CICS
- ID użytkownika przestrzeni adresowej regionu IMS dla połączeń IMS
- ID użytkownika przestrzeni adresowej inicjatora kanału dla połączeń inicjatora kanału

Ostrzeżenie: Opcja RESLEVEL jest bardzo wydajna; może spowodować pominięcie wszystkich sprawdzeń bezpieczeństwa zasobów dla konkretnego połączenia.

Jeśli profil RESLEVEL nie jest zdefiniowany, należy uważać, aby żaden inny profil w klasie MQADMIN nie był zgodny z profilem hlq.RESLEVEL. Na przykład, jeśli w programie MQADMIN istnieje profil o nazwie hlq. * * i nie ma profilu hlq.RESLEVEL , należy uważać na konsekwencje działania hlq. * * ponieważ jest on używany do sprawdzania RESLEVEL.

Zdefiniuj profil hlq.RESLEVEL i ustaw wartość dostawcy UACC na NONE, zamiast w ogóle nie mieć profilu RESLEVEL. Na liście dostępu znajduje się jak najmniej użytkowników lub grup. Szczegółowe informacje na temat kontroli dostępu RESLEVEL zawiera sekcja “Uwagi dotyczące kontroli w systemie z/OS” na stronie 274.

Jeśli używane są tylko zabezpieczenia na poziomie menedżera kolejek, program IBM MQ wykonuje sprawdzanie RESLEVEL dla profilu `qmgr-name.RESLEVEL` . Jeśli używane są tylko zabezpieczenia na poziomie grupy współużytkowania kolejek, program IBM MQ wykonuje sprawdzenia RESLEVEL dla profilu `qsg-name.RESLEVEL` . Jeśli używana jest kombinacja zarówno menedżera kolejek, jak i zabezpieczeń na poziomie grupy współużytkowania kolejek, program IBM MQ najpierw sprawdza, czy istnieje profil RESLEVEL na poziomie menedżera kolejek. Jeśli nie znajdzie profilu, sprawdza profil RESLEVEL na poziomie grupy współużytkowania kolejki.

Jeśli nie może znaleźć profilu RESLEVEL, IBM MQ włącza sprawdzanie zarówno zadania, jak i zadania (lub alternatywnego użytkownika) dla połączenia CICS lub IMS . W przypadku połączenia wsadowego IBM MQ włącza sprawdzanie ID użytkownika zadania (lub alternatywnego). W przypadku inicjatora kanału produkt IBM MQ umożliwia sprawdzanie identyfikatora użytkownika kanału i identyfikatora użytkownika MCA (lub alternatywnego).

Jeśli istnieje profil RESLEVEL, poziom sprawdzania zależy od środowiska i poziomu dostępu dla profilu.

Należy pamiętać, że jeśli menedżer kolejek jest elementem grupy współużytkowania kolejek, a użytkownik nie zdefiniuje tego profilu na poziomie menedżera kolejek, na poziomie grupy współużytkowania kolejek może istnieć taka definicja, która będzie miała wpływ na poziom sprawdzania. Aby aktywować sprawdzanie dwóch identyfikatorów użytkowników, należy zdefiniować profil RESLEVEL (poprzedzony nazwą menedżera kolejek grupy współużytkowania kolejki) z wartością UACC (NONE) i upewnić się, że odpowiedni użytkownicy nie mają dostępu do tego profilu.

Podczas rozważania dostępu, jaki ID użytkownika inicjatora kanału ma do RESLEVEL, należy pamiętać, że połączenie nawiązane przez inicjator kanału jest również połączeniem używanym przez kanały. Ustawienie, które powoduje pominięcie wszystkich sprawdzeń bezpieczeństwa zasobów dla ID użytkownika inicjatora kanału, skutecznie pomija sprawdzenia bezpieczeństwa dla wszystkich kanałów. Jeśli ID użytkownika inicjatora kanału ma dostęp do RESLEVEL inny niż NONE, wówczas tylko jeden ID użytkownika (dla poziomu dostępu READ lub UPDATE) lub żaden ID użytkownika (dla poziomu dostępu CONTROL lub ALTER) nie jest sprawdzany pod kątem dostępu. Jeśli dla identyfikatora użytkownika inicjatora kanału zostanie nadany poziom dostępu inny niż NONE do RESLEVEL, należy zrozumieć wpływ tego ustawienia na sprawdzanie bezpieczeństwa wykonywane dla kanałów.

Użycie profilu RESLEVEL oznacza, że nie są pobierane normalne rekordy kontroli bezpieczeństwa. Na przykład, jeśli użytkownik ma uprawnienia UAUDIT, dostęp do profilu hlq.RESLEVEL w programie MQADMIN nie jest kontrolowany.

Jeśli w profilu hlq.RESLEVEL zostanie użyta opcja RACF WARNING, dla profili w klasie RESLEVEL nie będą generowane żadne komunikaty ostrzegawcze RACF .

Sprawdzanie zabezpieczeń dla komunikatów raportów, takich jak COD, jest sterowane przez profil RESLEVEL powiązany z aplikacją inicjującą. Na przykład, jeśli identyfikator użytkownika zadania wsadowego ma uprawnienie CONTROL lub ALTER do profilu RESLEVEL, to wszystkie operacje sprawdzania zasobów wykonywane przez zadanie wsadowe są pomijane, w tym sprawdzanie bezpieczeństwa komunikatów raportu.

W przypadku zmiany profilu RESLEVEL użytkownicy muszą rozłączyć się i ponownie nawiązać połączenie przed dokonaniem zmiany. (Obejmuje to zatrzymanie i zrestartowanie inicjatora kanału w przypadku zmiany dostępu ID użytkownika rozproszonej przestrzeni adresowej kolejkowania do profilu RESLEVEL).

Aby wyłączyć kontrolę RESLEVEL, należy użyć parametru systemowego RESAUDIT.

z/OS *RESLEVEL i połączenia wsadowe*

Domyślnie, gdy dostęp do zasobu IBM MQ jest uzyskiwany za pośrednictwem połączeń wsadowych i wsadowych, użytkownik musi mieć uprawnienia dostępu do tego zasobu dla konkretnej operacji. Sprawdzanie zabezpieczeń można pominąć, konfigurując odpowiednią definicję RESLEVEL.

To, czy użytkownik jest sprawdzany, czy nie, jest oparte na ID użytkownika używanym podczas nawiązywania połączenia, tym samym ID użytkownika używanym podczas sprawdzania połączenia.

Na przykład można skonfigurować RESLEVEL w taki sposób, aby gdy użytkownik, któremu ufasz, uzyskuje dostęp do pewnych zasobów za pośrednictwem połączenia wsadowego, nie były wykonywane żadne sprawdzenia zabezpieczeń zasobów interfejsu API, ale gdy użytkownik, któremu nie ufasz, próbuje uzyskać dostęp do tych samych zasobów, kontrole bezpieczeństwa są przeprowadzane normalnie. Sprawdzanie RESLEVEL należy skonfigurować w taki sposób, aby pomijało sprawdzanie zabezpieczeń zasobów API tylko wtedy, gdy użytkownik i programy uruchamiane przez niego są wystarczająco zaufane.

W poniższej tabeli przedstawiono sprawdzenia połączeń wsadowych.

Tabela 52. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla połączeń wsadowych

RACF poziom dostępu	**Poziom kontroli**
Brak	Wykonane sprawdzenia zasobów
ODCZYT	Wykonane sprawdzenia zasobów
TEMPERATURY	Wykonane sprawdzenia zasobów
CONTROL	Bez sprawdzania.
Zmień	Bez sprawdzania.

z/OS *RESLEVEL i funkcje systemowe*

Zastosowanie RESLEVEL do paneli operacyjnych i sterujących oraz do CSQUTIL.

Panele operacji i sterowania oraz program narzędziowy CSQUTIL są aplikacjami wsadowymi, które wysyłają żądania do serwera komend menedżera kolejek i dlatego podlegają uwagach opisanych w sekcji “RESLEVEL i połączenia wsadowe” na stronie 248. Komenda RESLEVEL umożliwia pominięcie sprawdzania zabezpieczeń w systemie SYSTEM.COMMAND.INPUT i SYSTEM.COMMAND.REPLY.MODEL , których używają, ale nie dla kolejek dynamicznych SYSTEM.CSQXCMD. *, SYSTEM.CSQOREXX.*, i SYSTEM.CSQUTIL. *.

Serwer komend jest integralną częścią menedżera kolejek i dlatego nie jest z nim powiązane sprawdzanie połączenia lub RESLEVEL. Aby zachować bezpieczeństwo, serwer komend musi potwierdzić, że ID użytkownika aplikacji żądającej ma uprawnienia do otwierania kolejki używanej na potrzeby odpowiedzi. W przypadku operacji i paneli sterujących 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 218, oprócz autoryzacji RESLEVEL, która im została nadana.

W przypadku innych aplikacji korzystających z serwera komend jest to kolejka, którą nazywają jako kolejkę zwrotną. Takie inne aplikacje mogą wprowadzić serwer komend w błąd podczas umieszczania komunikatów w nieautoryzowanych kolejkach, przekazując (w kontekście komunikatu) bardziej zaufany ID użytkownika niż własny do serwera komend. Aby temu zapobiec, należy użyć profilu CONTEXT w celu zabezpieczenia kontekstu tożsamości komunikatów umieszczonych w systemie SYSTEM.COMMAND.INPUT.

z/OS *Połączenia RESLEVEL i CICS*

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API w połączeniu z systemem CICS sprawdzane są dwa identyfikatory użytkowników. Można zmienić identyfikatory użytkowników, które są sprawdzane, konfigurując profil RESLEVEL.

Pierwszym sprawdzany ID użytkownika jest identyfikator przestrzeni adresowej CICS . Jest to identyfikator użytkownika na karcie pracy zadania CICS lub identyfikator użytkownika przypisany do uruchomionego zadania CICS przez klasę z/OS STARTED lub tabelę uruchomionych procedur. (Nie jest to DFLTUSER w systemie CICS).

Drugim sprawdzanym ID użytkownika jest ID użytkownika powiązany z transakcją CICS .

Jeśli jeden z tych identyfikatorów użytkownika nie ma dostępu do zasobu, żądanie kończy się niepowodzeniem z kodem zakończenia MQRC_NOT_AUTHORIZED. Zarówno identyfikator użytkownika przestrzeni adresowej CICS , jak i identyfikator użytkownika, który uruchomiła transakcję CICS , muszą mieć dostęp do zasobu na odpowiednim poziomie.

W jaki sposób RESLEVEL może wpłynąć na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL można zmienić identyfikatory użytkowników, które są sprawdzane podczas żądania dostępu do zasobu. Więcej informacji można znaleźć w sekcji Tabela 53 na stronie 249.

Sprawdzane identyfikatory użytkowników zależą od identyfikatora użytkownika używanego w czasie połączenia, czyli identyfikatora użytkownika przestrzeni adresowej CICS . Ten element sterujący umożliwia pominięcie sprawdzania zabezpieczeń zasobów API dla żądań IBM MQ pochodzących z jednego systemu (na przykład systemu testowego, TESTCICS), ale implementowanie ich dla innego systemu (na przykład systemu produkcyjnego, PRODCICS).

Uwaga: Jeśli identyfikator użytkownika przestrzeni adresowej CICS zostanie skonfigurowany z atrybutem "trusted" w klasie STARTED lub RACF tabeli uruchomionych procedur ICHRIN03, spowoduje to nadpisanie wszystkich sprawdzeń identyfikatora użytkownika dla przestrzeni adresowej CICS ustanowionych przez profil RESLEVEL dla menedżera kolejek (to znaczy, że menedżer kolejek nie wykonuje sprawdzania zabezpieczeń dla przestrzeni adresowej CICS). Więcej informacji na ten temat zawiera sekcja Zabezpieczanie serwera CICS.

W poniższej tabeli przedstawiono sprawdzenia dotyczące połączeń CICS .

Tabela 53. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla połączeń CICS

RACF poziom dostępu	**Poziom kontroli**
Brak	IBM MQ sprawdza ID użytkownika przestrzeni adresowej CICS oraz ID użytkownika transakcji.
ODCZYT	IBM MQ sprawdza tylko ID użytkownika przestrzeni adresowej CICS .
TEMPERATURY	Jeśli transakcja jest zdefiniowana w CICS z opcją RESSEC (YES), IBM MQ sprawdza ID użytkownika przestrzeni adresowej CICS oraz ID użytkownika transakcji.

Tabela 53. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla połączeń CICS (kontynuacja)	
RACF poziom dostępu	**Poziom kontroli**
TEMPERATURY	Jeśli transakcja jest zdefiniowana w CICS z RESSEC (NO), IBM MQ sprawdza tylko ID użytkownika przestrzeni adresowej CICS .
CONTROL lub ALTER	IBM MQ nie sprawdza żadnych identyfikatorów użytkowników.

z/OS *Połączenia RESLEVEL i IMS*

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API dla połączenia IMS sprawdzane są dwa identyfikatory użytkowników. Można zmienić identyfikatory użytkowników, które są sprawdzane, konfigurując profil RESLEVEL.

Domyślnie podczas sprawdzania zabezpieczeń zasobów interfejsu API dla połączenia IMS sprawdzane są dwa identyfikatory użytkowników w celu sprawdzenia, czy dostęp do zasobu jest dozwolony.

Pierwszym sprawdzany ID użytkownika jest identyfikator przestrzeni adresowej regionu IMS . Jest on pobierany 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 ID użytkownika jest powiązany z pracą wykonywaną w regionie zależnym. Jest on określany na podstawie typu regionu zależnego, jak to pokazano w sekcji Sposób określania drugiego ID użytkownika dla połączenia IMS(tm).

Jeśli pierwszy lub drugi identyfikator użytkownika IMS nie ma dostępu do zasobu, żądanie kończy się niepowodzeniem z kodem zakończenia MQRC_NOT_AUTHORIZED.

Ustawienie profili IBM MQ RESLEVEL nie może zmienić identyfikatora użytkownika, pod którym są zaplanowane transakcje IMS z dostarczanego przez IBM MQ-IMS programu monitora wyzwalacza CSQQTRMN. Ten ID użytkownika jest PSBNAME tego monitora wyzwalacza, który domyślnie jest CSQQTRMN.

W jaki sposób RESLEVEL może wpłynąć na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL można zmienić identyfikatory użytkowników, które są sprawdzane podczas żądania dostępu do zasobu. Możliwe są następujące kontrole:

- Sprawdź identyfikator użytkownika przestrzeni adresowej regionu IMS oraz drugi lub alternatywny identyfikator użytkownika.
- Sprawdź tylko ID użytkownika przestrzeni adresowej regionu IMS .
- Nie sprawdzaj żadnych identyfikatorów użytkowników.

W poniższej tabeli przedstawiono sprawdzenia dotyczące połączeń IMS .

Tabela 54. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla połączeń IMS	
RACF poziom dostępu	**Poziom kontroli**
Brak	Sprawdź identyfikator użytkownika przestrzeni adresowej IMS oraz drugi lub alternatywny identyfikator użytkownika systemu IMS .
ODCZYT	Sprawdź ID użytkownika przestrzeni adresowej IMS .
TEMPERATURY	Sprawdź ID użytkownika przestrzeni adresowej IMS .
CONTROL	Bez sprawdzania.
Zmień	Bez sprawdzania.

z/OS *RESLEVEL i połączenie inicjatora kanału*

Domyślnie, gdy inicjator kanału sprawdza zabezpieczenia zasobów interfejsu API, sprawdzane są dwa identyfikatory użytkowników. Można zmienić identyfikatory użytkowników, które są sprawdzane, konfigurując profil RESLEVEL.

Domyślnie, gdy inicjator kanału dokonuje sprawdzenia bezpieczeństwa zasobów API, sprawdzane są dwa identyfikatory użytkowników w celu sprawdzenia, czy dostęp do zasobu jest dozwolony.

Sprawdzone identyfikatory użytkowników mogą być określone przez atrybut kanału MCAUSER, odebrane z sieci, z przestrzeni adresowej inicjatora kanału lub alternatywny identyfikator użytkownika dla deskryptora komunikatu. To, które identyfikatory użytkowników są sprawdzane, zależy od używanego protokołu komunikacyjnego i ustawienia atrybutu kanału PUTAUT. Więcej informacji zawiera sekcja “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 256.

Jeśli jeden z tych identyfikatorów użytkownika nie ma dostępu do zasobu, żądanie kończy się niepowodzeniem z kodem zakończenia MQRC_NOT_AUTHORIZED.

W jaki sposób RESLEVEL może wpłynąć na wykonane kontrole

W zależności od sposobu skonfigurowania profilu RESLEVEL można zmienić identyfikatory użytkowników, które są sprawdzane podczas żądania dostępu do zasobu, oraz liczbę sprawdzanych użytkowników.

W poniższej tabeli przedstawiono sprawdzenia dokonane dla połączenia inicjatora kanału oraz dla wszystkich kanałów, ponieważ używają one tego połączenia.

Tabela 55. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla połączeń inicjatora kanału

RACF poziom dostępu	**Poziom kontroli**
Brak	Sprawdź dwa identyfikatory użytkowników.
ODCZYT	Sprawdź jeden identyfikator użytkownika.
TEMPERATURY	Sprawdź jeden identyfikator użytkownika.
CONTROL	Bez sprawdzania.
Zmień	Bez sprawdzania.
Uwaga: Sekcja “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 256 zawiera definicję sprawdzanych identyfikatorów użytkowników.	

z/OS *Kolejkowanie RESLEVEL i kolejkowanie wewnątrz grupy*

Domyślnie, gdy agent kolejkowania wewnątrz grupy sprawdza zabezpieczenia zasobów API, sprawdzane są dwa identyfikatory użytkowników w celu sprawdzenia, czy dostęp do zasobu jest dozwolony. Można zmienić identyfikatory użytkowników, które są sprawdzane, konfigurując profil RESLEVEL.

Sprawdzane identyfikatory użytkowników mogą być identyfikatorem użytkownika określonym przez atrybut IGQUSER odbierającego menedżera kolejek, identyfikatorem użytkownika menedżera kolejek w grupie współużytkowania kolejek, który umieścił 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 261.

Ponieważ wewnątrzgrupowy agent kolejkowania jest wewnętrznym zadaniem menedżera kolejek, nie wydaje jawnego żądania połączenia i jest uruchamiany przy użyciu identyfikatora użytkownika menedżera kolejek. Agent kolejkowania wewnątrz grupy jest uruchamiany podczas inicjowania menedżera kolejek.

Podczas inicjowania agenta kolejkowania wewnątrz grupy produkt 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, IBM MQ włącza sprawdzanie dwóch identyfikatorów użytkowników. Jeśli istnieje profil RESLEVEL, poziom sprawdzania zależy od poziomu dostępu nadanego identyfikatorowi użytkownika menedżera kolejek dla profilu. Kontrole wykonywane na różnych poziomach dostępu RACF(r) dla agenta kolejkowania wewnątrz grupy przedstawiają sprawdzenia wykonywane dla agenta kolejkowania wewnątrz grupy.

Tabela 56. Sprawdzenia wykonywane na różnych poziomach dostępu RACF dla agenta kolejkowania wewnątrz grupy

RACF poziom dostępu	**Poziom kontroli**
Brak	Sprawdź dwa identyfikatory użytkowników.
ODCZYT	Sprawdź jeden identyfikator użytkownika.
TEMPERATURY	Sprawdź jeden identyfikator użytkownika.
CONTROL	Bez sprawdzania.
Zmień	Bez sprawdzania.
Uwaga: Sekcja “Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania” na stronie 261 zawiera definicję sprawdzanych identyfikatorów użytkowników.	

Jeśli uprawnienia nadane profilowi RESLEVEL dla identyfikatora użytkownika menedżera kolejek zostaną zmienione, agent kolejkowania wewnątrz grupy musi zostać zatrzymany i zrestartowany w celu pobrania nowych uprawnień. Ponieważ nie ma możliwości niezależnego zatrzymania i zrestartowania wewnątrzgrupowego agenta kolejkowania, aby to osiągnąć, menedżer kolejek musi zostać zatrzymany i zrestartowany.

z/OS *RESLEVEL i sprawdzone ID użytkowników*

Przykład ustawiania profilu RESLEVEL i nadawania do niego dostępu.

Sprawdzanie identyfikatora użytkownika w odniesieniu do nazwy profilu dla połączeń wsadowych za pośrednictwem opcji Identyfikatory użytkownika w odniesieniu do nazwy profilu dla jednostki logicznej 6.2 i kanałów połączenia serwera TCP/IP pokazują, w jaki sposób opcja RESLEVEL wpływa na to, które identyfikatory użytkowników są sprawdzane dla różnych żądań MQI.

Na przykład istnieje menedżer kolejek o nazwie QM66 z następującymi wymaganiami:

- Użytkownik WS21B ma zostać zwolniony z ochrony zasobów.
- CICS uruchomione zadanie WXNCICS działające pod identyfikatorem użytkownika przestrzeni adresowej CICSWXN ma wykonywać pełne sprawdzanie zasobów tylko dla transakcji zdefiniowanych za pomocą RESSEC (YES).

Aby zdefiniować odpowiedni profil RESLEVEL, należy wprowadzić następującą komendę systemu RACF :

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Następnie nadaj użytkownikom dostęp do tego profilu za pomocą 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 ID użytkowników są połączone z menedżerem kolejek QM66, użytkownicy muszą się rozłączyć i ponownie nawiązać połączenie przed wprowadzeniem zmian.

Jeśli ochrona podsystemu nie jest aktywna, gdy użytkownik łączy się, ale gdy ten użytkownik jest nadal połączony, ochrona podsystemu staje się aktywna, do użytkownika stosowane jest pełne sprawdzanie bezpieczeństwa zasobów. Użytkownik musi ponownie nawiązać połączenie, aby uzyskać poprawne przetwarzanie RESLEVEL.

z/OS Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS

Program IBM MQ inicjuje sprawdzanie 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 kontroli bezpieczeństwa.

z/OS *Identyfikatory użytkowników na potrzeby ochrony połączenia*

Identyfikator użytkownika używany do ochrony połączenia zależy od typu połączenia.

Typ połączenia	Treść identyfikatora użytkownika
Połączenie wsadowe	Identyfikator użytkownika zadania połączenia. Na przykład: • Identyfikator użytkownika TSO • Identyfikator użytkownika przypisany do zadania wsadowego przez parametr 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 IMS .
Połączenie inicjatora kanału	ID użytkownika przestrzeni adresowej inicjatora kanału.

z/OS *Identyfikatory użytkowników dla ochrony zasobów komend i komend*

Identyfikator użytkownika używany do ochrony komend lub zasobów komend zależy od miejsca wydania komendy.

Wystawione od ...	Treść identyfikatora użytkownika
CSQINP1, CSQINP2lub CSQINPT	Nie jest wykonywane żadne sprawdzenie.
Kolejka wejściowa komend systemowych	Identyfikator użytkownika znajdujący się w pliku *UserIdentifier* deskryptora komunikatu zawierającego komendę. Jeśli komunikat nie zawiera znaku *UserIdentifier*, do menedżera zabezpieczeń przekazywany jest identyfikator użytkownika o wartości pustej.
Konsola	Identyfikator użytkownika wpisany do konsoli. Jeśli konsola nie jest zalogowana, jest to domyślny ID użytkownika ustawiony przez parametr systemowy CMDUSER w CSQ6SYSP. Aby wydawać komendy z konsoli, konsola musi mieć atrybut z/OS SYS AUTHORITY.
Konsola SDSF/TSO	Identyfikator użytkownika TSO lub zadania.

Wystawione od ...	Treść identyfikatora użytkownika
Obsługa i panele sterowania	Identyfikator użytkownika TSO. Jeśli mają być używane operacje i panele sterowania, użytkownik musi mieć odpowiednie uprawnienia do wydawania komend odpowiadających wybranym działaniom. Ponadto użytkownik musi mieć dostęp do odczytu do wszystkich plików hlq.DISPLAY. Profile *obiektów* w klasie MQCMDS, ponieważ panele używają różnych komend DISPLAY do zbierania informacji, które zawierają.
MGM	Jeśli komenda MGCRE jest używana z opcją UTOKEN, jest to identyfikator użytkownika w znaczniku UTOKEN. Jeśli komenda MGCRE jest wydawana bez znacznika UTOKEN, używany jest identyfikator TSO lub ID użytkownika zadania.
CSQ0UTIL	ID użytkownika zadania.
CSQUTIL	ID użytkownika zadania.
KSQINPX	Identyfikator 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 ID użytkownika jest używany dla wywołań **MQOPEN**, **MQSUB**lub **MQPUT1** .

Uwaga: Wszystkie pola ID użytkownika są sprawdzane dokładnie w takiej postaci, w jakiej zostały odebrane. Nie są wykonywane żadne konwersje, a na przykład trzy pola ID użytkownika zawierające "Bob", "BOB"i "bob" nie są równoważne.

z/OS *Identyfikatory użytkowników sprawdzone pod kątem połączeń wsadowych*

Identyfikator użytkownika sprawdzany dla połączenia wsadowego zależy od sposobu uruchomienia zadania oraz od tego, czy określono alternatywny identyfikator użytkownika.

Tabela 57. Sprawdzanie identyfikatora użytkownika względem nazwy profilu dla połączeń wsadowych

Alternatywny ID użytkownika podany 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 TSO lub z/OS UNIX System Services sign-on.
- Identyfikator użytkownika przypisany do zadania wsadowego.
- Identyfikator użytkownika przypisany do uruchomionego zadania przez klasę STARTED lub tabelę uruchomionych procedur.
- Identyfikator użytkownika powiązany z wykonywaną procedurą składowaną Db2

Zadanie wsadowe wykonuje operację MQPUT1 na kolejce o nazwie Q1 z opcją RESLEVEL ustawioną na wartość READ i wyłączonym sprawdzaniem alternatywnego identyfikatora użytkownika.

Sprawdzanie na różnych poziomach dostępu RACF(r) dla połączeń wsadowych i Sprawdzanie ID użytkownika w odniesieniu do nazwy profilu dla połączeń wsadowych wskazuje, że ID użytkownika zadania jest sprawdzany dla profilu hlq.Q1.

z/OS *Identyfikatory użytkowników sprawdzone pod kątem połączeń CICS*

Identyfikatory użytkowników sprawdzane dla połączeń CICS zależą od tego, czy ma zostać przeprowadzone jedno, czy dwa sprawdzenia oraz od tego, czy określono alternatywny identyfikator użytkownika.

Tabela 58. Sprawdzanie identyfikatora użytkownika względem nazwy profilu dla identyfikatorów użytkowników typu CICS

Alternatywny ID użytkownika podany przy otwarciu?	**hlq.ALTERNATE.USER.userid**	**Profil hlq.CONTEXT.queuename**	**Profil hlq.resourcename**
Nie, 1 sprawdzenie	-	Usługi dodatkowe	Usługi dodatkowe
Nie, 2 sprawdzenia	-	ADS + TXN	ADS + TXN
Tak, 1 sprawdzenie	Usługi dodatkowe	Usługi dodatkowe	Usługi dodatkowe
Tak, 2 sprawdzenia	ADS + TXN	ADS + TXN	ADS + ALT

Klucz:

ALT
Alternatywne ID użytkownika

Usługi dodatkowe
Identyfikator użytkownika powiązany z zadaniem wsadowym CICS lub, jeśli CICS działa jako uruchomione zadanie, za pośrednictwem klasy STARTED lub tabeli uruchomionych procedur.

TXN
Identyfikator użytkownika powiązany z transakcją CICS . Zwykle jest to identyfikator użytkownika terminalu, który uruchomił transakcję. Może to być użytkownik CICS DFLTUSER, punkt końcowy zabezpieczeń PRESET lub użytkownik wpisany ręcznie.

Określ identyfikatory użytkowników, dla których są sprawdzane następujące warunki:

- Poziom dostępu RACF do profilu RESLEVEL dla ID użytkownika przestrzeni adresowej CICS jest ustawiony na NONE.
- Wywołanie MQOPEN jest wykonywane względem kolejki z MQOO_OUTPUT i MQOO_PASS_IDENTITY_CONTEXT.

Najpierw należy sprawdzić, ile identyfikatorów użytkowników CICS jest sprawdzanych w oparciu o dostęp identyfikatora użytkownika przestrzeni adresowej CICS do profilu RESLEVEL. Jeśli dla profilu RESLEVEL ustawiono wartość NONE, w sekcji Tabela 53 na stronie 249 w temacie "Połączenia RESLEVEL i CICS" na stronie 249sprawdzane są dwa identyfikatory użytkowników. Następnie, począwszy od Tabela 58 na stronie 255 , przeprowadzane są następujące sprawdzenia:

- Wartość parametru hlq.ALTERNATE bazy danych hlq.ALTERNATE.USER.userid nie jest sprawdzany.
- Profil hlq.CONTEXT.queuename jest sprawdzany zarówno przy użyciu identyfikatora użytkownika przestrzeni adresowej CICS , jak i identyfikatora użytkownika transakcji CICS .
- Profil hlq.resourcename jest sprawdzany zarówno przy użyciu identyfikatora użytkownika przestrzeni adresowej CICS , jak i identyfikatora użytkownika transakcji CICS .

Oznacza to, że dla tego wywołania MQOPEN wykonywane są cztery sprawdzenia zabezpieczeń.

z/OS *Identyfikatory użytkowników sprawdzone pod kątem połączeń IMS*

Identyfikatory użytkowników sprawdzane dla połączeń IMS zależą od tego, czy ma zostać wykonane jedno, czy dwa sprawdzenia oraz od tego, czy określono alternatywny identyfikator użytkownika. Jeśli sprawdzany jest drugi ID użytkownika, zależy on od typu regionu zależnego i od tego, które ID użytkownika są dostępne.

Tabela 59. Sprawdzanie identyfikatora użytkownika względem nazwy profilu dla identyfikatorów użytkowników typu IMS

Alternatywny ID użytkownika podany przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
Nie, 1 sprawdzenie	-	REG	REG
Nie, 2 sprawdzenia	-	REG + S	REG + S
Tak, 1 sprawdzenie	REG	REG	REG
Tak, 2 sprawdzenia	REG + S	REG + S	REG + ALT

Klucz:

ALT
Alternatywny ID użytkownika.

REG
Identyfikator użytkownika jest zwykle ustawiany za pomocą klasy STARTED lub tabeli uruchomionych procedur albo, jeśli jest uruchomiony (IMS), za pomocą wprowadzonego zadania, za pomocą parametru USER JCL.

sek.
Drugi ID użytkownika jest powiązany z pracą wykonywaną w regionie zależnym. Jest on określany na podstawie wartości Tabela 60 na stronie 256.

Tabela 60. Sposób określania drugiego ID użytkownika dla połączenia IMS

Typy regionów zależnych	Hierarchia określania drugiego ID użytkownika
• Wydano komendę GET UNIQUE sterowaną komunikatami BMP. • IFP i GET UNIQUE wydane. • MPP.	Identyfikator użytkownika powiązany z transakcją IMS , jeśli użytkownik jest zalogowany. Nazwa LTERM, jeśli jest dostępna. PSBNAME.
• Nie wydano komendy GET UNIQUE sterowanej komunikatami BMP i zakończonego powodzeniem. • BMP nie jest sterowany komunikatami. • IFP i GET UNIQUE nie zostały wydane.	ID użytkownika powiązany z przestrzenią adresową regionu zależnego IMS , jeśli nie jest to same spacje lub same zera. PSBNAME.

z/OS *Identyfikatory użytkowników używane przez inicjatora kanału*

Ta kolekcja tematów zawiera opis identyfikatorów użytkowników używanych i sprawdzanych dla kanałów odbiorczych i żądań MQI klienta wysyłanych za pośrednictwem kanałów połączenia z serwerem.
Informacje dotyczące protokołu TCP/IP i LU6.2

Aby określić typ używanego sprawdzania zabezpieczeń, można użyć parametru PUTAUT definicji kanału odbierającego. Aby uzyskać spójne sprawdzanie bezpieczeństwa w sieci IBM MQ , można użyć opcji ONLYMCA i ALTMCA.

Aby określić identyfikator użytkownika używany przez agent MCA, można użyć komendy DISPLAY CHSTATUS.

z/OS *Odbieranie kanałów przy użyciu protokołu TCP/IP*

Sprawdzane identyfikatory użytkowników zależą od opcji PUTAUT kanału oraz od tego, czy ma zostać wykonane jedno, czy dwa sprawdzenia.

Tabela 61. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kanałów TCP/IP

W kanale odbiorczym lub kanale requestera określono opcję PUTAUT	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 sprawdzenie	-	CHL	CHL
DEF, 2 sprawdzenia	-	CHL + MCA	CHL + MCA
CTX, 1 sprawdzenie	CHL	CHL	CHL
CTX, 2 sprawdzenia	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 check	-	MCA	MCA
ONLYMCA, 2 sprawdzenia	-	MCA	MCA
ALTMCA, 1 sprawdzenie	MCA	MCA	MCA
ALTMCA, 2 sprawdzenia	MCA	MCA	MCA + ALT

Klucz:

MCA (identyfikator użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER w odbiorniku; jeśli pole jest puste, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału po stronie odbiornika lub requestera.

CHL (ID użytkownika kanału)
W protokole TCP/IP bezpieczeństwo nie jest obsługiwane przez system komunikacyjny dla kanału. Jeśli używany jest protokół TLS (Transport Layer Security) i certyfikat cyfrowy został wydany przez partnera, używany jest identyfikator użytkownika powiązany z tym certyfikatem (jeśli jest zainstalowany) lub identyfikator użytkownika powiązany ze zgodnym filtrem znalezionym za pomocą filtru CNF (RACF Certificate Name Filtering). Jeśli nie zostanie znaleziony powiązany ID użytkownika lub jeśli protokół TLS nie jest używany, ID użytkownika przestrzeni adresowej inicjatora kanału odbiorcy lub zakończenia requestera jest używany jako ID użytkownika kanału w kanałach zdefiniowanych za pomocą parametru PUTAUT ustawionego na DEF lub CTX.

Uwaga: Użycie funkcji filtrowania nazw certyfikatów (Certificate Name Filtering-CNF) systemu RACF umożliwia przypisanie tego samego identyfikatora użytkownika RACF do wielu zdalnych użytkowników, na przykład wszystkich użytkowników w tej samej jednostce organizacyjnej, którzy oczywiście mają takie same uprawnienia. Oznacza to, że serwer nie musi mieć kopii certyfikatu każdego możliwego zdalnego użytkownika na całym świecie i znacznie upraszcza zarządzanie certyfikatami i ich dystrybucję.

Jeśli parametr PUTAUT jest ustawiony na wartość ONLYMCA lub ALTMCA dla kanału, identyfikator użytkownika kanału jest ignorowany i używany jest identyfikator użytkownika MCA odbiorcy lub requestera. Dotyczy to również kanałów TCP/IP korzystających z protokołu TLS.

ALT (alternatywny ID użytkownika)
Identyfikator użytkownika z informacji o kontekście (pole *UserIdentifier*) w deskryptorze komunikatu. Ten ID użytkownika jest przenoszony do pola *AlternateUserID* w deskryptorze obiektu przed wywołaniem wywołania **MQOPEN** lub **MQPUT1** dla kolejki docelowej.

z/OS *Odbieranie kanałów przy użyciu jednostki logicznej 6.2*
Sprawdzane identyfikatory użytkowników zależą od opcji PUTAUT kanału oraz od tego, czy ma zostać wykonane jedno, czy dwa sprawdzenia.

Tabela 62. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kanałów LU 6.2

W kanale odbiorczym lub kanale requestera określono opcję PUTAUT	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 sprawdzenie	-	CHL	CHL
DEF, 2 sprawdzenia	-	CHL + MCA	CHL + MCA
CTX, 1 sprawdzenie	CHL	CHL	CHL
CTX, 2 sprawdzenia	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 check	-	MCA	MCA
ONLYMCA, 2 sprawdzenia	-	MCA	MCA
ALTMCA, 1 sprawdzenie	MCA	MCA	MCA
ALTMCA, 2 sprawdzenia	MCA	MCA	MCA + ALT

Klucz:

MCA (identyfikator użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER w odbiorniku; jeśli pole jest puste, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału po stronie odbiornika lub requestera.

CHL (ID użytkownika kanału)

Kanał requestera - kanał serwera
Jeśli kanał jest uruchamiany z requestera, nie ma możliwości odebrania ID użytkownika sieci (ID użytkownika kanału).

Jeśli parametr PUTAUT jest ustawiony na DEF lub CTX w kanale requestera, ID użytkownika kanału jest identyfikatorem przestrzeni adresowej inicjatora kanału requestera, ponieważ z sieci nie został odebrany żaden ID użytkownika.

Jeśli parametr PUTAUT ma wartość ONLYMCA lub ALTMCA, identyfikator użytkownika kanału jest ignorowany i używany jest identyfikator użytkownika MCA requestera.

Inne typy kanałów
Jeśli parametr PUTAUT jest ustawiony na DEF lub CTX w kanale odbiorczym lub requestera, ID użytkownika kanału jest ID użytkownika odebranym z systemu komunikacyjnego podczas inicjowania kanału.

- Jeśli kanał nadawczy znajduje się w systemie z/OS, odebrany identyfikator użytkownika kanału jest identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału nadawcy.
- Jeśli kanał nadawczy znajduje się na innej platformie (na przykład AIX), odebrany identyfikator użytkownika kanału jest zwykle udostępniany przez parametr USERID w definicji kanału.

Jeśli odebrany ID użytkownika jest pusty lub nie został odebrany ID użytkownika, używany jest ID użytkownika kanału o wartości pustej.

ALT (alternatywny ID użytkownika)
Identyfikator użytkownika z informacji o kontekście (pole *UserIdentifier*) w deskryptorze komunikatu. Ten ID użytkownika jest przenoszony do pola *AlternateUserID* w deskryptorze obiektu przed wywołaniem wywołania MQOPEN lub MQPUT1 dla 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 względem różnych profili, w zależności od użytej opcji PUTAUT i od tego, czy określono alternatywny ID użytkownika.

W tej sekcji opisano identyfikatory użytkowników sprawdzane pod kątem żądań MQI klienta wysyłanych przez kanały połączenia serwera dla TCP/IP i LU 6.2. Identyfikator użytkownika MCA i identyfikator użytkownika kanału są takie same 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 108.

W przypadku żądań klienta **MQOPEN**, **MQSUB**i **MQPUT1** należy użyć następujących reguł, aby określić sprawdzany profil:

- Jeśli żądanie określa uprawnienie alternatywnego użytkownika, wykonywane jest sprawdzenie z wartością *hlq*.ALTERNATE.USER. Profil *userid* .
- Jeśli żądanie określa uprawnienie kontekstowe, wykonywane jest sprawdzenie z wartością *hlq*.KONTEKST. Profil *queuename* .
- Dla wszystkich żądań **MQOPEN**, **MQSUB**i **MQPUT1** wykonywane jest sprawdzenie profilu *hlq.resourcename* .

Po określeniu, które profile są sprawdzane, należy skorzystać z poniższej tabeli, aby określić, które identyfikatory użytkowników są sprawdzane w odniesieniu do tych profili.

Tabela 63. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kanałów połączeń serwera LU 6.2 i TCP/IP

W kanale połączenia z serwerem podano opcję PUTAUT	Alternatywny ID użytkownika podany przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 sprawdzenie	Nie	-	CHL	CHL
DEF, 1 sprawdzenie	Tak	CHL	CHL	CHL
DEF, 2 sprawdzenia	Nie	-	CHL + MCA	CHL + MCA
DEF, 2 sprawdzenia	Tak	CHL + MCA	CHL + MCA	CHL + ALT

Tabela 63. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kanałów połączeń serwera LU 6.2 i TCP/IP (kontynuacja)

W kanale połączenia z serwerem podano opcję PUTAUT	Alternatywny ID użytkownika podany przy otwarciu?	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
ONLYMCA, 1 check	Nie	-	MCA	MCA
ONLYMCA, 1 check	Tak	MCA	MCA	MCA
ONLYMCA, 2 sprawdzenia	Nie	-	MCA	MCA
ONLYMCA, 2 sprawdzenia	Tak	MCA	MCA	MCA + ALT

Klucz:

MCA (identyfikator użytkownika MCA)
Identyfikator użytkownika określony dla atrybutu kanału MCAUSER w serwerze-connection; jeśli pole jest puste, używany jest identyfikator użytkownika przestrzeni adresowej inicjatora kanału.

CHL (ID użytkownika kanału)
W protokole TCP/IP bezpieczeństwo nie jest obsługiwane przez system komunikacyjny dla kanału. Jeśli używany jest protokół TLS (Transport Layer Security) i certyfikat cyfrowy został wydany przez partnera, używany jest identyfikator użytkownika powiązany z tym certyfikatem (jeśli jest zainstalowany) lub identyfikator użytkownika powiązany ze zgodnym filtrem znalezionym za pomocą filtru CNF (RACF Certificate Name Filtering). Jeśli nie znaleziono powiązanego ID użytkownika lub jeśli nie jest używany protokół TLS, ID użytkownika przestrzeni adresowej inicjatora kanału jest używany jako ID użytkownika kanału w kanałach zdefiniowanych za pomocą parametru PUTAUT ustawionego na DEF lub CTX.

Uwaga: Użycie funkcji filtrowania nazw certyfikatów (Certificate Name Filtering-CNF) systemu RACF umożliwia przypisanie tego samego identyfikatora użytkownika RACF do wielu zdalnych użytkowników, na przykład wszystkich użytkowników w tej samej jednostce organizacyjnej, którzy oczywiście mają takie same uprawnienia. Oznacza to, że serwer nie musi mieć kopii certyfikatu każdego możliwego zdalnego użytkownika na całym świecie i znacznie upraszcza zarządzanie certyfikatami i ich dystrybucję.

Jeśli parametr PUTAUT jest ustawiony na wartość ONLYMCA lub ALTMCA dla kanału, identyfikator użytkownika kanału jest ignorowany i 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 o kontekście (pole *UserIdentifier*) w deskryptorze komunikatu. Ten ID użytkownika jest przenoszony do pola *AlternateUserID* w deskryptorze obiektu lub subskrypcji przed wywołaniem **MQOPEN**, **MQSUB** lub **MQPUT1** w imieniu aplikacji klienckiej.

z/OS *Przykład inicjatora kanału*
Przykład sprawdzania identyfikatorów użytkowników w profilach RACF .

Użytkownik wykonuje operację **MQPUT1** względem kolejki w menedżerze kolejek QM01 , która jest tłumaczona na kolejkę o nazwie QB w menedżerze kolejek QM02. Komunikat jest wysyłany przez kanał TCP/IP o nazwie QM01.TO.QM02. RESLEVEL ma wartość NONE, a operacja otwierania jest wykonywana z alternatywnym ID użytkownika i sprawdzaniem kontekstu. Definicja kanału odbiorczego ma ustawioną wartość PUTAUT (CTX) i identyfikator użytkownika MCA. Które identyfikatory użytkowników są używane w kanale odbiorczym do umieszczenia komunikatu w kolejce QB?

Odpowiedź: Tabela 55 na stronie 251 pokazuje, że sprawdzane są dwa identyfikatory użytkowników, ponieważ RESLEVEL ma wartość NONE.

Tabela 61 na stronie 257 pokazuje, że w przypadku ustawienia parametru PUTAUT na wartość CTX i 2 sprawdzane są następujące identyfikatory użytkowników:

- Identyfikator użytkownika inicjatora kanału i identyfikator użytkownika MCAUSER są porównywane z identyfikatorem hlq.ALTERNATE produktu hlq.ALTERNATE.USER.userid .
- ID użytkownika inicjatora kanału i ID użytkownika MCAUSER są porównywane z profilem hlq.CONTEXT.queuename .
- ID użytkownika inicjatora kanału i alternatywny ID użytkownika określone w deskryptorze komunikatu (MQMD) są sprawdzane względem profilu hlq.Q2 .

z/OS *Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania*

Identyfikatory użytkowników, które są sprawdzane, gdy agent kolejkowania wewnątrz grupy otwiera kolejki docelowe, są określane przez wartości atrybutów **IGQAUT** i **IGQUSER** menedżera kolejek.

Możliwe są następujące identyfikatory użytkowników:

ID użytkownika kolejkowania wewnątrz grupy (IGQ)
Identyfikator użytkownika określony przez atrybut **IGQUSER** odbierającego menedżera kolejek. Jeśli ta właściwość jest ustawiona na wartość pustą, używany jest identyfikator użytkownika odbierającego menedżera kolejek. Jednak ze względu na to, że odbierający menedżer kolejek ma uprawnienia dostępu do wszystkich zdefiniowanych kolejek, nie są wykonywane sprawdzenia zabezpieczeń dla identyfikatora użytkownika odbierającego menedżera kolejek. W tym przypadku:

- Jeśli ma zostać sprawdzony tylko jeden identyfikator użytkownika, a identyfikator użytkownika jest identyfikatorem odbierającego menedżera kolejek, nie są wykonywane żadne sprawdzenia zabezpieczeń. Taka sytuacja może wystąpić, gdy parametr **IGQAUT** ma wartość `ONLYIGQ` lub `ALTIGQ`.
- Jeśli mają zostać sprawdzone dwa identyfikatory użytkowników, a jeden z nich jest identyfikatorem odbierającego menedżera kolejek, wykonywane są sprawdzenia zabezpieczeń tylko dla drugiego identyfikatora użytkownika. Taka sytuacja może wystąpić, gdy parametr **IGQAUT** ma wartość `DEF`, `CTX`lub `ALTIGQ`.
- Jeśli mają zostać sprawdzone dwa identyfikatory użytkowników, a oba identyfikatory są identyfikatorami odbierającego menedżera kolejek, nie są wykonywane żadne sprawdzenia zabezpieczeń. Taka sytuacja może wystąpić, gdy parametr **IGQAUT** ma wartość `ONLYIGQ`.

ID użytkownika wysyłającego menedżera kolejek (SND)
Identyfikator użytkownika menedżera kolejek w grupie współużytkowania kolejek, który umieścił komunikat w systemie SYSTEM.QSG.TRANSMIT.QUEUE.

Alternatywny ID użytkownika (ALT)
Identyfikator użytkownika podany w polu *UserIdentifier* w deskryptorze komunikatu.

Tabela 64. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kolejkowania wewnątrz grupy

Określono opcję IGQAUT podczas odbierania menedżera kolejek	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 1 sprawdzenie	-	SND	SND

Tabela 64. Identyfikatory użytkowników sprawdzane względem nazwy profilu dla kolejkowania wewnątrz grupy (kontynuacja)

Określono opcję IGQAUT podczas odbierania menedżera kolejek	hlq.ALTERNATE.USER.userid	Profil hlq.CONTEXT.queuename	Profil hlq.resourcename
DEF, 2 sprawdzenia	-	SND + IGQ	SND + IGQ
CTX, 1 sprawdzenie	SND	SND	SND
CTX, 2 sprawdzenia	SND + IGQ	SND + IGQ	SND + ALT
ONLYIGQ, 1 sprawdzenie	-	IGQ	IGQ
WYŁĄCZNIEIGQ, 2 sprawdzenia	-	IGQ	IGQ
ALTIGQ, 1 sprawdzenie	-	IGQ	IGQ
ALTIGQ, 2 sprawdzenia	IGQ	IGQ	IGQ + AlAT

Klucz:

ALT
Alternatywny ID użytkownika.

IGQ
ID użytkownika IGQ.

SND
ID użytkownika wysyłającego menedżera kolejek.

z/OS *Puste identyfikatory użytkowników i poziomy UACC*

Jeśli identyfikator użytkownika będzie pusty, zostanie wpisany RACF niezdefiniowany użytkownik. Nie należy nadawać szerokiego dostępu niezdefiniowanemu użytkownikowi.

Puste identyfikatory użytkowników mogą istnieć, gdy użytkownik manipuluje komunikatami przy użyciu zabezpieczeń kontekstu lub alternatywnego użytkownika lub gdy do parametru IBM MQ przekazywany jest pusty identyfikator użytkownika. Na przykład pusty ID użytkownika jest używany, gdy komunikat jest zapisywany do kolejki wejściowej komendy systemowej bez kontekstu.

Uwaga: ID użytkownika " * " (oznacza to, że znak gwiazdki, po którym następuje siedem spacji) jest traktowany jako niezdefiniowany ID użytkownika.

IBM MQ przekazuje pusty identyfikator użytkownika do RACF i RACF niezdefiniowany użytkownik jest zalogowany. Wszystkie kontrole bezpieczeństwa używają uniwersalnego dostępu (UACC) dla odpowiedniego profilu. W zależności od tego, w jaki sposób zostały ustawione poziomy dostępu, uprawnienie UACC może nadać niezdefiniowanyemu użytkownikowi szeroki zakres dostępu.

Na przykład, jeśli ta komenda RACF zostanie wydana z TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

Użytkownik definiuje profil, który włącza zarówno identyfikatory użytkowników zdefiniowane przez z/OS(które nie zostały umieszczone na liście dostępu), jak i niezdefiniowany identyfikator użytkownika RACF , aby umieścić komunikaty w tej kolejce i pobrać z niej komunikaty.

Aby chronić się przed pustymi identyfikatorami użytkowników, należy dokładnie zaplanować poziomy dostępu i ograniczyć liczbę osób, które mogą korzystać z zabezpieczeń kontekstowych i alternatywnych.

Należy uniemożliwić osobom, które używają niezdefiniowanego identyfikatora użytkownika RACF , uzyskiwanie dostępu do zasobów, do których nie mają dostępu. Jednocześnie należy jednak zezwolić na dostęp do osób ze zdefiniowanymi identyfikatorami użytkowników. W tym celu w komendzie RACF PERMIT można podać identyfikator użytkownika w postaci gwiazdki (*), co umożliwia dostęp do zasobów dla wszystkich zdefiniowanych identyfikatorów użytkowników. Dlatego wszystkie niezdefiniowane identyfikatory użytkowników (takie jak " * ") odmowa dostępu. Na przykład następujące komendy RACF uniemożliwiają niezdefiniowalnemu identyfikatorowi użytkownika RACF uzyskanie 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 bezpieczeństwem w systemie 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 wydajnie zarządzać tą tabelą i zmniejszyć liczbę żądań wysyłanych z produktu IBM MQ do zewnętrznego menedżera zabezpieczeń (ESM), dostępnych jest wiele elementów sterujących.

Te elementy sterujące są dostępne zarówno za pośrednictwem operacji, paneli sterowania, jak i komend IBM MQ .

z/OS *Ponowna weryfikacja identyfikatora użytkownika*

Jeśli definicja RACF użytkownika korzystającego z zasobów IBM MQ została zmieniona, na przykład przez połączenie użytkownika z nową grupą, można poinformować menedżer kolejek, aby wpisał się ponownie przy następnej próbie uzyskania dostępu do zasobu IBM MQ . Można to zrobić za pomocą komendy IBM MQ RVERIFY SECURITY.

- Użytkownik HX0804 otrzymuje i umieszcza komunikaty w kolejkach PAYROLL w menedżerze kolejek PRD1. Jednak zadanie HX0804 wymaga teraz dostępu do niektórych kolejek PENSION w tym samym menedżerze kolejek (PRD1).
- Administrator bezpieczeństwa danych łączy użytkownika HX0804 z grupą RACF , która umożliwia dostęp do kolejek PENSION.
- Aby użytkownik HX0804 mógł natychmiast uzyskać dostęp do kolejek PENSION (czyli bez zamykania menedżera kolejek PRD1 lub oczekiwania na limit czasu HX0804), należy użyć komendy IBM MQ :

```
RVERIFY SECURITY(HX0804)
```

Uwaga: Jeśli limit czasu ID użytkownika zostanie wyłączony na długi czas (dni lub nawet tygodnie) podczas działania menedżera kolejek, należy pamiętać o uruchomieniu komendy RVERIFY SECURITY dla wszystkich użytkowników, którzy zostali odwołani lub usunięci w tym czasie.

z/OS *Limity czasu ID użytkownika*

Program IBM MQ może wypisywać użytkownika z menedżera kolejek po okresie nieaktywności.

Gdy użytkownik uzyskuje dostęp do zasobu IBM MQ , menedżer kolejek próbuje zalogować tego użytkownika do menedżera kolejek (jeśli zabezpieczenia podsystemu są aktywne). Oznacza to, że użytkownik jest uwierzytelniony w menedżerze ESM. Ten użytkownik pozostaje zalogowany w programie IBM MQ do czasu zamknięcia menedżera kolejek lub do czasu *przekroczenia limitu czasu* (uwierzytelnienie wygasa) albo ponownego zweryfikowania (ponowne uwierzytelnienie).

Gdy użytkownik przekroczył limit czasu, jego identyfikator jest *wypisany* w menedżerze kolejek, a wszelkie informacje związane z bezpieczeństwem przechowywane dla tego użytkownika są odrzucane. Wpisywanie się i wylogowywanie użytkownika w menedżerze kolejek nie jest widoczne dla aplikacji ani dla użytkownika.

Użytkownicy są uprawnieni do przekroczenia limitu czasu, jeśli nie używali żadnych zasobów IBM MQ przez wcześniej określony czas. Ten okres jest ustawiany przez komendę MQSC ALTER SECURITY.

W komendzie ALTER SECURITY można podać dwie wartości:

TIMEOUT
Przedział czasu (w minutach), przez który nieużywany ID użytkownika i powiązane z nim zasoby mogą pozostawać w menedżerze kolejek produktu IBM MQ .

INTERVAL
Wyrażony w minutach przedział czasu między operacjami sprawdzania identyfikatorów użytkowników i powiązanych z nimi zasobów w celu określenia, czy upłynął limit czasu (*TIMEOUT*).

Na przykład, jeśli wartość *TIMEOUT* wynosi 30, a wartość *INTERVAL* wynosi 10, co 10 minut IBM MQ sprawdza identyfikatory użytkowników i powiązane z nimi zasoby, aby określić, czy nie były używane 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 powiązane z identyfikatorami użytkowników, które nie przekroczyły limitu czasu, te informacje o zasobach zostaną odrzucone. Aby nie ustawiać limitu czasu dla identyfikatorów użytkowników, należy ustawić wartość *INTERVAL* na zero. Jeśli jednak wartość *INTERVAL* wynosi zero, pamięć masowa zajęta 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 w przypadku wielu jednorazowych użytkowników. Jeśli zostaną ustawione małe wartości odstępu czasu i limitu czasu, zasoby, które nie są już potrzebne, zostaną zwolnione.

Uwaga: Jeśli używane są wartości *INTERVAL* lub *TIMEOUT* inne niż wartości domyślne, należy ponownie wprowadzić komendę przy każdym uruchomieniu menedżera kolejek. Można to zrobić 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 buforowane informacje. Zabezpieczenia są odświeżane rzadko, ze względu na wydajność. Można również wybrać opcję odświeżania tylko informacji o zabezpieczeniach TLS.

Gdy kolejka jest otwierana po raz pierwszy (lub po raz pierwszy od czasu odświeżenia zabezpieczeń) IBM MQ wykonuje sprawdzenie 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 zostanie ponownie otwarta przez tego samego użytkownika, obecność danych w pamięci podręcznej oznacza, że produkt IBM MQ nie musi wydawać sprawdzeń RACF , co zwiększa wydajność. Działanie odświeżania zabezpieczeń polega na odrzuceniu wszystkich buforowanych informacji o zabezpieczeniach i wymuszaniu na produkcie IBM MQ wykonania nowego sprawdzenia względem pliku RACF. Po każdym dodaniu, zmianie lub usunięciu profilu zasobu RACF , który jest przechowywany w klasie MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST lub MXTOPIC, należy poinformować menedżery kolejek, które używają tej klasy, aby odświeżały informacje o zabezpieczeniach, które przechowują. W tym celu należy wydać następujące komendy:

- Komenda RACF SETROPTS RACLIST (nazwa_klasy) REFRESH służy do odświeżania na poziomie serwera RACF .
- Komenda IBM MQ REFRESH SECURITY służy do odświeżania informacji o zabezpieczeniach przechowywanych przez menedżer kolejek. Ta komenda musi zostać wydana przez każdy menedżer kolejek, który uzyskuje dostęp do zmienionych profili. Jeśli istnieje grupa współużytkowania kolejek, można użyć atrybutu zasięgu komendy, aby skierować komendę do wszystkich menedżerów kolejek w grupie.

  Uwaga: Jeśli nowy użytkownik został połączony z istniejącą grupą, należy uruchomić komendę IBM MQ RVERIFY SECURITY(userid). Komenda REFRESH SECURITY (*) nie pozwala na ponowne podpisanie tego użytkownika przez menedżer kolejek przy następnej próbie uzyskania dostępu do zasobu IBM MQ .

Jeśli w dowolnej klasie IBM MQ używane są profile ogólne, w przypadku zmiany, dodania lub usunięcia dowolnego profilu ogólnego należy również wydać normalne komendy odświeżania RACF . Na przykład SETROPTS GENERIC (nazwa klasy) ODŚWIEŻ.

Jeśli jednak profil zasobu RACF zostanie dodany, zmieniony lub usunięty, a zasób, którego dotyczy, nie jest jeszcze dostępny (dlatego żadne informacje nie są buforowane), program IBM MQ użyje nowych informacji RACF bez wydawania komendy REFRESH SECURITY.

Jeśli kontrola RACF jest włączona (na przykład za pomocą komendy RACF RALTER AUDIT (access-attempt (audit_access_level))), nie jest wykonywane buforowanie, a zatem IBM MQ odwołuje się bezpośrednio do obszaru danych RACF dla każdego sprawdzenia. W związku z tym zmiany są pobierane natychmiast, a opcja REFRESH SECURITY nie jest wymagana w celu uzyskania dostępu do zmian. Aby sprawdzić, czy kontrola RACF jest włączona, należy użyć komendy RACF RLIST. Na przykład można wydać komendę

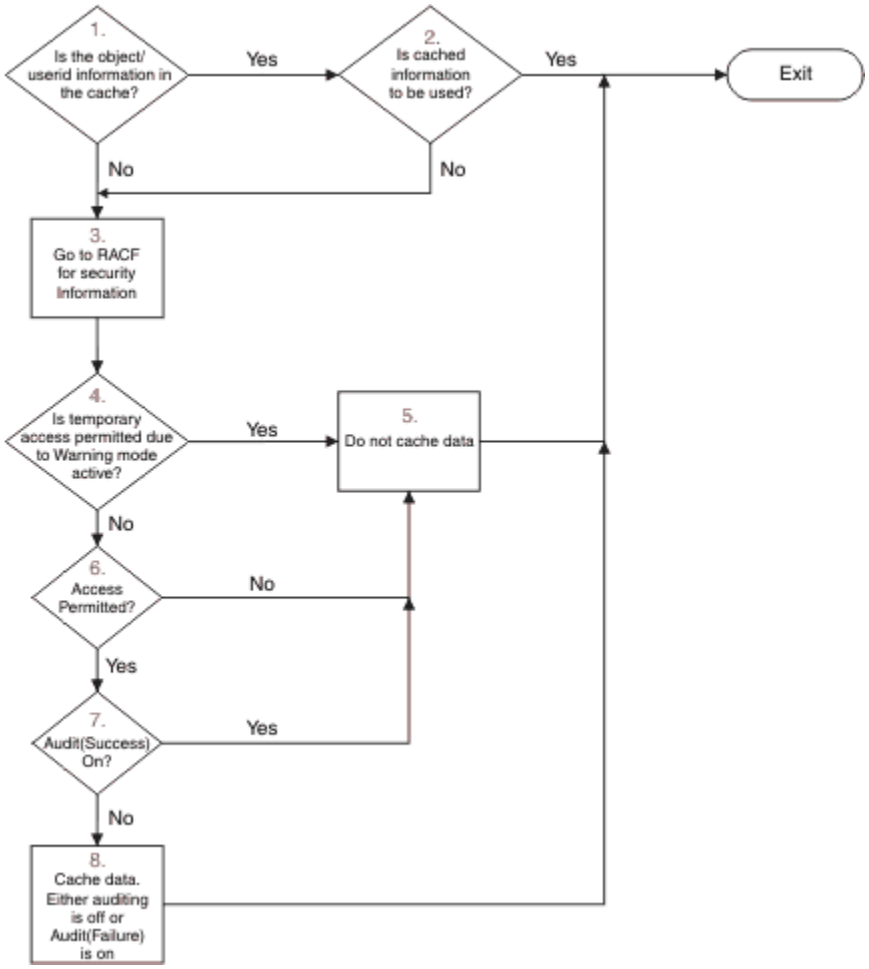
```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

i otrzymywać wyniki

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

Oznacza to, że kontrola jest włączona. Więcej informacji zawiera podręcznik *z/OS Security Server RACF Auditor's Guide* oraz podręcznik *z/OS Security Server RACF Command Language Reference*.

Rysunek 17 na stronie 267 zawiera podsumowanie sytuacji, w których informacje o zabezpieczeniach są buforowane i w których używane są informacje z pamięci podręcznej.



Rysunek 17. Przepływ logiki dla buforowania zabezpieczeń systemu 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 dynamicznie wprowadzić te zmiany:

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. Nie ma potrzeby używania opcji REFRESH SECURITY w przypadku zmiany profilu w klasach MQCONN lub MQCMDS.

Uwaga: Odświeżenie klasy MQADMIN lub MXADMIN nie jest wymagane w przypadku zmiany profilu zabezpieczeń RESLEVEL.

Ze względu na wydajność należy używać opcji REFRESH SECURITY tak rzadko, jak to możliwe, najlepiej poza godzinami szczytu. Można zminimalizować liczbę operacji odświeżania zabezpieczeń, łącząc użytkowników z grupami RACF , które znajdują się już na liście dostępu dla profili IBM MQ , zamiast umieszczania poszczególnych użytkowników na listach dostępu. W ten sposób można zmienić użytkownika, a nie profil zasobu. Zamiast odświeżania zabezpieczeń można również użyć opcji RVERIFY SECURITY dla odpowiedniego użytkownika.

Na przykład REFRESH SECURITY można zdefiniować nowe profile w celu zabezpieczenia dostępu do kolejek począwszy od produktu INSURANCE.LIFE w menedżerze kolejek PRMQ. Należy użyć następujących komend RACF :

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Należy wydać następującą komendę, aby nakazać produktowi RACF odświeżenie przechowywanych w nim informacji o zabezpieczeniach, na przykład:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Ponieważ te profile są ogólne, należy poinformować produkt RACF o konieczności odświeżenia profili ogólnych dla kolejki MQQUEUE. Na przykład:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Następnie należy użyć tej komendy, aby poinformować menedżer kolejek PRMQ, że profile kolejek uległy zmianie:

```
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 bezpieczeństwem, należy wydać komendę MQSC DISPLAY SECURITY.

Poniższy rysunek przedstawia 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 pokazano, że menedżer kolejek, który odpowiedział na komendę, ma podsystem, komendę, alternatywnego użytkownika, proces, listę nazw i zabezpieczenia kolejki aktywne na poziomie menedżera kolejek, ale nie na poziomie grupy współużytkowania kolejek. Połączenia, zasoby komend i zabezpieczenia kontekstu nie są aktywne. Ponadto wyświetlane są informacje o tym, że limity czasu identyfikatorów użytkowników są aktywne i że 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 bezpieczeństwa. Nie musi on odzwierciedlać bieżącego statusu profili przełączników zdefiniowanych w pliku RACFani statusu klas RACF . Na przykład profile przełącznika mogły zostać zmienione od ostatniego restartu tego menedżera kolejek lub komendy REFRESH SECURITY.

z/OS Czynności instalacyjne dotyczące zabezpieczeń dla systemu z/OS

Po zainstalowaniu i dostosowaniu produktu IBM MQnależy autoryzować uruchomione procedury zadań do produktu RACF, autoryzować dostęp do różnych zasobów i skonfigurować definicje RACF . Opcjonalnie skonfiguruj system do obsługi protokołu TLS.

Gdy produkt IBM MQ jest instalowany i dostosowywany po raz pierwszy, należy wykonać następujące czynności związane z bezpieczeństwem:

1. Skonfiguruj zestaw danych IBM MQ i bezpieczeństwo systemu, korzystając z następujących opcji:
   - Autoryzowanie procedury uruchomionego zadania menedżera kolejek xxxxMSTR i procedury uruchomionego zadania rozproszonego kolejkowania xxxxCHIN do uruchomienia w systemie RACF.
   - Autoryzowanie dostępu do zestawów danych menedżera kolejek.
   - Autoryzowanie dostępu do zasobów dla tych identyfikatorów użytkowników, które będą używać menedżera kolejek i programów narzędziowych.
   - Autoryzowanie dostępu dla tych menedżerów kolejek, które będą używać struktur listy narzędzia CF.
   - Autoryzowanie dostępu dla tych menedżerów kolejek, które będą używać produktu Db2.
2. Skonfiguruj definicje RACF dla zabezpieczeń IBM MQ .
3. Aby używać protokołu TLS (Transport Layer Security), należy przygotować system do używania certyfikatów i kluczy.

z/OS *Konfigurowanie zabezpieczeń zestawu danych IBM MQ for z/OS*

Istnieje wiele typów użytkowników IBM MQ . Aby sterować dostępem do zestawów danych systemowych, należy użyć parametru RACF .

Możliwymi użytkownikami zestawów danych IBM MQ są następujące jednostki:

- Sam menedżer kolejek.
- Inicjator kanału
- Administratorzy IBM MQ , którzy muszą tworzyć zestawy danych IBM MQ , uruchamiać programy narzędziowe i podobne zadania.
- Programiści aplikacji, którzy muszą korzystać z dostarczonych przez IBM MQstruktur copybook, dołączają zestawy danych, makra i podobne zasoby.
- Aplikacje obejmujące jeden lub więcej z następujących elementów:
  - Zadania wsadowe
  - Użytkownicy TSO
  - CICS regiony
  - IMS regiony
- Zestawy danych CSQOUTX i CSQSNAP
- Kolejki dynamiczne SYSTEM.CSQXCMD.*

Dla wszystkich tych potencjalnych użytkowników chroń zestawy danych IBM MQ za pomocą RACF.

Należy również kontrolować dostęp do wszystkich zestawów danych 'CSQINP'.

z/OS *Autoryzacja RACF dla procedur uruchomionych zadań*

Niektóre zestawy danych IBM MQ są przeznaczone do wyłącznego użytku przez menedżer kolejek. Jeśli zestawy danych IBM MQ są chronione za pomocą programu RACF, należy również autoryzować procedurę uruchomionego zadania menedżera kolejek xxxxMSTRoraz procedurę uruchomionego zadania

rozproszonego kolejkowania xxxxCHINza pomocą programu RACF. W tym celu należy użyć klasy STARTED. Alternatywnie można użyć tabeli procedur uruchomionych (ICHRIN03), ale aby zmiany odniosły skutek, należy wykonać IPL systemu z/OS .

Więcej informacji na ten temat zawiera podręcznik *z/OS Security Server RACF System Programmer's Guide*.

Zidentyfikowany ID użytkownika RACF musi mieć wymagany dostęp do zestawów danych w procedurze uruchomionego zadania. Na przykład po powiązaniu procedury uruchomionego zadania menedżera kolejek o nazwie CSQ1MSTR z identyfikatorem użytkownika RACF QMGRCSQ1, identyfikator użytkownika QMGRCSQ1 musi mieć dostęp do zasobów z/OS , do których dostęp ma menedżer kolejek CSQ1 .

Ponadto zawartość pola GROUP w identyfikatorze użytkownika menedżera kolejek musi być taka sama, jak zawartość pola GROUP w profilu STARTED dla tego menedżera kolejek. Jeśli treść w każdym polu GROUP nie jest zgodna, wówczas odpowiedni ID użytkownika nie może wejść do systemu. Ta sytuacja powoduje, że program IBM MQ jest uruchamiany z niezdefiniowanym identyfikatorem użytkownika, a następnie jest zamykane z powodu naruszenia zabezpieczeń.

Identyfikatory użytkowników RACF powiązane z procedurami uruchomionego zadania menedżera kolejek i inicjatora kanału nie mogą mieć ustawionego atrybutu TRUSTED.

z/OS *Autoryzowanie dostępu do zestawów danych*

Zestawy danych IBM MQ powinny być chronione, aby żaden nieautoryzowany użytkownik nie mógł uruchomić instancji menedżera kolejek ani uzyskać dostępu do danych menedżera kolejek. W tym celu należy użyć normalnej ochrony zestawu danych z/OS RACF .

Tabela 65 na stronie 270 zawiera podsumowanie praw dostępu RACF , które musi mieć procedura uruchomionego zadania menedżera kolejek do różnych zestawów danych.

Tabela 65. Dostęp RACF do zestawów danych powiązanych z menedżerem kolejek

RACF dostęp	**Zestawy danych**
ODCZYT	• `thqual.SCSQAUTH` i `thqual.SCSQANLx` (gdzie x jest literą języka dla danego języka narodowego). • Zestawy danych, do których odwołują się CSQINP1, CSQINP2 i CSQXLIB w procedurze uruchomionego zadania menedżera kolejek. • Zestawy danych SMDS należące do innych menedżerów kolejek w grupie. • Zestawy danych dziennika, BSDS i dziennika archiwalnego dla innych menedżerów kolejek w grupie.
TEMPERATURY	• Wszystkie zestawy stron oraz zestawy danych dziennika i BSDS. • Zestawy danych SMDS należące do menedżera kolejek • Zestawy danych SMDS należące do innych menedżerów kolejek w grupie, dla struktur, które menedżer kolejek wykonuje za pomocą komendy RECOVER CFSTRUCT.
Zmień	• Wszystkie archiwalne zestawy danych dziennika.

Tabela 66 na stronie 271 zawiera podsumowanie dostępu RACF , jaki musi mieć procedura uruchomionego zadania dla rozproszonego kolejkowania do różnych zestawów danych.

Tabela 66. Dostęp RACF do zestawów danych powiązanych z kolejkowaniem rozproszonym	
RACF dostęp	**Zestawy danych**
ODCZYT	• thlqual.SCSQAUTH, thlqual.SCSQANLx (gdzie x jest literą języka dla danego języka) i thlqual.SCSQMVR1. • Zestawy danych biblioteki LE. • Zestawy danych, do których odwołują się CSQXLIB i CSQINPX w procedurze uruchomionego zadania inicjatora kanału.
TEMPERATURY	• Zestawy danych CSQOUTX i CSQSNAP

Więcej informacji na ten temat zawiera publikacja *z/OS Security Server RACF Security Administrator's Guide*.

z/OS *Szyfrowanie zestawów danych*

Zestawy danych IBM MQ mogą być szyfrowane za pomocą szyfrowania zestawu danych z/OS , dzięki czemu dane są chronione lub ze względów prawnych.

Za pomocą szyfrowania zestawu danych z/OS można chronić wszystkie zestawy stron, aktywny dziennik, dziennik archiwalny i zestawy danych programu startowego (BSDS).

Ostrzeżenie: Nie można chronić współużytkowanych zestawów danych komunikatów (SMDS) za pomocą szyfrowania zestawu danych z/OS za pomocą systemu IBM MQ for z/OS 9.1.4 lub wcześniejszego.

Patrz sekcja poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych . :NONE.

z/OS *Konfigurowanie ochrony zasobów IBM MQ for z/OS*

Istnieje wiele typów użytkowników IBM MQ . Aby kontrolować dostęp do zasobów IBM MQ , należy użyć parametru RACF .

Możliwymi użytkownikami zasobów IBM MQ , takich jak kolejki i kanały, są następujące obiekty:

- Sam menedżer kolejek.
- Inicjator kanału
- Administratorzy IBM MQ , którzy muszą tworzyć zestawy danych IBM MQ , uruchamiać programy narzędziowe i podobne zadania
- Programiści aplikacji, którzy muszą korzystać z dostarczonych przez IBM MQstruktur copybook, dołączają zestawy danych, makra i podobne zasoby.
- Aplikacje obejmujące jeden lub więcej z następujących elementów:
  - 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 IBM MQ za pomocą RACF. W szczególności należy zauważyć, że inicjator kanału musi mieć dostęp do różnych zasobów, zgodnie z opisem w sekcji “Uwagi dotyczące bezpieczeństwa inicjatora kanału w systemie z/OS” na stronie 278, dlatego identyfikator użytkownika, pod którym jest uruchamiany, musi mieć uprawnienia dostępu do tych zasobów.

Jeśli używana jest grupa współużytkowania kolejek, menedżer kolejek może wydawać różne komendy wewnętrznie, więc używany przez niego ID użytkownika musi mieć uprawnienia do wydawania takich komend. Komendy są następujące:

- DEFINE, ALTER i DELETE dla każdego obiektu, który zawiera QSGDISP (GROUP)
- START i STOP CHANNEL dla każdego kanału używanego z CHLDISP (SHARED)

z/OS *Konfigurowanie systemu z/OS do używania protokołu TLS*

Ten temat zawiera przykład konfigurowania produktu IBM MQ for z/OS z protokołem TLS (Transport Layer Security) przy użyciu komend RACF .

Aby używać protokołu TLS na potrzeby ochrony kanału, należy wykonać w systemie kilka zadań. Szczegółowe informacje na temat używania komend RACF dla certyfikatów i repozytoriów kluczy (pliki kluczy) zawiera sekcja Praca z protokołem TLS w produkcie z/OS .

1. Za pomocą komendy RACDCERT systemu RACF należy utworzyć plik kluczy w systemie RACF , w którym będą przechowywane wszystkie klucze i certyfikaty systemu. 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 być to plik kluczy współużytkowanych.

2. Utwórz certyfikat cyfrowy dla każdego menedżera kolejek przy użyciu komendy RACDCERT produktu RACF .

   Etykieta certyfikatu musi być wartością atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiony) lub wartością domyślną `ibmWebSphereMQ` z dodaną 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 znajdujący się w pliku RACF z bazą kluczy, używając komendy RACDCERT systemu RACF . Na przykład:

   ```
   RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
   CONNECT ID(CHINUSER)
   ```

   Należy również połączyć wszystkie odpowiednie certyfikaty osoby podpisującej (z ośrodka certyfikacji) z bazą kluczy. Oznacza to, że wszystkie ośrodki certyfikacji dla certyfikatu TLS tego menedżera kolejek i wszystkie ośrodki certyfikacji dla wszystkich certyfikatów TLS, z którymi komunikuje się ten menedżer kolejek. Na przykład:

   ```
   RACDCERT ID(CHINUSER)
   CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
   ```

4. W każdym z menedżerów kolejek należy użyć komendy IBM MQ ALTER QMGR, aby określić repozytorium kluczy, które ma wskazywać menedżer kolejek. Na przykład, jeśli plik kluczy należy do przestrzeni adresowej inicjatora kanału:

```
ALTER QMGR SSLKEYR(QM1RING)
```

   lub jeśli używany jest plik kluczy współużytkowanych:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

   gdzie *id_użytkownika* jest identyfikatorem użytkownika, który jest właścicielem pliku kluczy współużytkowanych.

5. Listy odwołań certyfikatów (Certificate Revocation List-CRL) umożliwiają odwoływanie certyfikatów przez ośrodki certyfikacji, które nie mogą być już zaufane. 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 za pomocą 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 wymagane.

   Następnie umieść obiekt AUTHINFO na liście nazw za pomocą komendy IBM MQ DEFINE NAMELIST. Na przykład:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

   Na koniec powiąż listę nazw z każdym menedżerem kolejek za pomocą komendy IBM MQ ALTER QMGR. Na przykład:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Skonfiguruj menedżer kolejek do uruchamiania wywołań TLS przy użyciu komendy IBM MQ ALTER QMGR. Definiuje podzadania serwera, które obsługują tylko wywołania SSL, co pozostawia normalne przekaźniki, aby kontynuować przetwarzanie w normalny sposób bez wpływu na żadne wywołania SSL. Wymagane są co najmniej dwie z tych podczynności. Na przykład:

```
ALTER QMGR SSLTASKS(8)
```

   Ta zmiana jest uwzględniana tylko po zrestartowaniu inicjatora kanału.

7. Określ specyfikację szyfru, która ma być używana dla każdego kanału, za pomocą 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 grupie QSG

Rekordy uwierzytelniania kanału mają zastosowanie do menedżera kolejek, w którym zostały utworzone. Nie są one współużytkowane w całej grupie współużytkowania kolejek (QSG). Dlatego jeśli wszystkie menedżery kolejek w grupie współużytkowania kolejek muszą mieć takie same reguły, należy przeprowadzić pewne zarządzanie, aby zachować spójność wszystkich reguł.

1. Zawsze należy dodawać opcję `CMDSCOPE(*)` do wszystkich komend `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 ze wszystkich menedżerów kolejek są takie same. Po znalezieniu niespójności można wydać komendę `SET CHLAUTH` zawierającą tę samą regułę co `CMDSCOPE(*)` lub `CMDSCOPE(`*qmgr-name*`)`.
3. Dodaj element do konkatenacji CSQINP2 menedżera kolejek (szczegółowe informacje zawiera sekcja Komendy inicjowania), która zawiera pełny zestaw reguł. Zostaną one odczytane w ramach procesu inicjowania menedżera kolejek. Jeśli komenda `SET CHLAUTH` używa `ACTION(ADD)` , reguła zostanie dodana tylko wtedy, gdy nie istnieje. Użycie opcji `ACTION(REPLACE)` spowoduje zastąpienie istniejącej reguły, jeśli już istnieje, lub dodanie jej, jeśli nie istnieje. Ten sam element można następnie umieścić w konkatenacji CSQINP2 wszystkich menedżerów kolejek w grupie współużytkowania kolejek.
4. Użyj programu narzędziowego CSQUTIL (szczegółowe informacje na ten temat zawiera sekcja Wysyłanie komend do IBM MQ (COMMAND)), aby wyodrębnić reguły z jednego menedżera kolejek przy użyciu opcji `MAKEDEF` lub `MAKEREP` . Następnie należy odtworzyć dane wyjściowe przy użyciu programu 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 Uwagi dotyczące kontroli w systemie z/OS

Zwykłe elementy sterujące kontroli produktu RACF są dostępne na potrzeby przeprowadzania kontroli zabezpieczeń menedżera kolejek. IBM MQ nie gromadzi własnych statystyk bezpieczeństwa. Jedynymi statystykami są te, które mogą być tworzone przez kontrolę.

Kontrola 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 obniża wydajność; im więcej kontroli jest implementowanych, tym większa wydajność jest obniżona. Jest to również istotne w przypadku użycia opcji RACF WARNING.

z/OS *Kontrola RESLEVEL*

Parametr systemowy RESAUDIT służy do sterowania produkcją rekordów kontroli RESLEVEL. RACF generowane są ogólne rekordy kontroli.

Utwórz rekordy kontroli RESLEVEL, ustawiając parametr systemowy RESAUDIT na wartość YES. Jeśli parametr RESAUDIT ma wartość NO, rekordy kontroli nie są generowane. Więcej informacji na temat ustawiania tego parametru zawiera sekcja Używanie komendy CSQ6SYSP.

Jeśli opcja RESAUDIT ma wartość YES, podczas sprawdzania RESLEVEL nie są wykonywane żadne normalne rekordy kontroli RACF w celu sprawdzenia, jaki dostęp ma ID użytkownika przestrzeni adresowej do profilu hlq.RESLEVEL . Zamiast tego IBM MQ żąda, aby RACF utworzył rekord kontroli OGÓLNE (numer zdarzenia 27). Te sprawdzenia są wykonywane tylko w czasie połączenia, więc koszt wydajności jest minimalny.

Ostrzeżenie: RACFRW nie jest już sugerowanym programem narzędziowym do przetwarzania rekordów kontroli produktu RACF . Należy użyć RACF Narzędzie do wyjmowania danych SMF , ponieważ jest to preferowana metoda raportowania.

Rekordy kontroli ogólnej systemu IBM MQ można raportować przy użyciu programu zapisującego raporty systemu RACF (RACFRW). Do raportowania dostępu RESLEVEL można użyć następujących komend RACFRW:

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

Przykładowy raport z RACFRW, z wyłączeniem pól *Date*, *Time*i *SYSID* , przedstawia Rysunek 19 na stronie 275.

```
       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 komendy RACFRW przedstawiające ogólne rekordy kontroli RESLEVEL

Po sprawdzeniu danych LOGSTR w tych przykładowych danych wyjściowych można zauważyć, że użytkownik TSO WS21B ma dostęp CONTROL do produktu QM66.RESLEVEL. Oznacza to, że wszystkie sprawdzenia bezpieczeństwa zasobów są pomijane, gdy użytkownik WS21B uzyskuje dostęp do zasobów QM66 .

Więcej informacji na temat używania narzędzia RACFRW zawiera sekcja Program zapisujący raporty RACF w publikacji *z/OS Security Server RACF Auditor's Guide*.

z/OS Dostosowywanie zabezpieczeń

Aby zmienić sposób działania zabezpieczeń systemu IBM MQ , należy użyć wyjścia SAF (ICHRFR00) lub wyjść z zewnętrznego menedżera zabezpieczeń.

Więcej informacji na temat wyjść z systemu RACF zawiera dokumentacja *z/OS Security Server RACROUTE Macro Reference* .

Uwaga: Ponieważ produkt IBM MQ optymalizuje wywołania do menedżera ESM, żądania RACROUTE mogą nie być wykonywane na przykład w przypadku każdego otwarcia danej kolejki przez konkretnego użytkownika.

z/OS Komunikaty o naruszeniu zabezpieczeń w systemie z/OS

Naruszenie zabezpieczeń jest wskazywane przez kod powrotu MQRC_NOT_AUTHORIZED w aplikacji lub przez komunikat w dzienniku zadania.

Kod powrotu MQRC_NOT_AUTHORIZED może zostać zwrócony do aplikacji z następujących powodów:

- Użytkownik nie może nawiązać połączenia z menedżerem kolejek. W takim przypadku w dzienniku zadania wsadowego/TSO, CICSlub IMS zostanie wyświetlony komunikat ICH408I .
- Wpisanie się użytkownika do menedżera kolejek nie powiodło się, ponieważ na przykład ID użytkownika zadania jest niepoprawny lub odpowiedni albo ID użytkownika zadania lub alternatywny ID użytkownika jest niepoprawny. Co najmniej jeden z tych identyfikatorów może nie być poprawny, ponieważ zostały odwołane lub usunięte. W takim przypadku w protokole zadania menedżera kolejek pojawi się komunikat ICHxxxx i prawdopodobnie 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 alternatywnego użytkownika, ale identyfikator użytkownika zadania lub czynności nie ma dostępu do alternatywnego identyfikatora użytkownika. W przypadku tego niepowodzenia w protokole zadania odpowiedniego menedżera kolejek zostanie wyświetlony komunikat o naruszeniu.
- Opcja kontekstu została użyta lub jest implikowana przez otwarcie kolejki transmisji dla danych wyjściowych, ale identyfikator użytkownika zadania lub, jeśli ma to zastosowanie, zadanie lub alternatywny identyfikator użytkownika nie ma dostępu do opcji kontekstu. W takim przypadku komunikat o naruszeniu jest umieszczany w protokole zadania odpowiedniego menedżera kolejek.
- Nieautoryzowany użytkownik próbował uzyskać dostęp do zabezpieczonego obiektu menedżera kolejek, na przykład do kolejki. W takim przypadku komunikat ICH408I dotyczący naruszenia jest umieszczany w protokole zadania odpowiedniego menedżera kolejek. Przyczyną tego naruszenia może być zadanie lub, jeśli ma to zastosowanie, zadanie lub alternatywny identyfikator użytkownika.

Komunikaty o naruszeniu bezpieczeństwa komend i bezpieczeństwa zasobów komend można również znaleźć w protokole zadania menedżera kolejek.

Jeśli komunikat o naruszeniu ICH408I zawiera nazwę zadania menedżera kolejek, a nie identyfikator użytkownika, zwykle jest to wynikiem podania pustego alternatywnego identyfikatora użytkownika. Na przykład:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          INSUFFICIENT ACCESS AUTHORITY
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

Aby dowiedzieć się, kto może używać pustych alternatywnych identyfikatorów użytkowników, należy sprawdzić listę dostępu profilu hlq.ALTERNATE.USER.-BLANK-.

Komunikat o naruszeniu ICH408I może również zostać wygenerowany przez:

- Komenda wysyłana do kolejki wejściowej komendy systemowej bez kontekstu. Programy napisane przez użytkownika, które zapisują dane do kolejki wejściowej komend systemowych, powinny zawsze używać opcji kontekstu. Więcej informacji na ten temat zawiera “Profile zabezpieczeń kontekstu” na stronie 230.

- Gdy zadanie uzyskujące dostęp do zasobu IBM MQ nie ma powiązanego z nim identyfikatora użytkownika lub gdy adapter IBM MQ nie może wyodrębnić identyfikatora użytkownika ze środowiska adaptera.

Komunikaty o naruszeniu mogą być również wysyłane, jeśli używana jest zarówno grupa współużytkowania kolejek, jak i zabezpieczenia na poziomie menedżera kolejek. Mogą zostać wyświetlone komunikaty wskazujące, że nie znaleziono żadnego profilu na poziomie menedżera kolejek, ale nadal przyznano do niego dostęp z powodu profilu na poziomie 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   )
```

Więcej informacji na temat komunikatów ICH408I zawiera dokumentacja produktu z/OS for Security Server RACF Messages and Codes .

z/OS Co zrobić, jeśli dostęp jest dozwolony lub niedozwolony niepoprawnie

Oprócz informacji opisanych w dokumentacji z/OS należy skorzystać z tej listy kontrolnej, jeśli dostęp do zasobu wydaje się być nieprawidłowo kontrolowany.

Szczegółowe kroki, które należy wykonać, jeśli dostęp jest dozwolony lub niedozwolony, zawiera publikacja *z/OS Security Server RACF Security Administrator's Guide* .

- 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.
  - Komenda IBM MQ DISPLAY SECURITY umożliwia wyświetlenie bieżącego statusu przełącznika z menedżera kolejek.
  - Sprawdź profile przełącznika w klasie MQADMIN.

    W tym celu należy użyć komend RACF SEARCH i RLIST.
  - Sprawdź ponownie profile przełącznika RACF , wprowadzając komendę IBM MQ REFRESH SECURITY (MQADMIN).
- Czy profil zasobu RACF został zmieniony? Na przykład, czy zmieniono dostęp uniwersalny do profilu, czy zmieniono listę dostępu do profilu?
  - Czy profil jest ogólny?

    Jeśli tak, wydaj komendę RACF , SETROPTS GENERIC (nazwa klasy) ODŚWIEŻ.
  - Czy zabezpieczenia tego menedżera kolejek zostały odświeżone?

    Jeśli jest to wymagane, wydaj komendę RACF SETROPTS RACLIST (nazwa_klasy) ODŚWIEŻ.

    Jeśli jest to wymagane, wydaj komendę IBM MQ REFRESH SECURITY (*).
- Czy definicja RACF użytkownika została zmieniona? Na przykład, czy użytkownik był połączony z nową grupą lub czy odebrano mu uprawnienie dostępu?
  - Czy użytkownik został ponownie zweryfikowany za pomocą komendy IBM MQ RVERIFY SECURITY (userid)?
- Czy kontrole bezpieczeństwa są pomijane z powodu RESLEVEL?
  - Sprawdź dostęp ID użytkownika nawiązującego połączenie do profilu RESLEVEL. Rekordy kontroli RACF umożliwiają określenie wartości ustawionej dla parametru RESLEVEL.

  - W przypadku kanałów należy pamiętać, że poziom dostępu, który ID użytkownika inicjatora kanału ma do RESLEVEL, jest dziedziczony przez wszystkie kanały, więc poziom dostępu, taki jak ALTER, powoduje, że wszystkie sprawdzenia są pomijane, co powoduje, że kontrole bezpieczeństwa są pomijane dla wszystkich kanałów.
  - Jeśli uruchamiasz program CICS, sprawdź ustawienie RESSEC transakcji.
  - Jeśli RESLEVEL został zmieniony, gdy użytkownik jest połączony, musi się rozłączyć i ponownie nawiązać połączenie, zanim nowe ustawienie RESLEVEL zacznie obowiązywać.
- Czy używane są 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, że profil nie został znaleziony.
  - Czy użyto kombinacji ustawień przełącznika, które nie są poprawne, aby włączyć pełne sprawdzanie zabezpieczeń?
  - Czy konieczne jest zdefiniowanie przełączników zabezpieczeń w celu przesłonięcia niektórych ustawień grupy współużytkowania kolejek dla menedżera kolejek?
  - Czy profil na poziomie menedżera kolejek ma pierwszeństwo przed profilem na poziomie grupy współużytkowania kolejki?

z/OS Uwagi dotyczące bezpieczeństwa inicjatora kanału w systemie z/OS

Jeśli zabezpieczenia zasobów są używane w rozproszonym środowisku kolejkowania, przestrzeń adresowa inicjatora kanału wymaga odpowiedniego dostępu do różnych zasobów IBM MQ . Algorytm ochrony hasła można zainicjować za pomocą narzędzia ICSF (Integrated Cryptographic Support Facility).

Więcej informacji na temat ICSF zawiera dokumentacja z/OS Cryptographic Services .

Korzystanie z ochrony zasobów

Jeśli używane są zabezpieczenia zasobów, należy rozważyć następujące kwestie w przypadku korzystania z rozproszonego kolejkowania:

kolejki systemowe
Przestrzeń adresowa inicjatora kanału wymaga dostępu RACF UPDATE do kolejek systemowych wymienionych w “Bezpieczeństwo kolejki systemowej” na stronie 218oraz do wszystkich kolejek docelowych użytkownika i kolejki niedostarczonych komunikatów (patrz sekcja “Bezpieczeństwo kolejki niedostarczonych komunikatów” na stronie 216).

Kolejki transmisji
Przestrzeń adresowa inicjatora kanału wymaga dostępu typu ALTER do wszystkich kolejek transmisji użytkownika.

zabezpieczenie kontekstu
Identyfikator użytkownika kanału (oraz identyfikator użytkownika MCA, jeśli został określony) wymagają dostępu RACF CONTROL do profili hlq.CONTEXT.queuename w klasie MQADMIN.
W zależności od profilu RESLEVEL identyfikator użytkownika kanału może również wymagać dostępu na poziomie CONTROL do tych profili.

Wszystkie kanały wymagają dostępu na poziomie CONTROL do hlq.CONTEXTMQADMIN. profil kolejki niedostarczonych komunikatów. Wszystkie kanały (niezależnie od tego, czy są inicjowane, czy odpowiadają) mogą generować raporty i w związku z tym muszą mieć dostęp na poziomie 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 poprawnego zakończenia działania kanału.

Uwaga: Jeśli ID użytkownika kanału lub grupa RACF , z którą połączony jest ID użytkownika kanału, ma dostęp na poziomie CONTROL lub ALTER do hlq.RESLEVEL, to nie ma sprawdzania zasobów dla inicjatora kanału ani dla żadnego z jego kanałów.

Więcej informacji na ten temat zawierają “Profile zabezpieczeń kontekstu” na stronie 230 “RESLEVEL i połączenie inicjatora kanału” na stronie 251 i “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253 .

KSQINPX
Jeśli używany jest zestaw danych wejściowych CSQINPX, inicjator kanału wymaga również dostępu READ do CSQINPX oraz dostępu UPDATE do zestawu danych CSQOUTX i kolejek dynamicznych SYSTEM.CSQXCMD. *.

Bezpieczeństwo połączenia
Żądania połączenia przestrzeni adresowej inicjatora kanału używają typu połączenia CHIN, dla którego należy ustawić odpowiednie zabezpieczenia dostępu, patrz sekcja “Profile zabezpieczeń połączenia dla inicjatora kanału” na stronie 211.

Zestawy danych
Przestrzeń adresowa inicjatora kanału wymaga odpowiedniego dostępu do zestawów danych menedżera kolejek, patrz sekcja “Autoryzowanie dostępu do zestawów danych” na stronie 270.

Komendy
Rozproszone komendy kolejkowania (na przykład DEFINE CHANNEL, START CHINIT, START LISTENER i inne komendy kanału) muszą mieć odpowiedni zestaw zabezpieczeń komend, patrz sekcja Tabela 49 na stronie 233.

Jeśli używana jest grupa współużytkowania kolejek, inicjator kanału może wydawać różne komendy wewnętrznie, więc używany przez niego ID użytkownika musi mieć uprawnienia do wydawania takich komend. Komendy te to START i STOP CHANNEL dla każdego kanału używanego z CHLDISP (SHARED).

Jeśli parametr PSMODE menedżera kolejek nie ma wartości DISABLED, inicjator kanału musi mieć dostęp do odczytu (READ) do komendy DISPLAY PUBSUB.

Zabezpieczenia kanału
Kanały, w szczególności odbiorniki i połączenia serwera, wymagają odpowiedniej ochrony. Więcej informacji na ten temat zawiera sekcja “Identyfikatory użytkowników do sprawdzania zabezpieczeń w systemie z/OS” na stronie 253 .

Do zapewnienia bezpieczeństwa kanałów można również użyć protokołu TLS (Transport Layer Security). Więcej informacji na temat używania protokołu TLS z produktem IBM MQzawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24 .

Więcej informacji na temat zabezpieczeń połączenia z serwerem zawiera sekcja “Kontrola dostępu dla klientów” na stronie 108 .

Identyfikatory użytkownika
Identyfikatory użytkowników opisane w sekcjach “Identyfikatory użytkowników używane przez inicjatora kanału” na stronie 256 i “Identyfikatory użytkowników używane przez wewnątrzgrupowy agent kolejkowania” na stronie 261 wymagają następujących uprawnień dostępu:

- RACF Dostęp UPDATE do odpowiednich kolejek docelowych i kolejki niedostarczonych komunikatów
- RACF CONTROL dostęp do profilu `hlq.CONTEXT.queuename` , jeśli sprawdzanie kontekstu jest wykonywane w odbiorniku
- Odpowiedni dostęp do pliku hlq.ALTERNATE.USER.userid profile, których mogą potrzebować.
- W przypadku klientów-odpowiedni dostęp RACF do zasobów, które mają być używane.

Ochrona APPC
Ustaw odpowiednie zabezpieczenia APPC, jeśli używany jest protokół transmisji LU 6.2 . (Na przykład można użyć klasy APPCLU RACF). Informacje na temat konfigurowania ochrony APPC znajdują się w następującej dokumentacji:

- *z/OS MVS Planowanie: Zarządzanie APPC*

- *z/OS MVS Programowanie: Pisanie serwerów dla APPC/MVS*

W przypadku transmisji wychodzących używana jest opcja APPC "SECURITY (SAME)" . W wyniku tego ID użytkownika przestrzeni adresowej inicjatora kanału i jego profil domyślny (RACF GROUP) są przesyłane przez sieć do odbiornika z indykatorem, że ID użytkownika został już zweryfikowany (ALREADYV).

Jeśli stroną odbierającą jest także strona z/OS, ID użytkownika i profil są weryfikowane przez APPC, a ID użytkownika jest wyświetlany w kanale odbiorczym i używany jako ID użytkownika kanału.

W środowisku, w którym menedżer kolejek używa komunikacji APPC do komunikacji z innym menedżerem kolejek w tym samym lub innym systemie z/OS , należy upewnić się, że:

- Definicja VTAM dla komunikującej się jednostki logicznej określa SETACPT (ALREADYV)
- Istnieje profil RACF APPCLU dla połączenia między jednostkami logicznymi, który określa parametr CONVSEC (ALREADYV)

zmiana ustawień zabezpieczeń
Jeśli zostanie zmieniony poziom dostępu produktu RACF , który ID użytkownika kanału lub ID użytkownika MCA dla kolejki docelowej ma zostać zmieniony, zmiana ta ma zastosowanie tylko w przypadku nowych uchwytów obiektów (czyli nowych uchwytów `MQOPEN`) dla kolejki docelowej. Czasy, w których otwarte i zamknięte kolejki MCA są zmienne; jeśli kanał jest już uruchomiony po wprowadzeniu takiej zmiany dostępu, agent MCA może kontynuować umieszczanie komunikatów w kolejce docelowej przy użyciu istniejącego dostępu do zabezpieczeń identyfikatorów użytkowników, a nie zaktualizowanego dostępu do zabezpieczeń. Zatrzymanie i zrestartowanie kanałów w celu wymuszenia zaktualizowanego poziomu dostępu pozwala uniknąć tego scenariusza.

automatyczne restartowanie
Jeśli do restartowania inicjatora kanału używany jest program z/OS Automatic Restart Manager (ARM), ID użytkownika powiązany z przestrzenią adresową XCFAS musi mieć uprawnienia do uruchamiania komendy IBM MQ START CHINIT.

Korzystanie z narzędzia ICSF (Integrated Cryptographic Service Facility)

Inicjator kanału może użyć ICSF do wygenerowania losowej liczby podczas inicjowania algorytmu zabezpieczania hasłem w celu zaciemnienia haseł przesyłanych przez kanały klienta, jeśli nie jest używany protokół TLS. Proces generowania liczby losowej nosi nazwę *entropii*.

Jeśli składnik z/OS został zainstalowany, ale narzędzie ICSF nie zostało uruchomione, zostanie wyświetlony komunikat CSQX213E , a inicjator kanału użyje STCK do entropii.

Komunikat CSQX213E ostrzega, że algorytm ochrony hasła nie jest tak bezpieczny, jak to możliwe. Można jednak kontynuować proces; nie ma to żadnego innego wpływu na środowisko wykonawcze.

Jeśli opcja z/OS nie jest zainstalowana, inicjator kanału automatycznie użyje STCK.

Uwagi:

1. Użycie ICSF dla entropii generuje więcej losowych sekwencji niż użycie STCK.
2. Po uruchomieniu ICSF należy zrestartować inicjatora kanału.
3. Plik ICSF jest wymagany dla niektórych CipherSpecs. Jeśli zostanie podjęta próba użycia jednej z tych CipherSpecs , a narzędzie ICSF nie jest zainstalowane, zostanie wyświetlony komunikat CSQX629E.

z/OS Zabezpieczenia w klastrach menedżera kolejek w systemie z/OS

Uwagi dotyczące zabezpieczeń klastrów są takie same dla menedżerów kolejek i kanałów, które nie są klastrowe. Inicjator kanału potrzebuje dostępu do dodatkowych kolejek systemowych, a niektóre dodatkowe komendy wymagają odpowiedniego zestawu bezpieczeństwa.

Do uwierzytelniania kanałów klastra (tak jak w przypadku kanałów konwencjonalnych) można użyć identyfikatora użytkownika MCA, rekordów uwierzytelniania kanału, protokołu TLS i wyjść zabezpieczeń. Rekordy uwierzytelniania kanału lub wyjście zabezpieczeń dotyczące kanału odbiorczego klastra muszą sprawdzać, czy zdalny menedżer kolejek ma dostęp do kolejek klastra menedżera kolejek serwera.

Można rozpocząć korzystanie z obsługi klastra IBM MQ 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 zostać przyłączone do klastra.

Obsługa klastrów IBM MQ nie udostępnia mechanizmu ograniczającego element klastra tylko do roli klienta. W związku z tym należy upewnić się, że wszystkie menedżery kolejek, które są dozwolone w klastrze, są zaufane. Jeśli dowolny menedżer kolejek w klastrze utworzy kolejkę o określonej nazwie, może odbierać komunikaty dla tej kolejki, niezależnie od tego, czy aplikacja umieszczająca komunikaty w tej kolejce zamierzała to zrobić, czy nie.

Aby ograniczyć przynależność do klastra, należy wykonać to samo działanie, co w celu uniemożliwienia menedżerom kolejek nawiązywania połączeń z kanałami odbiorczymi. Przypisanie do klastra można ograniczyć, używając rekordów uwierzytelniania kanału lub pisząc program obsługi wyjścia zabezpieczeń w kanale odbiorczym. Można również napisać program obsługi wyjścia, aby uniemożliwić 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 jest również wskazane zezwolenie aplikacji na bezpośrednie otwarcie jakiejkolwiek innej kolejki transmisji.

Jeśli używane są zabezpieczenia zasobów, oprócz uwag zawartych w sekcji “Uwagi dotyczące bezpieczeństwa inicjatora kanału w systemie z/OS” na stronie 278należy wziąć pod uwagę następujące kwestie:

kolejki systemowe
Inicjator kanału potrzebuje dostępu RACF ALTER do następujących kolejek systemowych:

- SYSTEM SYSTEM.CLUSTER.COMMAND KOMENDY
- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

i dostęp UPDATE do SYSTEM.CLUSTER.REPOSITORY.QUEUE

Wymaga również dostępu READ do wszystkich list nazw używanych do łączenia w klastry.

Komendy
Ustaw odpowiednie zabezpieczenia komend (zgodnie z opisem w sekcji Tabela 49 na stronie 233) dla komend obsługi klastrów (REFRESH i RESET CLUSTER, SUSPEND i RESUME QMGR).

z/OS Zagadnienia dotyczące zabezpieczeń związane z używaniem produktu IBM MQ z produktem CICS

Wszystkie wersje produktu CICS obsługiwane przez produkt IBM MQ 9.0.0i nowsze używają dostarczonej przez firmę CICS wersji adaptera i mostu.

Szczegółowe informacje na temat zabezpieczeń można znaleźć w następujących sekcjach:

- Zabezpieczenia dla adaptera CICS-MQ.
- Zabezpieczenia dla mostu CICS-MQ.

z/OS Zagadnienia dotyczące zabezpieczeń związane z używaniem produktu IBM MQ z produktem IMS

Ten temat zawiera informacje dotyczące planowania wymagań bezpieczeństwa w przypadku używania produktu IBM MQ z produktem IMS.

Korzystanie z klasy OPERCMDS

Jeśli do ochrony zasobów w klasie OPERCMDS używany jest produkt RACF , upewnij się, że identyfikator użytkownika powiązany z przestrzenią adresową menedżera kolejek produktu IBM MQ ma uprawnienie do wydawania komendy MODIFY dla dowolnego systemu IMS , z którym może się połączyć.

Uwagi dotyczące zabezpieczeń mostu IMS

Podczas określania wymagań bezpieczeństwa dla mostu IMS należy wziąć pod uwagę cztery aspekty:

- Jaka autoryzacja zabezpieczeń jest wymagana do połączenia produktu IBM MQ z produktem IMS
- Stopień sprawdzania zabezpieczeń aplikacji korzystających z mostu w celu uzyskania dostępu do produktu IMS
- Które zasoby IMS mogą być używane przez te aplikacje
- Jakie uprawnienia mają być używane dla komunikatów, które są umieszczane i odbierane przez most

Podczas definiowania wymagań bezpieczeństwa dla mostu IMS należy wziąć pod uwagę następujące kwestie:

- Komunikaty przekazywane przez most mogły pochodzić z aplikacji na platformach, które nie oferują silnych zabezpieczeń.
- Komunikaty przekazywane przez most mogły pochodzić z aplikacji, które nie są kontrolowane przez to samo przedsiębiorstwo lub organizację.

z/OS *Uwagi dotyczące zabezpieczeń podczas nawiązywania połączenia z produktem IMS*

Nadaj ID użytkownika przestrzeni adresowej menedżera kolejek IBM MQ dostęp do grupy OTMA.

Most IMS jest klientem OTMA. Połączenie z programem IMS działa przy użyciu identyfikatora użytkownika przestrzeni adresowej menedżera kolejek systemu IBM MQ . Zwykle jest on definiowany jako członek uruchomionej grupy zadań. Ten ID użytkownika musi mieć nadany dostęp do grupy OTMA (chyba że ustawienie /SECURE OTMA ma wartość NONE).

W tym celu należy zdefiniować następujący profil w klasie FACILITY:

```
IMSXCF.xcfgname.mqxcfmname
```

Gdzie `xcfgname` jest nazwą grupy XCF, a `mqxcfmname` jest nazwą elementu XCF IBM MQ.

Należy nadać identyfikatorowi użytkownika menedżera kolejek produktu IBM MQ prawo do odczytu tego profilu.

Uwaga:

1. Jeśli uprawnienia w klasie FACILITY zostaną zmienione, należy użyć komendy RACF SETROPTS RACLIST (FACILITY) REFRESH, aby aktywować zmiany.
2. Jeśli profil hlq.NO.SUBSYS.SECURITY istnieje w klasie MQADMIN, do programu IMS nie jest przekazywany żaden identyfikator użytkownika, a połączenie kończy się niepowodzeniem, chyba że ustawienie /SECURE OTMA ma wartość NONE.

z/OS *Kontrola dostępu aplikacji do 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 stopień sprawdzania zabezpieczeń dla każdego komunikatu przekazywanego do systemu IMS .

```
IMSXCF.xcfgname.imsxcfmname
```

Gdzie `xcfgname` jest nazwą grupy XCF, a `imsxcfmname` jest nazwą elementu XCF w systemie IMS. (Należy zdefiniować osobny profil dla każdego systemu IMS).

Poziom dostępu dozwolony dla identyfikatora użytkownika menedżera kolejek IBM MQ w tym profilu jest zwracany do produktu IBM MQ , gdy most IMS łączy się z serwerem IMS, i wskazuje poziom zabezpieczeń wymagany w kolejnych transakcjach. W przypadku kolejnych transakcji IBM MQ żąda odpowiednich usług od RACF i, jeśli ID użytkownika jest autoryzowany, przekazuje komunikat do IMS.

OTMA nie obsługuje komendy IMS /SIGN; jednak IBM MQ umożliwia ustawienie sprawdzania dostępu dla każdego komunikatu w celu włączenia implementacji wymaganego poziomu kontroli.

Mogą być zwracane następujące informacje o poziomie dostępu:

NIE ZNALEZIONO PROFILU LUB NIE ZNALEZIONO PROFILU
Te wartości wskazują, że wymagane jest maksymalne bezpieczeństwo, tzn. uwierzytelnianie jest wymagane dla każdej transakcji. Wykonywane jest sprawdzenie, czy identyfikator użytkownika określony w polu *UserIdentifier* struktury MQMD oraz hasło lub PassTicket w polu *Authenticator* struktury MQIIH są znane programowi RACFi są poprawną kombinacją. UTOKEN jest tworzony z hasłem lub PassTicketi przekazywany do IMS ; UTOKEN nie jest buforowany.

Uwaga: Jeśli profil hlq.NO.SUBSYS.SECURITY istnieje w klasie MQADMIN, ten poziom zabezpieczeń nadpisuje wszystko, co jest zdefiniowane w profilu.

ODCZYT
Ta wartość wskazuje, że takie samo uwierzytelnianie ma być wykonywane jak w przypadku NONE w następujących okolicznościach:

- Przy pierwszym napotkaniu konkretnego ID użytkownika
- Jeśli identyfikator użytkownika został napotkany wcześniej, ale buforowany znacznik UTOKEN nie został utworzony z hasłem lub PassTicket

IBM MQ żąda UTOKEN, jeśli jest wymagany, i przekazuje go do IMS.

Uwaga: Jeśli żądanie ponownej weryfikacji zabezpieczeń zostało wykonane, wszystkie informacje w pamięci podręcznej zostaną utracone, a żądanie UTOKEN zostanie wysłane przy pierwszym napotkaniu każdego identyfikatora użytkownika.

TEMPERATURY
Wykonywane jest sprawdzenie, czy identyfikator użytkownika w polu *UserIdentifier* struktury MQMD jest znany programowi RACF.

UTOKEN jest budowany i przekazywany do IMS ; UTOKEN jest buforowany.

KONTROLA/ZMIANA
Te wartości wskazują, że nie ma potrzeby określania żadnych identyfikatorów UTOKEN zabezpieczeń dla tego systemu IMS . (Ta opcja jest prawdopodobnie używana tylko w przypadku systemów programistycznych i testowych).

Ostrzeżenie: Należy zauważyć, że identyfikator użytkownika zawarty w polu *UserIdentifier* struktury MQMD jest nadal przekazywany dla **CONTROL/ALTER**.

Uwaga:

1. Ten dostęp jest definiowany, gdy program IBM MQ łączy się z serwerem IMSi trwa przez cały czas trwania połączenia. Aby zmienić poziom zabezpieczeń, należy zmienić dostęp do profilu zabezpieczeń, a następnie zatrzymać i zrestartować most (na przykład zatrzymując i restartując komponent OTMA).
2. Jeśli uprawnienia w klasie FACILITY zostaną zmienione, należy użyć komendy RACF SETROPTS RACLIST (FACILITY) REFRESH, aby aktywować zmiany.
3. Można użyć hasła lub PassTicket, ale należy pamiętać, że most IMS nie szyfruje danych. Informacje na temat korzystania z opcji PassTicketszawiera sekcja “Korzystanie z opcji RACF PassTickets w nagłówku IMS” na stronie 285.
4. Na niektóre z tych wyników mogą mieć wpływ ustawienia zabezpieczeń w programie IMSza pomocą komendy /SECURE OTMA.
5. Buforowane informacje UTOKEN są przechowywane przez czas zdefiniowany przez parametry INTERVAL i TIMEOUT komendy IBM MQ ALTER SECURITY.

6. Opcja RACF WARNING nie ma wpływu na profil IMSXCF.xcfgname.imsxcfmname . Jego użycie nie ma wpływu na nadany poziom dostępu i nie są generowane żadne komunikaty ostrzegawcze systemu RACF .

z/OS *Sprawdzanie zabezpieczeń w systemie IMS*

Komunikaty przekazywane przez most zawierają informacje o zabezpieczeniach. Wykonywane sprawdzenia bezpieczeństwa 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* struktury MQMD.
- Zasięg zabezpieczeń zawarty w polu *SecurityScope* struktury MQIIH (jeśli istnieje struktura MQIIH)
- UTOKEN (chyba że podsystem IBM MQ ma dostęp na poziomie CONTROL lub ALTER do odpowiedniego profilu `IMSXCF.xcfgname.imsxcfmname`),

Wykonywane sprawdzenia bezpieczeństwa zależą od ustawienia komendy IMS /SECURE OTMA, w następujący sposób:

/SECURE OTMA BRAK
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 komendy.

Program ACEE (Accessor Environment Element) jest zbudowany w regionie sterującym IMS .

/SECURE OTMA PEŁNY
Pole *UserIdentifier* struktury MQMD jest przekazywane do IMS w celu sprawdzenia uprawnień transakcji lub komendy.

Platforma ACEE jest zbudowana w zależnym regionie IMS , a także w regionie sterującym IMS .

/BEZPIECZNY PROFIL OTMA
Pole *UserIdentifier* struktury MQMD jest przekazywane do IMS w celu sprawdzenia uprawnień transakcji lub komendy

Pole *SecurityScope* w strukturze MQIIH służy do określania, czy ma zostać zbudowany element ACEE w regionie zależnym IMS oraz w regionie sterującym.

Uwaga:

1. W przypadku zmiany uprawnień w klasie TIMS lub CIMS albo w powiązanych klasach grupy GIMS lub DIMSnależy wprowadzić następujące komendy IMS , aby aktywować zmiany:
   - /MODIFY PREPARE RACF
   - /MODYFIKUJ ZATWIERDZENIE
2. Jeśli nie jest używany profil /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
Używa uprawnień identyfikatora użytkownika w polu *UserIdentifier* struktury MQMD.

Umieszczanie komunikatu odpowiedzi
Używa uprawnień identyfikatora użytkownika w polu *UserIdentifier* struktury MQMD oryginalnego komunikatu.

Umieszczanie komunikatu w kolejce niedostarczonych komunikatów
Nie są wykonywane żadne sprawdzenia zabezpieczeń.

Uwaga:

1. W przypadku zmiany profili klas IBM MQ należy wprowadzić komendę IBM MQ REFRESH SECURITY (*), aby aktywować zmiany.
2. W przypadku zmiany uprawnień użytkownika należy wydać komendę MQSC RVERIFY SECURITY, aby aktywować zmianę.

z/OS *Korzystanie z opcji RACF PassTickets w nagłówku IMS*

Zamiast hasła w nagłówku IMS można użyć hasła PassTicket .

Aby użyć atrybutu PassTicket zamiast hasła w nagłówku IMS (MQIIH), należy określić nazwę aplikacji, dla której sprawdzana jest poprawność PassTicket w atrybucie PASSTKTA definicji STGCLASS kolejki mostu IMS , do której ma być kierowany komunikat.

Jeśli wartość PASSTKTA jest pusta, należy wygenerować PassTicket . W tym przypadku nazwa aplikacji musi mieć postać MVSxxxx, gdzie xxxx jest identyfikatorem SMFID systemu z/OS , w którym działa docelowy menedżer kolejek.

PassTicket jest budowany na podstawie identyfikatora użytkownika, nazwy aplikacji docelowej i klucza tajnego. Jest to wartość 8-bajtowa zawierająca wielkie litery i cyfry. Może być używana tylko raz i jest ważna przez okres 20 minut. Jeśli PassTicket jest generowany przez lokalny system RACF , system RACF sprawdza tylko, czy profil istnieje, a nie czy użytkownik ma uprawnienia do tego profilu. Jeśli PassTicket został wygenerowany w systemie zdalnym, program RACF sprawdza poprawność dostępu identyfikatora użytkownika do profilu. Pełne informacje na temat opcji PassTicketszawiera publikacja *z/OS Security Server RACF Security Administrator's Guide*.

PassTickets w nagłówkach IMS są nadawane RACF przez IBM MQ, a nie IMS.

z/OS Migrowanie menedżera kolejek systemu z/OS do zabezpieczeń z mieszaną wielkością liter

Aby przeprowadzić migrację menedżera kolejek do zabezpieczeń z mieszaną wielkością liter, należy wykonać następujące kroki. Należy przejrzeć poziom używanego produktu zabezpieczeń i aktywować nowe klasy zewnętrznego menedżera zabezpieczeń IBM MQ . Uruchom komendę **REFRESH SECURITY** , aby aktywować profile z mieszanymi przypadkami.

Zanim rozpoczniesz

1. Upewnij się, że wszystkie klasy zewnętrznego menedżera zabezpieczeń IBM MQ są aktywowane.
2. Upewnij się, że menedżer kolejek jest uruchomiony.

O tym zadaniu

Aby przekształcić menedżer kolejek w zabezpieczenia z mieszanymi wielkami liter, należy wykonać następujące kroki.

Procedura

1. Skopiuj wszystkie istniejące profile i poziomy dostępu z klas pisanych wielkimi literami do równoważnej klasy zewnętrznego menedżera zabezpieczeń z mieszanymi literami.
   a) `MQADMIN` na `MXADMIN`.
   b) `MQPROC` na `MXPROC`.
   c) `MQNLIST` na `MXNLIST`.
   d) `MQQUEUE` na `MXQUEUE`.
2. Zmień wartość atrybutu menedżera kolejek `SCYCASE` na `MIXED` , wprowadzając następującą komendę.

```
ALTER QMGR SCYCASE(MIXED)
```

3. Aktywuj profile zabezpieczeń, wydając następującą komendę.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. Sprawdź, czy profile zabezpieczeń działają poprawnie.

Co dalej

Przejrzyj definicje obiektów i w razie potrzeby utwórz nowe profile z mieszanymi przypadkami, korzystając z komendy **REFRESH SECURITY** do aktywowania profili.

Konfigurowanie zabezpieczeń systemu IBM MQ MQI client

Należy wziąć pod uwagę bezpieczeństwo systemu IBM MQ MQI client , aby aplikacje klienckie nie miały nieograniczonego dostępu do zasobów na serwerze.

Podczas uruchamiania aplikacji klienckiej nie należy uruchamiać aplikacji przy użyciu identyfikatora użytkownika, który ma więcej praw dostępu niż jest to konieczne, na przykład użytkownika należącego do grupy `mqm` lub nawet samego użytkownika `mqm` .

Uruchamiając aplikację jako użytkownik ze zbyt wieloma prawami dostępu, można ryzykować, że aplikacja będzie uzyskiwać dostęp do części menedżera kolejek i zmieniać je przez przypadek lub w sposób złośliwy.

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 konkretny użytkownik jest tym, za kogo się mówi. Korzystając z uwierzytelniania, można uniemożliwić atakującemu uzyskanie dostępu do menedżera kolejek przez imitowanie jednej z aplikacji.

  W produkcie IBM MQ 8.0uwierzytelnianie jest zapewniane przez jedną z dwóch opcji:

  – Funkcja uwierzytelniania połączenia.

    Więcej informacji na temat uwierzytelniania połączenia zawiera sekcja “Uwierzytelnianie połączenia” na stronie 74.

  – Uwierzytelnianie wzajemne w protokole TLS.

    Więcej informacji na temat protokołu TLS zawiera sekcja “Praca z protokołem SSL/TLS” na stronie 293.

- Kontrola dostępu może być używana 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 praw dostępu, aby upewnić się, że aplikacja nie ma dostępu do części menedżera kolejek, do których aplikacja nie powinna mieć dostępu.

  Podczas konfigurowania kontroli dostępu należy wziąć pod uwagę reguły uwierzytelniania kanału i pole MCAUSER kanału. Obie te funkcje mają możliwość zmiany identyfikatora użytkownika używanego do weryfikowania praw dostępu.

  Więcej informacji na temat kontroli dostępu zawiera sekcja “Autoryzowanie dostępu do obiektów” na stronie 395.

Jeśli aplikacja kliencka została skonfigurowana do nawiązywania połączenia z konkretnym kanałem z ograniczonym identyfikatorem, ale w polu MCAUSER kanału jest ustawiony identyfikator administratora, to identyfikator administratora jest używany do sprawdzania kontroli dostępu, pod warunkiem, że aplikacja kliencka pomyślnie nawiąże połączenie. Oznacza to, że aplikacja kliencka będzie miała pełne prawa dostępu do menedżera kolejek.

Więcej informacji na temat atrybutu MCAUSER zawiera sekcja “Odwzorowanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER” na stronie 432.

Reguł uwierzytelniania kanału można również użyć jako metody sterowania dostępem do menedżera kolejek, konfigurując konkretne reguły i kryteria dla połączenia, które ma zostać zaakceptowane.

Więcej informacji na temat reguł uwierzytelniania kanału zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.

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.

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Aby repozytoria kluczy były zgodne ze standardem FIPS w czasie wykonywania, muszą być utworzone i zarządzane tylko za pomocą 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 sekcji SSL pliku konfiguracyjnego klienta na wartość YES.

Domyślnie specyfikacje szyfrowania CipherSpecs z certyfikatem FIPS nie są wymagane.

Te wartości mają takie same znaczenie jak równoważne wartości parametrów w systemie **ALTER QMGR SSLFIPS** (patrz sekcja **ALTER QMGR** (zmiana ustawień menedżera kolejek)). 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.

Jeśli skonfigurowano CipherSpecs tylko dla FIPS, klient MQI odrzuci połączenia, które określają specyfikację szyfrowania CipherSpec z wartością `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 AIX, Linux, and Windows” na stronie 36
Jeśli szyfrowanie jest wymagane w kanale SSL/TLS w systemach AIX, Linux, and Windows , IBM MQ używa pakietu kryptograficznego o nazwie IBM Crypto for C (ICC). Na platformach AIX, Linux, and Windows oprogramowanie ICC przeszło program FIPS (Federal Information Processing Standards) Cryptomodule Validation Program) amerykańskiego National Institute of Standards and Technology na poziomie 140-2.

AIX Uruchamianie aplikacji klienckich TLS z wieloma instalacjami produktu GSKit 8.0 w systemie AIX

Aplikacje klienckie TLS w systemie AIX mogą napotkać błąd MQRC_CHANNEL_CONFIG_ERROR i błąd AMQ6175 w przypadku uruchamiania w systemach AIX z wieloma instalacjami produktu IBM Global Security Kit (GSKit) w wersji 8.0 .

W przypadku uruchamiania aplikacji klienckich w systemie AIX z wieloma instalacjami produktu GSKit 8.0 wywołania połączenia klienta mogą zwracać wartość MQRC_CHANNEL_CONFIG_ERROR , jeśli używany jest protokół TLS. Dzienniki /var/mqm/errors rejestrują błąd AMQ6175 i AMQ9220 dla aplikacji klienckiej, która się nie powiodła, 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 ----------------------------------------------------------
```

Typową 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 GSKit 8.0 . Ten błąd może być spowodowany wykonaniem aplikacji klienckiej IBM MQ w środowisku Db2 .

Aby uniknąć tego błędu, należy dołączyć katalogi bibliotek produktu IBM MQ na początku ścieżki biblioteki, aby biblioteki produktu IBM MQ miały pierwszeństwo. Można to zrobić za pomocą komendy **setmqenv** z parametrem **-k** , na przykład:

```
. /usr/mqm/bin/setmqenv -s -k
```

Więcej informacji na temat używania komendy **setmqenv** zawiera sekcja setmqenv (set IBM MQ environment) .

Konfigurowanie kanałów TLS za pomocą komend MQSC

Aby skonfigurować kanały TLS, należy użyć komend **runmqsc** i ALTER CHANNEL. Opcjonalnie można skonfigurować kanał w celu akceptowania tylko certyfikatów z atrybutami w nazwie wyróżniającej właściciela, które są zgodne z podanymi wartościami. Opcjonalnie można także skonfigurować kanał menedżera kolejek, tak aby menedżer kolejek odrzucał połączenie, jeśli strona inicjująca nie wyśle certyfikatu osobistego.

O tym zadaniu

Informacje na temat konfigurowania kanałów w produkcie IBM MQ Explorerzawiera sekcja Konfigurowanie kanałów TLS za pomocą produktu IBM MQ Explorer.

Aby skonfigurować kanały za pomocą programu **runmqsc**, wykonaj następujące kroki.

Procedura

1. Wywołaj komendę **runmqsc** łączącą się z docelowym menedżerem kolejek.
2. Zidentyfikuj kanał, który ma zostać włączony dla protokołu TLS.

   Zanotuj zarówno nazwę kanału, jak i typ kanału.
3. Komenda ALTER CHANNEL służy do zmiany różnych właściwości kanału IBM MQ .

   Oprócz komendy należy podać nazwę i typ kanału. Na przykład w celu zmiany kanału nadawczego o nazwie MQ.TEST : Uruchom następującą komendę:

   ```
   ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR)
   ```

   Istnieją różne atrybuty kanału związane z protokołem TLS, które można dopasować w definicjach kanałów systemu IBM MQ .

Co dalej

Ustawianie zabezpieczeń komunikatu

Przesyłanie komunikatów z włączonym TLS oferuje dwie metody zabezpieczania komunikatu:

- Szyfrowanie gwarantuje, że w przypadku przechwycenia komunikat nie zostanie odczytany.
- Funkcje mieszania gwarantują, że w przypadku wykrycia komunikat zostanie zmieniony.

Kombinacja tych metod jest nazywana specyfikacją szyfrowania (cipher specification) lub CipherSpec. Dla obu końców kanału musi zostać ustawiony taki sam atrybut CipherSpec, ponieważ w przeciwnym razie przesyłanie komunikatów z włączonym protokołem TLS zakończy się niepowodzeniem. Więcej informacji na ten temat zawiera "zabezpieczanieIBM MQ" na stronie 7.

Aby zmienić ustawienie TLS włączenia kanału IBM MQ , należy podać wartość atrybutu SSLCIPH. Ten atrybut musi być ustawiony na poprawną wartość atrybutu CipherSpec dla platformy kolejki menedżera kolejek z listy "Włączanie CipherSpecs" na stronie 466.

Aby zmienić kanał IBM MQ w celu wyłączenia protokołu TLS, należy ustawić wartość parametru SSLCIPH na pustą wartość. Na przykład:

```
ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR) SSLCIPH(ANY_TLS12_OR_HIGHER)
```

Uwaga: Aby zachować wielkość liter, należy umieścić nazwę kanału w apostrofach. Bez pojedynczych cudzysłowów IBM MQ przekształca wszystkie łańcuchy w wielkie litery.

Filtrowanie certyfikatów według nazwy właściciela

Certyfikaty zawierają nazwę wyróżniającą właściciela certyfikatu. Opcjonalnie można skonfigurować kanał w celu akceptowania tylko certyfikatów z atrybutami w nazwie wyróżniającej właściciela, które są zgodne z podanymi wartościami.

Nazwy atrybutów, które mogą być filtrowane przez produkt IBM MQ, zostały przedstawione w następującej tabeli:

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

Znaku wieloznacznego (*) można użyć na początku lub na końcu wartości atrybutu zamiast dowolnej liczby znaków. Na przykład, aby akceptować tylko certyfikaty otrzymane od osoby o nazwisku `Smith` pracującej dla firmy `IBM` w Anglii (`GB`), wpisz:

```
CN=*Smith, O=IBM, C=GB
```

Na przykład:

```
ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR) SSLPEER('CN=*Smith, O=IBM, C=GB')
```

Uwaga: Aby zachować wielkość liter, należy umieścić łańcuch SSLPEER w pojedynczych cudzysłowach. Bez pojedynczych cudzysłowów IBM MQ przekształca wszystkie łańcuchy w wielkie litery.

Uwierzytelnianie stron inicjujących połączenia z menedżerem kolejek

Jeśli strona inicjuje połączenie z włączonym TLS z menedżerem kolejek, menedżer kolejek musi wysłać certyfikat osobisty do strony inicjującej jako dowód tożsamości. Opcjonalnie można także skonfigurować kanał menedżera kolejek, tak aby menedżer kolejek odrzucał połączenie, jeśli strona inicjująca nie wyśle certyfikatu osobistego.

W tym celu należy ustawić atrybut SSLCAUTH. Ten atrybut jest atrybutem boolowskim i może mieć wartości OPTIONAL lub REQUIRED:

- Opcjonalnie uwierzytelnia certyfikat klienta nawiązującego połączenie, jeśli taki certyfikat został udostępniony, ale nie wymaga od klienta wysłania certyfikatu. Klient jest odrzucany, jeśli wysyła certyfikat, który nie jest poprawny.

- WYMAGANE odrzuca wszystkie klienty nawiązujące połączenie, które nie udostępniają poprawnego certyfikatu TLS

Na przykład:

```
ALTER CHANNEL('MQ.TEST') CHLTYPE(SDR) SSLCAUTH(REQUIRED)
```

IBM i Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie IBM i

Bezpieczna komunikacja, która korzysta z protokołów szyfrujących SSL lub TLS, obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację SSL lub TLS, należy zdefiniować kanały tak, aby używały SSL lub TLS. Należy również utworzyć certyfikaty cyfrowe i zarządzać nimi. W niektórych systemach operacyjnych można wykonać testy z samopodpisanymi certyfikatami. Jednak w systemie IBM inależy używać 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 293.

Ta kolekcja tematów zawiera wprowadzenie do niektórych zadań związanych z konfigurowaniem komunikacji SSL lub TLS oraz udostępnia wskazówki krok po kroku dotyczące wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które są opcjonalnymi częściami protokołów SSL i TLS. Podczas uzgadniania SSL lub TLS klient SSL lub TLS zawsze uzyskuje i sprawdza poprawność certyfikatu cyfrowego z serwera. W 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 etykietę w poprawnym formacie IBM MQ :

- W przypadku menedżera kolejek nazwa `ibmwebspheremq` , po której następuje nazwa menedżera kolejek zmieniona na małe litery. Na przykład dla systemu `QM1`: `ibmwebspheremqqm1`.
- W przypadku programu IBM MQ C Client for IBM i `ibmwebspheremq` , po którym następuje identyfikator logowania użytkownika zmieniony na małe litery, na przykład `ibmwebspheremqmyuserid`.

IBM MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć pomyłek z certyfikatami dla innych produktów. Upewnij się, że podano całą etykietę certyfikatu małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli został wysłany. Jeśli klient SSL lub TLS nie wysyła certyfikatu, uwierzytelnianie kończy się niepowodzeniem tylko wtedy, gdy koniec kanału działającego jako serwer SSL lub TLS jest zdefiniowany z parametrem SSLCAUTH ustawionym na wartość REQUIRED lub wartością parametru SSLPEER. Więcej informacji na ten temat zawiera sekcja Nawiązywanie połączenia z dwoma menedżerami kolejek przy użyciu protokołu SSL lub TLS.

ALW Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie AIX, Linux, and Windows

Bezpieczna komunikacja, która korzysta z protokołów szyfrujących SSL lub TLS, obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację SSL lub TLS, należy zdefiniować kanały tak, aby używały SSL lub TLS. Należy również utworzyć certyfikaty cyfrowe i zarządzać nimi. W systemach AIX, Linux, and Windows można wykonać testy z samopodpisanymi certyfikatami.

Ostrzeżenie: W menedżerach kolejek, które mają zostać połączone za pomocą kanałów z włączoną obsługą protokołu TLS, nie można używać kombinacji certyfikatów podpisanych przez krzywą eliptyczną (Elliptic Curve-signed certificates) i certyfikatów podpisanych przez RSA.

Wszystkie menedżery kolejek używające kanałów z włączoną obsługą protokołu TLS muszą używać certyfikatów podpisanych przy użyciu protokołu RSA lub wszystkich certyfikatów podpisanych przy użyciu protokołu EC, a nie obu tych metod.

Więcej informacji zawiera sekcja “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48.

Nie można unieważnić samopodpisanych certyfikatów, co może umożliwić atakującemu podszywanie się pod tożsamość po naruszeniu klucza prywatnego. Ośrodki CA mogą unieważnić certyfikat z naruszoną ochroną, co uniemożliwia dalsze korzystanie z niego. Certyfikaty podpisane przez ośrodek CA są zatem bezpieczniejsze w środowisku produkcyjnym, chociaż certyfikaty samopodpisane są wygodniejsze w systemie testowym.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL/TLS w systemie AIX, Linux, and Windows” na stronie 312.

Ta kolekcja tematów zawiera wprowadzenie do niektórych zadań związanych z konfigurowaniem komunikacji SSL oraz zawiera szczegółowe wskazówki dotyczące wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które jest opcjonalną częścią protokołów. Podczas uzgadniania SSL lub TLS klient SSL lub TLS zawsze uzyskuje i sprawdza poprawność certyfikatu cyfrowego z serwera. W implementacji IBM MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

W systemie AIX, Linux, and Windowsklient SSL lub TLS wysyła certyfikat tylko wtedy, gdy ma on etykietę w poprawnym formacie IBM MQ :

- W przypadku menedżera kolejek obowiązuje format `ibmwebspheremq` , po którym następuje nazwa menedżera kolejek zmieniona na małe litery. Na przykład dla systemu `QM1`: `ibmwebspheremqqm1`
- W przypadku klienta systemu IBM MQ nazwa `ibmwebspheremq` , po której następuje identyfikator logowania, została zmieniona na małe litery, na przykład `ibmwebspheremqmyuserid`.

IBM MQ używa przedrostka `ibmwebspheremq` na etykiecie, aby uniknąć pomyłek z certyfikatami dla innych produktów. Upewnij się, że podano całą etykietę certyfikatu małymi literami.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli został wysłany. Jeśli klient nie wysyła certyfikatu, uwierzytelnianie kończy się niepowodzeniem tylko wtedy, gdy koniec kanału działającego jako serwer SSL lub TLS jest zdefiniowany z parametrem SSLCAUTH ustawionym na wartość REQUIRED lub wartością parametru SSLPEER. Więcej informacji na ten temat zawiera sekcja Nawiązywanie połączenia z dwoma menedżerami kolejek przy użyciu protokołu SSL lub TLS.

z/OS Konfigurowanie komunikacji dla protokołu SSL lub TLS w systemie z/OS

Bezpieczna komunikacja, która korzysta z protokołów szyfrujących SSL lub TLS, obejmuje konfigurowanie kanałów komunikacyjnych i zarządzanie certyfikatami cyfrowymi, które będą używane do uwierzytelniania.

Aby skonfigurować instalację SSL lub TLS, należy zdefiniować kanały tak, aby używały SSL lub TLS. Należy również utworzyć certyfikaty cyfrowe i zarządzać nimi. W systemie z/OS można wykonać testy z certyfikatami samopodpisanymi lub z certyfikatami osobistymi podpisanymi przez lokalny ośrodek certyfikacji (CA).

Nie można unieważnić samopodpisanych certyfikatów, co może umożliwić atakującemu podszywanie się pod tożsamość po naruszeniu klucza prywatnego. Ośrodki CA mogą unieważnić certyfikat z naruszoną ochroną, co uniemożliwia dalsze korzystanie z niego. Certyfikaty podpisane przez ośrodek CA są zatem bezpieczniejsze w środowisku produkcyjnym, chociaż certyfikaty samopodpisane są wygodniejsze w systemie testowym.

Pełne informacje na temat tworzenia certyfikatów i zarządzania nimi zawiera sekcja “Praca z protokołem SSL/TLS w systemie z/OS” na stronie 352.

Więcej informacji zawierają parametry CERTLABL i CERTQSGL komendy ALTER QMGR oraz parametr CERLABL komendy DEFINE CHANNEL .

Kolejność wykonywania operacji jest następująca:

- Parametr CERTLABL kanału
- Parametr QMGR CERTQSGL, jeśli kanał jest współużytkowany.

  Dla kanału nadawczego oznacza to, że kolejka transmisji (XMITQ) jest współużytkowana. W przypadku kanału odbiorczego oznacza to, że kanał został uruchomiony przez współużytkowany program nasłuchujący, czyli program nasłuchujący z INDISP (GROUP).
- KMGR CERTLABL
- Domyślna etykieta `ibmWebSphereMQ` , po której następuje nazwa grupy współużytkowania kolejek dla kanałów współużytkowanych lub nazwa menedżera kolejek.

Ta kolekcja tematów zawiera wprowadzenie do niektórych zadań związanych z konfigurowaniem komunikacji SSL lub TLS oraz zawiera szczegółowe wskazówki dotyczące wykonywania tych zadań.

Można również przetestować uwierzytelnianie klienta SSL lub TLS, które jest opcjonalną częścią protokołów. Podczas uzgadniania SSL lub TLS klient SSL lub TLS zawsze uzyskuje i sprawdza poprawność certyfikatu cyfrowego z serwera. W implementacji IBM MQ serwer SSL lub TLS zawsze żąda certyfikatu od klienta.

Jeśli kanał jest współużytkowany, kanał najpierw próbuje znaleźć certyfikat dla grupy współużytkowania kolejek. Jeśli nie znajdzie certyfikatu dla grupy współużytkowania kolejek, spróbuje znaleźć certyfikat dla menedżera kolejek.

W systemie z/OSprodukt IBM MQ używa przedrostka `ibmWebSphereMQ` na etykiecie, aby uniknąć pomyłek z certyfikatami dla innych produktów.

Serwer SSL lub TLS zawsze sprawdza poprawność certyfikatu klienta, jeśli został wysłany. Jeśli klient SSL lub TLS nie wysyła certyfikatu, uwierzytelnianie kończy się niepowodzeniem tylko wtedy, gdy koniec kanału działającego jako serwer SSL lub TLS jest zdefiniowany z parametrem SSLCAUTH ustawionym na wartość REQUIRED lub wartością parametru SSLPEER. Więcej informacji na ten temat zawiera sekcja Nawiązywanie połączenia z dwoma menedżerami kolejek przy użyciu protokołu SSL lub TLS.

Praca z protokołem SSL/TLS

Te tematy zawierają 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 365
- “Autoryzowanie dostępu do obiektów” na stronie 395
- “Poufność komunikatów” na stronie 466
- “Integralność danych komunikatów” na stronie 525
- “Zabezpieczanie klastrów” na stronie 526

IBM i Praca z protokołem SSL/TLS w systemie IBM i

Ta kolekcja tematów zawiera instrukcje dotyczące poszczególnych zadań związanych z protokołem TLS (Transport Layer Security) w produkcie IBM MQ for IBM i.

W systemie IBM i obsługa protokołu TLS jest integralną częścią systemu operacyjnego. Upewnij się, że zostały zainstalowane wymagania wstępne wymienione w sekcji Wymagania sprzętowe i programowe w systemie IBM i.

W systemie IBM ikluczami i certyfikatami cyfrowymi zarządza się za pomocą narzędzia Digital Certificate Manager (DCM).

Uzyskiwanie dostępu do programu DCM

Aby uzyskać dostęp do interfejsu DCM, należy postępować zgodnie z poniższymi instrukcjami.

O tym zadaniu

Wykonaj następujące kroki w przeglądarce WWW obsługującej 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 na żądanie.

   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 przeglądać podpisy obiektów, do których jest uprawniony. Jeśli użytkownik ma uprawnienia do korzystania z aplikacji do podpisywania obiektów, może również podpisywać obiekty z programu DCM.
3. Na stronie Konfiguracje internetowe kliknij opcję **Digital Certificate Manager**.

   Zostanie wyświetlona strona Digital Certificate Manager (Menedżer certyfikatów cyfrowych).

Przypisywanie certyfikatu do menedżera kolejek w systemie IBM i

Użyj programu DCM, aby przypisać certyfikat do menedżera kolejek.

Użyj tradycyjnego zarządzania certyfikatami cyfrowymi IBM i , aby przypisać certyfikat do menedżera kolejek. Oznacza to, że można określić, że menedżer kolejek używa bazy certyfikatów systemu i że menedżer kolejek jest zarejestrowany do użycia jako aplikacja w programie Digital Certificate Manager. W tym celu należy zmienić wartość atrybutu **SSLKEYR** menedżera kolejek na *SYSTEM.

Po zmianie wartości parametru **SSLKEYR** na *SYSTEMprogram IBM MQ rejestruje menedżer 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. Menedżer kolejek jest następnie wyświetlany jako aplikacja serwera w programie Digital Certificate Manager, a użytkownik może przypisać do tej aplikacji dowolny certyfikat serwera lub klienta w bazie danych systemu.

Ponieważ menedżer kolejek jest zarejestrowany jako aplikacja, można wykonać zaawansowane funkcje programu DCM, takie jak definiowanie list zaufanych ośrodków certyfikacji (CA).

Jeśli wartość parametru **SSLKEYR** zostanie zmieniona na inną niż *SYSTEM, program IBM MQ wyrejestrowuje menedżer kolejek jako aplikację z programem Digital Certificate Manager. Jeśli menedżer kolejek zostanie usunięty, zostanie również wyrejestrowany z programu DCM. Użytkownik z wystarczającymi uprawnieniami *SECADM może również ręcznie dodawać lub usuwać aplikacje z programu DCM.

Konfigurowanie repozytorium kluczy w systemie IBM i

Repozytorium kluczy musi być skonfigurowane na obu końcach połączenia. Można użyć domyślnych baz certyfikatów lub utworzyć własne.

Połączenie TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek i program IBM MQ MQI client muszą mieć dostęp do repozytorium kluczy. Jeśli chcesz uzyskać dostęp do repozytorium kluczy przy użyciu nazwy pliku i hasła (nie używając opcji *SYSTEM), upewnij się, że profil użytkownika QMQM ma następujące uprawnienia:

- Uprawnienie do wykonywania dla katalogu zawierającego repozytorium kluczy
- Uprawnienie do odczytu 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 zarządzanej za pomocą programu DCM. Te certyfikaty cyfrowe mają etykiety, które wiążą certyfikat z menedżerem kolejek lub programem IBM MQ MQI client. Protokół TLS używa certyfikatów do celów uwierzytelniania.

Etykieta jest wartością atrybutu **CERTLABL** (jeśli został ustawiony) lub domyślną wartością `ibmwebspheremq` z dodaną nazwą menedżera kolejek lub identyfikatorem logowania użytkownika IBM MQ MQI client (wszystkie te wartości są zapisane małymi literami). Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Nazwa bazy certyfikatów menedżera kolejek lub systemu IBM MQ MQI client składa się ze ścieżki i nazwy rdzenia. 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 również nazywana `*SYSTEM`. Opcjonalnie można zdefiniować własną ścieżkę i nazwę rdzenia.

Jeśli zostanie zdefiniowana własna ścieżka lub nazwa pliku, należy ustawić uprawnienia do tego pliku, aby ściśle kontrolować dostęp do niego.

Sekcja “Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie IBM i” na stronie 298 zawiera informacje na temat określania nazwy bazy certyfikatów. Nazwę bazy certyfikatów można określić przed lub po utworzeniu bazy certyfikatów.

Uwaga: Operacje, które można wykonać za pomocą programu DCM, mogą być ograniczone przez uprawnienia profilu użytkownika. Na przykład do utworzenia certyfikatu ośrodka CA wymagane są uprawnienia *ALLOBJ i *SECADM.

Szyfrowanie haseł repozytorium kluczy w systemie IBM i

Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

Następujące komponenty i opcje produktu IBM MQ obsługują dwie różne metody przechowywania haseł repozytorium kluczy:

- Repozytorium kluczy TLS menedżera kolejek.
- IBM MQ MQI clients , które używają protokołu TLS.

Hasła repozytorium kluczy używane przez te komponenty są chronione za pomocą systemu ochrony haseł IBM MQ . Mechanizm udostępniania hasła i szyfrowania różni się nieznacznie w zależności od komponentu:

Repozytorium kluczy TLS menedżera kolejek

Hasło jest szyfrowane, gdy atrybut menedżera kolejek **SSLKEYRPWD** jest ustawiony za pomocą komendy CHGMQM (Change Message Queue Manager-Zmiana menedżera kolejek komunikatów) .

Hasło jest szyfrowane przy użyciu algorytmu AES-128 . Szczegóły tego algorytmu są publicznie znane i uważane za bezpieczne.

Hasło jest przechowywane w pliku ukrytych haseł w formacie, który nie jest zrozumiały dla innego oprogramowania, które może uzyskać dostęp do repozytorium kluczy.

Hasło zaszyfrowane przez jeden komponent IBM MQ nie może być używane przez inny komponent IBM MQ .

Unikalny klucz szyfrowania można podać, gdy hasło repozytorium kluczy jest zaszyfrowane. Unikalny klucz szyfrowania uniemożliwia osobie, która nie ma dostępu do klucza szyfrowania, deszyfrowanie hasła. Klucz ten należy podać za pomocą atrybutu menedżera kolejek **INITKEY** , który musi zostać ustawiony przed podaniem hasła do zaszyfrowania.

Więcej informacji na temat systemu zabezpieczenia hasłem IBM MQ zawiera sekcja “Ochrona haseł w plikach konfiguracyjnych komponentu IBM MQ” na stronie 617.

IBM MQ MQI clients , które korzystają z protokołu TLS

"IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla systemu IBM i" na stronie 309 może zapisać hasło repozytorium kluczy w pliku ukrytych haseł. Patrz także sekcja Administrowanie za pomocą komend MQSC w systemie IBM i.

Hasło jest szyfrowane przy użyciu algorytmu AES-128 . Szczegóły tego algorytmu są publicznie znane i uważane za bezpieczne.

Hasło jest przechowywane w pliku ukrytych haseł w formacie, który nie jest zrozumiały dla innego oprogramowania, które może uzyskać dostęp do repozytorium kluczy.

Unikalny klucz szyfrowania można podać, gdy hasło repozytorium kluczy jest zaszyfrowane. Unikalny klucz szyfrowania uniemożliwia osobie, która nie ma dostępu do klucza szyfrowania, deszyfrowanie hasła. Klucz ten można podać za pomocą parametru **-sf** .

Zaszyfrowane hasło jest przechowywane w pliku ukrytych haseł w tym samym katalogu, co plik repozytorium kluczy.

Produkt IBM MQ MQI clients obsługuje również hasła udostępniane za pośrednictwem innych mechanizmów. Patrz "Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie IBM i" na stronie 299.

Niezależnie od wybranej metody szyfrowania hasła repozytorium kluczy należy pamiętać o ograniczeniach związanych z szyfrowaniem zapisanych haseł. Patrz sekcja "Ograniczenia ochrony przez szyfrowanie haseł" na stronie 625.

Pojęcia pokrewne

"Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie IBM i" na stronie 298
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

"Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie IBM i" na stronie 299
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

"Praca z protokołem SSL/TLS w systemie IBM i" na stronie 293
Ta kolekcja tematów zawiera instrukcje dotyczące poszczególnych zadań związanych z protokołem TLS (Transport Layer Security) w produkcie IBM MQ for IBM i.

Tworzenie bazy certyfikatów w systemie IBM i
Jeśli nie chcesz używać domyślnej bazy certyfikatów, wykonaj tę procedurę, aby utworzyć własną bazę.

O tym zadaniu

Nową bazę certyfikatów należy utworzyć tylko wtedy, gdy nie ma być używana domyślna baza certyfikatów IBM i .

Aby określić, że ma być używana baza certyfikatów systemu IBM i , zmień wartość atrybutu SSLKEYR menedżera kolejek na *SYSTEM. Ta wartość wskazuje, że menedżer kolejek używa bazy certyfikatów systemu, a menedżer kolejek jest zarejestrowany jako aplikacja w programie Digital Certificate Manager (DCM).

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji "Uzyskiwanie dostępu do programu DCM" na stronie 294
2. W panelu nawigacyjnym kliknij opcję **Create New Certificate Store**(Utwórz nową bazę certyfikatów).
   W ramce zadań zostanie wyświetlona strona Tworzenie nowej bazy certyfikatów (Create New Certificate Store).
3. W ramce zadań wybierz **Inna baza certyfikatów systemu** i kliknij **Kontynuuj**(Continue).

W ramce zadania zostanie wyświetlona strona Tworzenie certyfikatu w nowej bazie certyfikatów.

4. Wybierz opcję **Nie-nie twórz certyfikatu w bazie certyfikatów** i 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 i nazwę pliku IFS, 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 którym rozróżniana jest wielkość liter), ponieważ jest ono potrzebne podczas składowania klucza repozytorium.
7. Aby wyjść z programu DCM, zamknij okno przeglądarki.

Co dalej

Po utworzeniu bazy certyfikatów za pomocą programu DCM należy upewnić się, że hasło zostało zeskładowane zgodnie z opisem w sekcji “Ukrycie hasła bazy certyfikatów w systemach IBM i” na stronie 297

Zadania pokrewne

“Importowanie certyfikatu do repozytorium kluczy w systemie IBM i” na stronie 307
Wykonaj tę procedurę, aby zaimportować certyfikat.

Ukrycie hasła bazy certyfikatów w systemach IBM i

Zeskładuj hasło bazy certyfikatów za pomocą komend CL.

Poniższe instrukcje dotyczą ukrywania hasła bazy certyfikatów w systemie IBM i dla menedżera kolejek. Alternatywnie w przypadku systemu IBM MQ MQI client, jeśli nie jest używana baza certyfikatów *SYSTEM (środowisko MQSSLKEYR jest ustawione na wartość inną niż *SYSTEM), należy wykonać procedurę opisaną w sekcji “Zeskładuj hasło bazy certyfikatów” na stronie 310 w sekcji “IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla systemu IBM i” na stronie 309.

Jeśli określono, że baza certyfikatów *SYSTEM ma być używana (przez zmianę wartości atrybutu SSLKEYR menedżera kolejek na *SYSTEM), nie należy wykonywać tych czynności.

Po utworzeniu bazy certyfikatów 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. Musi być ujęta w apostrofy dokładnie tak, jak została wprowadzona w kroku 6 procedury “Tworzenie bazy certyfikatów w systemie IBM i” na stronie 296.

Uwaga: Jeśli nie jest używana domyślna baza certyfikatów systemu i hasło nie zostanie zeskładowane, próby uruchomienia kanałów TLS nie powiodą się, ponieważ nie będą mogły uzyskać hasła wymaganego do uzyskania dostępu do bazy certyfikatów.

Zabezpieczenie hasłem

V 9.3.0

Jeśli zostanie podane hasło do repozytorium kluczy, program IBM MQ zaszyfruje je je za pomocą systemu IBM MQ Password Protection. Do zaszyfrowania hasła używany jest klucz początkowy. Jeśli nie zostanie on dostarczony do menedżera kolejek, zostanie użyty klucz domyślny.

Przed podaniem hasła repozytorium kluczy należy ustawić unikalny klucz początkowy dla menedżera kolejek. Można to zrobić za pomocą atrybutu **INITKEY** komendy MQSC **ALTER QMGR** :

```
ALTER QMGR INITKEY('value')
```

Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie IBM i

Ta procedura służy do uzyskania 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 pod kątem ścieżki i nazwy rdzenia 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 za pomocą komendy CHGMQM lub ALTER QMGR.

Procedura

Użyj komendy CHGMQM lub ALTER QMGR MQSC, aby ustawić atrybut repozytorium kluczy menedżera kolejek.

a) Użycie komendy CHGMQM: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb')`

b) Przy użyciu instrukcji ALTER QMGR: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb')`

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 starego miejsca. Jeśli certyfikaty ośrodka CA instalowane fabrycznie 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 307. Należy również zeskładować hasło dla nowego położenia, zgodnie z opisem w sekcji “Ukrycie hasła bazy certyfikatów w systemach IBM i” na stronie 297.

V 9.3.0 IBM i V 9.3.0 *Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie IBM i*

Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

Produkt IBM MQ udostępnia mechanizm dostarczania hasła repozytorium kluczy do menedżera kolejek:

- Parametr **SSLKEYRPWD** komendy **CHGMQM**

Hasło repozytorium kluczy jest szyfrowane za pomocą systemu ochrony haseł IBM MQ . Więcej informacji na temat metod ochrony hasła repozytorium kluczy zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie IBM i” na stronie 295.

Patrz także sekcja Administrowanie za pomocą komend MQSC w systemie IBM i.

Atrybut SSLKEYRPWD

Aby podać hasło repozytorium kluczy bezpośrednio dla menedżera kolejek, uruchom następującą komendę systemu **CHGMQM** , zastępując zmienną *queue_manager* nazwą menedżera kolejek, a zmienną *password* hasłem repozytorium kluczy.

```
CHGMQM MQMNAME('queue_manager') SSLKEYRPWD('password')
```

Ostrzeżenie: Należy upewnić się, że nazwa menedżera kolejek i hasło są ujęte w pojedynczy cudzysłów, w przeciwnym razie program IBM MQ przekształci znaki na wielkie litery.

Jeśli hasło repozytorium kluczy jest określone za pomocą tej metody, jest ono szyfrowane za pomocą systemu zabezpieczenia hasłem IBM MQ przed jego zapisaniem.

Do zaszyfrowania hasła używany jest klucz szyfrowania, który jest nazywany kluczem początkowym. Ustaw menedżer kolejek tak, aby używał unikalnego klucza początkowego w celu bezpiecznego zabezpieczenia hasła. Jeśli nie podasz klucza początkowego, zostanie użyty klucz domyślny.

Przed ustawianiem hasła repozytorium kluczy upewnij się, że menedżer kolejek jest skonfigurowany z unikalnym kluczem początkowym. Klucz początkowy można zmodyfikować za pomocą atrybutu **INITKEY** komendy **ALTER QMGR** . Na przykład:

```
ALTER QMGR INITKEY('mykey')
```

Ostrzeżenie: Jeśli klucz początkowy zostanie zmodyfikowany po ustawieniu hasła repozytorium kluczy, hasło repozytorium kluczy nie zostanie zaszyfrowane przy użyciu nowego klucza początkowego. Jeśli klucz początkowy zostanie zmieniony, należy również zresetować hasło repozytorium kluczy. W przeciwnym razie program IBM MQ nie będzie mógł zdeszyfrować hasła repozytorium kluczy i z tego powodu nie będzie mógł uzyskać dostępu do repozytorium kluczy.

Więcej informacji na temat atrybutu **SSLKEYRPWD** zawiera sekcja Parametr **SSLKEYRPWD** komendy **CHGMQM**.

Pojęcia pokrewne

“Szyfrowanie haseł repozytorium kluczy w systemie IBM i” na stronie 295
Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

“Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie IBM i” na stronie 299
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

V 9.3.0 IBM i V 9.3.0 *Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie IBM i*

Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

IBM MQ udostępnia cztery mechanizmy dostarczania hasła repozytorium kluczy do IBM MQ MQI client:

- “Pola KeyRepoPassword obiektu MQSCO ” na stronie 299
- “Zmienna środowiskowa MQKEYRPWD” na stronie 300
- “Atrybut SSLKeyRepositoryPassword pliku konfiguracyjnego klienta” na stronie 300
- “Plik ukryty repozytorium kluczy” na stronie 300

Jeśli plik ukryty repozytorium kluczy nie jest używany, można podać hasło repozytorium kluczy w postaci jawnego łańcucha tekstowego lub łańcucha, który jest szyfrowany za pomocą systemu ochrony hasłem IBM MQ . Więcej informacji na temat metod ochrony hasła repozytorium kluczy zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie IBM i” na stronie 295.

Pola KeyRepoPassword obiektu MQSCO

Aby podać hasło repozytorium kluczy przy użyciu struktury MQSCO, należy użyć kombinacji następujących trzech zmiennych pól łańcuchowych:

KeyRepoPasswordLength
Długość hasła.

KeyRepoPasswordPtr
Wskaźnik do miejsca w pamięci, które zawiera hasło.

KeyRepoPasswordOffset
Położenie hasła w pamięci, reprezentowane przez liczbę bajtów od początku struktury MQSCO.

Uwaga: Można podać tylko jedną z wartości: **KeyRepoPasswordPtr** lub **KeyRepoPasswordOffset**.

Na przykład:

```
char * pwd = "passw0rd";
MQSCO  SslConnOptions = {MQSCO_DEFAULT};

SslConnOptions.KeyRepoPasswordPtr = pwd;
SslConnOptions.KeyRepoPasswordLength = (MQLONG)strlen(SslConnOptions.KeyRepoPasswordPtr);
SslConnOptions.Version = MQSCO_VERSION_6;
```

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed przekazaniem do aplikacji IBM MQ client . Więcej informacji na ten temat zawiera sekcja “Szyfrowanie hasła repozytorium kluczy” na stronie 301.

Więcej informacji na temat struktury MQCSO zawiera sekcja Opcje konfiguracyjne MQSCO-SSL/TLS.

Zmienna środowiskowa *MQKEYRPWD*

Jeśli hasło do repozytorium kluczy nie zostanie dostarczone do klienta przy użyciu struktury MQSCO, można określić hasło do repozytorium kluczy za pomocą zmiennej środowiskowej *MQKEYRPWD* . Na przykład:

```
export MQKEYRPWD=passw0rd
```

lub wersji

```
set MQKEYRPWD=passw0rd
```

gdzie *passw0rd* jest hasłem użytkownika.

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed ustawianiem wartości zmiennej środowiskowej. Więcej informacji na ten temat zawiera “Szyfrowanie hasła repozytorium kluczy” na stronie 301.

Atrybut SSLKeyRepositoryPassword pliku konfiguracyjnego klienta

Jeśli hasło repozytorium kluczy nie zostanie dostarczone do klienta za pomocą jednej z innych metod, hasło repozytorium kluczy można określić za pomocą atrybutu **SSLKeyRepositoryPassword** w sekcji **SSL** pliku konfiguracyjnego klienta. Na przykład:

```
SSL:
    SSLKeyRepositoryPassword=passw0rd
```

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed ustawieniem wartości atrybutu **SSLKeyRepositoryPassword** . Więcej informacji na ten temat zawiera sekcja “Szyfrowanie hasła repozytorium kluczy” na stronie 301.

Więcej informacji na temat sekcji SSL pliku konfiguracyjnego klienta zawiera sekcja Sekcja SSL pliku konfiguracyjnego klienta.

Plik ukryty repozytorium kluczy

Jeśli hasło repozytorium kluczy nie zostanie dostarczone do klienta przy użyciu jednej z innych metod, program IBM MQ przyjmuje, że plik ukrytych haseł istnieje w tym samym katalogu, co repozytorium kluczy. Plik ukrytych haseł ma taką samą nazwę rdzenia, jak repozytorium kluczy, ale ma rozszerzenie `.sth` .

Plik ukrytych haseł repozytorium kluczy jest tworzony za pomocą narzędzia wiersza komend **amqrsslc** . Aby utworzyć plik ukrytych haseł, uruchom następującą komendę:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Ta komenda wyświetla monit o podanie hasła do zaszyfrowania. Hasło jest szyfrowane przez system zabezpieczenia hasłem IBM MQ przy użyciu domyślnego klucza szyfrowania, chyba że został on podany za pomocą parametru **-sf** .

Więcej informacji na ten temat zawierają sekcje “IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla systemu IBM i” na stronie 309 i “Szyfrowanie hasła repozytorium kluczy” na stronie 301.

Szyfrowanie hasła repozytorium kluczy

Jeśli hasło repozytorium kluczy zostanie podane przy użyciu innej metody niż plik ukrytych haseł, należy zaszyfrować hasło przy użyciu systemu zabezpieczenia hasłem IBM MQ . Aby zaszyfrować hasło, uruchom komendę **runmqicred** . Po wyświetleniu zapytania wprowadź hasło repozytorium kluczy. Komenda wyświetli zaszyfrowane hasło. Zaszyfrowane hasło można podać w pliku IBM MQ MQI client zamiast hasła w postaci jawnej, używając dowolnej z opisanych metod.

Do zaszyfrowania hasła używany jest klucz szyfrowania, który jest nazywany kluczem początkowym. Podczas szyfrowania hasła należy użyć unikalnego klucza początkowego, aby zabezpieczyć hasło. Aby podać własny klucz początkowy, należy użyć parametru **-sf** komendy **runmqicred** . Jeśli nie podasz klucza początkowego, zostanie użyty klucz domyślny.

Więcej informacji na ten temat zawiera sekcja runmqicred (protect IBM MQ client passwords).

Jeśli użytkownik poda własny klucz początkowy, gdy hasło repozytorium kluczy jest zaszyfrowane, i przekaże zaszyfrowane hasło do serwera IBM MQ MQI client, należy również upewnić się, że ten sam klucz początkowy został dostarczony do serwera IBM MQ MQI client. Więcej informacji na temat udostępniania początkowego klucza IBM MQ MQI clientzawiera sekcja “Podawanie klucza początkowego dla IBM MQ MQI client w systemie IBM i” na stronie 301.

Pojęcia pokrewne

“Szyfrowanie haseł repozytorium kluczy w systemie IBM i” na stronie 295
Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

“Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie IBM i” na stronie 298
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

V 9.3.0 IBM i V 9.3.0 *Podawanie klucza początkowego dla IBM MQ MQI client w systemie IBM i*
Jeśli do IBM MQ MQI client zostaną podane zmienne, które zostały zaszyfrowane za pomocą systemu IBM MQ Password Protection System, może być konieczne podanie odpowiedniego klucza początkowego, który został użyty do zaszyfrowania wartości.

Jeśli podczas szyfrowania wartości nie określono klucza początkowego, nie trzeba podawać żadnej początkowej wartości klucza do IBM MQ client. Jeśli jednak użyto unikalnego klucza początkowego, można udostępnić klucz początkowy dla IBM MQ client za pomocą następujących metod:

- “Podawanie klucza początkowego przy użyciu struktury MQCSP” na stronie 302
- “Podawanie klucza początkowego za pomocą zmiennej środowiskowej MQS_MQI_KEYFILE” na stronie 302
- “Podawanie klucza początkowego przy użyciu pliku konfiguracyjnego klienta” na stronie 302

Podawanie klucza początkowego przy użyciu struktury MQCSP

Aby podać klucz początkowy przy użyciu struktury MQCSP, należy użyć kombinacji następujących trzech zmiennych pól łańcuchowych:

InitialKeyLength
Długość klucza początkowego

InitialKeyPtr
Wskaźnik do położenia w pamięci zawierającej klucz początkowy

InitialKeyOffset
Położenie klucza początkowego w pamięci, reprezentowane jako liczba bajtów od początku struktury MQCSP.

Uwaga: Można podać tylko jedną z wartości: **InitialKeyPtr** lub **InitialKeyOffset**.

Na przykład:

```
char * initialKey = "myInitialKey";
MQCSP  cspOptions = {MQCSP_DEFAULT};


cspOptions.InitialKeyPtr = initialKey;
cspOptions.InitialKeyLength = (MQLONG)strlen(cspOptions.InitialKeyPtr);
cspOptions.Version = MQCSP_VERSION_2;
```

Podawanie klucza początkowego za pomocą zmiennej środowiskowej MQS_MQI_KEYFILE

Jeśli klucz początkowy nie zostanie dostarczony do klienta przy użyciu struktury MQCSP, produkt IBM MQ sprawdza zmienną środowiskową *MQS_MQI_KEYFILE* . Tę zmienną środowiskową należy ustawić na położenie pliku zawierającego pojedynczy wiersz tekstu, składający się z klucza początkowego, który ma być używany.

Jeśli na przykład plik o nazwie `mykey.key` istnieje w katalogu głównym i zawiera klucz początkowy, należy ustawić zmienną środowiskową w następujący sposób:

```
export MQS_MQI_KEYFILE=/mykey.key
```

lub wersji

```
set MQS_MQI_KEYFILE=C:\mykey.key
```

Podawanie klucza początkowego przy użyciu pliku konfiguracyjnego klienta

Jeśli klucz początkowy nie został dostarczony do klienta przy użyciu poprzedniego mechanizmu, program IBM MQ sprawdza atrybut **MQIInitialKeyFile** w sekcji Security pliku `mqclient.ini` . Atrybut ten należy ustawić na położenie pliku zawierającego pojedynczy wiersz tekstu, składający się z klucza początkowego, który ma być używany.

Na przykład, jeśli plik o nazwie `mykey.key` istnieje w katalogu głównym i zawiera klucz początkowy, plik konfiguracyjny klienta powinien zawierać:

```
Security:
    MQIInitialKeyFile=/mykey.key
```

Pojęcia pokrewne

“Szyfrowanie haseł repozytorium kluczy w systemie IBM i” na stronie 295
Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może

je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

"Praca z protokołem SSL/TLS w systemie IBM i" na stronie 293
Ta kolekcja tematów zawiera instrukcje dotyczące poszczególnych zadań związanych z protokołem TLS (Transport Layer Security) w produkcie IBM MQ for IBM i.

Tworzenie ośrodka certyfikacji i certyfikatu na potrzeby testowania w systemie IBM i

Ta procedura służy do tworzenia certyfikatu lokalnego ośrodka CA do podpisywania żądań certyfikatów oraz do tworzenia i instalowania certyfikatu ośrodka CA.

Zanim rozpoczniesz

Instrukcje w tym temacie zakładają, że lokalny ośrodek certyfikacji (CA) nie istnieje. Jeśli lokalny ośrodek CA istnieje, przejdź do sekcji "Żądanie certyfikatu serwera w systemie IBM i" na stronie 304.

O tym zadaniu

Certyfikaty ośrodka CA, które są udostępniane podczas instalowania protokołu TLS, są podpisywane przez ośrodek CA, który je wystawiał. W systemie IBM imożna wygenerować lokalny ośrodek certyfikacji, który będzie mógł podpisywać certyfikaty serwera na potrzeby testowania komunikacji TLS w systemie. Aby utworzyć certyfikat lokalnego ośrodka CA, wykonaj następujące czynności w przeglądarce WWW:

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji "Uzyskiwanie dostępu do programu DCM" na stronie 294.
2. W panelu nawigacyjnym kliknij opcję **Create a Certificate Authority**(Utwórz ośrodek certyfikacji).

   W ramce zadania zostanie wyświetlona strona Tworzenie ośrodka certyfikacji (Create a Certificate Authority).
3. Wpisz hasło w polu **Certificate store password** (Hasło bazy certyfikatów) i wpisz je ponownie w polu **Confirm password** (Potwierdź hasło).
4. Wpisz nazwę w polu **Certificate Authority (CA) name** (Nazwa ośrodka CA), na przykład `TLS Test Certificate Authority`.
5. Wpisz odpowiednie wartości w polach **Nazwa zwykła** i **Organizacja** , a następnie wybierz kraj. W pozostałych polach opcjonalnych wpisz wymagane wartości.
6. W polu **Okres ważności** wpisz okres ważności dla lokalnego ośrodka CA.

   Wartością domyślną jest 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 ścieżkę do pliku tymczasowego, w którym ma być przechowywany certyfikat ośrodka CA, i 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 na podstawie typu certyfikatu** i kliknij przycisk **Dalej**.
14. Kliknij przycisk **Zakończ**.

    Zostanie wyświetlone okno z potwierdzeniem.

15. Kliknij przycisk **OK**.
16. W oknie Certyfikat kliknij przycisk **OK**.
17. Kliknij opcję **Continue**.

    W ramce zadań zostanie wyświetlona strona Strategia ośrodka certyfikacji (Certificate Authority Policy).
18. W polu **Zezwalaj na tworzenie certyfikatów użytkowników** wybierz opcję **Tak**.
19. W polu **Okres ważności** wpisz okres ważności certyfikatów wystawianych przez lokalny ośrodek CA.

    Wartością domyślną jest 365 dni.
20. Kliknij opcję **Continue**.

    W ramce zadania zostanie wyświetlona strona Tworzenie certyfikatu w nowej bazie certyfikatów.
21. Sprawdź, czy żadna z aplikacji nie została wybrana.
22. Kliknij przycisk **Kontynuuj** , aby zakończyć konfigurowanie lokalnego ośrodka CA.

Co dalej

Jeśli konieczne jest odnowienie istniejącego certyfikatu, należy zapoznać się z sekcją Odnawianie istniejącego certyfikatu w dokumentacji produktu IBM i .

Żądanie certyfikatu serwera w systemie IBM i

Certyfikaty cyfrowe chronią przed imitowaniem, poświadczając, że klucz publiczny należy do określonej jednostki. Nowy certyfikat 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 DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
3. Wybierz bazę certyfikatów, której chcesz użyć, i kliknij **Kontynuuj**(Continue).
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło składnicy systemu i 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, które zostały ustawione podczas tworzenia bazy certyfikatów. Wpisz również hasło w polu **Certificate Store Password** (Hasło bazy certyfikatów). Następnie kliknij przycisk **Kontynuuj** .
6. W panelu nawigacyjnym kliknij opcję **Create Certificate**(Utwórz certyfikat).
7. W ramce zadań wybierz przełącznik **Certyfikat serwera lub klienta** i kliknij przycisk **Kontynuuj**.

   W ramce zadania zostanie wyświetlona strona Wybór ośrodka certyfikacji (CA).
8. Jeśli na stacji roboczej znajduje się lokalny ośrodek certyfikacji (CA), do podpisania certyfikatu należy wybrać lokalny ośrodek certyfikacji (CA) lub komercyjny ośrodek certyfikacji (CA). Zaznacz przełącznik dla wybranego ośrodka CA i kliknij przycisk **Kontynuuj**.

   W ramce zadań zostanie wyświetlona strona Tworzenie certyfikatu (Create a Certificate).
9. Opcjonalne: W przypadku menedżera kolejek w polu **Etykieta certyfikatu** wprowadź etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli został ustawiony) lub wartością domyślną `ibmwebspheremq` z dodaną nazwą menedżera kolejek zapisaną małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Na przykład dla menedżera kolejek QM1wpisz `ibmwebspheremqqm1` , aby użyć wartości domyślnej.

10. Opcjonalne: W przypadku systemu IBM MQ MQI clientw polu **Certificate label** (Etykieta certyfikatu) wpisz `ibmwebspheremq` , a następnie ID użytkownika używany podczas logowania (małe litery). Wpisz na przykład: `ibmwebspheremqmyuserID`
11. Wpisz odpowiednie wartości w polach **Nazwa zwykła** i **Organizacja** , a następnie wybierz kraj. W pozostałych polach opcjonalnych wpisz wymagane wartości.

Wyniki

Jeśli do podpisania certyfikatu wybrano komercyjny ośrodek CA, program DCM utworzy żądanie certyfikatu w formacie PEM (Privacy-Enhanced Mail). Prześlij żądanie do wybranego ośrodka CA.

Jeśli do podpisania certyfikatu wybrano lokalny ośrodek CA, program DCM poinformuje, że certyfikat został utworzony w bazie certyfikatów i może być używany.

Żądanie certyfikatu serwera dla programu IBM Key Manager (Menedżer kluczy) w systemie IBM i

Poniższa procedura umożliwia utworzenie certyfikatu podpisanego przez lokalny ośrodek certyfikacji (CA) lub zastosowanie certyfikatu serwera podpisanego przez komercyjny ośrodek certyfikacji (CA) w celu zaimportowania do programu narzędziowego IBM Key Management (iKeyman).

O tym zadaniu

Certyfikat użytkownika musi być używany, gdy program Digital Certificate Manager (DCM) działa jako menedżer certyfikatów dla systemu IBM MQ na wielu platformach. W przypadku certyfikatów osobistych dystrybuowanych na inne platformy i importowanych do programu narzędziowego iKeyman wykonaj następujące kroki w przeglądarce WWW:

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W panelu **nawigacyjnym** kliknij opcję **Utwórz certyfikat**.

   W ramce zadań zostanie wyświetlona strona **Tworzenie certyfikatu** (Create Certificate).
3. Na panelu **Create Certificate** (Utwórz certyfikat) wybierz przełącznik **User certificate** (Certyfikat użytkownika) i kliknij przycisk **Continue**(Kontynuuj).

   Zostanie wyświetlona strona **Utwórz certyfikat użytkownika** .
4. Na panelu **Create User Certificate** (Utwórz certyfikat użytkownika) wypełnij wymagane pola w sekcji Certificate Information (Informacje o certyfikacie) dla **Organization name**(Nazwa organizacji), **State** lub **province**(Województwo), **Country** lub **region**(Region). Opcjonalnie można wprowadzić wartości w polach **Jednostka organizacyjna** i **Lokalizacja** lub **Miasto** . Kliknij opcję **Continue**.

   Nazwa zwykła jest automatycznie ustawiana na identyfikator użytkownika, który jest zalogowany w systemie iSeries .
5. Na następnym panelu **Create User Certificate** (Utwórz certyfikat użytkownika) kliknij opcję **Install certificate** (Zainstaluj certyfikat) i kliknij **Continue**(Kontynuuj).

   Zostanie wyświetlony komunikat `Certyfikat osobisty został zainstalowany. Należy zachować kopię zapasową tego certyfikatu.`
6. Kliknij przycisk **OK**.
7. W zależności od przeglądarki internetowej, której użyto do uzyskania dostępu do programu DCM, wykonaj następujące czynności:
   a) W przypadku przeglądarki Microsoft Edge wybierz: **Narzędzia > Opcje internetowe > Karta Treść > Przycisk Certyfikaty > Karta Osobiste >**. Wybierz certyfikat i kliknij opcję **Eksportuj**.
   b) W przeglądarce Mozilla Firefox wybierz kartę **Narzędzia > Opcje > Zaawansowane > Szyfrowanie > Wyświetl certyfikaty > Karta Certyfikaty użytkownika >**. Wybierz certyfikat i kliknij opcję **Backup**(Utwórz kopię zapasową). Wybierz ścieżkę i nazwę pliku, a następnie kliknij przycisk **OK**.

8. Prześlij wyeksportowany certyfikat do systemu zdalnego przy użyciu 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 przy użyciu programu Microsoft Edge, należy postępować zgodnie z instrukcjami zawartymi w sekcji Importowanie z pliku Microsoft `.pfx` .
   b) Jeśli certyfikat został zapisany w przeglądarce Mozilla Firefox, użyj 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 wartość oczekiwaną przez produkt IBM MQ . Etykieta musi być wartością atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` z dodaną nazwą menedżera kolejek (wszystkie te wartości muszą być zapisane 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 wysyła certyfikat jako część wiadomości e-mail, skopiuj certyfikat do osobnego pliku.

Uwaga:

- Nie trzeba wykonywać tej procedury, jeśli certyfikat serwera jest podpisany przez lokalny ośrodek CA.
- Przed zaimportowaniem certyfikatu serwera w formacie PKCS #12 do programu DCM należy najpierw zaimportować odpowiedni certyfikat ośrodka CA.

Aby pobrać certyfikat serwera do bazy certyfikatów menedżera kolejek, wykonaj następującą procedurę:

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W kategorii zadań **Manage Certificates** (Zarządzanie certyfikatami) na panelu nawigacyjnym kliknij opcję **Import Certificate**(Importuj certyfikat).

   W ramce zadań zostanie wyświetlona strona Importowanie certyfikatu.
3. Zaznacz przełącznik odpowiadający typowi certyfikatu i kliknij przycisk **Kontynuuj**.

   W ramce zadania zostanie wyświetlona strona Importowanie certyfikatu serwera lub klienta lub Importowanie certyfikatu ośrodka certyfikacji (CA).
4. W polu **Importuj plik** wpisz nazwę pliku certyfikatu, który ma zostać zaimportowany, i kliknij przycisk **Kontynuuj**.

   Program DCM automatycznie określa format pliku.
5. Jeśli certyfikat jest certyfikatem **serwera lub klienta** , wpisz hasło w ramce zadań i kliknij **Kontynuuj**(Continue).

   Program DCM informuje, że certyfikat został zaimportowany.

Eksportowanie certyfikatu z repozytorium kluczy w systemie IBM i

Wyeksportowanie certyfikatu powoduje wyeksportowanie zarówno klucza publicznego, jak i prywatnego. Działanie to powinno być podejmowane z zachowaniem szczególnej ostrożności, ponieważ przekazanie klucza prywatnego mogłoby całkowicie zagrozić bezpieczeństwu.

Zanim rozpoczniesz

Jeśli certyfikat użytkownika jest współużytkowany z innym użytkownikiem, klucze publiczne są wymieniane. Ten proces jest opisany w sekcji **Czynność 5. Współużytkowanie certyfikatów** w sekcji Współużytkowanie certyfikatów w pliku “Publikacja Szybki start dla produktu AMS w systemie AIX and Linux” na stronie 669. Podczas eksportowania certyfikatu zgodnie z opisem w tym miejscu eksportowany jest zarówno klucz publiczny, jak i klucz prywatny. Działanie to powinno być podejmowane z zachowaniem szczególnej ostrożności, ponieważ przekazanie klucza prywatnego mogłoby całkowicie zagrozić bezpieczeństwu.

O tym zadaniu

Wykonaj następujące kroki na komputerze, z którego chcesz wyeksportować certyfikat:

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
3. Wybierz bazę certyfikatów, której chcesz użyć, i kliknij **Kontynuuj**(Continue).
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło składnicy systemu i 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, które zostały ustawione podczas tworzenia bazy certyfikatów i wpisz hasło w polu **Hasło bazy certyfikatów** . Następnie kliknij przycisk **Kontynuuj** .
6. W kategorii zadania **Zarządzanie certyfikatami** w panelu nawigacyjnym kliknij opcję **Eksportuj certyfikat**.

   W ramce zadania zostanie wyświetlona strona Eksportowanie certyfikatu.
7. Zaznacz przełącznik odpowiadający typowi certyfikatu i kliknij przycisk **Kontynuuj**.

   W ramce zadania zostanie wyświetlona strona Eksportowanie certyfikatu serwera lub klienta lub Eksportowanie certyfikatu ośrodka certyfikacji (CA).
8. Wybierz certyfikat, który chcesz wyeksportować.
9. Zaznacz przełącznik, aby określić, czy chcesz wyeksportować certyfikat do pliku, czy bezpośrednio do innej bazy certyfikatów.
10. Jeśli wybrano eksportowanie certyfikatu serwera lub klienta do pliku, podaj następujące informacje:
    - Ścieżka i nazwa pliku, w którym ma zostać zapisany wyeksportowany certyfikat.
    - W przypadku certyfikatu osobistego jest to hasło używane do szyfrowania wyeksportowanego certyfikatu i wersji docelowej. W przypadku certyfikatów CA nie trzeba podawać hasła.
11. Jeśli wybrano eksportowanie certyfikatu bezpośrednio do innej bazy certyfikatów, podaj docelową bazę certyfikatów i jej hasło.
12. Kliknij opcję **Continue**.

Importowanie certyfikatu do repozytorium kluczy w systemie IBM i

Wykonaj tę procedurę, aby zaimportować certyfikat.

Zanim rozpoczniesz

Przed zaimportowaniem certyfikatu osobistego w formacie PKCS #12 do programu DCM należy najpierw zaimportować odpowiedni certyfikat ośrodka CA.

O tym zadaniu

Wykonaj następujące kroki na komputerze, na który chcesz zaimportować certyfikat.

Procedura

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
3. Wybierz bazę certyfikatów, której chcesz użyć, i kliknij **Kontynuuj**(Continue).
4. Opcjonalne: Jeśli w kroku 3 wybrano wartość ***SYSTEM** , wprowadź hasło składnicy systemu i 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, które zostały ustawione podczas tworzenia bazy certyfikatów i wpisz hasło w polu **Hasło bazy certyfikatów** . Następnie kliknij przycisk **Kontynuuj** .
6. W kategorii zadań **Manage Certificates** (Zarządzanie certyfikatami) na panelu nawigacyjnym kliknij opcję **Import Certificate**(Importuj certyfikat).

   W ramce zadania zostanie wyświetlona strona Importowanie certyfikatu.
7. Zaznacz przełącznik odpowiadający typowi certyfikatu i kliknij przycisk **Kontynuuj**.

   W ramce zadania zostanie wyświetlona strona Importowanie certyfikatu serwera lub klienta lub Importowanie certyfikatu ośrodka certyfikacji (CA).
8. W polu **Importuj plik** wpisz nazwę pliku certyfikatu, który ma zostać zaimportowany, i kliknij przycisk **Kontynuuj**.

   Program DCM automatycznie określa format pliku.
9. Jeśli certyfikat jest certyfikatem **serwera lub klienta** , wpisz hasło w ramce zadań i kliknij **Kontynuuj**(Continue). 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 DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów).

   W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
3. Zaznacz pole wyboru **Inna baza certyfikatów systemu** i kliknij przycisk **Kontynuuj**.

   Zostanie wyświetlona strona Baza certyfikatów i hasło.
4. W polu **Ścieżka i nazwa pliku bazy certyfikatów** wpisz ścieżkę i nazwę pliku IFS, które zostały ustawione podczas tworzenia bazy certyfikatów.
5. Wpisz hasło w polu **Certificate Store Password** (Hasło bazy certyfikatów). Kliknij opcję **Continue**.

   W ramce zadań zostanie wyświetlona strona Bieżąca baza certyfikatów.
6. W kategorii zadania **Zarządzanie certyfikatami** w 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 zamiar usunięcia certyfikatu. W przeciwnym razie kliknij opcję **Nie**.

   Program DCM informuje, czy certyfikat został usunięty.

*Korzystanie z bazy certyfikatów *SYSTEM do uwierzytelniania jednokierunkowego w systemie IBM i*

Wykonaj poniższe instrukcje, aby skonfigurować uwierzytelnianie jednokierunkowe.

Zanim rozpoczniesz

- Utwórz menedżer kolejek, kanały i kolejki transmisji.
- Utwórz certyfikat serwera lub klienta w menedżerze kolejek serwera.
- Prześlij certyfikat ośrodka CA do menedżera kolejek klienta i zaimportował go do repozytorium kluczy.
- Uruchom program nasłuchujący w menedżerach kolejek serwera i klienta.

O tym zadaniu

Aby użyć uwierzytelniania jednokierunkowego, na komputerze z systemem IBM i jako serwerem TLS, należy ustawić parametr repozytorium kluczy SSL (SSLKEYR) na wartość *SYSTEM. To ustawienie powoduje zarejestrowanie menedżera kolejek produktu IBM MQ jako aplikacji. Następnie można przypisać certyfikat do menedżera kolejek, aby włączyć uwierzytelnianie jednokierunkowe.

Za pomocą prywatnych magazynów kluczy można również zaimplementować uwierzytelnianie jednokierunkowe, tworząc fikcyjny certyfikat dla menedżera kolejek klienta w repozytorium kluczy.

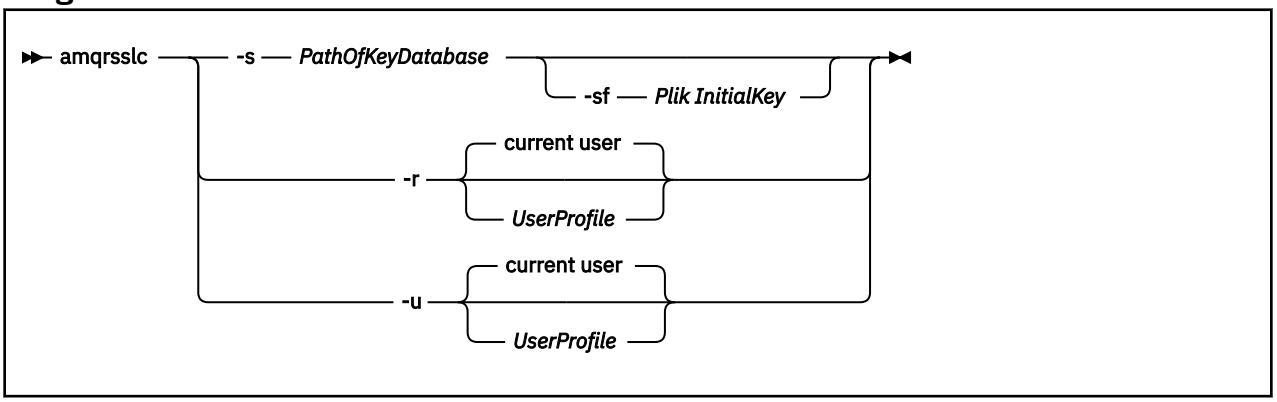
Procedura

1. Wykonaj następujące kroki na menedżerach kolejek serwera i klienta:
   a) Zmień menedżer kolejek, aby ustawić parametr SSLKEYR, wprowadzając komendę `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.
   b) Zeskładować hasło dla domyślnego repozytorium kluczy, wprowadzając komendę `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')`.
      Hasło musi być ujęte w pojedynczy cudzysłów.
   c) Zmień kanały tak, aby w parametrze SSLCIPHER była podana poprawna wartość CipherSpec .
   d) Odśwież zabezpieczenia TLS, wprowadzając 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 DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
   b) W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów).
      W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
   c) Wybierz bazę certyfikatów *SYSTEM i kliknij **Kontynuuj**(Continue).
   d) W panelu po lewej stronie rozwiń pozycję **Zarządzaj 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**(Update Certificate Assignment).
   g) Wybierz opcję **Serwer** i kliknij przycisk **Kontynuuj**.
   h) Wybierz QMGRNAME (WMQ) i kliknij opcję **Aktualizuj przypisanie certyfikatu**.
   i) Wybierz certyfikat i kliknij **Przypisz nowy certyfikat**. Zostanie wyświetlone okno informujące, że certyfikat został przypisany do aplikacji.

IBM MQ Program narzędziowy klienta SSL (amqrsslc) dla systemu IBM i

Program narzędziowy klienta SSL IBM MQ (amqrsslc) dla systemu IBM i jest używany przez serwer IBM MQ MQI client w systemach IBM i do rejestrowania lub wyrejestrowywania profilu użytkownika klienta lub do ukrywania hasła bazy certyfikatów. Program narzędziowy może być uruchamiany tylko przez użytkownika z profilem z uprawnieniem specjalnym *ALLOBJ lub przez członka grupy QMQMADM, który ma możliwość tworzenia lub usuwania rejestracji aplikacji w programie Digital Certificate Manager (DCM).

Diagram składni



Zarejestruj profil użytkownika klienta

Jeśli IBM MQ MQI client używa bazy certyfikatów *SYSTEM, należy zarejestrować profil użytkownika klienta (zalogowanego użytkownika) w celu użycia go jako aplikacji w programie Digital Certificate Manager (DCM).

Aby zarejestrować profil użytkownika klienta, uruchom program **amqrsslc** z opcją `-r` z opcją *UserProfile*. Profil użytkownika używany podczas wywoływania systemu **amqrsslc** musi mieć uprawnienie *USE. Podanie opcji *UserProfile* z opcją `-r` powoduje zarejestrowanie *UserProfile* jako aplikacji serwera z unikalną etykietą aplikacji QIBM_WEBSPHERE_MQ_*UserProfile* oraz etykietą z opisem *UserProfile* (WMQ). Aplikacja serwera jest następnie wyświetlana w programie DCM i można przypisać do niej dowolny certyfikat serwera lub klienta w bazie danych systemu.

Uwaga: Jeśli profil użytkownika nie zostanie podany z opcją `-r` , zostanie zarejestrowany profil użytkownika uruchamiającego narzędzie **amqrsslc** .

W poniższym kodzie do zarejestrowania profilu użytkownika używany jest kod **amqrsslc** . W pierwszym przykładzie rejestrowany jest określony profil użytkownika, a w drugim profil zalogowanego użytkownika:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

Wyrejestruj profil użytkownika klienta

Aby wyrejestrować profil klienta, uruchom program **amqrsslc** z opcją `-u` z opcją *UserProfile*. Profil użytkownika używany podczas wywoływania systemu **amqrsslc** musi mieć uprawnienie *USE. Podanie wartości *UserProfile* z opcją `-u` powoduje wyrejestrowanie profilu *UserProfile* z etykietą QIBM_WEBSPHERE_MQ_*UserProfile* z programu DCM.

Uwaga: Jeśli profil użytkownika nie zostanie podany z opcją `-u` , profil użytkownika uruchamiającego narzędzie **amqrsslc** zostanie wyrejestrowany.

W poniższym kodzie użyto komendy **amqrsslc** do wyrejestrowania profilu użytkownika. W pierwszym przykładzie określony profil użytkownika jest wyrejestrowany, a w drugim profil zalogowanego użytkownika:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Zeskładuj hasło bazy certyfikatów

Jeśli IBM MQ MQI client nie korzysta z bazy certyfikatów *SYSTEM i korzysta z innej bazy certyfikatów (wartość MQSSLKEYR jest inna niż *SYSTEM), hasło bazy danych kluczy można schować tak, aby nie było konieczne jego określenie przez aplikację kliencką podczas uruchamiania systemu.

Użyj opcji `-s` , aby ukryć hasło bazy danych kluczy. V 9.3.0 Podaj pełną ścieżkę i nazwę bazy danych kluczy. Jeśli rozszerzenie nazwy pliku nie zostanie podane, przyjmuje się, że jest to rozszerzenie `.kdb`.

W poniższym kodzie pełna nazwa pliku bazy certyfikatów to `/Path/Of/KeyDatabase/MyKey.kdb`:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

Uruchomienie tego kodu spowoduje wysłanie żądania hasła do tej bazy danych kluczy. To hasło jest przechowywane w pliku o takiej samej nazwie jak baza danych kluczy z rozszerzeniem `.sth` .

V 9.3.0 Dodatkowo można określić klucz początkowy do zaszyfrowania hasła. Klucz początkowy powinien być przechowywany w pliku jako pojedynczy wiersz tekstu, a następnie położenie tego pliku jest dostarczane do programu za pomocą opcji **`-sf`** . Jeśli nie zostanie podany początkowy plik kluczy, do zaszyfrowania hasła zostanie użyty klucz domyślny.

Plik ukrytych haseł 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 jest właścicielem grupy dla tego zbioru. QMQM i QMQMADM mają uprawnienia do odczytu, zapisu, a inne profile mają tylko uprawnienia do odczytu.

Gdy zmiany w certyfikatach lub w bazie certyfikatów zaczną obowiązywać w dniu IBM i

Po zmianie certyfikatów w bazie certyfikatów lub lokalizacji bazy certyfikatów zmiany są uwzględniane w zależności od typu kanału i sposobu jego działania.

Zmiany certyfikatów w bazie certyfikatów i w atrybucie repozytorium kluczy zaczynają obowiązywać w następujących sytuacjach:

- Gdy nowy wychodzący proces pojedynczego kanału po raz pierwszy uruchamia kanał TLS.
- Gdy nowy przychodzący proces pojedynczego kanału TCP/IP po raz pierwszy otrzyma żądanie uruchomienia kanału TLS.
- Po wydaniu komendy MQSC REFRESH SECURITY TYPE (SSL) w celu odświeżenia środowiska TLS produktu IBM MQ .
- W przypadku procesów aplikacji klienckiej, gdy ostatnie połączenie TLS w procesie jest zamknięte. Następne połączenie TLS pobierze zmiany certyfikatu.
- Dla kanałów, które działają jako wątki procesu zestawiania procesów (amqrmppa), gdy proces zestawiania procesów jest uruchamiany lub restartowany i po raz pierwszy uruchamia kanał TLS. Jeśli proces zestawiania procesów już uruchomił kanał TLS, a zmiana ma zostać natychmiast uwzględniona, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- Dla kanałów, które działają jako wątki inicjatora kanału, gdy inicjator kanału jest uruchamiany lub restartowany i najpierw uruchamia kanał TLS. Jeśli proces inicjatora kanału uruchomił już kanał TLS, a zmiana ma zostać natychmiast uwzględniona, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- Dla kanałów, które działają jako wątki programu nasłuchującego TCP/IP, gdy program nasłuchujący jest uruchamiany lub restartowany i najpierw otrzymuje żądanie uruchomienia kanału TLS. Jeśli program nasłuchujący już uruchomił kanał TLS i chcesz, aby zmiany zostały uwzględnione natychmiast, 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 umożliwić skonfigurowanie sprzętu 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 żądaniem podania nazwy użytkownika i hasła.
2. Wpisz poprawny profil użytkownika IBM i i hasło.
3. Przejdź do sekcji Kryptografia i skorzystaj z odpowiednich odsyłaczy, aby uzyskać więcej informacji.

Co dalej

Bardziej szczegółowe informacje na temat konfigurowania koprocesora szyfrującego 4767 Cryptographic Coprocessorzawiera sekcja 4767 Cryptographic Coprocessor.

ALW Praca z protokołem SSL/TLS w systemie AIX, Linux, and Windows

W systemach AIX, Linux, and Windows obsługa protokołu TLS (Transport Layer Security) jest instalowana z produktem IBM MQ.

Więcej szczegółowych informacji na temat strategii sprawdzania poprawności certyfikatów zawiera sekcja Sprawdzanie poprawności certyfikatów i projektowanie zaufanych strategii.

ALW *Używanie komend runmqckm, runmqakm i strmqikm do zarządzania certyfikatami cyfrowymi*

W systemach AIX, Linux, and Windows można zarządzać kluczami i certyfikatami cyfrowymi za pomocą programu **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub wiersza komend za pomocą komendy **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

Uwaga: V 9.3.4 Deprecated Obsługa magazynu kluczy CMS dla aplikacji IBM MQ Java , AMQP i MQTT jest nieaktualna od wersji IBM MQ 9.3.4. Jeśli magazyn kluczy CMS jest używany z aplikacjami IBM MQ Java , AMQP i MQTT, należy przeprowadzić migrację do obsługi repozytorium kluczy PKCS#12 zwolnionego w wersji IBM MQ 9.3.0.

Narzędzia **runmqckm**, **strmqikm**, **mqiptKeycmd** i **mqiptKeyman** są również nieaktualne. Komenda **runmqakm** z katalogu IBM MQ i komenda **keytool** ze środowiska JRE są dostępne jako alternatywa.

Ostrzeżenie: Zarówno komendy **runmqckm** , jak i **strmqikm** zależą od środowiska IBM MQ Java Runtime Environment (JRE). Jeśli środowisko JRE nie jest zainstalowane w systemie IBM MQ 9.1, zostanie wyświetlony komunikat AMQ9183.

- Linux AIX W systemach **AIX and Linux** :
  - Użyj komendy **strmqikm** (iKeyman), aby uruchomić interfejs GUI iKeyman .
  - Komenda **runmqckm** służy do wykonywania zadań w interfejsie wiersza komend.
  - Użyj komendy **runmqakm** (GSKCapiCmd), aby wykonać zadania za pomocą interfejsu wiersza komend runmqakm. Składnia komendy **runmqakm** jest taka sama jak składnia komendy **runmqckm**.

    Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend **runmqckm** lub **strmqikm** .

  Pełny opis interfejsów wiersza komend dla komend **runmqckm** i **runmqakm** zawiera sekcja Zarządzanie kluczami i certyfikatami .

  Jeśli używane są certyfikaty lub klucze przechowywane na sprzęcie szyfrującym PKCS #11 , należy pamiętać, że programy **runmqckm** 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 na tych platformach programy iKeyman i **runmqckm** są 32-bitowe.

  Więcej informacji na ten temat zawiera sekcja IBM Global Security Kit (GSKit): PKCS#11 i IBM MQ tryb adresowania JRE .

Przed uruchomieniem komendy **strmqikm** w celu uruchomienia interfejsu GUI iKeyman upewnij się, że pracujesz na komputerze, który może uruchomić system X Window, i wykonaj następujące czynności:

- Ustaw zmienną środowiskową DISPLAY, na przykład:

```
export DISPLAY=mypc:0
```

- Upewnij się, że zmienna środowiskowa PATH zawiera ścieżki **/usr/bin** i **/bin**. Jest to również wymagane dla komend **runmqckm** i **runmqakm** . Na przykład:

```
export PATH=$PATH:/usr/bin:/bin
```

- Windows W systemach **Windows** :
  - Użyj komendy **strmqikm** , aby uruchomić interfejs GUI programu iKeyman .
  - Komenda **runmqckm** służy do wykonywania zadań w interfejsie wiersza komend.

    Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komend **runmqckm** lub **strmqikm** .
  - Użyj komendy **runmqakm -keydb** z opcją *stashpw* lub *stash* .

    Jeśli komenda **runmqakm -keydb** jest używana w ten sposób, na przykład:

```
runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
```

    Wynikowy plik `.sth` nie ma włączonego uprawnienia do odczytu dla grupy `mqm` .

    Tylko twórca może odczytać plik. Po utworzeniu pliku zeskładowanego za pomocą komendy **runmqakm** należy sprawdzić uprawnienia do pliku i nadać uprawnienie do konta usługi, na którym działa menedżer kolejek, lub do grupy, takiej jak lokalna grupa `mqm`.

ALW Aby zażądać śledzenia TLS w systemach AIX, Linux, and Windows , patrz strmqtrc.

Odsyłacze pokrewne

“Komendy runmqckm i runmqakm w systemie AIX, Linux, and Windows” na stronie 594
W tej sekcji opisano komendy **runmqckm** i **runmqakm** zgodnie z ich obiektem.

ALW *Konfigurowanie repozytorium kluczy w systemie AIX, Linux, and Windows*

Repozytorium kluczy można skonfigurować za pomocą programu narzędziowego **strmqikm** (iKeyman) Interfejs GUI lub z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

Zanim rozpoczniesz

Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Przed utworzeniem magazynu kluczy należy przejrzeć opcje udostępniane przez produkt IBM MQ w celu bezpiecznego przechowywania hasła repozytorium kluczy. Więcej informacji na ten temat zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316.

Uwaga: V 9.3.4 Deprecated Obsługa magazynu kluczy CMS dla aplikacji IBM MQ Java , AMQP i MQTT jest nieaktualna od wersji IBM MQ 9.3.4. Jeśli magazyn kluczy CMS jest używany z aplikacjami IBM MQ Java , AMQP i MQTT, należy przeprowadzić migrację do obsługi repozytorium kluczy PKCS#12 zwolnionego w wersji IBM MQ 9.3.0.

Narzędzia **runmqckm**, **strmqikm**, **mqiptKeycmd** i **mqiptKeyman** są również nieaktualne. Komenda **runmqakm** z katalogu IBM MQ i komenda **keytool** ze środowiska JRE są dostępne jako alternatywa.

O tym zadaniu

Połączenie TLS wymaga *repozytorium kluczy* na każdym końcu połączenia. Każdy menedżer kolejek systemu IBM MQ i program 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 AIX, Linux, and Windows certyfikaty cyfrowe są przechowywane w pliku bazy danych kluczy, który jest zarządzany za pomocą interfejsu użytkownika **strmqikm** lub za pomocą komend **runmqckm** lub **runmqakm** . Te certyfikaty cyfrowe mają etykiety. Konkretna etykieta wiąże certyfikat osobisty z menedżerem kolejek lub programem IBM MQ MQI client. Protokół TLS używa tego certyfikatu do celów uwierzytelniania. W systemach AIX, Linux, and Windows program IBM MQ używa albo wartości atrybutu **CERTLABL** , jeśli jest ustawiony, albo domyślnej wartości `ibmwebspheremq` z dodaną nazwą menedżera kolejek lub identyfikatorem logowania użytkownika IBM MQ MQI client (wszystkie te wartości są zapisane małymi literami). Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Nazwa pliku bazy danych kluczy składa się ze ścieżki i nazwy rdzenia:

- W systemach AIX and Linux domyślna ścieżka dla menedżera kolejek (ustawiana podczas tworzenia menedżera kolejek) to `/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`* jest katalogiem, w którym zainstalowano produkt IBM MQ . Na przykład `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl`.

  V 9.3.0 Domyślna nazwa pliku to `key.kdb`. Opcjonalnie można użyć własnej ścieżki i nazwy pliku.

  Jeśli zostanie wybrana własna ścieżka lub nazwa pliku, należy ustawić uprawnienia do tego pliku tak, aby dostęp do niego był ściśle kontrolowany.

- V 9.3.0 Dla klienta IBM MQ nie ma domyślnej ścieżki ani nazwy pliku. Ściśle kontrolują dostęp do tego pliku.

Nie należy tworzyć repozytoriów kluczy w systemie plików, który nie obsługuje blokad na poziomie plików, na przykład NFS wersja 2 w systemach Linux .

Informacje na temat sprawdzania i określania nazwy pliku bazy danych kluczy zawiera sekcja "Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows" na stronie 320 . Nazwę zbioru bazy danych kluczy można określić przed utworzeniem zbioru bazy danych kluczy lub po jego utworzeniu.

ID użytkownika, z którego uruchamiane są komendy **strmqikm** lub **runmqckm** , musi mieć uprawnienie do zapisu w katalogu, w którym plik bazy danych kluczy jest tworzony lub aktualizowany. W przypadku menedżera kolejek używającego domyślnego katalogu `ssl` ID użytkownika, z którego uruchamiany jest produkt **strmqikm** lub **runmqckm** , musi być członkiem grupy mqm. W przypadku systemu IBM MQ MQI client, jeśli program **strmqikm** lub **runmqckm** jest uruchamiany z ID użytkownika innego niż ten, z którego uruchamiany jest klient, należy zmienić uprawnienia do pliku, aby umożliwić programowi IBM MQ MQI client dostęp do pliku bazy danych kluczy w czasie wykonywania. Więcej informacji na ten temat zawiera sekcja "Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemie Windows" na stronie 318 lub "Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemach AIX and Linux" na stronie 318.

W produkcie **strmqikm** lub **runmqckm** for IBM Global Security Kit (GSKit) w wersji 7.0nowe bazy danych kluczy są automatycznie zapełniane zestawem predefiniowanych certyfikatów ośrodka certyfikacji (CA). W produkcie **strmqikm** lub **runmqckm** for GSKit 8.0bazy danych kluczy nie są automatycznie zapełniane, co powoduje, że początkowa konfiguracja jest bezpieczniejsza, ponieważ w pliku bazy danych kluczy uwzględniane są tylko żądane certyfikaty ośrodka CA.

Uwaga: Ponieważ ta zmiana zachowania programu GSKit 8.0 powoduje, że certyfikaty ośrodka CA nie są już automatycznie dodawane do repozytorium, należy ręcznie dodać preferowane certyfikaty ośrodka CA. Ta zmiana zachowania zapewnia bardziej szczegółową kontrolę nad używanymi certyfikatami CA. Patrz "Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy w systemie AIX, Linux, and Windows z systemem GSKit 8.0" na stronie 319.

Bazę danych kluczy można utworzyć za pomocą wiersza komend lub interfejsu użytkownika **strmqikm** (iKeyman).

Uwaga: Jeśli konieczne jest zarządzanie certyfikatami TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** . Interfejs użytkownika **strmqikm** nie udostępnia opcji zgodnych ze standardem FIPS.

Procedura

Utwórz bazę danych kluczy przy użyciu wiersza komend.

1. Uruchom jedną z następujących komend:

   - W systemie **runmqckm**:

     V 9.3.0 V 9.3.0

     ```
     runmqckm -keydb -create -db filename -pw password -type cms | p12 -stash
     ```

   - W systemie **runmqakm**:

     V 9.3.0 V 9.3.0

     ```
     runmqakm -keydb -create -db filename -pw password -type cms | p12
     -stash -fips -strong
     ```

   gdzie:

   -db *nazwa_pliku*
   Określa pełną nazwę pliku bazy danych kluczy CMS.

   -pw *hasło*

   Określa hasło do bazy danych kluczy CMS V 9.3.0 V 9.3.0 lub PKCS#12 .

   V 9.3.0 V 9.3.0 **-type *cms | p12***
   Określa typ bazy danych. (W przypadku systemu IBM MQmusi to być `cms` lub `pkcs12`).

   -stash

   V 9.3.0 V 9.3.0 Opcjonalne. Powoduje zapisanie hasła bazy danych kluczy w pliku. Podaj tę opcję, aby zapisać hasło bazy danych kluczy w pliku ukrytych haseł. Nie ma potrzeby przechowywania hasła w pliku ukrytych haseł, jeśli hasło jest szyfrowane za pomocą systemu IBM MQ zabezpieczającego hasłem.

   -fips,
   określa, że komenda jest uruchamiana w trybie FIPS. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

   -silne
   Sprawdza, czy wprowadzone hasło spełnia minimalne wymagania dotyczące mocy hasła. Minimalne wymagania dotyczące hasła są następujące:

   - Hasło musi mieć co najmniej 14 znaków długości.
   - Hasło musi zawierać co najmniej jedną małą literę, jedną wielką literę i jedną cyfrę lub znak specjalny. Znaki specjalne to gwiazdka (*), znak dolara ($), znak numeru (#) i znak procentu (%). Spacja jest klasyfikowana jako znak specjalny.
   - Każdy znak może wystąpić maksymalnie trzy razy w haśle.
   - Maksymalnie dwa kolejne znaki w haśle mogą być identyczne.
   - Wszystkie znaki znajdują się w standardowym drukowalnym zestawie znaków ASCII z zakresu 0x20 - 0x7E.

Alternatywnie można utworzyć bazę danych kluczy za pomocą interfejsu użytkownika **strmqikm** (iKeyman).

2. W systemach AIX and Linux zaloguj się jako użytkownik root. W systemach Windows zaloguj się jako administrator lub 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 **Typ bazy danych kluczy** i wybierz opcję **CMS** (Certificate Management System) V 9.3.0 V 9.3.0 lub **PKCS#12**.
6. W polu **Nazwa pliku** wpisz nazwę pliku.

   To pole zawiera już tekst `key.kdb` V 9.3.0 V 9.3.0 lub `key.p12`. Jeśli nazwą rdzenia jest `key`, należy pozostawić to pole bez zmian. Jeśli podano inną nazwę rdzenia, należy zastąpić łańcuch `key` nazwą rdzenia. .
7. W polu **Położenie** wpisz ścieżkę.

   Na przykład:

   - Dla menedżera kolejek: `/var/mqm/qmgrs/QM1/ssl` (w systemach AIX and Linux) lub `C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (w systemach Windows).

     Ścieżka musi być zgodna z wartością atrybutu **SSLKeyRepository** menedżera kolejek.
   - Dla klienta systemu IBM MQ : `/var/mqm/ssl` (w systemach AIX and Linux) lub `C:\mqm\ssl` (w systemach Windows).
8. Kliknij przycisk **OK**.

   Zostanie wyświetlone okno Podaj hasło.
9. Wpisz hasło w polu **Hasło** , a następnie wpisz je ponownie w polu **Potwierdź hasło** .
10. V 9.3.0

    Opcjonalne: Aby zapisać hasło bazy danych kluczy w pliku, zaznacz pole wyboru **Zapisz hasło w pliku** .

    Podaj tę opcję, aby zapisać hasło bazy danych kluczy w pliku ukrytych haseł. Nie ma potrzeby przechowywania hasła w pliku ukrytych haseł, jeśli hasło jest szyfrowane za pomocą systemu IBM MQ zabezpieczającego hasłem.
11. Kliknij przycisk **OK**.

    Zostanie wyświetlone okno Certyfikaty osobiste.
12. Ustaw uprawnienia dostępu zgodnie z opisem w sekcji “Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemie Windows” na stronie 318 lub “Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemach AIX and Linux” na stronie 318.
13. V 9.3.0

    Jeśli nie jest używany plik ukrytych haseł, należy podać hasło magazynu kluczy dla menedżera kolejek lub aplikacji klienckiej, postępując zgodnie z instrukcjami zawartymi w sekcji “Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows” na stronie 321 lub “Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323.

V 9.3.0 ALW V 9.3.0 *Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows*

Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

Następujące komponenty i opcje produktu IBM MQ obsługują dwie różne metody przechowywania haseł repozytorium kluczy:

- Repozytorium kluczy TLS menedżera kolejek.

- IBM MQ MQI clients , które używają protokołu TLS.
- V 9.3.2 Rodzima konfiguracja wysokiej dostępności w sekcji **NativeHALocalInstance** pliku `qm.ini` .
- V 9.3.4 Konfiguracja uwierzytelniania tokenu w sekcji **AuthToken** pliku `qm.ini` .

Hasła repozytorium kluczy używane przez te komponenty mogą być szyfrowane i zapisywane przy użyciu jednej z następujących metod:

System zabezpieczenia hasłem IBM MQ .

Każdy komponent IBM MQ udostępnia komendę do zaszyfrowania hasła repozytorium kluczy. Zaszyfrowana komenda, której dane wyjściowe są przechowywane w pliku.

W przypadku repozytorium kluczy TLS menedżera kolejek hasło jest szyfrowane po ustawieniu atrybutu menedżera kolejek produktu **SSLKEYRPWD** .

Hasło jest szyfrowane przy użyciu algorytmu AES-128 . Szczegóły tego algorytmu są publicznie znane i uważane za bezpieczne.

Hasło jest przechowywane w formacie zastrzeżonym, który nie jest zrozumiały dla innego oprogramowania, które może uzyskać dostęp do repozytorium kluczy.

Hasło zaszyfrowane przez jeden komponent IBM MQ nie może być używane przez inny komponent IBM MQ .

Unikalny klucz szyfrowania można podać, gdy hasło repozytorium kluczy jest zaszyfrowane. Unikalny klucz szyfrowania uniemożliwia osobie, która nie ma dostępu do klucza szyfrowania, deszyfrowanie hasła.

Hasło repozytorium kluczy w postaci jawnej jest wymagane do zarządzania certyfikatami znajdującymi się w repozytorium kluczy. Oprócz szyfrowania hasła repozytorium kluczy za pomocą systemu zabezpieczenia hasłem IBM MQ , należy również zapisać hasło repozytorium kluczy w bezpiecznym miejscu, w którym można uzyskać do niego dostęp w tym celu.

Więcej informacji na temat systemu zabezpieczenia hasłem IBM MQ zawiera sekcja “Ochrona haseł w plikach konfiguracyjnych komponentu IBM MQ” na stronie 617.

Plik ukrytych haseł repozytorium kluczy.

Komendy **runmqakm** i **runmqckm** mogą przechowywać hasło repozytorium kluczy w pliku ukrytych haseł.

Hasło jest szyfrowane przy użyciu zastrzeżonej metody specyficznej dla IBM MQ dostawcy usług kryptograficznych IBM Global Security Kit (GSKit).

Nie można podać unikalnego klucza szyfrowania.

Zaszyfrowane hasło jest przechowywane w pliku ukrytych haseł w tym samym katalogu, co plik repozytorium kluczy.

Każdy, kto ma prawo do odczytu zarówno repozytorium kluczy, jak i pliku ukrytych haseł, może uzyskać dostęp do treści repozytorium kluczy i zarządzać nią.

Niezależnie od wybranej metody szyfrowania hasła repozytorium kluczy należy pamiętać o ograniczeniach związanych z szyfrowaniem zapisanych haseł. Więcej informacji na ten temat zawiera “Ograniczenia ochrony przez szyfrowanie haseł” na stronie 625.

Pojęcia pokrewne

“Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows” na stronie 321

Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

“Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

“Praca z protokołem SSL/TLS w systemie AIX, Linux, and Windows” na stronie 312
W systemach AIX, Linux, and Windows obsługa protokołu TLS (Transport Layer Security) jest instalowana z produktem IBM MQ.

Windows *Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemie Windows*
Pliki bazy danych kluczy mogą nie mieć odpowiednich uprawnień dostępu. Należy ustawić odpowiednie prawa dostępu do tych plików.

Ustaw prawa dostępu do plików V 9.3.0 V 9.3.0 *key*.p12, *key*.kdb, *key*.sth, *key*.crli *key*.rdb, gdzie *klucz* jest nazwą rdzenia bazy danych kluczy, aby nadać uprawnienia do ograniczonego zbioru użytkowników.

V 9.3.0 V 9.3.0 Jeśli użyto innego rozszerzenia repozytorium kluczy niż .p12 lub .kdb, należy również upewnić się, że uprawnienia do tego pliku zostały ustawione.

Rozważ przyznanie dostępu w następujący sposób:

pełne uprawnienia
BUILTIN\Administrators, NT AUTHORITY\SYSTEM i użytkownik, który utworzył zbiory bazy danych.

uprawnienie do odczytu
W przypadku menedżera kolejek tylko lokalna grupa mqm. Zakłada się, że agent MCA działa z identyfikatorem użytkownika w grupie mqm.

W przypadku klienta jest to identyfikator użytkownika, który uruchomiła proces klienta.

Linux AIX *Uzyskiwanie dostępu do plików bazy danych kluczy i zabezpieczanie ich w systemach AIX and Linux*
Pliki bazy danych kluczy mogą nie mieć odpowiednich uprawnień dostępu. Należy ustawić odpowiednie prawa dostępu do tych plików.

W przypadku menedżera kolejek należy ustawić uprawnienia do plików bazy danych kluczy, aby menedżer kolejek i procesy kanału mogły je odczytywać w razie potrzeby, ale inni użytkownicy nie mogą ich odczytywać ani modyfikować. Zwykle użytkownik mqm wymaga uprawnień do odczytu. Jeśli plik bazy danych kluczy został utworzony przez zalogowanie się jako użytkownik mqm, uprawnienia są prawdopodobnie wystarczające. Jeśli użytkownik nie jest użytkownikiem mqm, ale jest innym użytkownikiem 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, aby procesy aplikacji klienckiej mogły je odczytywać w razie potrzeby, ale inni użytkownicy nie mogą ich odczytywać ani modyfikować. Zwykle użytkownik, który uruchomił proces klienta, musi mieć uprawnienia do odczytu. Jeśli plik bazy danych kluczy został utworzony przez zalogowanie się jako ten użytkownik, uprawnienia są prawdopodobnie wystarczające. Jeśli nie jesteś użytkownikiem procesu klienta, ale innym użytkownikiem w tej grupie, prawdopodobnie musisz nadać uprawnienia do odczytu innym użytkownikom w tej grupie.

Ustaw uprawnienia do plików V 9.3.0 V 9.3.0 *key*.p12, *key*.kdb, *key*.sth, *key*.crli *key*.rdb, gdzie *klucz* jest nazwą rdzenia bazy danych kluczy, na read i write dla właściciela pliku oraz na read dla grupy mqm lub grupy użytkownika klienta (-rw-r -----).

V 9.3.0 V 9.3.0 Jeśli użyto innego rozszerzenia repozytorium kluczy niż .p12 lub .kdb, należy również upewnić się, że uprawnienia do tego pliku zostały ustawione.

ALW *Dodawanie domyślnych certyfikatów CA do pustego repozytorium kluczy w systemie AIX, Linux, and Windows z systemem GSKit 8.0*

Aby dodać jeden lub więcej domyślnych certyfikatów ośrodka CA do pustego repozytorium kluczy w produkcie IBM Global Security Kit (GSKit) w wersji 8.0, należy wykonać poniższą procedurę.

W programie GSKit 7.0podczas tworzenia nowego repozytorium kluczy zachowanie polegało na automatycznym dodaniu zestawu domyślnych certyfikatów CA dla powszechnie używanych ośrodków certyfikacji. W systemie GSKit 8.0zachowanie to uległo zmianie, dzięki czemu certyfikaty ośrodka CA nie są już automatycznie dodawane do repozytorium. Użytkownik musi teraz ręcznie dodać certyfikaty ośrodka 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 AIX, 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** (System zarządzania certyfikatami) V 9.3.0 V 9.3.0 lub PKCS#12.
4. Kliknij przycisk **Browse** (Przeglądaj), aby przejść do katalogu zawierającego pliki bazy danych kluczy.
5. Wybierz plik bazy danych kluczy, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij opcję **Open** (Otwórz). Zostanie otwarte okno Password Prompt (Zapytanie o hasło).
7. Wpisz hasło ustawione podczas tworzenia bazy danych kluczy i kliknij przycisk **OK**. Nazwa pliku bazy danych kluczy zostanie wyświetlona w polu **File Name** (Nazwa pliku).
8. W polu **Key database content** (Zawartość bazy danych kluczy) wybierz opcję **Signer Certificates** (Certyfikaty osoby podpisującej).
9. Kliknij przycisk **Zapełnij**. Zostanie otwarte okno Add CA's Certificate (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 CA.
11. Wybierz z listy certyfikaty ośrodka CA, którym chcesz ufać, i kliknij **OK**. Certyfikaty są dodawane do repozytorium kluczy.

Za pomocą wiersza komend

Użyj następujących komend, aby wyświetlić, a następnie dodać certyfikaty ośrodka CA za pomocą komendy **runmqckm**:

- Wydaj następującą komendę, aby wyświetlić listę domyślnych certyfikatów CA wraz z wydającymi je organizacjami:

```
runmqckm -cert -listsigners
```

- Wykonaj 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 wszystkim certyfikatom osobistym podpisanym przez ten ośrodek CA. Należy dokładnie rozważyć, które ośrodki certyfikacji mają być zaufane i dodać tylko zestaw certyfikatów ośrodka certyfikacji (CA) potrzebnych do uwierzytelniania klientów i menedżerów. Nie zaleca się dodawania pełnego zestawu domyślnych certyfikatów ośrodka CA, chyba że jest to ostateczne wymaganie strategii bezpieczeństwa.

ALW *Znajdowanie repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows*

Użyj tej procedury, aby uzyskać położenie pliku bazy danych kluczy menedżera kolejek

Procedura

1. Wyświetl atrybuty menedżera kolejek za pomocą 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 pod kątem ścieżki i nazwy rdzenia zbioru bazy danych kluczy. Na przykład składnia
   a. w systemie AIX 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 wysokiego poziomu, w którym jest zainstalowany produkt IBM MQ .

   Uwaga: V 9.3.0 V 9.3.0 W systemie IBM MQ 9.3.0 pole SSLKEYR obsługuje zarówno pełną nazwę pliku (wraz z rozszerzeniem), jak i nazwę rdzenia (bez rozszerzenia). Jeśli nazwa rdzenia jest ustawiona, IBM MQ automatycznie dołącza `.kdb` i używa tego repozytorium kluczy.

ALW *Zmiana położenia repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows*

Położenie pliku bazy danych kluczy menedżera kolejek można zmienić w różny sposób, w tym za pomocą komendy MQSC ALTER QMGR.

Położenie pliku bazy danych kluczy menedżera kolejek można zmienić za pomocą komendy MQSC ALTER QMGR w celu ustawienia atrybutu repozytorium kluczy menedżera kolejek. Na przykład w systemie AIX and Linux:

V 9.3.0 V 9.3.0
```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey.kdb')
```

W systemie Windows:

V 9.3.0 V 9.3.0
```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb')
```

Plik bazy danych kluczy ma pełną nazwę: `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb`

V 9.3.0 V 9.3.0

Ostrzeżenie: W systemach Windows i Linux, jeśli używane są kanały TLS AMQP, przyrostek pliku repozytorium kluczy musi mieć jedną z następujących wartości:

- `.kdb`dla repozytorium kluczy CMS
- `.p12` lub `.pkcs12`dla repozytorium kluczy PKCS #12 .

Atrybuty menedżera kolejek można również zmieniać przy użyciu komend programu IBM MQ Explorer lub PCF.

Po zmianie położenia pliku bazy danych kluczy menedżera kolejek certyfikaty nie są przesyłane ze starego miejsca. Jeśli plik bazy danych kluczy, do którego uzyskiwany jest dostęp, jest nowym plikiem bazy danych kluczy, należy go zapełnić potrzebnymi certyfikatami CA i osobistymi, zgodnie z opisem w sekcji "Importowanie certyfikatu osobistego do repozytorium kluczy w systemie AIX, Linux, and Windows" na stronie 341.

V 9.3.0 V 9.3.0 *Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows*

Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

Program IBM MQ udostępnia dwa mechanizmy dostarczania hasła repozytorium kluczy do menedżera kolejek:

- "Atrybut KEYRPWD" na stronie 321
- "Plik ukryty repozytorium kluczy" na stronie 321

Jeśli plik ukryty repozytorium kluczy nie jest używany, hasło repozytorium kluczy jest szyfrowane przy użyciu systemu ochrony hasłem IBM MQ . Więcej informacji na temat metod ochrony hasła repozytorium kluczy zawiera sekcja "Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows" na stronie 316.

Atrybut KEYRPWD

Aby podać hasło repozytorium kluczy bezpośrednio dla menedżera kolejek, uruchom następującą komendę MQSC, zastępując *hasło* hasłem repozytorium kluczy:

```
ALTER QMGR KEYRPWD('password')
```

Ostrzeżenie: Hasło należy ująć w pojedynczy cudzysłów, w przeciwnym razie program IBM MQ zamienia znaki na wielkie litery.

Jeśli hasło repozytorium kluczy jest określone za pomocą tej metody, jest ono szyfrowane za pomocą systemu zabezpieczenia hasłem IBM MQ przed jego zapisaniem.

Do zaszyfrowania hasła używany jest klucz szyfrowania, który jest nazywany kluczem początkowym. Ustaw menedżer kolejek tak, aby używał unikalnego klucza początkowego w celu bezpiecznego zabezpieczenia hasła. Jeśli nie podasz klucza początkowego, zostanie użyty klucz domyślny.

Przed ustawianiem hasła repozytorium kluczy upewnij się, że menedżer kolejek jest skonfigurowany z unikalnym kluczem początkowym. Klucz początkowy można zmodyfikować za pomocą atrybutu **INITKEY** komendy **ALTER QMGR** . Na przykład:

```
ALTER QMGR INITKEY('mykey')
```

Ostrzeżenie: Zmodyfikowanie klucza początkowego po ustawieniu hasła repozytorium kluczy nie powoduje, że hasło repozytorium kluczy jest szyfrowane przy użyciu nowego klucza początkowego. Zmiana klucza początkowego bez resetowania hasła repozytorium kluczy powoduje, że program IBM MQ nie może zdeszyfrować hasła repozytorium kluczy i dlatego nie może uzyskać dostępu do repozytorium kluczy.

Więcej informacji na temat atrybutu **KEYRPWD** zawiera sekcja KEYRPWD.

Plik ukryty repozytorium kluczy

Jeśli hasło repozytorium kluczy nie zostanie dostarczone do menedżera kolejek za pomocą atrybutu **KEYRPWD** , program IBM MQ przyjmuje, że plik ukrytych haseł istnieje w tym samym katalogu, co

repozytorium kluczy. Plik ukrytych haseł ma taką samą nazwę rdzenia, jak repozytorium kluczy, ale ma rozszerzenie `.sth` .

Plik ukrytych haseł repozytorium kluczy jest tworzony w tym samym czasie, co repozytorium kluczy lub później, jako oddzielna komenda **runmqakm** .

Ostrzeżenie: Format pliku zeskładowanego jest specyficzny dla IBM MQ dostawcy usług kryptograficznych IBM Global Security Kit (GSKit)i nie jest dostępny na platformach używających innego dostawcy usług kryptograficznych.

Aby utworzyć plik ukrytych haseł podczas tworzenia repozytorium kluczy, należy podać parametr **-stash** . Na przykład:

```
runmqakm -keydb -create -db key.kdb -pw passw0rd -stash
```

gdzie *passw0rd* jest hasłem repozytorium kluczy.

Aby później utworzyć plik ukrytych haseł, uruchom następującą komendę:

```
runmqakm -keydb -stashpw -db key.kdb -pw passw0rd
```

gdzie *passw0rd* jest hasłem repozytorium kluczy.

Pojęcia pokrewne

“Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316
Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

“Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

ALW *Znajdowanie repozytorium kluczy dla systemu IBM MQ MQI client w systemie AIX, Linux, and Windows*

Położenie repozytorium kluczy jest określone przez zmienną MQSSLKEYR lub określone w wywołaniu MQCONNX.

Sprawdź zmienną środowiskową MQSSLKEYR, aby znaleźć położenie pliku bazy danych kluczy dla 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 IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 322. Wartość ustawiona w wywołaniu MQCONNX przesłania wartość MQSSLKEYR.

ALW *Określanie położenia repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows*

Brak domyślnego repozytorium kluczy dla IBM MQ MQI client. Położenie można określić na jeden z dwóch sposobów. Upewnij się, że dostęp do pliku bazy danych kluczy mają tylko zamierzeni użytkownicy lub administratorzy, aby zapobiec nieautoryzowanemu kopiowaniu do innych systemów.

Położenie pliku bazy danych kluczy dla IBM MQ MQI client można określić na dwa sposoby:

- Ustawianie zmiennej środowiskowej MQSSLKEYR. Na przykład w systemie AIX and Linux:

  V 9.3.0 V 9.3.0
  ```
  export MQSSLKEYR=/var/mqm/ssl/key.kdb
  ```

  W systemie Windows:

  V 9.3.0 V 9.3.0
  ```
  set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key.kdb
  ```

- Podanie ścieżki i nazwy rdzenia pliku bazy danych kluczy w polu *KeyRepository* struktury MQSCO, gdy aplikacja wykonuje wywołanie MQCONNX. Więcej informacji na temat używania struktury MQSCO w programie MQCONNX zawiera sekcja MQSCO-przegląd.

V 9.3.0 V 9.3.0 *Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows*

Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

IBM MQ udostępnia cztery mechanizmy dostarczania hasła repozytorium kluczy do IBM MQ MQI client:

- “Pola KeyRepoPassword obiektu MQSCO ” na stronie 323
- “Zmienna środowiskowa MQKEYRPWD” na stronie 324
- “Atrybut SSLKeyRepositoryPassword pliku konfiguracyjnego klienta” na stronie 324
- “Plik ukryty repozytorium kluczy” na stronie 324

Jeśli plik ukryty repozytorium kluczy nie jest używany, można podać hasło repozytorium kluczy w postaci jawnego łańcucha tekstowego lub łańcucha, który jest szyfrowany za pomocą systemu ochrony hasłem IBM MQ . Więcej informacji na temat metod ochrony hasła repozytorium kluczy zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316.

Pola KeyRepoPassword obiektu MQSCO

Aby podać hasło repozytorium kluczy przy użyciu struktury MQSCO, należy użyć kombinacji następujących trzech zmiennych pól łańcuchowych:

KeyRepoPasswordLength
Długość hasła.

KeyRepoPasswordPtr
Wskaźnik do miejsca w pamięci, które zawiera hasło.

KeyRepoPasswordOffset
Położenie hasła w pamięci, reprezentowane przez liczbę bajtów od początku struktury MQSCO.

Uwaga: Można podać tylko jedną z wartości: **KeyRepoPasswordPtr** lub **KeyRepoPasswordOffset**.

Na przykład:

```
char * pwd = "passw0rd";
MQSCO  SslConnOptions = {MQSCO_DEFAULT};

SslConnOptions.KeyRepoPasswordPtr = pwd;
SslConnOptions.KeyRepoPasswordLength = (MQLONG)strlen(SslConnOptions.KeyRepoPasswordPtr);
SslConnOptions.Version = MQSCO_VERSION_6;
```

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed przekazaniem do aplikacji IBM MQ client . Więcej informacji na ten temat zawiera sekcja “Szyfrowanie hasła repozytorium kluczy” na stronie 325.

Więcej informacji na temat struktury MQCSO zawiera sekcja Opcje konfiguracyjne MQSCO-SSL/TLS.

Zmienna środowiskowa *MQKEYRPWD*

Jeśli hasło do repozytorium kluczy nie zostanie dostarczone do klienta przy użyciu struktury MQSCO, można określić hasło do repozytorium kluczy za pomocą zmiennej środowiskowej *MQKEYRPWD* . Na przykład:

```
export MQKEYRPWD=passw0rd
```

lub wersji

```
set MQKEYRPWD=passw0rd
```

gdzie `passw0rd` jest hasłem użytkownika.

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed ustawianiem wartości zmiennej środowiskowej. Więcej informacji na ten temat zawiera “Szyfrowanie hasła repozytorium kluczy” na stronie 325.

Atrybut SSLKeyRepositoryPassword pliku konfiguracyjnego klienta

Jeśli hasło repozytorium kluczy nie zostanie dostarczone do klienta za pomocą jednej z innych metod, hasło repozytorium kluczy można określić za pomocą atrybutu **SSLKeyRepositoryPassword** w sekcji **SSL** pliku konfiguracyjnego klienta. Na przykład:

```
SSL:
    SSLKeyRepositoryPassword=passw0rd
```

Ostrzeżenie: Jeśli hasło zostanie podane za pomocą tej metody, należy je zaszyfrować przed ustawieniem wartości atrybutu **SSLKeyRepositoryPassword** . Więcej informacji na ten temat zawiera sekcja “Szyfrowanie hasła repozytorium kluczy” na stronie 325.

Więcej informacji na temat sekcji SSL pliku konfiguracyjnego klienta zawiera sekcja Sekcja SSL pliku konfiguracyjnego klienta.

Plik ukryty repozytorium kluczy

Jeśli hasło repozytorium kluczy nie zostanie dostarczone do klienta przy użyciu jednej z innych metod, program IBM MQ przyjmuje, że plik ukrytych haseł istnieje w tym samym katalogu, co repozytorium kluczy. Plik ukrytych haseł ma taką samą nazwę rdzenia, jak repozytorium kluczy, ale ma rozszerzenie `.sth` .

Plik ukryty repozytorium kluczy jest tworzony w tym samym czasie, co repozytorium kluczy lub później, przy użyciu oddzielnej komendy **runmqakm** .

Ostrzeżenie: Format pliku zeskładowanego jest specyficzny dla IBM MQ dostawcy usług kryptograficznych IBM Global Security Kit (GSKit)i nie jest dostępny na platformach używających innego dostawcy usług kryptograficznych.

Aby utworzyć plik ukrytych haseł podczas tworzenia repozytorium kluczy, należy podać parametr **-stash** . Na przykład:

```
runmqakm -keydb -create -db key.kdb -pw passw0rd -stash
```

gdzie *passw0rd* jest hasłem repozytorium kluczy.

Aby później utworzyć plik ukrytych haseł, uruchom następującą komendę:

```
runmqakm -keydb -stashpw -db key.kdb -pw passw0rd
```

gdzie *passw0rd* jest hasłem repozytorium kluczy.

Szyfrowanie hasła repozytorium kluczy

Jeśli hasło repozytorium kluczy zostanie podane przy użyciu innej metody niż plik ukrytych haseł, należy zaszyfrować hasło przy użyciu systemu zabezpieczenia hasłem IBM MQ . Aby zaszyfrować hasło, uruchom komendę **runmqicred** . Po wyświetleniu zapytania wprowadź hasło repozytorium kluczy. Komenda wyświetli zaszyfrowane hasło. Zaszyfrowane hasło można podać w pliku IBM MQ MQI client zamiast hasła w postaci jawnej, używając dowolnej z opisanych metod.

Do zaszyfrowania hasła używany jest klucz szyfrowania, który jest nazywany kluczem początkowym. Podczas szyfrowania hasła należy użyć unikalnego klucza początkowego, aby zabezpieczyć hasło. Aby podać własny klucz początkowy, należy użyć parametru **-sf** komendy **runmqicred** . Jeśli nie podasz klucza początkowego, zostanie użyty klucz domyślny.

Więcej informacji na ten temat zawiera sekcja runmqicred (protect IBM MQ client passwords).

Jeśli użytkownik poda własny klucz początkowy, gdy hasło repozytorium kluczy jest zaszyfrowane, i przekaże zaszyfrowane hasło do serwera IBM MQ MQI client, należy również upewnić się, że ten sam klucz początkowy został dostarczony do serwera IBM MQ MQI client. Więcej informacji na temat udostępniania początkowego klucza IBM MQ MQI clientzawiera sekcja “Podawanie klucza początkowego dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 325.

Pojęcia pokrewne

“Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316
Kilka komponentów IBM MQ wymaga dostępu do repozytorium kluczy zawierającego certyfikaty cyfrowe lub klucze symetryczne. Repozytorium kluczy jest zabezpieczone hasłem, ponieważ zawiera poufne informacje. Hasło repozytorium kluczy musi być zapisane w miejscu, w którym program IBM MQ może je odczytać podczas uzyskiwania dostępu do repozytorium kluczy. Hasło musi być również zaszyfrowane, aby zmniejszyć prawdopodobieństwo dostępu bez uprawnień do repozytorium kluczy.

“Podawanie hasła repozytorium kluczy dla menedżera kolejek w systemie AIX, Linux, and Windows” na stronie 321
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

V 9.3.0 ALW V 9.3.0 *Podawanie klucza początkowego dla IBM MQ MQI client w systemie AIX, Linux, and Windows*

Jeśli do IBM MQ MQI client zostaną podane zmienne, które zostały zaszyfrowane za pomocą systemu IBM MQ Password Protection System, może być konieczne podanie odpowiedniego klucza początkowego, który został użyty do zaszyfrowania wartości.

Jeśli podczas szyfrowania wartości nie określono klucza początkowego, nie trzeba podawać żadnej początkowej wartości klucza do IBM MQ client. Jeśli jednak użyto unikalnego klucza początkowego, można udostępnić klucz początkowy IBM MQ client za pomocą następujących metod:

- “Podawanie klucza początkowego przy użyciu struktury MQCSP” na stronie 325
- “Podawanie klucza początkowego za pomocą zmiennej środowiskowej MQS_MQI_KEYFILE” na stronie 326
- “Podawanie klucza początkowego przy użyciu pliku konfiguracyjnego klienta” na stronie 326

Podawanie klucza początkowego przy użyciu struktury MQCSP

Aby podać klucz początkowy przy użyciu struktury MQCSP, należy użyć kombinacji następujących trzech zmiennych pól łańcuchowych:

InitialKeyLength
Długość klucza początkowego

InitialKeyPtr
Wskaźnik do położenia w pamięci zawierającej klucz początkowy

InitialKeyOffset
Położenie klucza początkowego w pamięci, reprezentowane jako liczba bajtów od początku struktury MQCSP.

Uwaga: Można podać tylko jedną z wartości: **InitialKeyPtr** lub **InitialKeyOffset**.

Na przykład:

```
char * initialKey = "myInitialKey";
MQCSP  cspOptions = {MQCSP_DEFAULT};


cspOptions.InitialKeyPtr = initialKey;
cspOptions.InitialKeyLength = (MQLONG)strlen(cspOptions.InitialKeyPtr);
cspOptions.Version = MQCSP_VERSION_2;
```

Podawanie klucza początkowego za pomocą zmiennej środowiskowej MQS_MQI_KEYFILE

Jeśli klucz początkowy nie zostanie dostarczony do klienta przy użyciu struktury MQCSP, produkt IBM MQ sprawdza zmienną środowiskową *MQS_MQI_KEYFILE* . Tę zmienną środowiskową należy ustawić na położenie pliku zawierającego pojedynczy wiersz tekstu, składający się z klucza początkowego, który ma być używany.

Jeśli na przykład plik o nazwie `mykey.key` istnieje w katalogu głównym i zawiera klucz początkowy, należy ustawić zmienną środowiskową w następujący sposób:

```
export MQS_MQI_KEYFILE=/mykey.key
```

lub wersji

```
set MQS_MQI_KEYFILE=C:\mykey.key
```

Podawanie klucza początkowego przy użyciu pliku konfiguracyjnego klienta

Jeśli klucz początkowy nie został dostarczony do klienta przy użyciu poprzedniego mechanizmu, program IBM MQ sprawdza atrybut **MQIInitialKeyFile** w sekcji Security pliku `mqclient.ini` . Atrybut ten należy ustawić na położenie pliku zawierającego pojedynczy wiersz tekstu, składający się z klucza początkowego, który ma być używany.

Na przykład, jeśli plik o nazwie `mykey.key` istnieje w katalogu głównym i zawiera klucz początkowy, plik konfiguracyjny klienta powinien zawierać:

```
Security:
    MQIInitialKeyFile=/mykey.key
```

Pojęcia pokrewne

“Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323
Ponieważ repozytorium kluczy zawiera poufne informacje, jest ono zabezpieczone hasłem. Aby można było uzyskać dostęp do treści repozytorium kluczy w celu wykonania operacji TLS, program IBM MQ musi mieć możliwość pobrania hasła repozytorium kluczy.

“Praca z protokołem SSL/TLS” na stronie 293
Te tematy zawierają instrukcje dotyczące wykonywania pojedynczych zadań związanych z używaniem protokołu TLS z produktem IBM MQ.

ALW *Gdy zmiany w certyfikatach lub w bazie certyfikatów zaczną obowiązywać w dniu AIX, Linux, and Windows*

Po zmianie certyfikatów w bazie certyfikatów lub lokalizacji bazy certyfikatów zmiany są uwzględniane w zależności od typu kanału i sposobu jego działania.

Zmiany certyfikatów w pliku bazy danych kluczy i w atrybucie repozytorium kluczy zaczynają obowiązywać w następujących sytuacjach:

- Gdy nowy wychodzący proces pojedynczego kanału po raz pierwszy uruchamia kanał TLS.
- Gdy nowy przychodzący proces pojedynczego kanału TCP/IP po raz pierwszy otrzyma żądanie uruchomienia kanału TLS.
- Po wywołaniu komendy MQSC REFRESH SECURITY TYPE (SSL) w celu odświeżenia środowiska TLS.
- W przypadku procesów aplikacji klienckiej, gdy ostatnie połączenie TLS w procesie jest zamknięte. Następne połączenie TLS będzie odbierać zmiany certyfikatu.
- Dla kanałów, które działają jako wątki procesu zestawiania procesów (amqrmppa), gdy proces zestawiania procesów jest uruchamiany lub restartowany i po raz pierwszy uruchamia kanał TLS. Jeśli proces zestawiania procesów już uruchomił kanał TLS, a zmiana ma zostać natychmiast uwzględniona, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- Dla kanałów, które działają jako wątki inicjatora kanału, gdy inicjator kanału jest uruchamiany lub restartowany i najpierw uruchamia kanał TLS. Jeśli proces inicjatora kanału uruchomił już kanał TLS, a zmiana ma zostać natychmiast uwzględniona, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).
- Dla kanałów, które działają jako wątki programu nasłuchującego TCP/IP, gdy program nasłuchujący jest uruchamiany lub restartowany i najpierw otrzymuje żądanie uruchomienia kanału TLS. Jeśli program nasłuchujący uruchomił już kanał TLS i chcesz, aby zmiany zostały uwzględnione natychmiast, uruchom komendę MQSC REFRESH SECURITY TYPE (SSL).

Środowisko TLS produktu IBM MQ można również odświeżyć przy użyciu Eksploratora IBM MQ lub komend PCF.

Ważne: . Zmiany w pliku konfiguracyjnym magazynu kluczy i/lub pliku kluczy używanych przez przechwytywacz MCA AMS (i AMS w zwykłym kliencie) są pobierane w menedżerze kolejek lub po restarcie aplikacji.

ALW *Tworzenie samopodpisanego certyfikatu osobistego w systemie AIX, Linux, and Windows*

Certyfikat samopodpisany można utworzyć za pomocą programu **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub wiersza komend za pomocą komendy **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

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 .

Deprecated Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .

Więcej informacji na temat powodów, dla których można użyć certyfikatów samopodpisanych, zawiera sekcja Używanie certyfikatów samopodpisanych do wzajemnego uwierzytelniania dwóch menedżerów kolejek.

Nie wszystkie certyfikaty cyfrowe mogą być używane ze wszystkimi CipherSpecs. Należy upewnić się, że został utworzony certyfikat, który jest zgodny ze CipherSpecs , które mają być używane. Produkt IBM MQ obsługuje trzy różne typy specyfikacji szyfrowania CipherSpec. Szczegółowe informacje zawiera sekcja “Współdziałanie krzywej eliptycznej i specyfikacji szyfrowania RSA CipherSpecs” na stronie 49 w temacie “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48 .

Aby użyć CipherSpecs typu 1 (nazwy zaczynają się od ECDHE_ECDSA_), należy użyć komendy **runmqakm** w celu utworzenia certyfikatu i podać parametr algorytmu podpisu ECDSA krzywej eliptycznej, na przykład **-sig_alg** EC_ecdsa_with_SHA384.

Listę opcji dostępnych z algorytmem mieszającym **-sig_alg** zawiera sekcja “Opcje runmqckm i runmqakm w systemie AIX, Linux, and Windows” na stronie 606 .

Jeśli używane są:

- Interfejs GUI, patrz sekcja “Korzystanie z interfejsu użytkownika strmqikm” na stronie 328
- Wiersz komend, patrz “Za pomocą wiersza komend” na stronie 328

ALW *Korzystanie z interfejsu użytkownika* ***strmqikm***

Certyfikat osobisty można utworzyć za pomocą programu **strmqikm** (iKeyman) Interfejs GUI.

O tym zadaniu

strmqikm nie udostępnia opcji zgodnej ze standardem FIPS. Aby zarządzać certyfikatami TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

Procedura

Aby utworzyć certyfikat osobisty dla menedżera kolejek lub programu 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 wygenerowane 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 **Utwórz** kliknij opcję **Nowy certyfikat samopodpisany**. Zostanie wyświetlone okno Utwórz nowy certyfikat samopodpisany.
9. W polu **Key Label** (Etykieta klucza) wpisz etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli został ustawiony) lub domyślną wartością ibmwebspheremq z dodaną nazwą menedżera kolejek lub ID użytkownika logowania IBM MQ MQI client (wszystkie te wartości są zapisane 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 w dowolnym polu **Alternatywna nazwa podmiotu** .
11. W pozostałych polach zaakceptuj wartości domyślne lub wybierz nowe.

    Więcej informacji na temat nazw wyróżniających zawiera sekcja “Nazwy wyróżniające” na stronie 15.
12. Kliknij przycisk **OK**.

    Lista **Certyfikaty osobiste** zawiera etykietę utworzonego samopodpisanego certyfikatu osobistego.

ALW *Za pomocą wiersza komend*

Certyfikat osobisty można utworzyć z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). Aby zarządzać certyfikatami SSL lub TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

Procedura

Utwórz samopodpisany certyfikat osobisty, używając komendy **runmqckm** lub **runmqakm** (GSKCapiCmd).

- W systemie **runmqckm**:

```
runmqckm -cert -create -db filename -pw password -label label
         -dn distinguished_name -size key_size
         -x509version version -expire days -sig_alg algorithm
```

  Zamiast -dn *distinguished_name*można użyć -san_dnsname *DNS_names*, -san_emailaddr *email_addresses*lub -san_ipaddr *IP_addresses*.

- W systemie **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 został ustawiony) lub wartością domyślną ibmwebspheremq z dodaną nazwą menedżera kolejek lub ID użytkownika logowania IBM MQ MQI client (wszystkie te wartości są zapisane małymi literami). Szczegółowe informacje na ten temat zawiera sekcja “Etykiety certyfikatów cyfrowych, zrozumienie wymagań” na stronie 27.

-dn *nazwa_wyróżniająca*
Określa nazwę wyróżniającą X.500 ujętą w cudzysłów. Wymagany jest co najmniej jeden atrybut. Można podać wiele atrybutów jednostki organizacyjnej i DC.

Uwaga: Narzędzia **runmqckm** i **runmqakm** odwołują się do atrybutu kodu pocztowego jako POSTALCODE, a nie jako PC. Zawsze należy podać wartość POSTALCODE w parametrze **-dn** , jeśli komendy zarządzania certyfikatami są używane do żądania certyfikatów z kodem pocztowym.

-size *wielkość_klucza*
Określa wielkość klucza. Jeśli używany jest system **runmqckm**, wartością może być 512 lub 1024. Jeśli używany jest system **runmqakm**, wartością może być 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 certyfikatu (w dniach). Wartością domyślną dla certyfikatu jest 365 dni.

-fips,
określa, że komenda jest uruchamiana w trybie FIPS. Używany jest tylko komponent FIPS IBM Crypto for C (ICC) , który musi zostać pomyślnie zainicjowany w trybie FIPS. W trybie FIPS komponent ICC używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

-sig_alg
W przypadku **runmqckm**określa asymetryczny algorytm podpisu używany do tworzenia pary kluczy pozycji. Możliwe wartości to: 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
Dla parametru **runmqakm**określa algorytm kodowania mieszającego używany podczas tworzenia żądania certyfikatu. Ten algorytm kodowania mieszającego jest używany do tworzenia podpisu powiązanego z nowo utworzonym żądaniem certyfikatu. 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.

-san_dnsname ***nazwy_DNS***
Określa rozdzielaną przecinkami lub spacjami listę nazw DNS dla tworzonej pozycji.

-san_emailaddr ***adres_e-mail***
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę adresów e-mail dla tworzonej pozycji.

-san_ipaddr ***adres_IP***
Określa rozdzielaną przecinkami lub spacjami listę adresów IP dla tworzonej pozycji.

ALW *Żądanie certyfikatu osobistego w systemie AIX, Linux, and Windows*

Można zażądać certyfikatu osobistego za pomocą programu narzędziowego **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). Aby zarządzać certyfikatami SSL lub TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

O tym zadaniu

Można zażądać certyfikatu osobistego za pomocą interfejsu GUI programu **strmqikm** lub z poziomu wiersza komend, z uwzględnieniem następujących kwestii:

- 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 .
- Deprecated Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .
- Nie wszystkie certyfikaty cyfrowe mogą być używane ze wszystkimi CipherSpecs. Upewnij się, że zażądano certyfikatu, który jest zgodny ze specyfikacją szyfrowania CipherSpecs , która ma być używana. Produkt IBM MQ obsługuje trzy różne typy specyfikacji szyfrowania CipherSpec. Szczegółowe informacje zawiera sekcja “Współdziałanie krzywej eliptycznej i specyfikacji szyfrowania RSA CipherSpecs” na stronie 49 w temacie “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48 .
- Aby użyć CipherSpecs typu 1 (z nazwami zaczynającymi się od ECDHE_ECDSA_), należy użyć komendy **runmqakm** w celu zażądania certyfikatu i podać parametr algorytmu podpisu ECDSA krzywej eliptycznej, na przykład **-sig_alg** EC_ecdsa_with_SHA384.

  Listę opcji dostępnych z algorytmem mieszającym **-sig_alg** zawiera sekcja “Opcje runmqckm i runmqakm w systemie AIX, Linux, and Windows” na stronie 606 .
- Tylko komenda **runmqakm** udostępnia opcję zgodną ze standardem FIPS.
- Jeśli używany jest sprzęt szyfrujący, należy zapoznać się z sekcją “Żądanie certyfikatu osobistego dla sprzętu PKCS #11” na stronie 350.

Jeśli używane są:

- Interfejs GUI, patrz sekcja “Korzystanie z interfejsu użytkownika strmqikm” na stronie 331
- Wiersz komend, patrz “Za pomocą wiersza komend” na stronie 331

ALW *Korzystanie z interfejsu użytkownika* ***strmqikm***

Można zażądać certyfikatu osobistego za pomocą programu narzędziowego **strmqikm** (iKeyman) Interfejs GUI. Aby zarządzać certyfikatami SSL lub TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

O tym zadaniu

strmqikm nie udostępnia opcji zgodnej ze standardem FIPS. Aby zarządzać certyfikatami TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

Procedura

Wykonaj następujące kroki, aby zastosować certyfikat osobisty przy użyciu 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 **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 wygenerowane 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 **Create** (Utwórz) kliknij opcję **New Certificate Request**(Nowe żądanie certyfikatu). Zostanie otwarte okno **Create New Key and Certificate Request** (Utwórz nowy klucz i żądanie certyfikatu).
9. W polu **Key Label** (Etykieta klucza) wpisz etykietę certyfikatu.

   Etykieta jest wartością atrybutu **CERTLABL** (jeśli został ustawiony) lub domyślną wartością `ibmwebspheremq` z dodaną nazwą menedżera kolejek lub ID użytkownika logowania IBM MQ MQI client (wszystkie te wartości są zapisane 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 w dowolnym polu **Alternatywna nazwa podmiotu** . W pozostałych polach zaakceptuj wartości domyślne lub wybierz nowe.

    Więcej informacji na temat nazw wyróżniających zawiera sekcja “Nazwy wyróżniające” na stronie 15.
11. W polu **Wprowadź nazwę pliku, w którym ma zostać 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**.

    Lista **Żądania certyfikatu osobistego** zawiera etykietę nowo utworzonego żądania certyfikatu osobistego. Żądanie certyfikatu jest przechowywane w pliku wybranym w kroku “11” na stronie 331.
14. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując plik do formularza żądania w serwisie WWW ośrodka CA.

ALW *Za pomocą wiersza komend*

Certyfikat osobisty można zażądać z wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd). Aby zarządzać certyfikatami SSL lub TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

Procedura

Zażądaj certyfikatu osobistego za pomocą komendy **runmqckm** lub **runmqakm** (GSKCapiCmd).

- W systemie **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
        -file filename -sig_alg algorithm
```

  Zamiast -dn *distinguished_name*można użyć -san_dsname *DNS_names*, -san_emailaddr *email_addresses*lub -san_ipaddr *IP_addresses*.

- W systemie **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 został ustawiony) lub wartością domyślną ibmwebspheremq z dodaną nazwą menedżera kolejek lub ID użytkownika logowania IBM MQ MQI client (wszystkie te wartości są zapisane małymi literami). Szczegółowe informacje na ten temat zawiera sekcja “Etykiety certyfikatów cyfrowych, zrozumienie wymagań” na stronie 27.

-dn *nazwa_wyróżniająca*
Określa nazwę wyróżniającą X.500 ujętą w cudzysłów. Wymagany jest co najmniej jeden atrybut. Można podać wiele atrybutów jednostki organizacyjnej i DC.

Uwaga: Narzędzia **runmqckm** i **runmqakm** odwołują się do atrybutu kodu pocztowego jako POSTALCODE, a nie jako PC. Zawsze należy podać wartość POSTALCODE w parametrze **-dn** , jeśli komendy zarządzania certyfikatami są używane do żądania certyfikatów z kodem pocztowym.

-size *wielkość_klucza*
Określa wielkość klucza. Jeśli używany jest system **runmqckm**, wartością może być 512 lub 1024. Jeśli używany jest system **runmqakm**, wartością może być 512, 1024lub 2048.

-file *nazwa_pliku*
Określa nazwę pliku dla żądania certyfikatu.

-fips,
określa, że komenda jest uruchamiana w trybie FIPS. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

-sig_alg
W przypadku **runmqckm**określa asymetryczny algorytm podpisu używany do tworzenia pary kluczy pozycji. Możliwe wartości to: 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
Dla parametru **runmqakm**określa algorytm kodowania mieszającego używany podczas tworzenia żądania certyfikatu. Ten algorytm kodowania mieszającego jest używany do tworzenia podpisu powiązanego z nowo utworzonym żądaniem certyfikatu. 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.

-san_dnsname ***nazwy_DNS***
Określa rozdzielaną przecinkami lub spacjami listę nazw DNS dla tworzonej pozycji.

-san_emailaddr ***adres_e-mail***
Określa rozdzielaną przecinkami lub rozdzielaną spacjami listę adresów e-mail dla tworzonej pozycji.

-san_ipaddr ***adres_IP***
Określa rozdzielaną przecinkami lub 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 AIX, Linux, and Windows” na stronie 335.

ALW *Odnawianie istniejącego certyfikatu osobistego w systemie AIX, Linux, and Windows*

Certyfikat osobisty można odnowić za pomocą programu **strmqikm** (iKeyman) Z poziomu interfejsu GUI lub wiersza komend za pomocą komend **runmqckm** (iKeycmd) lub **runmqakm** (GSKCapiCmd).

O tym zadaniu

Jeśli wymagane jest użycie większych kluczy dla certyfikatów osobistych, nie można odnowić istniejącego certyfikatu. Należy zastąpić istniejący klucz, wykonując kroki opisane w sekcji “Żądanie certyfikatu osobistego w systemie AIX, Linux, and Windows” na stronie 330 , aby utworzyć nowe żądanie certyfikatu, które używa wymaganych wielkości kluczy.

Certyfikat osobisty ma datę ważności, po upływie której certyfikat nie może być już używany. W tym zadaniu wyjaśniono, w jaki sposób odnowić istniejący certyfikat osobisty, zanim utraci on ważność.

Korzystanie z interfejsu użytkownika ***strmqikm***

O tym zadaniu

strmqikm nie udostępnia opcji zgodnej ze standardem FIPS. Aby zarządzać certyfikatami TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** .

Procedura

Wykonaj następujące kroki, aby zastosować certyfikat osobisty przy użyciu interfejsu użytkownika **strmqikm** :

1. Uruchom interfejs użytkownika za pomocą komendy **strmqikm** w systemie AIX, Linux, and Windows.
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz).
   Zostanie otwarte okno **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 wygenerowane 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 wybierz opcję **Certyfikaty osobiste** , a następnie wybierz certyfikat z listy, który chcesz odnowić.
9. Kliknij opcję **Ponownie utwórz żądanie ...** .

   Zostanie otwarte okno, w którym można wprowadzić nazwę pliku i informacje o położeniu pliku.
10. W polu **nazwa pliku** zaakceptuj wartość domyślną `certreq.arm`lub wpisz nową wartość, w tym pełną ścieżkę do pliku.
11. Kliknij przycisk **OK**. Żądanie certyfikatu jest przechowywane w pliku wybranym w kroku “9” na stronie 334.
12. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując plik do formularza żądania w serwisie WWW ośrodka CA.

Za pomocą wiersza komend

Procedura

Użyj następujących komend, aby zażądać certyfikatu osobistego za pomocą komendy **runmqckm** lub **runmqakm** :

- W systemie **runmqckm**:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- Używanie 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.

Uwaga: Ponieważ stare informacje o certyfikacie znajdują się w pamięci podręcznej, należy uruchomić komendę REFRESH SECURITY TYPE (SSL).

Co dalej

Po otrzymaniu podpisanego certyfikatu osobistego z ośrodka certyfikacji można dodać go do bazy danych kluczy, wykonując kroki opisane w sekcji “Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 335.

ALW *Odbieranie certyfikatów osobistych do repozytorium kluczy w systemie AIX, Linux, and Windows*

Ta procedura służy do pobierania certyfikatu osobistego do pliku bazy danych kluczy. Repozytorium kluczy musi być tym samym repozytorium, w którym utworzono 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 wysyła certyfikat jako część wiadomości e-mail, skopiuj certyfikat do osobnego pliku.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS.

Upewnij się, że plik certyfikatu do zaimportowania ma uprawnienie do zapisu dla bieżącego użytkownika, a następnie użyj następującej procedury dla menedżera kolejek lub programu IBM MQ MQI client , aby otrzymać certyfikat osobisty do pliku bazy danych kluczy:

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, do którego chcesz dodać certyfikat, na przykład `key.kdb`.
6. Kliknij przycisk **Otwórz**, a następnie 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** . Wybierz widok **Certyfikaty osobiste** .
8. Kliknij przycisk **Odbierz**. Zostanie otwarte okno Receive Certificate from a File (Pobierz certyfikat z pliku).
9. Wpisz nazwę pliku certyfikatu i położenie nowego certyfikatu osobistego lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
10. Kliknij przycisk **OK**. Jeśli w bazie danych kluczy znajduje się już certyfikat osobisty, zostanie wyświetlone okno z pytaniem, czy klucz dodawany jako klucz domyślny ma zostać ustawiony w bazie danych.
11. Kliknij przycisk **Tak** lub **Nie**. Zostanie otwarte okno Enter a Label (Wprowadzanie etykiety).
12. Kliknij przycisk **OK**. W polu **Certyfikaty osobiste** wyświetlana jest etykieta nowo dodanego certyfikatu osobistego.

Za pomocą wiersza komend

Aby dodać certyfikat osobisty do pliku bazy danych kluczy, użyj jednej z następujących komend:

- W systemie **runmqckm**:

```
runmqckm -cert -receive -file filename -db filename -pw password
         -format ascii
```

- W systemie **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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

Jeśli używany jest sprzęt szyfrujący, należy zapoznać się z sekcją "Odbieranie certyfikatu osobistego do sprzętu PKCS #11" na stronie 351.

ALW *Wyodrębnianie certyfikatu ośrodka CA z repozytorium kluczy w systemie AIX, Linux, and Windows*

Aby wyodrębnić certyfikat ośrodka CA, należy wykonać następującą procedurę.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Program **strmqikm** (iKeyman) nie udostępnia opcji zgodności ze standardem FIPS.

Wykonaj następujące kroki na komputerze, z którego chcesz wyodrębnić certyfikat 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 chcesz wyodrębnić dane, 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 chcesz wyodrębnić.
9. Kliknij przycisk **Wyodrębnij**. Zostanie otwarte okno Wyodrębnianie certyfikatu do pliku.
10. W polu **Typ danych** wybierz typ danych certyfikatu, na przykład **Base64-encoded ASCII data** (Dane ASCII) dla pliku z rozszerzeniem `.arm` .
11. Wpisz nazwę pliku certyfikatu i położenie, w którym ma zostać zapisany certyfikat, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
12. Kliknij przycisk **OK**. Certyfikat zostanie zapisany w określonym pliku.

Za pomocą wiersza komend

Użyj następujących komend, aby wyodrębnić certyfikat ośrodka CA za pomocą komendy **runmqckm** lub komendy **runmqakm** :

```
runmqckm -cert -extract -db filename -pw password -label label
         -target filename -format ascii
```

lub wersji

```
runmqakm -cert -extract -db filename -pw password -label label
         -target filename -format ascii -fips
```

gdzie:

`-db` *filename*	to pełna nazwa ścieżki 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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

ALW *Wyodrębnianie publicznej części certyfikatu samopodpisanego z repozytorium kluczy w systemie AIX, Linux, and Windows*

Wykonaj tę procedurę, aby wyodrębnić część publiczną certyfikatu samopodpisanego.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Program **strmqikm** (iKeyman) nie udostępnia opcji zgodności ze standardem FIPS.

Wykonaj następujące kroki na komputerze, z którego chcesz wyodrębnić publiczną część certyfikatu samopodpisanego:

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 chcesz wyodrębnić 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 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. W polu **Typ danych** wybierz typ danych certyfikatu, na przykład **Base64-encoded ASCII data** (Dane ASCII) dla pliku z rozszerzeniem `.arm` .
11. Wpisz nazwę pliku certyfikatu i położenie, w którym ma zostać zapisany certyfikat, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
12. Kliknij przycisk **OK**. Certyfikat zostanie zapisany w określonym pliku. Należy zauważyć, że podczas wyodrębniania (a nie eksportowania) certyfikatu dołączana jest tylko publiczna część certyfikatu, więc hasło nie jest wymagane.

Za pomocą wiersza komend

Użyj następujących komend, aby wyodrębnić publiczną część certyfikatu samopodpisanego za pomocą **runmqckm** lub **runmqakm**:

- Używanie komendy runmqckm:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Używanie komendy runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

gdzie:

-db *filename*	to pełna nazwa ścieżki 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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

ALW *Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie AIX, 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 kodowany w formacie ASCII (UTF-8) lub binarnym (DER), ponieważ produkt IBM Global Security Kit (GSKit) nie obsługuje certyfikatów z innymi typami kodowania.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . **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** .
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 CA do bazy danych kluczy, użyj jednej z następujących komend:

- W systemie **runmqckm**:

```
runmqckm -cert -add -db filename -pw password -label label
         -file filename -format ascii
```

- W systemie **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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

ALW *Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie AIX, Linux, and Windows*

Aby wyeksportować certyfikat osobisty, należy wykonać poniższą procedurę.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Program **strmqikm** (iKeyman) nie udostępnia opcji zgodności ze standardem FIPS.

Wykonaj następujące kroki na komputerze, z którego chcesz wyeksportować 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 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 chcesz wyeksportować 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 Eksportuj/Importuj klucz.
10. Wybierz opcję **Eksportuj klucz**.
11. Wybierz **Typ pliku kluczy** certyfikatu, który ma zostać wyeksportowany, na przykład **PKCS12**.
12. Wpisz nazwę pliku i położenie, do którego chcesz wyeksportować certyfikat, lub kliknij przycisk **Przeglądaj** , aby wybrać nazwę i położenie.
13. Kliknij przycisk **OK**. Zostanie otwarte okno Password Prompt (Zapytanie o hasło). Należy zauważyć, że podczas eksportowania (a nie wyodrębniania) certyfikatu uwzględniane są zarówno publiczne, jak i prywatne części certyfikatu. Dlatego wyeksportowany plik jest chroniony hasłem. Podczas wyodrębniania certyfikatu dołączana jest tylko jego część publiczna, więc hasło nie jest wymagane.
14. Wpisz hasło w polu **Hasło** i wpisz je ponownie w polu **Potwierdź hasło** .
15. Kliknij przycisk **OK**. Certyfikat zostanie wyeksportowany do podanego pliku.

Za pomocą wiersza komend

Wyeksportuj certyfikat osobisty za pomocą komendy **runmqckm** lub komendy **runmqakm** :

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

lub wersji

```
runmqakm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
        -encryption strong | weak -fips
```

gdzie:

`-db filename`	jest nazwą pełnej ścieżki do bazy danych kluczy CMS.
`-encryption`	to siła szyfrowania używana w komendzie eksportowania certyfikatu. Wartością może być `strong` lub `weak`. Wartością domyślną jest `strong`.

`-fips`	określa, że komenda jest uruchamiana w trybie FIPS. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **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*	jest hasłem do szyfrowania certyfikatu.
`-target_type` *pkcs12*	jest typem certyfikatu.

ALW *Importowanie certyfikatu osobistego do repozytorium kluczy w systemie AIX, 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 wystawiania certyfikatów CA do pliku bazy danych kluczy (patrz sekcja "Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie AIX, Linux, and Windows" na stronie 338).

Pliki PKCS #12 powinny być traktowane jako tymczasowe i usuwane po użyciu.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardami FIPS, należy użyć komendy **runmqakm** . **strmqikm** nie udostępnia opcji zgodnej ze standardem FIPS.

Wykonaj następujące kroki na komputerze, na który chcesz zaimportować 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 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**. Zostanie wyświetlone okno Password Prompt (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 opcję **Personal Certificates**(Certyfikaty osobiste).
9. Jeśli w widoku Certyfikaty osobiste znajdują się certyfikaty, wykonaj następujące czynności:
   a. Kliknij opcję **Eksportuj/Importuj**. Zostanie wyświetlone okno eksportowania/importowania klucza.
   b. Wybierz opcję **Importuj klucz**.
10. Jeśli w widoku Certyfikaty osobiste nie ma żadnych certyfikatów, kliknij przycisk **Importuj**.
11. Wybierz **Typ pliku kluczy** certyfikatu, który chcesz zaimportować, 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 Password Prompt (Pytanie o hasło).

14. W polu **Hasło** wpisz hasło używane podczas eksportowania certyfikatu.
15. Kliknij przycisk **OK**. Zostanie wyświetlone okno Zmień etykiety. Można zmienić etykiety importowanych certyfikatów, jeśli na przykład w docelowej bazie danych kluczy istnieje już certyfikat o takiej samej etykiecie. Zmiana etykiet certyfikatów nie ma wpływu na sprawdzanie poprawności łańcucha certyfikatów. Aby powiązać certyfikat z konkretnym menedżerem kolejek lub programem IBM MQ MQI client, program IBM MQ użyje wartości atrybutu **CERTLABL** (jeśli jest ustawiony) lub domyślnej wartości `ibmwebspheremq` z dodaną nazwą menedżera kolejek lub identyfikatorem logowania użytkownika IBM MQ MQI client (wszystkie te wartości są zapisane 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 zostanie skopiowana do pola wprowadzania **Wprowadź nową etykietę** . Zastąp tekst etykiety nową etykietą i kliknij przycisk **Zastosuj**.
17. Tekst w polu wprowadzania **Wprowadź nową etykietę** jest kopiowany z powrotem do pola **Wybierz etykietę do zmiany** , zastępując oryginalnie wybraną etykietę i ponownie oznaczając odpowiedni certyfikat.
18. Po zmianie wszystkich etykiet, które wymagały zmiany, kliknij przycisk **OK**. Okno Zmień etykiety zostanie zamknięte, a oryginalne okno IBM Key Management zostanie ponownie wyświetlone z polami **Personal Certificates** (Certyfikaty osobiste) i **Signer Certificates** (Certyfikaty podpisującego) zaktualizowanymi przy użyciu poprawnie oznaczonych certyfikatów.
19. Certyfikat zostanie zaimportowany do docelowej bazy danych kluczy.

Za pomocą wiersza komend

Aby zaimportować certyfikat osobisty za pomocą programu **runmqckm**, użyj następującej komendy:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

Aby zaimportować certyfikat osobisty za pomocą programu **runmqakm**, użyj następującej komendy:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips
```

gdzie:

`-file` *filename*	to pełna nazwa pliku zawierającego certyfikat PKCS #12 .
`-pw` *password*	jest hasłem dla certyfikatu PKCS #12 .
`-type` *pkcs12*	jest typem pliku.
`-target` *filename*	to nazwa docelowej bazy danych kluczy CMS .
`-target_pw` *password*	jest hasłem dla bazy danych kluczy CMS.
`-target_type` *cms*	to typ bazy danych określony przez opcję `-target`
`-label` *label*	jest etykietą certyfikatu, który ma zostać zaimportowany z źródłowej bazy danych kluczy.
`-new_label` *label*	jest etykietą, do której certyfikat zostanie przypisany w docelowej bazie danych. Jeśli opcja `-new_label` zostanie pominięta, domyślnie zostanie użyta ta sama opcja, co opcja `-label` .
`-fips`	określa, że komenda jest uruchamiana w trybie FIPS. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

runmqckm nie udostępnia komendy do bezpośredniej zmiany etykiet certyfikatów. Aby zmienić etykietę certyfikatu, wykonaj następujące kroki:

1. Wyeksportuj certyfikat do pliku PKCS #12 za pomocą komendy **-cert -export** . Podaj istniejącą etykietę certyfikatu dla opcji `-label` .
2. Usuń istniejącą kopię certyfikatu z oryginalnej bazy danych kluczy za pomocą komendy **-cert -delete** .
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.

ALW *Importowanie certyfikatu osobistego z pliku Microsoft.pfx*

Wykonaj tę procedurę, aby zaimportować plik Microsoft.pfx w systemie AIX, Linux, and Windows.

Plik .pfx może zawierać dwa certyfikaty związane z tym samym kluczem. Jednym z nich jest certyfikat osobisty lub certyfikat serwisu (zawierający zarówno klucz publiczny, jak i prywatny). Drugim jest certyfikat ośrodka CA (osoba podpisująca) (zawierający tylko klucz publiczny). Te certyfikaty nie mogą współistnieć w tym samym pliku bazy danych kluczy CMS , dlatego można zaimportować tylko jeden z nich. Ponadto etykieta lub nazwa przyjazna jest dołączona tylko do certyfikatu osoby podpisującej.

Certyfikat osobisty jest identyfikowany przez wygenerowany przez system unikalny identyfikator użytkownika (UUID). W tej sekcji przedstawiono importowanie certyfikatu osobistego z pliku pfx przy jednoczesnym oznaczeniu go przyjazną nazwą przypisaną wcześniej do certyfikatu ośrodka CA (osoby podpisującej). Wystawiające certyfikaty CA (osoby podpisującej) powinny być już dodane do docelowej bazy danych kluczy. Należy zauważyć, że pliki PKCS#12 powinny być traktowane jako tymczasowe i usuwane po użyciu.

Aby zaimportować certyfikat osobisty ze źródłowej bazy danych kluczy pfx, wykonaj następujące kroki:

1. Uruchom interfejs GUI za pomocą komendy **strmqikm** . Zostanie wyświetlone okno IBM Key Management (Zarządzanie kluczami IBM).
2. W menu **Key Database File** (Plik bazy danych kluczy) kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Otwieranie.
3. Wybierz typ bazy danych kluczy **PKCS12**.
4. **Przed wykonaniem tego kroku zaleca się utworzenie kopii zapasowej bazy danych pfx.** Wybierz bazę danych kluczy pfx, którą chcesz zaimportować. Kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Podaj hasło.
5. Wprowadź hasło bazy danych kluczy i kliknij przycisk **OK**. Zostanie wyświetlone okno IBM Key Management (Zarządzanie kluczami IBM). Na pasku tytułu wyświetlana jest nazwa wybranego pliku bazy danych kluczy pfx, co oznacza, że plik jest otwarty i gotowy.
6. Z listy wybierz pozycję **Signer Certificates** (Certyfikaty podpisującego). Nazwa przyjazna wymaganego certyfikatu jest wyświetlana jako etykieta na panelu Certyfikaty osoby podpisującej.
7. Wybierz pozycję etykiety i kliknij przycisk **Usuń** , aby usunąć certyfikat osoby podpisującej. Zostanie wyświetlone okno Potwierdzenie.
8. Kliknij przycisk **Tak**. Wybrana etykieta nie jest już wyświetlana na panelu Certyfikaty osoby podpisującej.
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 Otwieranie.
11. Wybierz docelową bazę danych kluczy CMS , do której jest importowany plik pfx. Kliknij opcję **Open** (Otwórz). Zostanie wyświetlone okno Podaj hasło.
12. Wprowadź hasło bazy danych kluczy i kliknij przycisk **OK**. Zostanie wyświetlone okno IBM Key Management (Zarządzanie kluczami IBM). Na pasku tytułu wyświetlana jest nazwa wybranego pliku bazy danych kluczy, co oznacza, 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 czynności:
    a. Kliknij opcję **Eksportuj/Importuj klucz**. Zostanie wyświetlone okno eksportowania/importowania klucza.
    b. Wybierz opcję **Importuj** w polu Wybierz typ czynności.
15. Jeśli w widoku Certyfikaty osobiste nie ma żadnych certyfikatów, kliknij przycisk **Importuj**.
16. Wybierz plik PKCS12 .
17. Wprowadź nazwę pliku pfx zgodnie z opisem w kroku 4. Kliknij przycisk **OK**. Zostanie wyświetlone okno Podaj hasło.
18. Podaj to samo hasło, które zostało podane podczas usuwania certyfikatu osoby podpisującej. Kliknij przycisk **OK**.
19. Zostanie wyświetlone okno Zmień etykiety (ponieważ powinien być dostępny tylko jeden certyfikat do zaimportowania). Etykieta certyfikatu powinna być identyfikatorem UUID w formacie `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.
20. Aby zmienić etykietę, wybierz identyfikator UUID na panelu **Wybór etykiety do zmiany** . Etykieta zostanie zreplikowana w polu **Wprowadź nową etykietę:** . Zastąp tekst etykiety nazwą przyjazną, która została usunięta w kroku 7, i kliknij przycisk **Zastosuj**. Nazwa przyjazna musi być wartością atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiona) lub wartością domyślną `ibmwebspheremq` (z dołączoną nazwą menedżera kolejek lub identyfikatora logowania użytkownika IBM MQ MQI client) zapisaną małymi literami. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
21. Kliknij przycisk **OK**. Okno Zmień etykiety zostanie usunięte, a oryginalne okno programu IBM Key Management zostanie ponownie wyświetlone z panelami Certyfikaty osobiste i Certyfikaty osoby podpisującej zaktualizowanymi przy użyciu poprawnie oznaczonego certyfikatu osobistego.
22. Certyfikat osobisty pfx jest teraz importowany do docelowej bazy danych.

Nie można zmienić etykiety certyfikatu za pomocą **runmqckm** lub **runmqakm**.

Za pomocą wiersza komend

Aby zaimportować certyfikat osobisty za pomocą programu **runmqckm**, użyj 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**, użyj 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*	jest hasłem dla certyfikatu PKCS #12 .
`-type` *pkcs12*	jest typem pliku.
`-target` *filename*	to nazwa docelowej bazy danych kluczy CMS .
`-target_pw` *password*	jest hasłem dla bazy danych kluczy CMS.
`-target_type` *cms*	to typ bazy danych określony przez opcję `-target`
`-label` *label*	jest etykietą certyfikatu, który ma zostać zaimportowany z źródłowej bazy danych kluczy.

-new_label *label*	jest etykietą, do której certyfikat zostanie przypisany w docelowej bazie danych. Jeśli opcja -new_label zostanie pominięta, domyślnie zostanie użyta ta sama opcja, co opcja -label .
-fips	określa, że komenda jest uruchamiana w trybie FIPS. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.
-pfx	oznacza format pliku PFX.

runmqckm nie udostępnia komendy do bezpośredniej zmiany etykiet certyfikatów. Aby zmienić etykietę certyfikatu, wykonaj następujące kroki:

1. Wyeksportuj certyfikat do pliku PKCS #12 za pomocą komendy **-cert -export** . Podaj istniejącą etykietę certyfikatu dla opcji -label .
2. Usuń istniejącą kopię certyfikatu z oryginalnej bazy danych kluczy za pomocą komendy **-cert -delete** .
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.

ALW *Importowanie certyfikatu osobistego z pliku PKCS #7*

Narzędzia **strmqikm** (iKeyman) i **runmqckm** (iKeycmd) nie obsługują PKCS #7 (.p7b) . Użyj narzędzia **runmqakm** , aby zaimportować certyfikaty z pliku PKCS #7 w systemie AIX, Linux, and Windows.

Użyj następującej komendy, aby dodać certyfikat CA z pliku PKCS #7 :

```
runmqakm -cert -add -db filename -pw password -type cms -file filename
-label label
```

-db *filename*	to pełna nazwa pliku bazy danych kluczy CMS .
-pw *password*	to hasło do bazy danych kluczy.
-type *cms*	jest typem bazy danych kluczy.
-file *filename*	to nazwa pliku PKCS #7 .
-label *label*	to etykieta przypisywana certyfikatowi w docelowej bazie danych. Pierwszy certyfikat przyjmuje podaną etykietę. Wszystkie inne certyfikaty, jeśli są obecne, są oznaczone nazwą podmiotu.

Użyj następującej komendy, aby zaimportować certyfikat osobisty z pliku PKCS #7 :

```
runmqakm -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*	jest hasłem dla certyfikatu PKCS #7 .
-type *pkcs7*	jest typem pliku.
-target *filename*	to nazwa docelowej bazy danych kluczy.
-target_pw *password*	jest hasłem docelowej bazy danych kluczy.
-target_type *cms*	to typ bazy danych określony przez opcję -target
-label *label*	jest etykietą certyfikatu, który ma zostać zaimportowany.

`-new_label` *label*	jest etykietą, do której certyfikat zostanie przypisany w docelowej bazie danych. Jeśli opcja `-new_label` zostanie pominięta, domyślnie zostanie użyta ta sama opcja, co opcja `-label` .

ALW *Usuwanie certyfikatu z repozytorium kluczy w systemie AIX, Linux, and Windows*

Ta procedura służy do usuwania certyfikatów osobistych lub certyfikatów ośrodka CA.

Użycie `strmqikm`

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** . Program **strmqikm** (iKeyman) nie udostępnia opcji zgodności ze standardem FIPS.

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 chcesz usunąć 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 podpisujących** .
9. Wybierz certyfikat, który chcesz usunąć.
10. Jeśli nie masz jeszcze kopii certyfikatu i chcesz ją zapisać, kliknij opcję **Eksportuj/Importuj** i wyeksportuj ją (patrz sekcja “Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 339).
11. Po wybraniu certyfikatu kliknij przycisk **Usuń**. Zostanie otwarte okno Potwierdź.
12. Kliknij przycisk **Tak**. W polu **Certyfikaty osobiste** nie jest już wyświetlana etykieta usuniętego certyfikatu.

Za pomocą wiersza komend

Użyj następujących komend, aby usunąć certyfikat za pomocą komendy **runmqckm** lub komendy **runmqakm** :

Używanie komendy runmqckm:

```
runmqckm -cert -delete -db filename -pw password -label label
```

Używanie komendy runmqakm:

```
runmqakm -cert -delete -db filename -pw password -label label -fips
```

gdzie:

`-db` *filename*	to pełna nazwa 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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **runmqakm** nie powiedzie się.

ALW *Generowanie silnych haseł dla ochrony repozytorium kluczy w systemie AIX, Linux, and Windows*

Silne hasła dla ochrony repozytorium kluczy można wygenerować za pomocą komendy **runmqakm** (GSKCapiCmd).

Aby wygenerować silne hasło, można użyć komendy **runmqakm** z następującymi parametrami:

```
runmqakm -random -create -length 14 -strong -fips
```

Jeśli w parametrze **-pw** kolejnych komend administrowania certyfikatami używane jest wygenerowane hasło, zawsze należy je ująć w cudzysłów. W systemach AIX and Linux należy również użyć ukośnika odwrotnego, aby zmienić znaczenie następujących znaków, jeśli występują one w łańcuchu hasła:

```
!  \  "  '
```

Podczas wprowadzania hasła w odpowiedzi na zapytanie z poziomu interfejsu **runmqckm**, **runmqakm** lub interfejsu GUI programu **strmqikm** nie ma konieczności podawania hasła w cudzysłowie ani zmiany znaczenia. Nie jest to konieczne, ponieważ w takich przypadkach powłoka systemu operacyjnego nie ma wpływu na wprowadzanie danych.

ALW *Konfigurowanie sprzętu szyfrującego w systemie AIX, Linux, and Windows*

Sprzęt szyfrujący dla menedżera kolejek lub klienta można skonfigurować na wiele sposobów.

Sprzęt szyfrujący dla menedżera kolejek w systemie AIX, Linux, and Windows można skonfigurować w jeden z następujących sposobów:

- Użyj komendy **ALTER QMGR** MQSC z parametrem SSLCRYP zgodnie z opisem w instrukcji ALTER QMGR.
- Aby skonfigurować sprzęt szyfrujący w systemie AIX, Linux, and Windows , należy użyć komendy IBM MQ Explorer . Więcej informacji na ten temat zawiera pomoc elektroniczna.

Sprzęt szyfrujący można skonfigurować dla klienta IBM MQ w systemie AIX, Linux, and Windows za pomocą jednej z następujących metod:

- Ustaw zmienną środowiskową **MQSSLCRYP** . Dozwolone wartości parametru **MQSSLCRYP** są takie same, jak dla parametru **SSLCRYP** , zgodnie z opisem w instrukcji ALTER QMGR. Aby ustawić tę zmienną środowiskową, użyj jednej z następujących komend:
  - Linux AIX W systemach AIX and Linux:

    ```
    export MQSSLCRYP=string
    ```

  - Windows W systemach Windows:

    ```
    SET MQSSLCRYP=string
    ```

  gdzie *string* reprezentuje łańcuch parametru, który ma być używany do konfigurowania sprzętu szyfrującego w systemie.

  Jeśli używana jest wersja GSK_PKCS11 parametru **SSLCRYP** , etykieta tokenu PKCS #11 musi być zgodna z etykietą, z którą skonfigurowano sprzęt.

- Ustaw atrybut **SSLCryptoHardware** w sekcji SSL pliku konfiguracyjnego IBM MQ client . Dozwolone wartości są takie same, jak dla 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 konfiguracyjnych protokołu SSL (MQSCO) w wywołaniu MQCONNX. Więcej informacji na ten temat zawiera sekcja Przegląd produktu MQSCO.

Ostrzeżenie: V 9.3.0 Podczas udostępniania konfiguracji sprzętu szyfrującego za pomocą zmiennej środowiskowej **MQSSLCRYP** lub atrybutu **SSLCryptoHardware** należy zabezpieczyć hasło przed zapisaniem. Więcej informacji na ten tematzawiera sekcja “IBM MQ clients , które używają sprzętu szyfrującego” na stronie 622.

Jeśli skonfigurowano sprzęt szyfrujący korzystający z interfejsu PKCS #11 przy użyciu dowolnej z tych metod, należy zapisać certyfikat osobisty do użycia w kanałach w pliku bazy danych kluczy dla skonfigurowanego tokenu szyfrującego. Zostało to opisane w sekcji “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 348.

ALW *Zarządzanie certyfikatami na sprzęcie PKCS #11*

Można zarządzać certyfikatami cyfrowymi na sprzęcie szyfrującym, który obsługuje interfejs PKCS #11 .

O tym zadaniu

Należy utworzyć bazę danych kluczy w celu przygotowania środowiska IBM MQ , nawet jeśli nie mają być w nim przechowywane certyfikaty ośrodka certyfikacji (CA), ale wszystkie certyfikaty będą przechowywane na sprzęcie szyfrującym. Baza danych kluczy jest wymagana, aby menedżer kolejek odwoływała się do niej w polu SSLKEYR lub aby aplikacja kliencka odwoływała się do niej w zmiennej środowiskowej MQSSLKEYR. Ta baza danych kluczy jest również wymagana w przypadku tworzenia żądania certyfikatu.

Bazę danych kluczy można utworzyć za pomocą wiersza komend lub interfejsu użytkownika **strmqikm** (iKeyman).

Procedura

Utwórz bazę danych kluczy przy użyciu wiersza komend.

1. Uruchom jedną z następujących komend:
   - W systemie **runmqckm**:

     V 9.3.0 V 9.3.0
     ```
     runmqckm -keydb -create -db filename -pw password -type type -stash
     ```
   - W systemie **runmqakm**:

     V 9.3.0 V 9.3.0
     ```
     runmqakm -keydb -create -db filename -pw password -type type
     ```

   gdzie:

   -db *nazwa_pliku*
   Określa pełną nazwę pliku bazy danych kluczy CMS.

   -pw *hasło*
   Określa hasło do bazy danych kluczy CMS V 9.3.0 V 9.3.0 lub PKCS#12 .

   V 9.3.0 V 9.3.0 **-type *typ***
   Określa typ bazy danych. (W przypadku systemu IBM MQmusi to być `cms` lub `pkcs12`).

   -stash
   V 9.3.0 V 9.3.0 Opcjonalne. Powoduje zapisanie hasła bazy danych kluczy w pliku.

Alternatywnie można utworzyć bazę danych kluczy za pomocą interfejsu użytkownika **strmqikm** (iKeyman).

2. W systemach AIX and Linux zaloguj się jako użytkownik root. W systemach Windows zaloguj się jako administrator lub członek grupy MQM.
3. Otwórz plik właściwości zabezpieczeń systemu Java , `java.security`.
   - W systemach AIX and Linux plik właściwości zabezpieczeń Java znajduje się w podkatalogu `java/jre64/jre/lib/security` katalogu instalacyjnego IBM MQ .
   - W systemach Windows plik właściwości zabezpieczeń Java znajduje się w podkatalogu `java\jre\lib\security` katalogu instalacyjnego IBM MQ .

   Jeśli nie ma go jeszcze 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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.
8. W polu **Położenie** wprowadź ścieżkę.
   - W systemach AIX and Linux może to być na przykład `/usr/lib/pksc11`.
   - W systemach Windows wpisz nazwę biblioteki. `cryptoki` na przykład.
9. Kliknij przycisk **OK**.

   Zostanie wyświetlone okno Open Cryptographic Token (Otwieranie tokenu szyfrującego).
10. Wybierz etykietę tokenu urządzenia szyfrującego, która ma być używana do przechowywania certyfikatów.
11. W polu **Hasło tokenu szyfrującego** wpisz hasło ustawione podczas konfigurowania sprzętu szyfrującego.
12. Jeśli sprzęt szyfrujący ma możliwość przechowywania certyfikatów osoby podpisującej wymaganych do odebrania lub zaimportowania certyfikatu osobistego, usuń zaznaczenie obu pól wyboru dodatkowej bazy danych kluczy i przejdź do kroku “17” na stronie 350.

    Jeśli do przechowywania certyfikatów osoby podpisującej wymagana jest dodatkowa baza danych CMS V 9.3.0 V 9.3.0 lub PKCS#12 , wybierz opcję **Otwórz istniejący dodatkowy plik bazy danych kluczy** lub **Utwórz nowy dodatkowy plik bazy danych kluczy**.
13. W polu **Nazwa pliku** wpisz nazwę pliku.

    To pole zawiera już tekst `key.kdb`. Jeśli nazwą rdzenia jest `key`, należy pozostawić to pole bez zmian. Jeśli podano inną nazwę rdzenia, należy zastąpić łańcuch `key` nazwą rdzenia.
14. W polu **Położenie** wpisz ścieżkę. Na przykład:
    - W przypadku menedżera kolejek: `/var/mqm/qmgrs/QM1/ssl`
    - W przypadku systemu IBM MQ MQI client: `/var/mqm/ssl`
15. Kliknij przycisk **OK**.

    Zostanie wyświetlone okno Podaj hasło.
16. Wprowadź hasło.

Jeśli w kroku “12” na stronie 349wybrano opcję **Otwórz istniejący dodatkowy plik bazy danych kluczy** , wpisz hasło w polu **Hasło** .

Jeśli w kroku “12” na stronie 349wybrano opcję **Utwórz nowy dodatkowy plik bazy danych kluczy** , wykonaj następujące kroki podrzędne:

a) Wpisz hasło w polu **Hasło** , a następnie wpisz je ponownie w polu **Potwierdź hasło** .

b) V 9.3.0 V 9.3.0
Aby zapisać hasło w pliku, wybierz opcję **Schować hasło w pliku**. Jeśli hasło nie zostanie zeskładowane, należy podać hasło bazy danych kluczy menedżerowi kolejek za pomocą atrybutu KEYRPWD lub IBM MQ MQI client za pomocą jednej z metod opisanych w sekcji “Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323.

c) V 9.3.0 V 9.3.0
Kliknij przycisk **OK**.

Jeśli wybrano opcję zapisania hasła w pliku, zostanie otwarte okno z potwierdzeniem, że hasło znajduje się w pliku `key.sth` (chyba że podano inną nazwę rdzenia).

17. Kliknij przycisk **OK**.
Zostanie wyświetlona ramka zawartości bazy danych kluczy.

ALW *Żądanie certyfikatu osobistego dla sprzętu PKCS #11*

Użyj tej procedury dla menedżera kolejek lub IBM MQ MQI client , aby zażądać certyfikatu osobistego dla sprzętu szyfrującego.

O tym zadaniu

W tym zadaniu opisano sposób użycia interfejsu użytkownika **strmqikm** do zażądania certyfikatu osobistego. Jeśli używany jest interfejs wiersza komend, należy zapoznać się z sekcją “Za pomocą wiersza komend” na stronie 331.

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 .

Deprecated Nazwy algorytmów podpisu cyfrowego SHA3WithRSA i SHA5WithRSA są nieaktualne, ponieważ są skróconą formą algorytmu odpowiednio SHA384WithRSA i SHA512WithRSA .

Procedura

Aby zażądać certyfikatu osobistego z poziomu interfejsu użytkownika **strmqikm** (iKeyman), wykonaj następujące kroki:

1. Wykonaj poniższe kroki, aby pracować ze sprzętem szyfrującym. Patrz sekcja “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 348.
2. W menu **Create** (Utwórz) kliknij opcję **New Certificate Request**(Nowe żądanie certyfikatu).
Zostanie otwarte okno Create New Key and Certificate Request (Utwórz nowy klucz i żądanie certyfikatu).
3. W polu **Key Label** (Etykieta klucza) wpisz etykietę certyfikatu.
Etykieta jest wartością atrybutu **CERTLABL** (jeśli został ustawiony) lub domyślną wartością `ibmwebspheremq` z dodaną nazwą menedżera kolejek lub ID użytkownika logowania IBM MQ MQI client (wszystkie te wartości są zapisane małymi literami). Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .
4. Wybierz wymaganą opcję **Wielkość klucza** i **Algorytm podpisu** .
5. Wprowadź wartości w polach **Nazwa zwykła** i **Organizacja**, a następnie wybierz opcję **Kraj**. Dla pozostałych pól opcjonalnych zaakceptuj wartości domyślne lub wpisz albo wybierz nowe wartości.
Należy zauważyć, że w polu **Jednostka organizacyjna** można podać tylko jedną nazwę. Więcej informacji na temat tych pól zawiera sekcja “Nazwy wyróżniające” na stronie 15.

6. W polu **Wprowadź nazwę pliku, w którym ma zostać 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**.

   Lista **Żądania certyfikatu osobistego** zawiera etykietę nowo utworzonego żądania certyfikatu osobistego. Żądanie certyfikatu jest przechowywane w pliku wybranym w kroku “6” na stronie 351.
9. Zażądaj nowego certyfikatu osobistego, wysyłając plik do ośrodka certyfikacji (CA) lub kopiując plik do formularza żądania w serwisie WWW ośrodka CA.

ALW *Odbieranie certyfikatu osobistego do sprzętu PKCS #11*

Ta procedura służy do odbierania certyfikatu osobistego do sprzętu szyfrującego przez menedżera kolejek lub IBM MQ MQI client .

Zanim rozpoczniesz

Dodaj certyfikat ośrodka CA, który podpisał certyfikat osobisty. Dodaj go do sprzętu szyfrującego lub dodatkowej bazy danych kluczy CMS . Należy to zrobić przed otrzymaniem podpisanego certyfikatu do sprzętu szyfrującego. Aby dodać certyfikat CA do pliku kluczy, wykonaj procedurę opisaną w sekcji “Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 338.

Procedura

- Aby otrzymać certyfikat osobisty za pomocą interfejsu użytkownika **strmqikm** (iKeyman), wykonaj następujące kroki:
  a) Wykonaj poniższe kroki, aby pracować ze sprzętem szyfrującym. Patrz sekcja “Zarządzanie certyfikatami na sprzęcie PKCS #11” na stronie 348.
  b) Kliknij opcję **Odbierz**. Zostanie otwarte okno Receive Certificate from a File (Pobierz certyfikat z pliku).
  c) Wpisz nazwę pliku certyfikatu i położenie 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 pytaniem, czy chcesz ustawić 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**. Lista **Certyfikaty osobiste** zawiera etykietę nowo dodanego certyfikatu osobistego. Ta etykieta jest tworzona przez dodanie etykiety tokenu szyfrującego przed podaną etykietą.
- Aby uzyskać certyfikat osobisty za pomocą komendy **runmqakm** (GSKCapiCmd), wykonaj następujące kroki:
  a) Otwórz okno komend skonfigurowane dla danego środowiska.
  b) Odbierz certyfikat osobisty 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 dostarczanej ze sprzętem szyfrującym.

-tokenlabel *hardware_token*
Określa etykietę tokenu urządzenia szyfrującego PKCS #11 .

-pw *hasło_do_sprzętu*
Określa hasło dostępu do sprzętu szyfrującego.

-format *format_certyfikatu*
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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów zgodnych ze standardem FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **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 TLS (Transport Layer Security).

Program IBM MQ Appliance zawiera odrębne komendy służące do zarządzania certyfikatami. Szczegółowe informacje na temat zarządzania certyfikatami zawiera dokumentacja IBM MQ Appliance , sekcja 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 poszczególnych zadań przy użyciu 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 do przetwarzania wywołań TLS, zgodnie z opisem w sekcji “Ustawianie parametru SSLTASKS w systemie z/OS” na stronie 353.

z/OS Obsługa protokołu TLS jest integralną częścią systemu operacyjnego i jest nazywana *systemową obsługą SSL*. Systemowa implementacja protokołu SSL jest częścią elementu Cryptographic Services Base produktu z/OS. Elementy programu Cryptographic Services Base są instalowane w *pdsname*. SIEALNKE- partycjonowany zestaw danych (PDS). Podczas instalowania systemowej implementacji protokołu SSL należy upewnić się, że wybrano odpowiednie opcje w celu udostępnienia wymaganych CipherSpecs .

Więcej informacji na temat odnawiania certyfikatu samopodpisanego zawiera sekcja Kroki odnawiania certyfikatu samopodpisanego w programie RACF .

z/OS *Dodatkowe wymagania dotyczące identyfikatora użytkownika dla protokołu TLS w systemie z/OS*

W tej sekcji opisano dodatkowe wymagania, jakie musi spełnić identyfikator użytkownika, aby mógł on skonfigurować protokół TLS w systemie z/OSi pracować z nim.

Upewnij się, że w systemie znajdują się wszystkie odpowiednie aktualizacje HIPER (High Impact lub Pervasive).

Jeśli repozytorium kluczy jest własnością identyfikatora użytkownika CHINIT, ten identyfikator użytkownika musi mieć prawo do odczytu IRR systemu IRR.DIGTCERT.LISTRING w klasie FACILITY i prawo do aktualizacji w przeciwnym razie oraz prawo do odczytu IRR.DIGTCERT.LIST . Nadanie dostępu za pomocą komendy PERMIT z odpowiednio ACCESS (UPDATE) lub ACCESS (READ)

Upewnij się, że zostały skonfigurowane następujące wymagania wstępne:

- Identyfikator użytkownika *ssidCHIN* jest poprawnie zdefiniowany w pliku RACF, a identyfikator użytkownika *ssidCHIN* ma odpowiedni dostęp do następujących profili:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Te zmienne są zdefiniowane w klasie RACF FACILITY.
- ID użytkownika *ssidCHIN* jest właścicielem pliku kluczy.
- Certyfikat osobisty menedżera kolejek, jeśli został utworzony za pomocą komendy RACDCERT, jest tworzony przy użyciu identyfikatora użytkownika typu certyfikatu, który jest również taki sam jak identyfikator użytkownika produktu *ssidCHIN* .
- Inicjator kanału jest restartowany lub jest wprowadzana komenda **REFRESH SECURITY TYPE(SSL)** w celu pobrania wszystkich zmian wprowadzonych w pliku kluczy.
- Procedura inicjatora kanału IBM MQ ma dostęp do systemowej biblioteki środowiska wykonawczego SSL *nazwa_zestawu_danych*.SIEALNKE za pośrednictwem listy dowiązań, LPA lub instrukcji STEPLIB DD. Ta biblioteka musi być autoryzowana przez APF.
- Identyfikator użytkownika, dla którego uruchomiono inicjatora kanału, jest skonfigurowany do używania produktu z/OS UNIX System Services (z/OS UNIX) zgodnie z opisem w dokumentacji z/OS UNIX System Services Planowanie .

  Użytkownicy, którzy nie chcą, aby inicjator kanału wywoływało funkcję z/OS UNIX przy użyciu guest/default UID i OMVS, muszą tylko modelować nowy segment OMVS na podstawie segmentu domyślnego, ponieważ inicjator kanału nie wymaga specjalnych uprawnień i nie jest uruchamiany w produkcie UNIX jako administrator.

  Przykładowe komendy można znaleźć w sekcji “Nadawanie inicjatorowi kanału poprawnych praw dostępu w systemie z/OS” na stronie 355 .

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, upewnij 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 jest sprawdzana lista odwołań certyfikatów (CRL).

Jeśli używane jest sprawdzanie listy CRL, kanał, którego to dotyczy, wstrzymuje zadanie SSLTASK przez czas trwania tego sprawdzania. Może to być długi czas, który upłynął podczas kontaktu z odpowiednim serwerem LDAP, ponieważ każdy parametr SSLTASK jest blokiem kontrolnym zadania systemu z/OS .

W przypadku zmiany wartości atrybutu SSLTASKS 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. Użyj parametru SSLKEYR komendy ALTER QMGR, aby powiązać repozytorium kluczy z menedżerem kolejek. Więcej informacji zawiera temat “Repozytorium kluczy SSL/TLS” na stronie 25.

W systemie z/OScertyfikaty cyfrowe są przechowywane w *pliku kluczy* zarządzanym przez zewnętrznego menedżera zabezpieczeń (External Security Manager-ESM). Te certyfikaty cyfrowe mają etykiety, które wiążą certyfikat z menedżerem kolejek. Protokół TLS używa tych certyfikatów do celów uwierzytelniania.

We wszystkich poniższych przykładach używane są komendy RACF . Dla innych programów ESM istnieją równoważne komendy.

W systemie z/OSprogram IBM MQ używa wartości atrybutu **CERTLABL** , jeśli jest ustawiony, lub domyślnej wartości `ibmWebSphereMQ` z dodaną nazwą menedżera kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

Nazwa repozytorium kluczy dla menedżera kolejek to nazwa pliku kluczy w bazie danych RACF . Nazwę pliku kluczy można określić przed utworzeniem pliku kluczy lub po jego utworzeniu.

Aby utworzyć nowy plik kluczy dla menedżera kolejek, wykonaj następującą procedurę:

1. Upewnij się, że masz odpowiednie uprawnienia do wydania komendy RACDCERT (więcej informacji na ten temat zawiera sekcja Sterowanie użyciem komendy RACDCERT).
2. Wydaj następującą komendę:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   gdzie:

   - *userid1* to identyfikator użytkownika przestrzeni adresowej inicjatora kanału lub identyfikator użytkownika, który będzie właścicielem pliku kluczy (jeśli plik kluczy jest współużytkowany).
   - *nazwa-pliku* jest nazwą, która ma zostać nadana pliku kluczy. Długość tej nazwy może wynosić do 237 znaków. W tej nazwie rozróżniana jest wielkość liter. Aby uniknąć problemów, należy podać *nazwę pliku* zapisaną wielkimi literami.

z/OS *Udostępnianie certyfikatów CA menedżerowi kolejek w systemie z/OS*

Po utworzeniu pliku kluczy połącz z nim wszystkie odpowiednie certyfikaty ośrodka CA.

Jeśli w zestawie danych znajduje się certyfikat ośrodka CA, należy najpierw dodać ten certyfikat do bazy danych RACF za pomocą następującej komendy:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Następnie, aby połączyć certyfikat ośrodka CA dla `My  CA` z bazą kluczy, użyj następującej komendy:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

gdzie *userid1* jest identyfikatorem użytkownika inicjatora kanału lub właścicielem pliku kluczy współużytkowanych.

Więcej informacji na temat certyfikatów CA zawiera sekcja “certyfikaty cyfrowe” na stronie 13.

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 za pomocą jednej z następujących komend MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Sprawdź dane wyjściowe komendy pod kątem 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 MQSC ALTER QMGR w celu ustawienia atrybutu repozytorium kluczy menedżera kolejek.

Na przykład:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

jeśli plik kluczy należy do przestrzeni adresowej inicjatora kanału, lub:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

jeśli jest to plik kluczy współużytkowanych, 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 niektórych profili zabezpieczeń.

Nadawanie dostępu CHINIT do odczytu repozytorium kluczy

Jeśli repozytorium kluczy jest własnością identyfikatora użytkownika CHINIT, ten identyfikator użytkownika musi mieć prawo do odczytu IRR systemu IRR.DIGTCERT.LISTRING w klasie FACILITY i prawo do aktualizacji w przeciwnym razie oraz prawo do odczytu IRR.DIGTCERT.LIST . Przyznaj dostęp za pomocą komendy PERMIT z odpowiednio ACCESS (UPDATE) lub ACCESS (READ):

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
PERMIT IRR.DIGTCERT.LIST CLASS(FACILITY) ID( userid ) ACCESS(READ)
```

gdzie *id_użytkownika* jest identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału.

Nadawanie prawa do odczytu CHINIT odpowiednim profilom CSF*

Aby korzystać z obsługi sprzętu udostępnianej za pośrednictwem narzędzia ICSF (Integrated Cryptographic Service Facility), upewnij się, że ID 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 *csf-resource* jest nazwą profilu CSF*, a *id_użytkownika* jest identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału.

Powtórz tę komendę dla każdego z następujących profili CSF*:

- CSFDSG
- CSFDSV
- CSFPKD
- CFPKE
- CSPKI

Identyfikator użytkownika CHINIT może również wymagać prawa do odczytu innych profili CSF*. Na przykład, jeśli używana jest specyfikacja szyfru ECDHE_RSA_AES_256_GCM_SHA384 , identyfikator użytkownika CHINIT musi mieć również prawo do odczytu następujących profili CSF*:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

Więcej informacji na ten temat zawiera sekcja RACF CSFSERV resource requirements(Wymagania dotyczące zasobów CSFSERV w systemie RACF).

Jeśli klucze certyfikatów są przechowywane w ICSF, a instalacja ustanowiła kontrolę dostępu do kluczy przechowywanych w ICSF, upewnij się, że ID użytkownika CHINIT ma prawo do odczytu profilu w klasie CSFKEYS, używając następującej komendy:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

gdzie *id_użytkownika* jest identyfikatorem użytkownika przestrzeni adresowej inicjatora kanału.

Korzystanie z narzędzia ICSF (Integrated Cryptographic Service Facility)

Inicjator kanału może użyć funkcji ICSF do wygenerowania losowej liczby podczas inicjowania algorytmu zabezpieczania hasłem w celu zaciemnienia haseł przesyłanych przez kanały klienta, jeśli nie jest używany protokół TLS.

Więcej informacji na ten temat zawiera sekcja “Korzystanie z narzędzia ICSF (Integrated Cryptographic Service Facility)” na stronie 280

z/OS *Gdy zmiany w certyfikatach lub repozytorium kluczy zaczną obowiązywać w systemie z/OS*

Zmiany zaczną obowiązywać po uruchomieniu inicjatora kanału lub odświeżeniu repozytorium.

Zmiany certyfikatów w pliku kluczy i w atrybucie repozytorium kluczy zaczynają obowiązywać w następujących sytuacjach:

- Gdy inicjator kanału jest uruchamiany lub restartowany.
- Po wydaniu komendy REFRESH SECURITY TYPE (SSL) w celu odświeżenia zawartości 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 klucza publicznego i prywatnego 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 bazą kluczy za pomocą 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 pliku kluczy współużytkowanych.
- *userid2* to identyfikator użytkownika powiązany z certyfikatem, który musi być identyfikatorem przestrzeni adresowej inicjatora kanału.

  userid1 i *userid2* mogą mieć taki sam identyfikator.
- *nazwa-pliku* to nazwa nadana przez użytkownika kluczowi w pliku “Konfigurowanie repozytorium kluczy w systemie z/OS” na stronie 353.

- *nazwa-etykiety* musi być wartością atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiony) lub wartością domyślną `ibmWebSphereMQ` z dodaną nazwą menedżera kolejek. Szczegółowe informacje na ten temat zawiera sekcja Etykiety certyfikatów cyfrowych .

z/OS *Żądanie certyfikatu osobistego w systemie z/OS*

Ubiegać się o certyfikat osobisty przy użyciu programu RACF.

Aby złożyć wniosek o certyfikat osobisty, należy użyć RACF w następujący sposób:

1. Utwórz samopodpisany certyfikat osobisty, na przykład “Tworzenie samopodpisanego certyfikatu osobistego w systemie z/OS” na stronie 356. 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 użytkownika przestrzeni adresowej inicjatora kanału.
   - *nazwa_etykiety* jest etykietą używaną podczas tworzenia certyfikatu samopodpisanego.

   Szczegółowe informacje można znaleźć w sekcji “Etykiety certyfikatów cyfrowych, zrozumienie wymagań” na stronie 27.
3. Wyślij zestaw danych do ośrodka certyfikacji (CA), aby zażądać nowego certyfikatu osobistego.
4. Po zwróceniu podpisanego certyfikatu przez ośrodek certyfikacji dodaj certyfikat z powrotem do bazy danych RACF , używając oryginalnej etykiety, zgodnie z opisem w sekcji “Dodawanie certyfikatów osobistych do repozytorium kluczy w systemie z/OS” na stronie 358.

z/OS *Tworzenie podpisanego certyfikatu osobistego RACF*

RACF może działać jako ośrodek certyfikacji i wystawiać własny certyfikat ośrodka CA.

W tej sekcji termin *certyfikat osoby podpisującej* oznacza certyfikat ośrodka CA wydany przez firmę RACF.

Klucz prywatny certyfikatu osoby podpisującej musi znajdować się w bazie danych RACF przed wykonaniem następującej procedury:

1. Użyj następującej komendy, aby wygenerować certyfikat osobisty podpisany przez RACFprzy użyciu certyfikatu osoby podpisującej znajdującego się w bazie danych 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 bazą kluczy za pomocą 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 pliku kluczy współużytkowanych.

- *userid2* to identyfikator użytkownika powiązany z certyfikatem, który musi być identyfikatorem przestrzeni adresowej inicjatora kanału.

  userid1 i *userid2* mogą mieć taki sam identyfikator.
- *nazwa-pliku* to nazwa nadana przez użytkownika kluczowi w pliku "Konfigurowanie repozytorium kluczy w systemie z/OS" na stronie 353.
- *nazwa-etykiety* musi być wartością atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiony) lub wartością domyślną `ibmWebSphereMQ` z dołączoną 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 dodaj go do pliku kluczy, wykonując następującą procedurę:

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 bazą kluczy za pomocą 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 pliku kluczy współużytkowanych.
- *userid2* to identyfikator użytkownika powiązany z certyfikatem, który musi być identyfikatorem przestrzeni adresowej inicjatora kanału.
- *nazwa-pliku* to nazwa nadana przez użytkownika kluczowi w pliku "Konfigurowanie repozytorium kluczy w systemie z/OS" na stronie 353.
- *nazwa-zestawu-danych-wejściowych* jest nazwą zestawu danych zawierającego certyfikat podpisany przez ośrodek CA. Zestaw danych musi być wpisany do katalogu i nie może być zestawem PDS ani elementem zestawu PDS. Format rekordu (RECFM) oczekiwany przez RACDCERT to VB. RACDCERT dynamicznie przydziela i otwiera zestaw danych oraz odczytuje z niego certyfikat jako dane binarne.
- *nazwa-etykiety* jest nazwą etykiety, która została użyta podczas tworzenia oryginalnego żądania. Musi to być wartość atrybutu IBM MQ **CERTLABL** (jeśli jest ustawiony) lub wartość domyślna `ibmWebSphereMQ` z dodaną 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* jest identyfikatorem użytkownika, pod którym certyfikat został dodany do pliku kluczy.
- *nazwa-etykiety* jest etykietą certyfikatu, który ma zostać wyodrębniony.

- *nazwa-zestawu-danych-wyjściowych* to zestaw danych, w którym umieszczany jest certyfikat.
- CERTB64 jest certyfikatem X.509 w formacie Base64 . Można wybrać alternatywny format, na przykład:

  CERTDER
  Certyfikat X.509 kodowany DER 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 przy użyciu komendy RACDCERT.

Przed usunięciem certyfikatu osobistego można zapisać jego kopię. Aby skopiować certyfikat osobisty do zestawu danych przed jego usunięciem, należy wykonać procedurę opisaną w sekcji “Eksportowanie certyfikatu osobistego z repozytorium kluczy w systemie z/OS” na stronie 358. Następnie użyj następującej komendy, aby usunąć certyfikat osobisty:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

gdzie:

- *userid2* jest identyfikatorem 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 znaleziono certyfikat z określoną etykietą, ale nie chcesz go usuwać, możesz zmienić jego nazwę tymczasowo za pomocą następującej komendy:

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

gdzie:

- *userid2* jest identyfikatorem użytkownika, pod którym certyfikat został dodany do pliku kluczy.
- *nazwa-etykiety* jest nazwą certyfikatu, którego nazwa ma zostać zmieniona.
- *new-label-name* to nowa nazwa certyfikatu.

Może to być przydatne podczas testowania uwierzytelniania klienta TLS.

z/OS *Powiązanie identyfikatora użytkownika z certyfikatem cyfrowym w systemie z/OS*

IBM MQ może używać identyfikatora użytkownika powiązanego z certyfikatem RACF jako identyfikatora użytkownika kanału. Powiąż ID użytkownika z certyfikatem, instalując go z tym ID użytkownika lub używając filtru nazwy certyfikatu.

Metoda opisana w tym temacie jest alternatywą dla niezależnej od platformy metody powiązania identyfikatora użytkownika z certyfikatem cyfrowym, który używa rekordów uwierzytelniania kanału. Więcej informacji na temat rekordów uwierzytelniania kanału zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.

Gdy jednostka na jednym końcu kanału TLS otrzymuje certyfikat ze zdalnego połączenia, jednostka pyta RACF , czy istnieje ID użytkownika powiązany z tym certyfikatem. Jednostka używa tego ID użytkownika jako ID użytkownika kanału. Jeśli z certyfikatem nie jest powiązany żaden identyfikator użytkownika, jednostka używa identyfikatora użytkownika, pod którym działa inicjator kanału.

Powiąż identyfikator użytkownika z certyfikatem w jeden z następujących sposobów:

- Zainstaluj ten certyfikat w bazie danych RACF , używając identyfikatora użytkownika, z którym chcesz go powiązać, zgodnie z opisem w sekcji "Dodawanie certyfikatów osobistych do repozytorium kluczy w systemie z/OS" na stronie 358.
- Użyj filtru nazwy certyfikatu (Certificate Name Filter-CNF), aby odwzorować nazwę wyróżniającą podmiotu lub wystawcy certyfikatu na identyfikator użytkownika zgodnie z opisem w sekcji "Konfigurowanie filtru nazwy certyfikatu w systemie z/OS" na stronie 360.

z/OS *Konfigurowanie filtru nazwy certyfikatu w systemie z/OS*

Komenda RACDCERT służy do definiowania filtru nazwy certyfikatu (Certificate Name Filter-CNF), który odwzorowuje nazwę wyróżniającą na identyfikator użytkownika.

Aby skonfigurować środowisko CNF, wykonaj następujące kroki.

1. Włącz funkcje CNF za pomocą następującej komendy. Do tego celu wymagane jest uprawnienie do aktualizacji klasy DIGTNMAP.

   ```
   SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
   ```

2. Zdefiniuj 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` i lokalizację `Internet`.

3. Odśwież odwzorowania CNF:

   ```
   SETROPTS RACLIST(DIGTNMAP) REFRESH
   ```

Uwaga:

1. Jeśli rzeczywisty certyfikat jest przechowywany w bazie danych RACF , identyfikator użytkownika, pod którym jest on zainstalowany, jest używany zamiast identyfikatora użytkownika powiązanego z dowolnym CNF. Jeśli certyfikat nie jest przechowywany w bazie danych RACF , używany jest identyfikator użytkownika powiązany z najbardziej zgodnym CNF. Dopasowania nazwy wyróżniającej podmiotu są uważane za bardziej szczegółowe niż dopasowania nazwy wyróżniającej wystawcy.
2. Zmiany w CNF nie mają zastosowania do czasu odświeżenia odwzorowań CNF.
3. Nazwa wyróżniająca jest zgodna z filtrem nazwy wyróżniającej w środowisku 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 są zwykle wyświetlane po prawej stronie nazwy wyróżniającej, ale pojawiają się na początku certyfikatu.

   Na przykład można rozważyć użycie filtru 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 nazwy wyróżniającej. Należy rozważyć wykluczenie tych certyfikatów, podając wzorzec nazwy wyróżniającej we wzorcu SSLPEER w komendzie DEFINE CHANNEL.
4. Jeśli najbardziej konkretny zgodny plik CNF jest zdefiniowany w pliku RACF jako NOTRUST, jednostka używa identyfikatora użytkownika, pod którym działa inicjator kanału.
5. RACF używa znaku `'.'` jako separatora. W systemie IBM MQ używany jest przecinek lub średnik.

Można zdefiniować funkcje CNF, aby zapewnić, że jednostka nigdy nie ustawi domyślnego identyfikatora użytkownika kanału, który jest identyfikatorem użytkownika, pod którym działa inicjator kanału. Dla

każdego certyfikatu ośrodka CA w pliku kluczy powiązanym z jednostką zdefiniuj CNF z IDNFILTER, który jest dokładnie zgodny z nazwą wyróżniającą (DN) tego certyfikatu ośrodka CA. Dzięki temu wszystkie certyfikaty, które mogą być używane przez jednostkę, będą zgodne z co najmniej jednym z tych CNF. Dzieje się tak, ponieważ wszystkie takie 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 używanych do manipulowania CNF zawiera publikacja *z/OS Security Server RACF Security Administrator's Guide* .

z/OS *Definiowanie kanału nadawczego i kolejki transmisji w systemie QMA w systemie z/OS*

Użyj komend **DEFINE CHANNEL** i **DEFINE QLOCAL** , aby skonfigurować wymagane obiekty.

Procedura

W systemie QMA wydaj komendy podobne do następujących:

```
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.QMBi kolejka transmisji QMB.

z/OS *Definiowanie kanału odbiorczego w QMB w systemie z/OS*

Użyj komendy **DEFINE CHANNEL** , aby skonfigurować wymagany obiekt.

Procedura

W systemie QMB wydaj komendę podobną do poniższej:

```
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, zostanie utworzony.

z/OS *Uruchamianie kanału nadawczego w autoryzacji QMA w systemie z/OS*

W razie potrzeby uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom program nasłuchujący w QMB.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i w razie potrzeby uruchamia kanał odbiorczy. Informacje na temat uruchamiania programu nasłuchującego zawiera sekcja Uruchamianie programu nasłuchującego kanału.
2. Opcjonalne: Jeśli kanały SSL/TLS były już wcześniej uruchomione, należy wydać komendę REFRESH SECURITY TYPE(SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
3. Uruchom kanał w systemie QMA za pomocą komendy START CHANNEL(TO.QMB).

Wyniki

Kanał nadawczy jest uruchomiony.

z/OS *Wymiana certyfikatów samopodpisanych w systemie z/OS*

Wymień wcześniej wyodrębnione certyfikaty. Jeśli używany jest protokół FTP, należy użyć poprawnego formatu.

Procedura

Prześlij część CA certyfikatu QM1 do systemu QM2 i na odwrót, na przykład przez FTP.

Jeśli certyfikaty są przesyłane przy użyciu protokołu FTP, należy to zrobić w poprawnym formacie.

Prześlij następujące typy certyfikatów w formacie *binarnym* :

- Binarny kod binarny kodowany DER X.509
- PKCS #7 (certyfikaty CA)
- PKCS #12 (certyfikaty osobiste)

Prześlij następujące typy certyfikatów w formacie ASCII:

- PEM (prywatność-rozszerzona poczta)
- Base64 encoded X.509

z/OS *Definiowanie kanału nadawczego i kolejki transmisji w menedżerze kolejek QM1 w systemie z/OS*

Użyj komend **DEFINE CHANNEL** i **DEFINE QLOCAL** , aby skonfigurować wymagane obiekty.

Procedura

W przypadku QM1wydaj komendy podobne do poniższych:

```
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)
```

CipherSpecs na każdym końcu kanału muszą być takie same.

Tylko parametr SSLCIPH jest obowiązkowy, jeśli kanał ma używać protokołu TLS. Informacje na temat dozwolonych wartości parametru SSLCIPH zawiera sekcja “CipherSpecs i CipherSuites w produkcie IBM MQ” na stronie 42 .

Wyniki

Kanał nadawczy, QM1.TO.QM2i kolejka transmisji, QM2, zostały utworzone.

z/OS *Definiowanie kanału odbiorczego w produkcie QM2 w systemie z/OS*

Użyj komendy **DEFINE CHANNEL** , aby skonfigurować wymagany obiekt.

Procedura

W przypadku QM2wprowadź komendę podobną do poniższej:

```
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 w produkcie “Definiowanie kanału nadawczego i kolejki transmisji w menedżerze kolejek QM1 w systemie z/OS” na stronie 362, i używać tej samej CipherSpec.

z/OS *Uruchamianie kanału nadawczego w produkcie QM1 w systemie z/OS*

W razie potrzeby uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom program nasłuchujący w QM2.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i w razie potrzeby uruchamia kanał odbiorczy. Informacje na temat uruchamiania programu nasłuchującego zawiera sekcja Uruchamianie programu nasłuchującego kanału .
2. Opcjonalne: Jeśli kanały SSL/TLS były uruchomione wcześniej, wydaj komendę REFRESH SECURITY TYPE (SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
3. W przypadku kolejki QM1uruchom kanał za pomocą komendy `START CHANNEL(QM1.TO.QM2)`.

Wyniki

Kanał nadawczy jest 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 w kanale odbiorczym w systemie z/OS*

Użyj komendy **ALTER CHANNEL** , aby ustawić uwierzytelnianie klienta SSL lub TLS jako opcjonalne.

Procedura

W QMB wprowadź następującą komendę:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Uruchamianie kanału nadawczego w produkcie QM1 w systemie z/OS*

W razie potrzeby uruchom inicjatora kanału, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura

1. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom inicjator kanału.
2. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom program nasłuchujący w QM2.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i w razie potrzeby uruchamia kanał odbiorczy. Informacje na temat uruchamiania programu nasłuchującego zawiera sekcja Uruchamianie programu nasłuchującego kanału .
3. Opcjonalne: Jeśli inicjator kanału był już uruchomiony lub wcześniej działał dowolny kanał SSL/TLS, wprowadź komendę REFRESH SECURITY TYPE (SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.

4. W przypadku kolejki QM1uruchom kanał za pomocą komendy START CHANNEL(QM1.TO.QM2).

Wyniki
Kanał nadawczy jest uruchomiony.

z/OS *Uruchamianie kanału nadawczego w autoryzacji QMA w systemie z/OS*
W razie potrzeby uruchom inicjatora kanału, uruchom program nasłuchujący i odśwież zabezpieczenia. Następnie uruchom kanał za pomocą komendy **START CHANNEL** .

Procedura
1. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom inicjator kanału.
2. Opcjonalne: Jeśli nie zostało to jeszcze wykonane, uruchom program nasłuchujący w QMB.

   Program nasłuchujący nasłuchuje przychodzących żądań sieciowych i w razie potrzeby uruchamia kanał odbiorczy. Informacje na temat uruchamiania programu nasłuchującego zawiera sekcja Uruchamianie programu nasłuchującego kanału.
3. Opcjonalne: Jeśli inicjator kanału był już uruchomiony lub jeśli wcześniej działały kanały SSL/TLS, należy wydać komendę REFRESH SECURITY TYPE(SSL).

   Dzięki temu wszystkie zmiany wprowadzone w repozytorium kluczy będą dostępne.
4. Uruchom kanał w systemie QMA za pomocą komendy START CHANNEL(TO.QMB).

Wyniki
Kanał nadawczy jest 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, które są określone przez klienta, jako łańcucha składającego się z co najmniej jednej wartości 4-znakowej w kolejności preferowanej do użycia.

Ważne: Należy zastosować poprawkę z/OS APAR OA61783 , aby umożliwić systemowi operacyjnemu zastosowanie pewnych krzywych eliptycznych, gdy używane są negocjowane połączenia TLS 1.0, TLS 1.1 i/lub TLS 1.2 .

Tę zmienną środowiskową TLS można ustawić w kodzie JCL uruchamiania inicjatora kanału za pomocą 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 używających tej instrukcji.

Upewnij się, że istnieje odniesienie do sekwencyjnego zestawu danych lub podzbioru partycjonowanego zestawu danych, aby to działanie było możliwe, gdy używana jest wartość SSLTASKS większa niż jeden.

Można również użyć analogowego odpowiednika serwera GSK_CLIENT_ECURVE_LIST, czyli GSK_SERVER_ALLOWED_KEX_ECURVES. Więcej informacji na ten temat zawiera sekcja Ograniczanie krzywych eliptycznych wymiany kluczy .

Ponadto listę poprawnych 4-znakowych krzywych eliptycznych i obsługiwanych specyfikacji grup zawiera tabela 5 w sekcji Definicje zestawów algorytmów szyfrowania .

Domyślną specyfikacją jest 00210023002400250019. Jeśli włączona jest obsługa protokołu TLS V1.3 , na końcu listy domyślnej dodawany jest łańcuch 0029 (x25519) .

Identyfikowanie i uwierzytelnianie użytkowników

Użytkowników można identyfikować i uwierzytelniać za pomocą certyfikatów X.509 , struktury MQCSP lub w programie obsługi wyjścia użytkownika kilku typów.

Korzystanie z certyfikatów X.509

Użytkowników można identyfikować i uwierzytelniać za pomocą certyfikatów X.509 za pomocą komendy **SET CHLAUTH** i parametru **SSLPEER** . Parametr **SSLPEER** określa filtr używany do porównania z nazwą wyróżniającą podmiotu certyfikatu pochodzącego od menedżera kolejek węzła sieci lub klienta na drugim końcu kanału.

Więcej informacji na temat używania komendy **SET CHLAUTH** i parametru **SSLPEER** zawiera sekcja SET CHLAUTH.

Certyfikaty cyfrowe mogą być unieważniane przez ośrodki certyfikacji. Status odwołań certyfikatów można sprawdzić przy użyciu protokołu OCSP lub list CRL na serwerach LDAP, w zależności od platformy. Więcej informacji na ten temat zawiera “Praca z odwołanymi certyfikatami” na stronie 382.

Korzystanie ze struktury MQCSP

Struktura parametrów zabezpieczeń połączenia MQCSP jest określona w wywołaniu MQCONNX. Ta struktura może zawierać referencje dostarczane przez aplikację. Aplikacja może podać identyfikator użytkownika i hasło w strukturze MQCSP. W produkcie IBM MQ 9.3.4aplikacje mogą również dostarczać znacznik uwierzytelniania. W razie potrzeby można zmienić protokół MQCSP w wyjściu zabezpieczeń.

Ostrzeżenie: Referencje w strukturze MQCSP są czasami przesyłane przez sieć w postaci zwykłego tekstu. Aby upewnić się, że referencje aplikacji klienckiej są chronione, należy zapoznać się z sekcją “Zabezpieczenie hasłem MQCSP” na stronie 32.

Więcej informacji na ten temat zawierają sekcje “Identyfikowanie i uwierzytelnianie użytkowników przy użyciu struktury MQCSP” na stronie 367 i “Praca ze znacznikami uwierzytelniania” na stronie 371.

Linux AIX W systemach AIX i Linuxidentyfikator użytkownika i hasło określone w strukturze MQCSP mogą zostać uwierzytelnione przy użyciu systemu operacyjnego lub metody PAM (Pluggable Authentication Method). Moduł PAM udostępnia ogólny mechanizm uwierzytelniania użytkowników, który ukrywa szczegóły przed usługami. Więcej informacji na ten tematzawiera sekcja “Korzystanie z metody PAM (Pluggable Authentication Method)” na stronie 394.

Implementowanie identyfikacji i uwierzytelniania w wyjściach

Użytkowników można identyfikować i uwierzytelniać za pomocą kilku typów programów użytkownika. Więcej informacji zawierają sekcje “Implementowanie identyfikacji i uwierzytelniania w wyjściach zabezpieczeń” na stronie 368, “Odwzorowanie tożsamości w wyjściach komunikatów” na stronie 369 i “Odwzorowanie tożsamości w wyjściu funkcji API i wyjściu funkcji API” na stronie 370.

Użytkownicy uprzywilejowani

Użytkownik uprzywilejowany to taki, który ma pełne uprawnienia administracyjne w systemie IBM MQ.

Oprócz użytkowników wymienionych w poniższej tabeli istnieją pewne obiekty i autoryzacje, dla których należy zachować szczególną ostrożność podczas nadawania dostępu, aby zapewnić integralność i bezpieczeństwo menedżera kolejek. Przy udzielaniu któregokolwiek z poniższych zezwoleń należy stosować dodatkową kontrolę:

- Wszelkie autoryzacje do obiektów SYSTEM
- Uprawnienia administracyjne do tworzenia, modyfikowania i usuwania obiektów.

  z/OS W systemie z/OSautoryzacja ta jest autoryzacją bezpieczeństwa komend i uprawnieniem bezpieczeństwa zasobów komend do wydawania komend DEFINE, ALTER i DELETE.

Multi Na wszystkich innych platformach są to autoryzacje administracyjne, takie jak `+crt`, `+chg` i `+dlt`.

- Uprawnienia administracyjne do usuwania zawartości kolejek.

  z/OS W systemie z/OSautoryzacja ta jest uprawnieniem do ochrony komend i zasobów komend do wydawania komend CLEAR.

  Multi Na wszystkich innych platformach autoryzacją tą jest `+clr`.
- Uprawnienia administracyjne do zatrzymywania kanałów, wycofywania lub zatwierdzania komunikatów.

  z/OS W systemie z/OSautoryzacja ta polega na ochronie komend i uprawnieniu do wykonywania 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/OSautoryzacja ta jest dowolnym uprawnieniem nadanym alternatywnym profilom ochrony użytkowników.

  Multi Na wszystkich innych platformach autoryzacją tą jest `+altusr`.
- Autoryzacje kontekstowe, które umożliwiają aplikacjom zmianę kontekstu zabezpieczeń komunikatów.

  z/OS W systemie z/OSautoryzacja ta jest dowolnym uprawnieniem nadanym profilom zabezpieczeń kontekstu.

  Multi Na wszystkich innych platformach autoryzacje te to `+setall` i `+setid`.

Ogólnie rzecz biorąc, aplikacje przesyłania komunikatów powinny mieć nadane tylko podstawowe autoryzacje MQI dla potrzebnych kolejek lub tematów. Kanały MCA, które są wykonywane w ramach nieuprzywilejowanego użytkownika MCAUSER i niektórych specjalnych typów aplikacji, takich jak programy obsługi kolejek niewysłanych wiadomości, mogą wymagać dodatkowych autoryzacji, które nie są normalnie przyznawane aplikacjom, aby działały poprawnie.

Tabela 67. Użytkownicy uprzywilejowani według platformy

Platforma	**Użytkownicy uprzywilejowani**
Systemy Windows	• SYSTEM • Członkowie grupy mqm • Członkowie grupy Administratorzy
Systemy AIX and Linux	• Członkowie grupy mqm
IBM i IBM i Systemy IBM i	• Profile qmqm i qmqmadm • Wszyscy członkowie grupy qmqmadm • Dowolny użytkownik zdefiniowany z ustawieniem *ALLOBJ

Tabela 67. Użytkownicy uprzywilejowani według platformy (kontynuacja)	
Platforma	**Użytkownicy uprzywilejowani**
z/OS	Identyfikator użytkownika, w ramach którego działa inicjator kanału, menedżer kolejek i przestrzenie adresowe zaawansowanych zabezpieczeń komunikatów. Te identyfikatory użytkowników nie mają automatycznie pełnych uprawnień administracyjnych do produktu IBM MQ, ale są uznawane za 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 MQCSP jest podstawowym sposobem sterowania referencjami używanymi do uwierzytelniania przez aplikacje używające interfejsu kolejki komunikatów (MQI).

Struktura MQCSP zawiera referencje, które mogą być używane przez usługę autoryzacji do identyfikowania i uwierzytelniania użytkownika.

Struktura MQCSP może być modyfikowana przez wyjścia zabezpieczeń po stronie klienta lub serwera, nawet jeśli aplikacja nie udostępnia jawnie struktury MQCSP. Przykładem aplikacji, która nie udostępnia jawnie struktury MQCSP, jest aplikacja używająca protokołu IBM MQ classes for JMS. Przykład wyjścia zabezpieczeń po stronie klienta, które wstawia identyfikator użytkownika i hasło w strukturze MQCSP, zawiera sekcja “Wyjście zabezpieczeń po stronie klienta służące do wstawiania identyfikatora użytkownika i hasła (mqccred)” na stronie 84.

V 9.3.4 Struktura MQCSP zawiera identyfikator użytkownika i hasło lub znacznik uwierzytelniania. Do referencji dostarczanych w strukturze MQCSP mają zastosowanie następujące ograniczenia:

- Aplikacja lub wyjście musi podać identyfikator użytkownika i hasło lub znacznik uwierzytelniania, ale nie oba te elementy jednocześnie.
- Do uzyskania dostępu do produktu IBM MQmogą być używane tylko znaczniki uwierzytelniania, które spełniają określone formaty i wymagania. Więcej informacji na temat wymagań dotyczących znaczników uwierzytelniania w produkcie IBM MQzawiera sekcja “Wymagania dotyczące znaczników uwierzytelniania” na stronie 373.
- Jeśli tożsamość w znaczniku uwierzytelniania ma być adoptowana jako kontekst dla aplikacji, znacznik musi udostępniać odpowiednie żądanie użytkownika, a wartość roszczenia musi być poprawnym identyfikatorem użytkownika IBM MQ . Na przykład nazwa użytkownika musi być zgodna z ograniczeniami dotyczącymi maksymalnej długości i znaków specjalnych. Więcej informacji na temat adoptowania ID użytkownika zawiera sekcja “Relacja między ustawieniami MQCSP i adoptowania CTX” na stronie 367.

Więcej informacji na temat struktury MQCSP zawiera sekcja MQCSP-parametry zabezpieczeń.

Ostrzeżenie: Referencje w strukturze MQCSP dla aplikacji klienckiej są czasami przesyłane przez sieć w postaci zwykłego tekstu. Aby upewnić się, że referencje aplikacji klienckiej są chronione, należy zapoznać się z sekcją “Zabezpieczenie hasłem MQCSP” na stronie 32.

Relacja między ustawieniami MQCSP i adoptowania CTX

Produkt IBM MQ zawsze uwierzytelnia referencje, które są przekazywane w strukturze MQCSP, jeśli funkcja uwierzytelniania połączenia jest włączona. Po pomyślnym uwierzytelnieniu referencji produkt IBM MQ może adoptować ID użytkownika na potrzeby kolejnych sprawdzeń autoryzacji operacji wykonywanych przez podłączoną aplikację. Identyfikator użytkownika w referencjach MQCSP jest

adoptowany, jeśli obiekt informacji uwierzytelniającej (AUTHINFO), do którego odwołuje się atrybut **CONNAUTH** menedżera kolejek, jest zdefiniowany z wartością **ADOPTCTX(YES)**.

IBM MQ ma ograniczenie długości identyfikatorów użytkowników, które mogą być używane do sprawdzania autoryzacji. Więcej informacji na temat tych limitów zawiera sekcja "Identyfikatory użytkownika" na stronie 93. Gdy identyfikator użytkownika przekazany w strukturze MQCSP jest adoptowany, produkt IBM MQ zachowuje się inaczej, w zależności od innych opcji konfiguracyjnych:

- W przypadku korzystania z uwierzytelniania połączenia LDAP program IBM MQ adoptuje identyfikator użytkownika znajdujący się w atrybucie krótkiej nazwy użytkownika w rekordzie LDAP użytkownika. Atrybut krótkiej nazwy użytkownika jest ustawiany za pomocą atrybutu **SHORTUSR** obiektu AUTHINFO.

  Na przykład, jeśli parametr **SHORTUSR** ma wartość `'CN'`, a rekord LDAP zawiera użytkownika `'CN=Test,SN=MQ,O=IBM,C=UK'`, używany jest identyfikator użytkownika `Test`.
- Jeśli podczas używania uwierzytelniania połączenia z systemem operacyjnym lub uwierzytelniania PAM, jeśli parametr ADOPTCTX ma wartość YES, identyfikator użytkownika przekazany w strukturze MQCSP jest obcinany w celu spełnienia 12-znakowego limitu identyfikatora użytkownika wynoszącego IBM MQ , gdy jest on przyjmowany 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 opcji AdteTCTX (NO) w konfiguracji CONNAUTH AUTHINFO i zastosować alternatywne podejście, takie jak reguła CHLAUTH USERMAP, wyjście zabezpieczeń lub ustawienie MCAUSER obiektu kanału, aby ustawić ID użytkownika dla kanału.

Implementowanie identyfikacji i uwierzytelniania w wyjściach zabezpieczeń

Wyjścia zabezpieczeń można użyć do zaimplementowania uwierzytelniania jednokierunkowego lub wzajemnego.

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 serwera kanału MQI agent MCA zwykle działa w imieniu menedżera kolejek, z którym jest połączony. Po stronie klienta kanału MQI agent MCA zazwyczaj działa w imieniu użytkownika aplikacji IBM MQ MQI client . W takiej sytuacji uwierzytelnianie wzajemne odbywa się między dwoma menedżerami kolejek lub między menedżerem kolejek i użytkownikiem aplikacji IBM MQ MQI client .

Dostarczone wyjście zabezpieczeń (wyjście kanału SSPI) ilustruje, w jaki sposób można zaimplementować wzajemne uwierzytelnianie, wymieniając znaczniki 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 164.

Uwierzytelnianie wzajemne można również zaimplementować przy użyciu technologii infrastruktury klucza publicznego (Public Key Infrastructure-PKI). Każde wyjście zabezpieczeń generuje losowe dane, podpisuje je przy użyciu klucza prywatnego reprezentowanego przez siebie menedżera kolejek lub użytkownika i wysyła podpisane dane do partnera w komunikacie bezpieczeństwa. Wyjście zabezpieczeń partnera przeprowadza uwierzytelnianie, sprawdzając podpis cyfrowy przy użyciu klucza publicznego

menedżera kolejek lub użytkownika. Przed wymianą podpisów cyfrowych wyjścia zabezpieczeń mogą wymagać uzgodnienia algorytmu generowania streszczenia komunikatu, jeśli dostępny jest więcej niż jeden algorytm.

Gdy wyjście zabezpieczeń wysyła podpisane dane do swojego partnera, musi także wysłać pewne środki w celu zidentyfikowania reprezentowanego przez siebie menedżera kolejek lub użytkownika. Może to być nazwa wyróżniająca, a nawet certyfikat cyfrowy. Jeśli zostanie wysłany certyfikat cyfrowy, wyjście zabezpieczeń partnera może sprawdzić poprawność certyfikatu, przechodząc przez łańcuch certyfikatów do certyfikatu głównego ośrodka CA. Zapewnia to prawo własności do klucza publicznego, który jest używany do sprawdzania podpisu cyfrowego.

Wyjście zabezpieczeń partnera może sprawdzić poprawność certyfikatu cyfrowego tylko wtedy, gdy ma dostęp do repozytorium kluczy zawierającego pozostałe certyfikaty w łańcuchu certyfikatów. Jeśli certyfikat cyfrowy dla menedżera kolejek lub użytkownika nie zostanie wysłany, musi być dostępny w repozytorium kluczy, do którego ma dostęp wyjście zabezpieczeń partnera. Wyjście zabezpieczeń partnera nie może sprawdzić podpisu cyfrowego, jeśli nie może znaleźć klucza publicznego osoby podpisującej.

Protokół TLS (Transport Layer Security) wykorzystuje techniki PKI, takie jak opisane powyżej. Więcej informacji na temat sposobu uwierzytelniania za pomocą protokołu Secure Sockets Layer zawiera sekcja “Pojęcia związane z protokołem TLS (Transport Layer Security)” na stronie 18.

Jeśli zaufany serwer uwierzytelniania lub obsługa infrastruktury PKI nie są dostępne, można użyć innych technik. Wspólna technika, którą można zaimplementować w wyjściach zabezpieczeń, używa algorytmu klucza symetrycznego.

Jedno z wyjść zabezpieczeń, wyjście A, generuje liczbę losową i wysyła ją w komunikacie bezpieczeństwa do wyjścia zabezpieczeń partnera, wyjście B. Wyjście B szyfruje liczbę przy użyciu kopii klucza, która jest znana tylko dwóm wyjściom zabezpieczeń. Wyjście B wysyła zaszyfrowaną liczbę do wyjścia A w komunikacie bezpieczeństwa z drugą liczbą losową wygenerowaną przez wyjście B. Wyjście A sprawdza, czy pierwsza liczba losowa została poprawnie zaszyfrowana, szyfruje drugą liczbę losową przy użyciu kopii klucza i wysyła zaszyfrowaną liczbę do wyjścia B w komunikacie bezpieczeństwa. Następnie wyjście B sprawdza, czy druga liczba losowa została poprawnie zaszyfrowana. Podczas tej wymiany, jeśli którekolwiek wyjście zabezpieczeń nie jest spełnione z uwierzytelnieniem innego, może nakazać agentowi MCA zamknięcie kanału.

Zaletą tej techniki jest to, że żaden klucz ani hasło nie są przesyłane przez połączenie komunikacyjne podczas wymiany. Wadą jest to, że nie stanowi ona rozwiązania problemu z dystrybucją klucza współużytkowanego w bezpieczny sposób. Jedno rozwiązanie tego problemu zostało opisane w sekcji “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 515. Podobną technikę stosuje się w SNA do wzajemnego uwierzytelniania dwóch jednostek logicznych, gdy są one powiązane z sesją. Technika ta została opisana w sekcji “Uwierzytelnianie na poziomie sesji” na stronie 129.

Wszystkie powyższe techniki uwierzytelniania wzajemnego można dostosować, aby zapewnić uwierzytelnianie jednokierunkowe.

Odwzorowanie tożsamości w wyjściach komunikatów

Programów zewnętrznych komunikatów można używać do przetwarzania informacji w celu uwierzytelniania ID użytkownika, ale lepszym rozwiązaniem może być 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 użyte do uwierzytelnienia ID użytkownika. Dane te mogą być dodawane przez wyjście komunikatu na wysyłającym końcu kanału i sprawdzane przez wyjście komunikatu na odbierającym końcu kanału. Dane uwierzytelniające mogą być na przykład zaszyfrowanym hasłem lub podpisem cyfrowym.

Ta usługa może być bardziej efektywna, jeśli jest zaimplementowana na poziomie aplikacji. Podstawowym wymaganiem jest, aby użytkownik aplikacji, która odbiera komunikat, mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała komunikat. Dlatego jest rzeczą naturalną, aby rozważyć wdrożenie tej

usługi na poziomie aplikacji. Więcej informacji na ten temat zawiera sekcja "Odwzorowanie tożsamości w wyjściu funkcji API i wyjściu funkcji API" na stronie 370.

Odwzorowanie tożsamości w wyjściu funkcji API i wyjściu funkcji API

Aplikacja, która odbiera komunikat, musi być w stanie zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała 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 komunikatu. Podstawowym wymaganiem jest, aby użytkownik aplikacji, która odbiera komunikat, mógł zidentyfikować i uwierzytelnić użytkownika aplikacji, która wysłała komunikat. Należy zauważyć, że wymaganie dotyczy uwierzytelniania jednokierunkowego, a nie dwukierunkowego.

W zależności od sposobu implementacji użytkownicy i ich aplikacje mogą potrzebować interfejsu, a nawet interakcji z usługą. Ponadto czas i sposób korzystania z usługi mogą zależeć od miejsca, w którym znajdują się użytkownicy i ich aplikacje, oraz od charakteru samych aplikacji. W związku z tym naturalne jest, że należy rozważyć wdrożenie usługi na poziomie aplikacji, a nie na poziomie łącza.

Jeśli użytkownik rozważa zaimplementowanie tej usługi na poziomie łącza, może być konieczne rozwiązanie następujących problemów:

- W przypadku kanału komunikatów, w jaki sposób można zastosować usługę tylko do tych komunikatów, które jej wymagają?
- W jaki sposób można umożliwić użytkownikom i ich aplikacjom interakcję z usługą, jeśli jest to wymagane?
- W sytuacji wieloprzeskokowej, gdy komunikat jest wysyłany przez więcej niż jeden kanał komunikatów w drodze do miejsca docelowego, gdzie są wywoływane komponenty usługi?

Poniżej przedstawiono kilka przykładów implementacji usługi 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 funkcji API może uzyskać znacznik uwierzytelniania z zaufanego serwera uwierzytelniającego, takiego jak Kerberos. Wyjście funkcji API może dodać ten znacznik do danych aplikacji w komunikacie. Po pobraniu komunikatu przez aplikację odbierającą drugie wyjście funkcji API może poprosić serwer uwierzytelniający o uwierzytelnienie nadawcy przez sprawdzenie znacznika.
- Gdy aplikacja umieszcza komunikat w kolejce, wyjście funkcji API może dodać następujące elementy do danych aplikacji w komunikacie:
  - Certyfikat cyfrowy nadawcy
  - Podpis cyfrowy nadawcy

  Jeśli dostępne są różne algorytmy generowania streszczenia komunikatu, wyjście funkcji API może zawierać nazwę używanego algorytmu.

  Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może wykonać następujące sprawdzenia:

  - Wyjście funkcji API może sprawdzić poprawność certyfikatu cyfrowego, przechodząc przez łańcuch certyfikatów do certyfikatu głównego ośrodka CA. W tym celu wyjście funkcji API musi mieć dostęp do repozytorium kluczy zawierającego 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 przy użyciu klucza publicznego zawartego w certyfikacie. To sprawdzenie uwierzytelnia nadawcę.

  Zamiast całego certyfikatu cyfrowego można wysłać nazwę wyróżniającą nadawcy. W takim przypadku repozytorium kluczy musi zawierać certyfikat nadawcy, aby drugie wyjście funkcji API było w stanie 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 funkcji API może dodać pewne dane, takie jak zaszyfrowane hasło, do danych aplikacji w komunikacie. Gdy komunikat jest pobierany przez aplikację odbierającą, drugie wyjście funkcji API może uwierzytelnić ID użytkownika przy użyciu danych, które przeszły z komunikatem.

  Technika ta może być uważana za wystarczającą dla komunikatów pochodzących z kontrolowanego i zaufanego środowiska oraz w sytuacjach, w których nie jest dostępna obsługa zaufanego serwera uwierzytelniającego lub infrastruktury PKI.

V 9.3.4 Linux AIX Praca ze znacznikami uwierzytelniania

Aplikacje klienckie IBM MQ 9.3.4 mogą udostępniać znaczniki na potrzeby uwierzytelniania w menedżerze kolejek działającym w systemie AIX lub Linux. Identyfikator użytkownika w tokenie może być również używany do autoryzacji dostępu do zasobów IBM MQ .

JWT (JSON Web Tokens) adoptuje model tożsamości oparty na roszczeniach. Tożsamość i kontrola dostępu są streszczane w ideach wystawców roszczeń i tokenów.

- Roszczenie to para nazwa-wartość, która zawiera informacje o użytkowniku i określa, kim jest użytkownik, a nie co może zrobić.
- Wystawca tokenu jest zaufaną osobą trzecią lub serwerem, który wystawia token dla użytkownika tylko na podstawie tożsamości użytkownika. Wystawca tokenu nie jest zainteresowany tym, co użytkownik może zrobić.

Token to prosta struktura, która zawiera roszczenia i może być łatwo przekazywana między stronami za pośrednictwem Internetu. Używanie tokenów do uwierzytelniania jest korzystne ze względu na scentralizowane zarządzanie tożsamością. Można użyć jednego zaufanego wystawcy tokenu, aby aplikacje mogły uwierzytelniać się w wielu usługach bez konieczności oddzielnego rejestrowania się w każdej z nich. Tokeny zapewniają większe bezpieczeństwo, ponieważ referencje nie są wysyłane do każdej usługi, tylko do zaufanego wystawcy.

Token JWT jest definiowany za pośrednictwem proponowanego standardu internetowego RFC7519.

W jaki sposób tokeny działają z produktem IBM MQ

Znaczniki, które są używane z produktem IBM MQ , muszą być poprawnymi znacznikami JWT, które zostały podpisane przy użyciu algorytmu obsługiwanego przez produkt IBM MQ . Znacznik JWT musi być podpisany zgodnie ze standardem JSON Web Signature (JWS). Tokeny korzystające z technologii JSON Web Encryption (JWE) i JSON Web Key (JWK) JOSE nie mogą być używane z produktem IBM MQ. Więcej informacji na ten temat zawiera sekcja “Wymagania dotyczące znaczników uwierzytelniania” na stronie 373.

Aplikacja, która dostarcza znacznik uwierzytelniania, może działać na dowolnej platformie obsługującej produkt IBM MQ clients. Aplikacja musi być napisana w języku C V 9.3.5 lub w języku IBM MQ 9.3.5, w języku Java, i nawiązywać połączenie z menedżerem kolejek przy użyciu powiązań klienta. Jednak menedżer kolejek musi działać w systemie AIX lub Linux. Menedżer kolejek musi być skonfigurowany do akceptowania znaczników uwierzytelniania. Repozytorium kluczy musi zawierać certyfikat klucza publicznego lub klucz symetryczny zaufanego wystawcy znacznika, w zależności od tego, który algorytm jest używany do podpisywania znacznika.

Wystawca tokenu jest zaufanym podmiotem, który ma delegowany dostęp do zabezpieczeń, co oznacza, że weryfikuje tożsamość użytkownika aplikacji. Menedżer kolejek sprawdza, czy znacznik uwierzytelniania jest poprawny i czy uwierzytelniony użytkownik ma uprawnienia dostępu do obiektów IBM MQ . Menedżer kolejek może, ale nie musi znać użytkowników przed pierwszym nawiązaniem połączenia ze znacznikiem. Administrator produktu IBM MQ musi skonfigurować uwierzytelnianie i autoryzację dla aplikacji, które łączą się z menedżerem kolejek, oraz ustawić wymagania dotyczące elementów, które muszą zawierać znaczniki.

Aplikacja kliencka może dynamicznie zażądać tokenu od wystawcy, którego używa do uwierzytelniania podczas nawiązywania połączenia z produktem IBM MQ. Następnie aplikacja używa struktury MQCSP V 9.3.5 lub, z produktu IBM MQ 9.3.5, odpowiednika w wybranym interfejsie API, w celu przekazania znacznika do menedżera kolejek podczas nawiązywania połączenia.

Jeśli nie można zmienić aplikacji w taki sposób, aby żądała znacznika uwierzytelniania i przedstawiała znacznik w menedżerze kolejek podczas nawiązywania połączenia, można alternatywnie użyć wyjścia zabezpieczeń w celu udostępnienia znacznika w strukturze MQCSP.

Jeśli znacznik spełnia wymagania dotyczące znaczników uwierzytelniania, a podpis znacznika jest poprawny, połączenie jest nawiązywane. Menedżer kolejek może również użyć identyfikatora użytkownika zawartego w znaczniku na potrzeby sprawdzania autoryzacji w celu uzyskania dostępu do zasobów IBM MQ , jeśli opcjonalne żądanie użytkownika jest zawarte w znaczniku. Żądanie użytkownika jest roszczeniem w znaczniku zawierającym identyfikator użytkownika, który menedżer kolejek adoptuje na potrzeby sprawdzania autoryzacji. Ta nazwa roszczenia użytkownika jest określana za pomocą atrybutu **UserClaim** w sekcji **AuthToken** pliku `qm.ini` .

Więcej informacji na ten temat zawierają sekcja “Używanie znaczników uwierzytelniania w aplikacji” na stronie 380 i sekcja MQCSP-parametry zabezpieczeń.

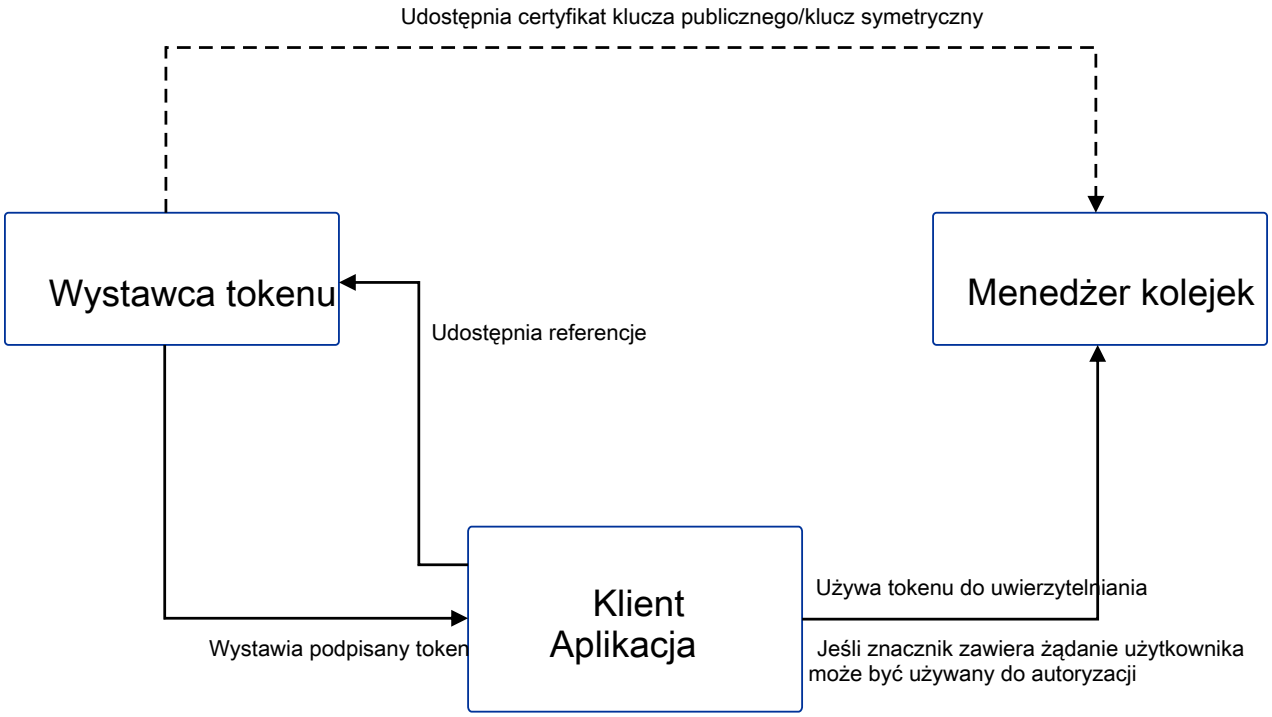


Diagram przedstawia podstawowy przykład oczekiwanego przepływu na potrzeby używania znaczników z produktem IBM MQ. Oczekiwany cykl życia jest następujący:

- Znacznik jest wystawiany aplikacji przez zaufanego wystawcę. Więcej informacji na ten temat zawiera sekcja Wymagania dotyczące znaczników uwierzytelniania.
- Aplikacja przekazuje znacznik do menedżera kolejek podczas nawiązywania połączenia. Więcej informacji na ten temat zawiera sekcja Używanie znaczników uwierzytelniania w aplikacji.
- Menedżer kolejek sprawdza poprawność podpisu znacznika względem klucza publicznego zaufanego wystawcy lub klucza symetrycznego w repozytorium kluczy. Aby skonfigurować menedżer kolejek, wykonaj kroki opisane w sekcji Konfigurowanie menedżera kolejek do akceptowania znaczników uwierzytelniania.
- Jeśli znacznik uwierzytelniania zawiera poprawne żądanie użytkownika, użytkownik w znaczniku może zostać adoptowany na potrzeby sprawdzania autoryzacji w celu uzyskania dostępu do zasobów IBM MQ . Więcej informacji na ten temat zawiera sekcja Adaptowanie użytkowników do autoryzacji.

- Administrator IBM MQ zarządza zaufanymi certyfikatami wystawcy tokenu. Po utracie ważności certyfikatu należy uzyskać nowy certyfikat od wystawcy tokenu i dodać go do repozytorium kluczy.
- Jeśli menedżer kolejek został skonfigurowany, a aplikacja nawiązuje połączenie, ale napotyka problemy ze znacznikiem, należy zapoznać się z sekcją Rozwiązywanie problemów z tokenem uwierzytelniania i sekcją Kody błędów uwierzytelniania tokenów.

Produkt IBM MQ współpracuje z dowolnym wystawcą znacznika, który udostępnia znaczniki zgodne ze standardami JWT i JWS.

Jeśli znaczniki nie są jeszcze używane, ale chcesz zrozumieć, co jest związane z serwerem znaczników, zapoznaj się z Podręcznikiem Pierwsze kroki dla projektu Keycloak, który jest darmowy i otwarty.

Odsyłacze pokrewne
Sekcja AuthToken pliku `qm.ini`

V 9.3.4 Linux AIX Wymagania dotyczące znaczników uwierzytelniania

Wymagania dotyczące sprawdzania poprawności, struktura i algorytmy dla znaczników uwierzytelniania używanych z produktem IBM MQ.

Wymagania

Znaczniki uwierzytelniania, które są używane z produktem IBM MQ , muszą spełniać następujące wymagania.

- Długość tokenu nie może przekraczać maksymalnej długości 8192 znaków. Więcej informacji na ten temat zawiera sekcja TokenLength (MQLONG) dla protokołu MQCSP.
- Struktura i kodowanie znacznika są poprawne zgodnie ze specyfikacją JSON Web Token (JWT) w dokumencie RFC7519i specyfikacją JSON Web Signature (JWS) w dokumencie RFC7515.
- Wymagane parametry nagłówka tokenu określone w parametrze Tabela 68 na stronie 374 są obecne, a wartości parametrów są poprawne.
- Wymagane roszczenia ładunku określone w parametrze Tabela 69 na stronie 375 są obecne, a wartości roszczeń są poprawne.
- Znacznik jest podpisywany przy użyciu algorytmu obsługiwanego przez program IBM MQ w języku Tabela 70 na stronie 375 .
- Wartość roszczenia utraty ważności (**exp**) jest późniejsza niż bieżąca godzina.
- Jeśli występuje roszczenie not before (**nbf**), wartość jest wcześniejsza od bieżącej godziny.
- Jeśli występuje roszczenie użytkownika, wartość musi spełniać wymagania dla “Identyfikatory użytkowników w znacznikach uwierzytelniania” na stronie 376.

Struktura tokenu

IBM MQ akceptuje żądania JT zgodne ze standardem RFC7519 . Znacznik JWT musi być podpisany i zakodowany zgodnie ze standardem JWS zdefiniowanym w dokumencie RFC7515.

Produkt IBM MQ oczekuje, że zabezpieczony znacznik JWS będzie zawierać następujące trzy komponenty:

Nagłówek JOSE

Obiekt JSON, który zawiera parametry opisujące typ tokenu i algorytmy szyfrowania używane do zabezpieczania jego treści.

W poniższym przykładzie nagłówka zadeklarowano, że zakodowany obiekt jest JWT, a nagłówek i ładunek są zabezpieczone przy użyciu algorytmu HMAC SHA-256 .

```
{
 "typ":"JWT",
```

```
 "alg":"HS256"
}
```

Ładunek JWS

Obiekt JSON, który zawiera roszczenia określone w standardzie JWT. Każdy element obiektu JSON jest roszczeniem. Roszczenia mogą potwierdzać tożsamość wystawcy tokenu lub identyfikator użytkownika okaziciela.

```
{
 "exp": 1685529153,
 "nbf": 1685528150,
 "AppUser": "MyUserName"
 }
```

Podpis JWS

Służy do sprawdzania, czy token jest wystawiany przez zaufanego wystawcę.

Te komponenty są reprezentowane w zabezpieczonym znaczniku JWS jako łańcuchy base64url-encoded rozdzielone kropką ('.').

Znacznik uwierzytelniania, który jest zgodny ze standardem JWS, jest podpisywany w celu umożliwienia sprawdzania jego autentyczności, ale nie jest szyfrowany. Dlatego może być odczytywana i ponownie wykorzystywana przez każdą osobę, która ma dostęp do znacznika. Skonfiguruj połączenie z menedżerem kolejek, aby zapewnić ochronę uwierzytelniania przy użyciu szyfrowania wysyłanego przez sieć, na przykład za pomocą protokołu TLS. Więcej informacji na temat opcji ochrony referencji dostarczanych przez aplikację zawiera sekcja Ochrona hasłem MQCSP.

Produkt IBM MQ obsługuje następujące parametry i roszczenia w nagłówku i ładunku znaczników uwierzytelniania. Wszelkie dodatkowe parametry lub roszczenia w znaczniku są ignorowane. Jeśli znacznik zawiera więcej niż jeden parametr lub roszczenie o tej samej nazwie, używany jest ostatni parametr lub roszczenie o zduplikowanej nazwie.

Tabela 68. Opisy parametrów nagłówka tokenu

Część tokenu	Nazwa parametru	Typ danych	Wymagany	Opis
Nagłówek	**typ**	Łańcuch	Tak	Typ tokenu. Wartością tego parametru musi być "JWT".
	alg	Łańcuch	Tak	Algorytm używany do zabezpieczania nagłówka i ładunku. Wartość tego parametru musi być jednym z algorytmów w programie Tabela 70 na stronie 375.

Tabela 69. Opisy żądań ładunku tokenu				
Część tokenu	**Nazwa parametru**	**Typ danych**	**Wymagany**	**Opis**
Ładunek	**exp**	Liczba całkowita	Tak	Czas utraty ważności tokenu, wyrażony jako liczba sekund od 1 stycznia 1979, 00:00 czasu uniwersalnego. Token nie jest akceptowany po tym czasie.
	nbf	Liczba całkowita	Nie	Czas, wyrażony jako liczba sekund od 1 stycznia 1979, 00:00 czasu uniwersalnego, przed którym token nie jest akceptowany.
	Nazwa roszczenia użytkownika została podana w polu **UserClaim** w sekcji **AuthToken** pliku `qm.ini` .	Łańcuch	Wymagane tylko wtedy, gdy żądanie użytkownika w znaczniku jest używane do autoryzacji.	Nazwa roszczenia, które zawiera ID użytkownika, który jest adoptowany na potrzeby sprawdzania autoryzacji. Jeśli na przykład znacznik ma roszczenie użytkownika `"AppUser": "MyUserName"`, należy podać wartość **UserClaim**=`AppUser` w sekcji **AuthToken** pliku `qm.ini` .

Dobry przykład zakodowanego i zdekodowanego tokenu można znaleźć na stronie debugera w serwisie WWW `jwt.io` .

Algorytmy

Produkt IBM MQ obsługuje podzbiór algorytmów, które są zawarte w specyfikacji JWA (JSON Web Algorithm) dla zabezpieczonych znaczników JWS .

Tabela 70. Algorytmy WWW JSON (JWA) obsługiwane przez produkt IBM MQ dla zabezpieczonych znaczników JWS	
alg wartość parametru	**Podpis cyfrowy lub algorytm MAC**
HS256	HMAC z użyciem SHA-256
HS384	HMAC przy użyciu SHA-384
HS512	HMAC przy użyciu SHA-512
RS256	RSASSA-PKCS1-v1_5 przy użyciu SHA-256
RS384	RSASSA-PKCS1-v1_5 przy użyciu SHA-384
RS512	RSASSA-PKCS1-v1_5 przy użyciu SHA-512

Wymagania dotyczące certyfikatu klucza asymetrycznego

Jeśli znacznik jest podpisany za pomocą klucza asymetrycznego, certyfikat klucza publicznego wystawcy znacznika musi znajdować się w repozytorium kluczy używanym przez menedżer kolejek do uwierzytelniania znacznika. Po odebraniu znacznika uwierzytelniania certyfikat musi znajdować się w okresie ważności. Nie są wykonywane żadne sprawdzenia w celu upewnienia się, że certyfikat wystawcy tokenu nie został unieważniony.

Identyfikatory użytkowników w znacznikach uwierzytelniania

Jeśli menedżer kolejek jest skonfigurowany do adoptowania identyfikatora użytkownika zawartego w roszczeniu użytkownika dotyczącym znacznika uwierzytelniania jako kontekstu dla aplikacji, adoptowany identyfikator użytkownika musi spełniać następujące wymagania:

- Może zawierać do 12 znaków.
- Musi zaczynać się od jednego z następujących znaków:

  A-Z a-z
- Może zawierać dowolny z następujących znaków:

  0-9 A-Z a-z +,-. : = _
- Nie może to być jeden z zastrzeżonych identyfikatorów użytkowników UNKNOWN i NOBODY.

Zadania pokrewne

Konfigurowanie menedżera kolejek do akceptowania programu **AuthTokens**

Odsyłacze pokrewne

Sekcja AuthToken pliku `qm.ini`

V 9.3.4 Linux AIX Konfigurowanie menedżera kolejek w celu akceptowania znaczników uwierzytelniania

Skonfiguruj menedżer kolejek systemu IBM MQ działający w systemie AIX lub Linux do uwierzytelniania użytkowników i aplikacji za pomocą znaczników uwierzytelniania.

Zanim rozpoczniesz

Więcej informacji na temat sposobu pracy znaczników z produktem IBM MQzawiera sekcja Praca ze znacznikami uwierzytelniania.

Przed skonfigurowaniem menedżera kolejek należy sprawdzić, czy obiekt AUTHINFO, do którego odwołuje się atrybut **CONNAUTH** menedżera kolejek, jest typu `IDPWOS`. Uwierzytelnianie za pomocą znacznika jest dostępne tylko wtedy, gdy menedżer kolejek jest skonfigurowany do sprawdzania identyfikatora i hasła użytkownika systemu operacyjnego.

Sprawdź, czy atrybut **SecurityPolicy** w sekcji Service nie jest ustawiony na wartość `Group`. Uwierzytelnianie przy użyciu znacznika nie jest dostępne, jeśli parametr **SecurityPolicy** jest jawnie ustawiony na wartość `Group`. Jeśli parametr **SecurityPolicy** ma wartość `Group`, usuń atrybut **SecurityPolicy** z sekcji Service, a następnie zrestartuj menedżer kolejek.

O tym zadaniu

Aplikacje produktu IBM MQ 9.3.4 mogą uwierzytelniać się w menedżerze kolejek przy użyciu znaczników. IBM MQ akceptuje tokeny JSON Web Token (*JWT*) od zaufanych wystawców, którzy postępują zgodnie z proponowanym standardem internetowym RFC7519. Tokeny mogą być używane do uwierzytelniania tożsamości, która może być następnie adoptowana na potrzeby przyszłych sprawdzeń autoryzacji.

Skonfiguruj menedżer kolejek tak, aby akceptował znaczniki, zapisując certyfikat klucza publicznego lub klucz symetryczny zaufanego wystawcy w repozytorium kluczy menedżera kolejek. Dodaj sekcję AuthToken do pliku `qm.ini` i odśwież konfigurację zabezpieczeń, aby menedżer kolejek pobrał nową konfigurację.

Procedura

1. Utwórz repozytorium kluczy.
   a) Utwórz repozytorium kluczy dla certyfikatu klucza publicznego lub klucza symetrycznego, który jest odbierany od zaufanego wystawcy. Można użyć repozytorium kluczy CMS z rozszerzeniem nazwy pliku `.kdb` lub repozytorium kluczy PKCS#12 z rozszerzeniem nazwy pliku `.p12`.

Wykonaj następującą komendę, aby utworzyć repozytorium kluczy CMS :

```
runmqakm -keydb -create -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
-type cms
```

Jeśli komenda **runmqakm** zwróci błąd, zapoznaj się z sekcją Kody błędów runmqakm. Jeśli komenda zakończy się pomyślnie, użyj komendy `ls` , aby wyświetlić zawartość katalogu:

```
ls -l /var/mqm/qmgrs/qm1/tokenissuer
```

Wyświetlane są następujące pliki:

```
-rw------- 1 adminuser mqm 88 Feb 22 07:50 key.crl
-rw------- 1 adminuser mqm 88 Feb 22 07:50 key.kdb
-rw------- 1 adminuser mqm 88 Feb 22 07:50 key.rdb
```

b) W razie potrzeby zmień prawo własności grupy dla utworzonych plików repozytorium kluczy, aby grupa mqm mogła mieć prawo do odczytu. Początkowo tylko administrator, który uruchomił komendę, ma dostęp do utworzonych plików.

```
chgrp mqm /var/mqm/qmgrs/qm1/tokenissuer/key.*
```

c) Zmień tryb plików repozytorium kluczy, aby dodać uprawnienia do odczytu dla grupy mqm. Na przykład poniższa komenda dodaje uprawnienia do odczytu/zapisu dla właściciela pliku i uprawnienia tylko do odczytu dla grupy.

```
chmod 640 /var/mqm/qmgrs/qm1/tokenissuer/key.*
```

2. Zaszyfruj hasło repozytorium kluczy za pomocą komendy **runqmcred** i zapisz zaszyfrowany łańcuch w pliku.

a) Utwórz plik zawierający klucz początkowy, który jest używany do szyfrowania hasła repozytorium kluczy.

Plik musi zawierać klucz początkowy w postaci pojedynczego wiersza tekstu. Maksymalna długość klucza początkowego wynosi 256 bajtów. Jeśli klucz początkowy dla menedżera kolejek został już ustawiony za pomocą atrybutu **INITKEY** menedżera kolejek, skopiuj wartość atrybutu **INITKEY** do nowego pliku. Jeśli nie ustawiono jeszcze klucza początkowego dla menedżera kolejek, utwórz nowy, unikalny klucz szyfrowania i dodaj go do początkowego pliku kluczy.

Uwaga: Więcej informacji na ten temat zawiera sekcja INITKEY. Jeśli klucz początkowy nie zostanie określony, zostanie użyty klucz domyślny. Bezpieczniej jest używać własnego klucza początkowego.

Uwaga: Nadaj minimalne wymagane uprawnienia do początkowego pliku kluczy, aby zabezpieczyć zawartość pliku. Początkowy plik kluczy jest używany tylko do szyfrowania hasła repozytorium kluczy. Dlatego tylko administratorzy, którzy używają klucza początkowego do szyfrowania haseł, muszą mieć dostęp do pliku klucza początkowego.

b) Jeśli klucz początkowy menedżera kolejek nie jest jeszcze ustawiony, ustaw wartość atrybutu **INITKEY** menedżera kolejek na klucz początkowy, który został utworzony w kroku “2.a” na stronie 377. Użyj komendy **ALTER QMGR** , aby ustawić klucz początkowy menedżera kolejek. Na przykład:

```
ALTER QMGR INITKEY('myEncrypt10nK3y')
```

c) Wprowadź komendę **runqmcred** , aby zaszyfrować hasło repozytorium kluczy. Parametr **-sf** umożliwia określenie ścieżki do pliku, który zawiera klucz początkowy.

```
runqmcred -sf initial.key
```

Po wyświetleniu zapytania wprowadź hasło repozytorium kluczy. Zaszyfrowane hasło jest wyprowadzane przez komendę.

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
Enter password:
```

```
*************
<QM>!2!b5rb01sMzFzc1ClZeQMryruWFM3HSm8DKyEaZK7qzWY=!TrWdU57DCDXM0Qah99I/Lg==
```

Skopiuj łańcuch w ostatnim wierszu i zapisz go w pliku.

3. Użyj jednej z następujących metod, aby dodać certyfikat klucza publicznego lub klucz symetryczny wystawcy znacznika do repozytorium kluczy.
   - Aby dodać certyfikat klucza publicznego RSA do repozytorium kluczy, wydaj następującą komendę:

     ```
     runmqakm -cert -add -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
     -label keylabel
              -file keyfile
     ```

   - Aby dodać do repozytorium kluczy klucz symetryczny zakodowany w formacie base64 , wydaj następującą komendę:

     ```
     runmqakm -secretkey -add -db /var/mqm/qmgrs/qm1/tokenissuer/key.kdb -pw MyKeystorePassword
     -label keylabel
              -file keyfile -format ascii
     ```

   Gdzie *etykieta_klucza* jest etykietą, która ma zostać dołączona do certyfikatu lub klucza tajnego, a *plik_klucza* jest nazwą pliku zawierającego certyfikat lub klucz tajny zakodowany w formacie base64 .
4. Dodaj sekcję **AuthToken** i następujące atrybuty do pliku `qm.ini` :
   - Ścieżka do repozytorium kluczy określona za pomocą atrybutu **KeyStore** .
   - Plik, który zawiera hasło dla repozytorium kluczy określonego za pomocą atrybutu **KeyStorePwdFile** .
   - Etykieta certyfikatu lub klucza symetrycznego, który został dodany w kroku “3” na stronie 378, określona za pomocą atrybutu **CertLabel** .

   Na przykład:

   ```
   AuthToken:
      KeyStore=/var/mqm/qmgrs/qm1/tokenissuer/key.kdb
      KeyStorePwdFile=/var/mqm/qmgrs/qm1/tokenissuer/key.pw
      CertLabel=rsakey
   ```

   Gdzie `key.kdb` jest nazwą repozytorium kluczy utworzonego w kroku “1.a” na stronie 376, a `key.pw` jest plikiem zawierającym zaszyfrowane hasło dla repozytorium kluczy utworzonego w kroku “2.c” na stronie 377.

   Więcej informacji na temat sekcji **AuthToken** zawiera sekcja AuthToken pliku `qm.ini`.
5. Jeśli menedżer kolejek jest skonfigurowany do adoptowania identyfikatora użytkownika zawartego w roszczeniu użytkownika znacznika do użycia podczas kolejnych sprawdzeń autoryzacji, należy dodać atrybut **UserClaim** do sekcji **AuthToken** .

   Aby określić, czy menedżer kolejek jest skonfigurowany do adoptowania identyfikatora użytkownika w znaczniku, należy wydać następującą komendę MQSC:

   ```
   DISPLAY AUTHINFO(authinfo_name) ADOPTCTX
   ```

   Gdzie *authinfo_name* jest wartością atrybutu **CONNAUTH** menedżera kolejek. Jeśli wartością atrybutu **ADOPTCTX** jest YES, menedżer kolejek jest skonfigurowany do adoptowania identyfikatora użytkownika w znaczniku, a atrybut **UserClaim** musi być określony w sekcji **AuthToken** .

   Ustaw wartość atrybutu **UserClaim** na nazwę żądania tokenu zawierającego ID użytkownika, który ma być adoptowany. Na przykład, jeśli znacznik zawiera roszczenie `"AppUser": "MyUserName"`, dodaj następujący wiersz do sekcji **AuthToken** :

   ```
   UserClaim=AppUser
   ```
6. Odśwież konfigurację zabezpieczeń menedżera kolejek, aby pobrać konfigurację znacznika z pliku `qm.ini` . Wprowadź następującą komendę, aby uruchomić komendę **runmqsc** :

```
runmqsc qm1
```

następnie wydaj następującą komendę MQSC:

```
REFRESH SECURITY TYPE(CONNAUTH)
```

Co dalej

Współpracuj z programistami, aby zrozumieć, w jaki sposób mogą używać znaczników w aplikacjach do uwierzytelniania w menedżerze kolejek.

Pojęcia pokrewne

Rozwiązywanie problemów z tokenem uwierzytelniania

Zadania pokrewne

Używanie znaczników uwierzytelniania w aplikacji

Odsyłacze pokrewne

Sekcja AuthToken pliku `qm.ini`

V 9.3.4 Uzyskiwanie znacznika uwierzytelniania od wybranego wystawcy znacznika

Napisz aplikację, aby uzyskać znacznik uwierzytelniania od wybranego wystawcy znacznika podczas nawiązywania połączenia z menedżerem kolejek produktu IBM MQ .

Zanim rozpoczniesz

Zapoznaj się z informacjami w sekcji “Używanie znaczników uwierzytelniania w aplikacji” na stronie 380.

Procedura

- Sposób uzyskiwania znacznika uwierzytelniania i jego dokładna zawartość różnią się w zależności od wystawcy znacznika.

  Napisz aplikację do interakcji z wybranym wystawcą znacznika w celu zażądania i uzyskania znacznika uwierzytelniania.

  Znacznik uwierzytelniania musi być zgodny z wymaganiami IBM MQ dotyczącymi znaczników uwierzytelniania. Więcej informacji na temat tych wymagań zawiera sekcja “Wymagania dotyczące znaczników uwierzytelniania” na stronie 373.

  Jeśli planowane jest adoptowanie identyfikatora użytkownika zawartego w roszczeniu znacznika jako kontekstu dla aplikacji, znacznik uwierzytelniania musi również spełniać następujące wymagania:

  – Znacznik uwierzytelniania musi zawierać roszczenie zgodne z nazwą roszczenia użytkownika w konfiguracji uwierzytelniania znacznika menedżera kolejek.
  – Wartość roszczenia użytkownika musi spełniać wymagania dotyczące identyfikatorów użytkowników w znacznikach uwierzytelniania. Więcej informacji na ten temat zawiera “Identyfikatory użytkowników w znacznikach uwierzytelniania” na stronie 376.

Wyniki

Uzyskano poprawnie sformatowany znacznik JWT , który można przedstawić w programie IBM MQ w celu sprawdzenia poprawności.

Zadania pokrewne

Konfigurowanie menedżera kolejek do akceptowania programu **AuthTokens**

Odsyłacze pokrewne

Sekcja AuthToken pliku `qm.ini`

MQCSP-parametry zabezpieczeń

V 9.3.4 Używanie znaczników uwierzytelniania w aplikacji

Napisz aplikację, aby dostarczała znacznik uwierzytelniania podczas nawiązywania połączenia z menedżerem kolejek produktu IBM MQ .

Zanim rozpoczniesz

Z poziomu produktu IBM MQ 9.3.4aplikacje mogą dostarczać znacznik uwierzytelniania podczas nawiązywania połączenia z menedżerem kolejek.

Aplikacja musi spełniać następujące wymagania:

- V 9.3.5 Musi być napisana w języku C lub Java (przy użyciu IBM MQ classes for JMS/ Jakarta Messaging)
- Musi on łączyć się z menedżerem kolejek jako IBM MQ client. Oznacza to, że aplikacja musi łączyć się z menedżerem kolejek przez sieć, zamiast korzystać z powiązań lokalnych.
- Musi on łączyć się z menedżerem kolejek, który działa w systemie AIX lub Linux.

Jeśli aplikacja nie spełnia tych wymagań, połączenie nie powiedzie się i do aplikacji zostanie zwrócony kod przyczyny MQRC_FUNCTION_NOT_SUPPORTED (2298).

Aplikacja, która dostarcza znacznik uwierzytelniania, może działać na dowolnej platformie obsługującej produkt IBM MQ MQI clients.

Klienty, które używają automatycznego ponownego połączenia klienta, nie mogą dostarczyć tokenu uwierzytelniania podczas nawiązywania połączenia. Jeśli aplikacja dostarcza znacznik uwierzytelniania i określa opcję MQCNO_RECONNECT lub MQCNO_RECONNECT_Q_MGR w strukturze MQCNO, połączenie kończy się niepowodzeniem i do aplikacji zwracany jest kod przyczyny MQRC_RECONNECT_NIEZGODNA (2547). Więcej informacji na temat automatycznego ponownego połączenia klienta zawiera sekcja Automatyczne ponowne połączenie klienta.

Jeśli ze względu na te wymagania nie można napisać aplikacji dostarczającej znacznik uwierzytelniania, można alternatywnie przeprowadzić migrację aplikacji, aby używała znaczników uwierzytelniania przy użyciu wyjścia zabezpieczeń klienta. Wyjście zabezpieczeń klienta można zapisać w celu ustawienia znacznika uwierzytelniania w strukturze MQCSP. Więcej informacji na temat wyjść zabezpieczeń zawiera sekcja Wyjścia zabezpieczeń w połączeniu klienta.

V 9.3.5 W produkcie IBM MQ 9.3.5aplikacje klienckie JMS mogą bezpośrednio udostępniać znacznik podczas nawiązywania połączenia (patrz sekcja “Uzyskiwanie znacznika uwierzytelniania od wybranego wystawcy znacznika” na stronie 379). W systemie IBM MQ 9.3.4aplikacje Java mogą pośrednio udostępniać token za pośrednictwem programu obsługi wyjścia. Więcej informacji na ten temat zawiera sekcja Klasa Java MQCSP.

O tym zadaniu

Uwaga: Znacznik uwierzytelniania zgodny ze standardem JSON Web Signature (JWS) jest podpisany, aby umożliwić sprawdzenie poprawności znacznika, ale nie jest on szyfrowany. Dlatego może być odczytywana i ponownie wykorzystywana przez każdą osobę, która ma dostęp do znacznika. Skonfiguruj połączenie z menedżerem kolejek, aby upewnić się, że znacznik uwierzytelniania jest chroniony przy użyciu szyfrowania podczas wysyłania go przez sieć, na przykład za pomocą protokołu TLS. Więcej informacji na temat opcji ochrony referencji dostarczanych przez aplikację zawiera sekcja “Zabezpieczenie hasłem MQCSP” na stronie 32.

Przed zmodyfikowaniem aplikacji w celu połączenia za pomocą znacznika należy upewnić się, że:

- Menedżer kolejek został skonfigurowany do akceptowania znaczników uwierzytelniania, wykonując kroki opisane w sekcji “Konfigurowanie menedżera kolejek w celu akceptowania znaczników uwierzytelniania” na stronie 376

- Aplikacja może uzyskać poprawny znacznik zgodnie z wymaganiami z serwera uwierzytelniającego, patrz sekcja “Uzyskiwanie znacznika uwierzytelniania od wybranego wystawcy znacznika” na stronie 379.

Aby podać znacznik uwierzytelniania podczas nawiązywania przez aplikację połączenia z menedżerem kolejek produktu IBM MQ , należy dołączyć następujący proces.

Procedura

- Aby dostarczyć znacznik uwierzytelniania z aplikacji C (MQI):

  Aplikacja musi nawiązać połączenie przy użyciu MQCONNX (zamiast MQCONN) i podać strukturę MQCSP :

  – Pole **AuthenticationType** musi być ustawione na wartość MQCSP_AUTH_ID_TOKEN.
  – Wersja struktury musi być ustawiona na wartość MQCSP_VERSION_3.
  – Pole **TokenPtr** lub **TokenOffset** musi odwoływać się do znacznika uwierzytelniania.
  – Pole **TokenLength** musi być ustawione na długość znacznika uwierzytelniania.

  Przykładowy kod w języku C służący do nawiązywania połączenia z menedżerem kolejek przy użyciu protokołu MQCSP w wersji 3 i znacznika uwierzytelniania:

```
MQCNO cno = {MQCNO_DEFAULT};   /* Connection options  */
MQCSP csp = {MQCSP_DEFAULT};   /* Security parameters */

char  token[MQ_CSP_TOKEN_LENGTH +1] = {0};  /* Authentication token string */

/* Set the connection options */
cno.SecurityParmsPtr = &csp;
cno.Version = MQCNO_VERSION_5;

/* Set the security parameters */
csp.Version = MQCSP_VERSION_3;
csp.AuthenticationType = MQCSP_AUTH_ID_TOKEN;
csp.TokenPtr = token;
csp.TokenLength = (MQLONG) strlen(token);

/* Connect to the queue manager */
MQCONNX(qmName,                 /* Queue manager name  */
        &cno,                   /* Connection options  */
        &hCon,                  /* Connection handle   */
        &compCode,              /* Completion code     */
        &reason);               /* Reason code         */
```

- V 9.3.5 Aby dostarczyć znacznik uwierzytelniania z aplikacji Java :

  Aplikacje używające interfejsu IBM MQ classes for JMS/Jakarta Messaging mogą udostępniać token za pomocą dowolnej z metod `createContext`lub `createConnection` , które przyjmują nazwę użytkownika i hasło.

  Aby udostępnić znacznik uwierzytelniania, wykonaj następujące czynności:

  – Parametr **UserID** musi być ustawiony na wartość NULL lub pusty łańcuch, czyli bez spacji, " "
  – Token jest udostępniany jako łańcuch **Password** .

  Dotyczy to wszystkich implementacji interfejsu `ConnectionFactory` w języku IBM MQ .

  Można użyć jawnych form parametrów, na przykład `createContext`(String **userID**, String **password**) lub niejawnych wersji parametrów, na przykład `createContext`().

  W tym drugim przypadku należy najpierw podać puste znaczniki **userID** i **Password** jako właściwości w fabryce połączeń.

  Przykładowy kod produktu Java używany do nawiązywania połączenia z menedżerem kolejek przy użyciu znacznika uwierzytelniania:

```
// Obtain token from authentication provider here:

String myToken = "xxxxxxxxxxxxxxx";
```

```
// Acquire instance of an MQ connection Factory:

JmsFactoryFactory ff = JmsFactoryFactory.getInstance(WMQConstants.WMQ_PROVIDER);

JmsConnectionFactory cf = ff.createConnectionFactory();

// Configure any required CF properties here - e.g. MQ Channel details

// Connect to (and authenticate with) the queue manager:

context = cf.createContext(null, myToken); // NOTE - null userID indicates token being
provided
```

Jeśli połączenie nie powiedzie się z kodem przyczyny MQRC_NOT_AUTHORIZED (2035) lub MQRC_SECURITY_ERROR (2063), sprawdź dziennik błędów menedżera kolejek pod kątem komunikatu o błędzie, który zawiera więcej informacji o przyczynie niepowodzenia. Więcej informacji na temat diagnozowania problemów ze znacznikami uwierzytelniania zawiera sekcja Rozwiązywanie problemów z znacznikami uwierzytelniania.

Wyniki

Aplikacja jest teraz połączona z menedżerem kolejek. Pozostaje on połączony do momentu rozłączenia, nawet jeśli znacznik, który był używany do uwierzytelniania, utraci ważność. Jeśli aplikacja rozłączy się z menedżerem kolejek i będzie musiała ponownie nawiązać połączenie, może być konieczne uzyskanie nowego znacznika uwierzytelniania z późniejszym czasem utraty ważności przed ponownym nawiązaniem połączenia.

Zadania pokrewne

Konfigurowanie menedżera kolejek do akceptowania programu **AuthTokens**

Odsyłacze pokrewne

Sekcja AuthToken pliku `qm.ini`

MQCSP-parametry zabezpieczeń

Praca z odwołanymi certyfikatami

Certyfikaty cyfrowe mogą być unieważniane przez ośrodki certyfikacji. Status odwołań certyfikatów można sprawdzić przy użyciu protokołu OCSP lub list CRL na serwerach LDAP, w zależności od platformy.

Podczas uzgadniania TLS partnerzy komunikujący się wzajemnie uwierzytelniają się przy użyciu certyfikatów cyfrowych. Uwierzytelnianie może obejmować również sprawdzanie, czy otrzymany certyfikat nadal jest zaufany. Ośrodki certyfikacji (CA) unieważniają certyfikaty z różnych powodów, w tym:

- Właściciel został przeniesiony do innej organizacji
- Klucz prywatny nie jest już kluczem tajnym

Ośrodki CA publikują unieważnione certyfikaty osobiste na liście odwołań certyfikatów (CRL). Unieważnione certyfikaty ośrodka CA są publikowane na liście odwołań uprawnień (Authority Revocation List-ARL).

ALW Na platformach AIX, Linux, and Windows obsługa protokołu SSL w systemie 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.

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.

z/OS IBM i Na platformach IBM i i z/OS obsługa protokołu SSL w systemie IBM MQ sprawdza odwołane certyfikaty przy użyciu list CRL i ARL dostępnych tylko na serwerach LDAP.

Więcej informacji na temat ośrodków certyfikacji zawiera sekcja “certyfikaty cyfrowe” na stronie 13.

Sprawdzanie OCSP/CRL

Sprawdzanie protokołu OCSP (Online Certificate Status Protocol) /listy odwołań certyfikatów (Certificate Revocation List-CRL) jest wykonywane dla zdalnych certyfikatów przychodzących. Proces sprawdza cały łańcuch od certyfikatu osobistego systemu zdalnego aż do certyfikatu głównego.

Używanie protokołu openSSL do sprawdzania poprawności protokołu OCSP

Jeśli w przedsiębiorstwie do sprawdzenia poprawności protokołu OCSP jest używany protokół openSSL , a następnie zostanie podjęta próba użycia połączenia TLS produktu IBM Global Security Kit (GSKit) , zostanie wyświetlone ostrzeżenie o statusie UNKNOWN.

Jest to spowodowane tym, że wszystkie certyfikaty w łańcuchu, oprócz certyfikatu głównego, są sprawdzane przez program GSKit pod kątem statusu odwołania. Operacja GSKit jest zgodna z dokumentem RFC 5280 i jest opisana w strategii zaufania GSKit . Algorytm GSKit próbuje wszystkich dostępnych źródeł informacji o odwołaniu, zgodnie z opisem w dokumencie RFC 5280 i strategii GSGSKitKit Trust Policy.

Jak działa sprawdzanie OCSP/CRL w IBM MQ?

Produkt IBM MQ obsługuje dwa mechanizmy sterowania zachowaniem podczas sprawdzania certyfikatów względem nazwanych punktów końcowych OCSP lub CRL w rozszerzeniu certyfikatu lub zgodnie z definicją w obiektach AUTHINFO:

- Atrybuty **OCSPCheckExtensions**, **CDPCheckExtensions**i **OCSPAuthentication** Sekcja SSL pliku qm.inioraz
- Użycie parametru SSLCRLNL menedżera kolejek oraz konfiguracji AUTHINFO OCSP i CRLLDAP. Więcej informacji na ten temat zawierają instrukcje ALTER AUTHINFO i ALTER QMGR .

Ostrzeżenie:

Komenda ALTER AUTHINFO z opcją **AUTHTYPE(OCSP)** nie ma zastosowania w przypadku menedżerów kolejek w systemie 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 przez klienta.

Atrybuty sekcji SSL produktów **OCSPCheckExtensions** i **CDPCheckExtensions** określają, czy produkt IBM MQ będzie weryfikować certyfikat z serwerem OCSP lub CRL, szczegółowo opisanym w rozszerzeniu AIA certyfikatu.

Jeśli ta opcja nie jest włączona, nie jest nawiązywane połączenie z serwerem OCSP lub CRL w rozszerzeniu certyfikatu.

Jeśli serwery OCSP lub CRL są szczegółowo opisane za pomocą obiektów AUTHINFO i odwołują się do nich za pomocą atrybutu SSLCRLNL **QMGR** , podczas przetwarzania odwołań certyfikatów produkt IBM MQ próbuje skontaktować się z tymi serwerami.

Ważne: Na liście nazw SSLCRLNL można zdefiniować tylko jeden obiekt AUTHINFO OCSP.

Jeżeli:

OCSPCheckExtensions= NO i **CDPCheckExtensions**=*NO* są ustawione oraz
W obiektach AUTHINFO nie zdefiniowano serwerów OCSP ani CRL

nie jest wykonywane sprawdzanie odwołań certyfikatów.

Podczas weryfikowania certyfikatu pod kątem jego statusu odwołania produkt IBM MQ kontaktuje się z serwerami OCSP lub CRL w następującej kolejności, jeśli jest włączony:

1. Serwer OCSP opisany szczegółowo w obiekcie **AUTHTYPE(OCSP)** i przywoływany w atrybucie SSLCRLNL **QMGR** .
2. Serwery OCSP wyszczególnione w rozszerzeniu AIA certyfikatów, jeśli **OCSPCheckExtensions**=*YES*.

3. Serwery CRL wyszczególnione w rozszerzeniu **CRLDistributionPoints** certyfikatów, jeśli **CDPCheckExtensions** =*YES*.
4. Wszystkie serwery CRL opisane szczegółowo w obiektach **AUTHINFO(CRLLDAP)** i przywoływane w atrybucie SSLCRLNL **QMGR** .

Podczas weryfikowania certyfikatu, jeśli wynikiem kroku jest serwer OCSP lub serwer CRL zwracający ostateczną odpowiedź REVOKED lub VALID na zapytanie o certyfikat, nie są wykonywane dalsze sprawdzenia, a przedstawiony status certyfikatu jest używany do określenia, czy certyfikat ma być zaufany, czy nie.

Jeśli serwer OCSP lub serwer CRL zwraca wynik UNKNOWN, przetwarzanie jest kontynuowane do momentu, gdy serwer OCSP lub CRL zwróci ostateczny wynik lub wszystkie opcje zostaną wyczerpane.

Zachowanie określające, czy certyfikat jest uznawany za unieważniony, jeśli nie można określić jego statusu, jest inne w przypadku serwerów OCSP i CRL:

- W przypadku serwerów CRL, jeśli nie można uzyskać żadnej 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 pliku qm.ini .

  Atrybut ten można skonfigurować w taki sposób, aby blokować połączenie, zezwalać na połączenie lub zezwalać na połączenie z komunikatem ostrzegawczym.

W razie potrzeby podczas sprawdzania protokołu OCSP można użyć atrybutu **SSLHTTPProxyName**=*string* w sekcji SSL plików qm.ini i mqclient.ini . Łańcuch jest nazwą hosta lub adresem sieciowym serwera proxy HTTP, który ma być używany przez produkt GSKit na potrzeby sprawdzania protokołu OCSP.

W pliku IBM MQ 9.1.5 można ustawić wartość **OCSPTimeout** w sekcji SSL pliku `qm.ini` lub `mqclient.ini` , która określa liczbę sekund oczekiwania na moduł odpowiadający OCSP podczas sprawdzania odwołania.

ALW 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 dotyczą tylko systemu IBM MQ w systemach AIX, Linux, and Windows .

Aby sprawdzić status odwołania certyfikatu cyfrowego przy użyciu protokołu OCSP, produkt IBM MQ może użyć dwóch metod w celu określenia, z którym programem odpowiadającym 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:

Dobry
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 przechowywany w jednym z następujących miejsc:

- Linux AIX W sekcji SSL pliku `qm.ini` w systemie AIX and Linux.
- Windows W rejestrze systemu Windows .

Ten atrybut można ustawić za pomocą atrybutu IBM MQ Explorer. W przypadku klientów atrybut ten znajduje się 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 trzeba konfigurować żadnego dodatkowego certyfikatu. Kroki, które zostały już wykonane 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 ją podpisał (a certyfikat ten jest podpisany przez ośrodek CA, który jest już zaufany dla połączeń TLS), nie jest wymagana żadna 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 OCSP. Patrz sekcja “Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 338. Certyfikat CA jest domyślnie dodawany jako zaufany certyfikat główny, co jest ustawieniem wymaganym w tym kontekście. Jeśli ten certyfikat nie zostanie dodany, produkt IBM MQ nie może zweryfikować podpisu cyfrowego w odpowiedzi OCSP i wynikiem sprawdzenia OCSP jest nieznany wynik, który może spowodować zamknięcie kanału przez produkt IBM MQ (w zależności od wartości atrybutu OCSPAuthentication).

Protokół OCSP (Online Certificate Status Protocol) w aplikacjach klienckich Java i JMS

Ze względu na ograniczenie interfejsu API Java produkt IBM MQ może używać sprawdzania odwołań certyfikatów protokołu OCSP (Online Certificate Status Protocol) dla gniazd chronionych TLS tylko wtedy, gdy protokół OCSP jest włączony dla całego procesu wirtualnej maszyny języka 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 klasy java.security.Security.setProperty() Interfejs API, zgodnie z obowiązującą strategią programu 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. Oto 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. Oto 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

Nazwa właściwości	Opis
	jest ustawiona, właściwości ocsp.responderCertIssuerName i ocsp.responderCertSerialNumber są ignorowane.
ocsp.responderCertIssuerName	Wartość tej właściwości jest nazwą wystawcy certyfikatu modułu odpowiadającego OCSP. Oto przykład: `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Domyślnie certyfikat modułu odpowiadającego OCSP jest certyfikatem wystawcy certyfikatu, którego poprawność jest sprawdzana. Ta właściwość określa certyfikat modułu odpowiadającego OCSP, gdy wartość domyślna nie ma zastosowania. Wartością jest nazwa wyróżniająca w postaci łańcucha (zdefiniowana w dokumencie RFC 2253), która identyfikuje certyfikat w zestawie certyfikatów dostarczonych podczas sprawdzania poprawności ścieżki certyfikatu. Jeśli ta właściwość jest ustawiona, musi być również ustawiona właściwość ocsp.responderCertSerialNumber. Gdy ustawiona jest właściwość ocsp.responderCertSubjectName, ta właściwość jest ignorowana.
ocsp.responderCertSerialNumber	Wartość tej właściwości jest numerem seryjnym certyfikatu modułu odpowiadającego OCSP. Oto 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 taka konfiguracja może mieć niepożądane skutki uboczne, gdy maszyna JVM jest współużytkowana z innym kodem aplikacji używającym 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 przechwytywacz AMS Java opisany w sekcji Włączanie sprawdzania OCSP w przechwytywaczach rodzimych, należy unikać używania konfiguracji OCSP java.security , która powoduje konflikt z konfiguracją OCSP AMS w pliku konfiguracyjnym magazynu kluczy.

Praca z listami odwołań certyfikatów i listami odwołań uprawnień

Obsługa list CRL i ARL przez IBM MQ różni się w zależności od platformy.

Obsługa list CRL i ARL na każdej platformie jest następująca:

- W systemie z/OSsystemowa implementacja protokołu 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 zaleceniami profilu CRL PKIX X.509 V2 .

Produkt IBM MQ przechowuje w pamięci podręcznej listy CRL i ARL, które były dostępne w ciągu ostatnich 12 godzin.

Gdy menedżer kolejek lub program IBM MQ MQI client odbierze certyfikat, sprawdza listę CRL, aby potwierdzić, że certyfikat jest nadal ważny. IBM MQ najpierw sprawdza pamięć podręczną, jeśli istnieje. Jeśli lista CRL nie znajduje się w pamięci podręcznej, program IBM MQ odpytuje położenia serwerów CRL LDAP w kolejności, w jakiej występują na liście nazw obiektów informacji uwierzytelniającej określonych przez atrybut *SSLCRLNL* , dopóki program IBM MQ nie znajdzie dostępnej listy CRL. Jeśli lista nazw nie jest określona lub jest podana z pustą wartością, listy CRL nie są sprawdzane.

Konfigurowanie serwerów LDAP

Skonfiguruj strukturę drzewa informacji katalogu LDAP, aby odzwierciedlić hierarchię nazw wyróżniających ośrodków CA. W tym celu należy użyć plików LDAP Data Interchange Format.

Skonfiguruj strukturę drzewa informacji katalogu LDAP (LDAP Directory Information Tree-DIT), aby używać hierarchii odpowiadającej nazwom wyróżniającym ośrodków CA wydających certyfikaty i listy CRL. Strukturę DIT można skonfigurować przy użyciu pliku, który używa formatu LDIF (LDAP Data Interchange Format). Do zaktualizowania katalogu można również użyć plików LDIF.

Pliki LDIF to pliki tekstowe ASCII, które zawierają informacje wymagane do definiowania obiektów w katalogu LDAP. Pliki LDIF zawierają jedną lub więcej pozycji, z których każda składa się z nazwy wyróżniającej, co najmniej jednej definicji klasy obiektu i, opcjonalnie, wielu definicji atrybutów.

Atrybut `certificateRevocationList;binary` zawiera listę unieważnionych certyfikatów użytkowników w postaci binarnej. Atrybut `authorityRevocationList;binary` zawiera binarną listę certyfikatów CA, które zostały unieważnione. W przypadku użycia z protokołem TLS produktu IBM MQ dane binarne dla tych atrybutów muszą być zgodne z formatem DER (Definite reguły kodowania). Więcej informacji na temat plików LDIF zawiera dokumentacja dostarczana z serwerem LDAP.

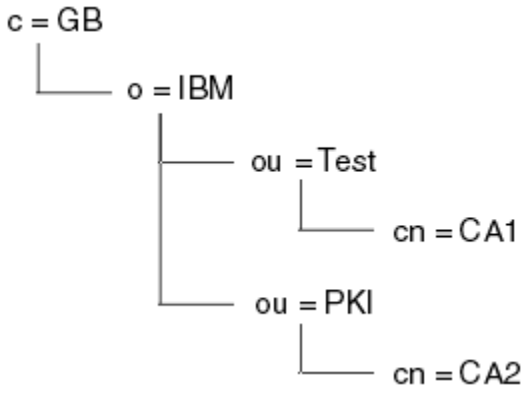
Rysunek 20 na stronie 388 przedstawia przykładowy plik LDIF, który można utworzyć jako dane wejściowe dla serwera LDAP w celu załadowania list CRL i ARL wydanych przez CA1, który jest wyimaginowanym ośrodkiem certyfikacji o nazwie wyróżniającej "CN=CA1, OU=Test, O=IBM, C=GB"i został skonfigurowany przez 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 się to różnić w zależności od implementacji.

Rysunek 21 na stronie 389 przedstawia strukturę DIT tworzoną przez serwer LDAP podczas ładowania przykładowego pliku LDIF, który przedstawia Rysunek 20 na stronie 388 , wraz z podobnym plikiem

dla CA2, urojonego ośrodka certyfikacji (CA), który został skonfigurowany przez organizację PKI, również w produkcie IBM.



Rysunek 21. Przykład struktury drzewa informacji katalogu LDAP

Program IBM MQ sprawdza zarówno listy CRL, jak i ARL.

Uwaga: Upewnij się, że lista kontroli dostępu dla serwera LDAP umożliwia autoryzowanym użytkownikom odczytywanie, wyszukiwanie i porównywanie pozycji, które zawierają listy CRL i ARL. Produkt IBM 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 od ośrodka certyfikacji lub ośrodka certyfikacji.
2. Za pomocą edytora tekstu lub narzędzia dostarczonego z serwerem LDAP utwórz jeden lub więcej plików LDIF, które zawierają nazwę wyróżniającą ośrodka CA i wymagane definicje klas obiektów. Skopiuj dane w formacie DER do pliku LDIF jako wartości atrybutu `certificateRevocationList;binary` dla list CRL i/lub atrybutu `authorityRevocationList;binary` dla list ARL.
3. Uruchom serwer LDAP.
4. Dodaj pozycje z pliku LDIF lub plików utworzonych w kroku “2” na stronie 389.

Po skonfigurowaniu serwera CRL LDAP sprawdź, czy jest on poprawnie skonfigurowany. Najpierw użyj certyfikatu, który nie został unieważniony w kanale, i sprawdź, czy kanał został poprawnie uruchomiony. Następnie użyj unieważnionego certyfikatu i sprawdź, czy uruchomienie kanału nie powiodło się.

Często pobieraj zaktualizowane listy CRL z ośrodków certyfikacji. Rozważ wykonanie tej czynności na serwerach LDAP co 12 godzin.

Uzyskiwanie dostępu do list CRL i ARL za pomocą menedżera kolejek

Menedżer kolejek jest powiązany z co najmniej jednym obiektem informacji uwierzytelniającej, który zawiera adres serwera CRL LDAP. IBM i IBM MQ w systemie IBM i zachowuje się inaczej niż na innych platformach.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation List-CRL) dotyczą również list odwołań uprawnień (Authority Revocation List-ARL).

Aby poinformować menedżera kolejek o sposobie dostępu do list CRL, należy dostarczyć menedżerowi kolejek obiekty informacji uwierzytelniającej, z których każdy zawiera adres serwera CRL LDAP. Obiekty informacji uwierzytelniającej są przechowywane na liście nazw określonej w atrybucie menedżera kolejek *SSLCRLNL* .

W poniższym przykładzie do określenia parametrów użyto komend MQSC:

1. Zdefiniuj obiekty informacji uwierzytelniającej za pomocą komendy DEFINE AUTHINFO MQSC

   z parametrem AUTHTYPE ustawionym na wartość 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 typu CRLLDAP, który został utworzony, zawiera adres serwera LDAP. Jeśli istnieje więcej niż jeden obiekt informacji uwierzytelniającej, serwery LDAP, do których one wskazują, muszą zawierać identyczne informacje. Zapewnia to ciągłość usługi w przypadku awarii co najmniej jednego serwera LDAP.

   z/OS Dodatkowo, tylko w systemie z/OS , dostęp do wszystkich serwerów LDAP musi być uzyskiwany za pomocą tego samego identyfikatora użytkownika i hasła. Używane są ID użytkownika i hasło określone w pierwszym obiekcie AUTHINFO na liście nazw.

   Na wszystkich platformach ID użytkownika i hasło są wysyłane do serwera LDAP w postaci niezaszyfrowanej.
2. Za pomocą komendy MQSC DEFINE NAMELIST zdefiniuj listę nazw dla nazw obiektów informacji uwierzytelniającej. z/OS W systemie z/OSupewnij się, że atrybut listy nazw NLTYPE jest ustawiony na wartość AUTHINFO.
3. Za pomocą komendy ALTER QMGR MQSC podaj listę nazw dla menedżera kolejek. Na przykład:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   gdzie `sslcrlnlname` jest listą 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 uwierzytelniającej, ale menedżer kolejek nie używa ani obiektów informacji uwierzytelniającej, ani listy nazw obiektów informacji uwierzytelniającej. Tylko klienty IBM MQ używające tabeli połączeń klienta wygenerowanej przez menedżer kolejek systemu IBM i używają informacji uwierzytelniających określonych dla tego menedżera kolejek systemu IBM i . Atrybut menedżera kolejek *SSLCRLNL* w systemie IBM i określa, jakich informacji uwierzytelniających używają klienty. See “Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i” na stronie 390 for information about telling an IBM i queue manager how to access CRLs.

Do listy nazw można dodać do 10 połączeń z alternatywnymi serwerami LDAP, aby zapewnić ciągłość usługi w przypadku awarii jednego lub większej liczby serwerów LDAP. Należy zauważyć, że serwery LDAP muszą zawierać identyczne informacje.

IBM i *Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i*

Ta procedura umożliwia dostęp do list CRL lub ARL dostępnych w systemie IBM i.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation List-CRL) dotyczą również list odwołań uprawnień (Authority Revocation List-ARL).

Aby skonfigurować położenie listy CRL dla określonego certyfikatu w systemie IBM i, wykonaj następujące kroki:

1. Uzyskaj dostęp do interfejsu DCM zgodnie z opisem w sekcji “Uzyskiwanie dostępu do programu DCM” na stronie 294.
2. W kategorii zadań **Zarządzanie położeniami CRL** na panelu nawigacyjnym kliknij opcję **Dodaj położenie CRL**. W ramce zadań zostanie wyświetlona strona Zarządzanie położeniami CRL.
3. W polu **Nazwa położenia CRL** wpisz nazwę położenia CRL, na przykład LDAP `Server #1` .
4. W polu **Serwer LDAP** wpisz nazwę serwera LDAP.
5. W polu **Użyj protokołu SSL (Secure Sockets Layer)** wybierz wartość **Tak** , jeśli chcesz połączyć się z serwerem LDAP za pomocą protokołu TLS. W przeciwnym razie wybierz opcję **Nie**.

6. W polu **Numer portu** wpisz numer portu serwera LDAP, na przykład 389.
7. Jeśli serwer LDAP nie zezwala anonimowym użytkownikom 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. W panelu nawigacyjnym kliknij opcję **Select a Certificate Store**(Wybierz bazę certyfikatów). W ramce zadań zostanie wyświetlona strona Wybór bazy certyfikatów (Select a Certificate Store).
10. Zaznacz pole wyboru **Inna baza certyfikatów systemu** i kliknij przycisk **Kontynuuj**. Zostanie wyświetlona strona Baza certyfikatów i hasło.
11. W polu **Certificate store path and filename** (Ścieżka i nazwa pliku bazy certyfikatów) wpisz ścieżkę i nazwę pliku IFS, które są ustawione w parametrze “Tworzenie bazy certyfikatów w systemie IBM i” na stronie 296.
12. Wpisz hasło w polu **Certificate Store Password** (Hasło bazy certyfikatów). Kliknij przycisk **Kontynuuj**. W ramce zadań zostanie wyświetlona strona Bieżąca baza certyfikatów.
13. W kategorii zadań **Manage Certificates** (Zarządzanie certyfikatami) na panelu nawigacyjnym kliknij opcję **Update CRL location assignment**(Aktualizuj przypisanie położenia listy CRL). W ramce zadań zostanie wyświetlona strona Przypisanie położenia listy CRL.
14. Zaznacz przełącznik dla certyfikatu ośrodka CA, do którego chcesz przypisać położenie CRL. Kliknij opcję **Aktualizacja przypisania położenia CRL**(Update CRL Location Assignment). W ramce zadań zostanie wyświetlona strona Aktualizacja przypisania położenia CRL.
15. Zaznacz przełącznik położenia listy CRL, która ma zostać przypisana do certyfikatu. Kliknij opcję **Aktualizuj przypisanie**. Program DCM informuje, że zaktualizował przypisanie.

Należy zauważyć, że program DCM umożliwia przypisanie innego serwera LDAP przez ośrodek certyfikacji.

Uzyskiwanie dostępu do list CRL i ARL za pomocą programu IBM MQ Explorer
Program IBM MQ Explorer umożliwia poinformowanie menedżera kolejek o sposobie dostępu do list CRL.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation List-CRL) dotyczą również list odwołań uprawnień (Authority Revocation List-ARL).

Aby skonfigurować połączenie LDAP z listą CRL, wykonaj następującą procedurę:

1. Upewnij się, że menedżer kolejek został uruchomiony.
2. Kliknij prawym przyciskiem myszy folder **Informacje uwierzytelniające** i kliknij opcję **Nowy-> Informacje uwierzytelniające**. W otwartym arkuszu właściwości:
   a. Na pierwszej stronie **Create Authentication Information**(Utwórz informacje uwierzytelniające) wpisz nazwę obiektu CRL (LDAP).
   b. Na stronie **Ogólne** opcji **Zmień właściwości**wybierz typ połączenia. Opcjonalnie można wprowadzić opis.
   c. Wybierz stronę **CRL (LDAP)** w oknie **Change Properties**(Zmiana właściwości).
   d. Wprowadź nazwę serwera LDAP jako nazwę sieciową lub adres IP.
   e. Jeśli serwer wymaga danych logowania, podaj ID użytkownika i hasło, jeśli jest to konieczne.
   f. Kliknij przycisk **OK**.
3. Kliknij prawym przyciskiem myszy folder Listy nazw i kliknij kolejno opcje **Nowa-> Lista nazw**. W otwartym arkuszu właściwości:
   a. Wpisz nazwę listy nazw.
   b. Dodaj nazwę obiektu CRL (LDAP) (z kroku “2.a” na stronie 391) do listy.
   c. Kliknij przycisk **OK**.
4. Kliknij prawym przyciskiem myszy menedżer kolejek, wybierz opcję **Właściwości**, a następnie wybierz stronę **SSL** :
   a. Zaznacz pole wyboru **Sprawdź certyfikaty odebrane przez tego menedżera kolejek w odniesieniu do list odwołań certyfikatów** .

b. Wpisz nazwę listy nazw (z kroku “3.a” na stronie 391) w polu **CRL Namelist** (Lista nazw CRL).

Uzyskiwanie dostępu do list CRL i ARL za pomocą IBM MQ MQI client

Istnieją trzy opcje określania serwerów LDAP przechowujących listy CRL na potrzeby sprawdzania przez serwer IBM MQ MQI client.

Należy zauważyć, że w tej sekcji informacje o listach odwołań certyfikatów (Certificate Revocation List-CRL) dotyczą również list odwołań uprawnień (Authority Revocation List-ARL).

Istnieją trzy sposoby określania serwerów LDAP:

- Korzystanie z tabeli definicji kanału
- Korzystanie ze struktury opcji konfiguracyjnych protokołu SSL (MQSCO) w wywołaniu MQCONNX
- Korzystanie z usługi Active Directory (w systemach Windows z obsługą Active Directory)

Więcej informacji można znaleźć w informacjach pokrewnych.

Można dołączyć do 10 połączeń z alternatywnymi serwerami LDAP, aby zapewnić ciągłość usług w przypadku awarii jednego lub większej liczby serwerów LDAP. Należy zauważyć, że serwery LDAP muszą zawierać identyczne informacje.

Nie można uzyskać dostępu do list CRL LDAP z kanału IBM MQ MQI client działającego na platformie Linux (zSeries).

Położenie modułu odpowiadającego OCSP i serwerów LDAP, które przechowują listy CRL
W systemie IBM MQ MQI client można określić położenie programu odpowiadającego OCSP oraz serwerów LDAP (Lightweight Directory Access Protocol), które przechowują listy odwołań certyfikatów (CRL).

Te lokalizacje można określić na trzy sposoby, opisane w tej sekcji, w kolejności malejącej.

IBM i W przypadku systemu IBM inależy zapoznać się z sekcją Uzyskiwanie dostępu do list CRL i ARL w systemie IBM i.

Gdy aplikacja IBM MQ MQI client wysyła wywołanie MQCONNX

W wywołaniu **MQCONNX** można określić program odpowiadający OCSP lub serwer LDAP przechowujący listy CRL.

W wywołaniu funkcji **MQCONNX** struktura opcji połączenia (MQCNO) może odwoływać się do struktury opcji konfiguracji SSL (MQSCO). Z kolei struktura MQSCO może odwoływać się do jednej lub większej liczby struktur rekordów informacji uwierzytelniającej (MQAIR). Każda struktura MQAIR zawiera wszystkie informacje wymagane przez produkt IBM MQ MQI client do uzyskania dostępu do modułu odpowiadającego OCSP lub serwera LDAP przechowującego listy CRL. Na przykład jednym z pól w strukturze MQAIR jest URL , pod 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 serwera odpowiadającego OCSP lub serwera LDAP

Aby produkt IBM MQ MQI client mógł uzyskać dostęp do serwera odpowiadającego OCSP lub serwera LDAP, który zawiera listy CRL, należy uwzględnić atrybuty jednego lub większej liczby obiektów informacji uwierzytelniającej w tabeli definicji kanału klienta.

W menedżerze kolejek serwera można zdefiniować jeden lub więcej obiektów informacji uwierzytelniającej. Atrybuty obiektu uwierzytelniania zawierają wszystkie informacje wymagane do uzyskania dostępu do programu odpowiadającego OCSP (na platformach, na których obsługiwany jest protokół OCSP) lub do serwera LDAP przechowującego listy CRL. Jeden z atrybutów określa adres URLprogramu odpowiadającego OCSP, drugi określa adres hosta lub adres IP systemu, w którym działa serwer LDAP.

z/OS IBM i Obiekt informacji uwierzytelniającej z opcją AUTHTYPE (OCSP) nie ma zastosowania w przypadku menedżerów kolejek systemu IBM i lub z/OS , ale można go określić na tych platformach w celu skopiowania do tabeli definicji kanału klienta (CCDT) na potrzeby klienta.

Aby umożliwić produktowi IBM MQ MQI client dostęp do programu odpowiadającego OCSP lub serwerów LDAP, które przechowują listy CRL, atrybuty jednego lub większej liczby obiektów informacji uwierzytelniającej mogą zostać uwzględnione w tabeli definicji kanału klienta. Takie atrybuty można dołączyć w jeden z następujących sposobów:

Multi

Na platformach serwerowych AIX, Linux, IBM ii Windows

Można zdefiniować listę nazw zawierającą nazwy jednego lub większej liczby obiektów informacji uwierzytelniającej. 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. Celem jest, aby każdy serwer LDAP przechowywał te same listy CRL. Jeśli jeden serwer LDAP jest niedostępny, gdy jest wymagany, IBM MQ MQI client może podjąć próbę uzyskania dostępu do innego serwera.

Atrybuty obiektów informacji uwierzytelniającej identyfikowanych przez listę nazw są tutaj zbiorczo nazywane *położeniem odwołania certyfikatu*. Po ustawieniu dla atrybutu menedżera kolejek **SSLCRLNL**nazwy listy nazw miejsce odwołania certyfikatu jest kopiowane do tabeli definicji kanału klienta powiązanej z menedżerem kolejek. Jeśli dostęp do tabeli CCDT można uzyskać z systemu klienckiego jako pliku współużytkowanego lub jeśli tabela CCDT jest następnie kopiowana do systemu klienckiego, plik IBM MQ MQI client w tym systemie może użyć położenia odwołania certyfikatu w tabeli CCDT, aby uzyskać dostęp do serwera odpowiadającego OCSP lub serwera LDAP, który zawiera listy CRL.

Jeśli położenie odwołania certyfikatu menedżera kolejek zostanie później zmienione, zmiana zostanie odzwierciedlona w tabeli definicji kanału klienta powiązanej z menedżerem kolejek. Jeśli atrybut menedżera kolejek **SSLCRLNL**jest pusty, położenie odwołania certyfikatu jest usuwane z tabeli definicji kanału klienta. Zmiany te nie są odzwierciedlane w żadnej kopii tabeli w systemie klienckim.

Jeśli wymagane jest, aby miejsce odwołania certyfikatu na kliencie i serwerze końców kanału MQI było inne, a menedżer kolejek serwera jest tym, który jest używany do tworzenia położenia odwołania certyfikatu, można to zrobić w następujący sposób:

1. W menedżerze kolejek serwera utwórz miejsce odwołania certyfikatu do użycia w systemie klienckim.
2. Skopiuj do systemu klienta plik CCDT zawierający położenie odwołania certyfikatu.
3. W menedżerze kolejek serwera zmień położenie odwołania certyfikatu na wymagane na końcu kanału MQI na serwerze.
4. Na komputerze klienta można użyć komendy **runmqsc** z parametrem **-n** .

Multi

Na platformach klienckich AIX, Linux, IBM ii Windows

Tabelę CCDT można zbudować na komputerze klienta przy użyciu komendy runmqsc z parametrem **-n** i obiektami **DEFINE AUTHINFO** w pliku CCDT. Kolejność, w jakiej obiekty są zdefiniowane, jest kolejnością, w jakiej są używane w pliku. Nazwa, której można użyć w obiekcie **DEFINE AUTHINFO** , nie jest zachowywana w pliku. W przypadku **DISPLAY** obiektów **AUTHINFO** w pliku CCDT używane są tylko liczby pozycyjne.

Uwaga: Jeśli zostanie podany parametr **-n** , nie wolno podawać żadnych innych parametrów.

Korzystanie z usługi Active Directory w systemie Windows

Windows

W systemach Windows można użyć komendy sterującej **setmqcrl** do opublikowania informacji o bieżącej liście CRL w katalogu 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 za pomocą programów 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 na innych platformach.

Informacje na temat pracy z listami CRL i ARL oraz z produktem IBM MQ classes for Javazawiera sekcja Korzystanie z list odwołań certyfikatów .

Informacje na temat pracy z listami CRL i ARL przy użyciu komendy IBM MQ classes for JMSzawiera sekcja Właściwość obiektu SSLCERTSTORES .

Manipulowanie obiektami informacji uwierzytelniającej

Obiektami informacji uwierzytelniającej można manipulować za pomocą komend MQSC, PCF lub IBM MQ Explorer.

Następujące komendy MQSC działają na obiektach informacji uwierzytelniającej:

- ZDEFINIUJ INFORMACJE O AUTORYZ.
- ZMIEŃ INFORMACJE O AUTORYZACJI
- USUŃ INFORMACJE O AUTORYZ
- WYŚWIETL INFORMACJE O AUTORYZ

Pełny opis tych komend zawiera sekcja Komendy MQSC.

Następujące komendy PCF (Programmable Command Format) działają na obiektach informacji uwierzytelniającej:

- Tworzenie informacji uwierzytelniającej
- Kopiowanie informacji uwierzytelniającej
- Zmień informacje uwierzytelniające
- Usuń informacje uwierzytelniające
- Sprawdź informacje uwierzytelniające
- Sprawdź nazwy informacji uwierzytelniających

Pełny opis tych komend zawiera sekcja Definicje formatów komend programowalnych.

Na platformach, na których jest on dostępny, można również użyć IBM MQ Explorer.

Linux AIX Korzystanie z metody PAM (Pluggable Authentication Method)

Modułu PAM można używać tylko na platformach AIX and Linux . Typowy system AIX lub Linux zawiera moduły PAM, które implementują tradycyjny mechanizm uwierzytelniania, ale może być ich więcej. Oprócz podstawowego zadania sprawdzania poprawności haseł można również wywoływać moduły PAM w celu wykonania dodatkowych reguł.

Pliki konfiguracyjne definiują, która metoda uwierzytelniania ma być używana dla każdej aplikacji. Przykładowe aplikacje to standardowe logowanie terminalowe, ftp i telnet.

Zaletą modułu PAM jest to, że aplikacja nie musi znać ani dbać o to, w jaki sposób identyfikator użytkownika jest w rzeczywistości uwierzytelniany. Dopóki aplikacja może udostępnić PAM poprawną formę danych uwierzytelniania, mechanizm, który za nią stoi, jest przezroczysty.

Forma danych uwierzytelniania zależy od używanego systemu. Na przykład IBM MQ uzyskuje hasło za pomocą parametrów, takich jak struktura MQCSP używana w wywołaniu interfejsu API MQCONNX .

Ważne: Nie można ustawić atrybutu **AUTHENMD** , dopóki nie zostanie zainstalowany produkt IBM MQ 8.0.0 Fix Pack 3, a następnie nie zostanie zrestartowany menedżer kolejek przy użyciu programu **-e CMDLEVEL=***Poziom* o wartości *802* (w komendzie strmqm,) w celu ustawienia wymaganego poziomu komend.

Konfigurowanie systemu do korzystania z modułu PAM

Nazwa usługi używana przez IBM MQpodczas wywoływania PAM to *ibmmq*.

Należy zauważyć, że podczas instalacji systemu IBM MQ podejmowana jest próba zachowania domyślnej konfiguracji PAM, która umożliwia nawiązywanie połączeń z użytkownikami systemu operacyjnego na podstawie znanych wartości domyślnych dla różnych systemów operacyjnych.

Jednak administrator systemu musi sprawdzić, czy reguły zdefiniowane w pliku `/etc/pam.conf`lub `/etc/pam.d/ibmmq`są nadal odpowiednie.

Autoryzowanie dostępu do obiektów

Ta sekcja zawiera informacje na temat używania menedżera uprawnień do obiektów i programów obsługi wyjścia kanału do sterowania dostępem do obiektów.

ALW W systemach AIX, Linux, and Windows . Dostęp do obiektów można kontrolować za pomocą menedżera uprawnień do obiektów (object authority manager-OAM). Ta kolekcja tematów zawiera informacje na temat używania interfejsu komend do OAM.

Ta sekcja zawiera również listę kontrolną, której można użyć do określenia, jakie czynności należy wykonać w celu zastosowania ochrony w systemie na wszystkich platformach, a także uwagi dotyczące nadawania użytkownikom uprawnień do administrowania systemem IBM MQ oraz do pracy z obiektami systemu IBM MQ .

Jeśli dostarczone mechanizmy zabezpieczeń nie spełniają potrzeb, można utworzyć 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.

V 9.3.4 W produkcie IBM MQ 9.3.4można podać znacznik na potrzeby uwierzytelniania, jeśli parametr **ADOPTCTX** ma wartość YES, użytkownik jest adoptowany z żądań zawartych w znaczniku.

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 395 , 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 71. 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`.

ALW Kontrolowanie dostępu do obiektów za pomocą OAM w systemie AIX, Linux, and Windows

Menedżer uprawnień do obiektów (object authority manager-OAM) udostępnia interfejs komend do nadawania i odbierania uprawnień do obiektów IBM MQ .

Użytkownik musi mieć odpowiednie uprawnienia do używania tych komend, zgodnie z opisem w sekcji “Uprawnienia do administrowania systemem IBM MQ w systemie AIX, Linux, and Windows” na stronie 446. Identyfikatory użytkowników autoryzowanych do administrowania systemem IBM MQ mają uprawnienie *administratora* do menedżera kolejek, co oznacza, że nie jest konieczne nadawanie im dalszych uprawnień do wydawania żądań lub komend MQI.

Linux AIX Uprawnienia OAM oparte na użytkownikach w systemie AIX and Linux

W systemie IBM MQ 8.0, w systemach UNIX and Linux , menedżer uprawnień do obiektów (OAM) może używać autoryzacji opartej na użytkownikach oraz autoryzacji opartej na grupach.

W systemach wcześniejszych niż IBM MQ 8.0listy kontroli dostępu (ACL) w systemie UNIX and Linux są oparte tylko na grupach. W produkcie IBM MQ 8.0listy ACL są oparte zarówno na identyfikatorach użytkowników, jak i na grupach. W celu autoryzacji można użyć modelu opartego na użytkownikach lub modelu opartego na grupach, ustawiając atrybut **SecurityPolicy** na odpowiednią wartość zgodnie z opisem w sekcjach Konfigurowanie usług instalowalnych i Konfigurowanie usług autoryzacji w systemie AIX and Linux.

Zmiany w działaniu produktu IBM MQ 8.0 i nowszych wersji

W produkcie IBM MQ 8.0niektóre komendy uruchamiane ze strategią opartą na użytkownikach zwracają inne informacje niż wcześniejsze wersje produktu:

- Komendy **dmpmqaut** i **dmpmqcfg** wyświetlają rekordy oparte na użytkownikach, podobnie jak równoważne operacje PCF.
- Wtyczka OAM dla IBM MQ Explorer wyświetla rekordy oparte na użytkownikach i umożliwia modyfikacje oparte na użytkownikach.
- Funkcja OAM **Inquire** zwraca wyniki, które wskazują, że obsługuje ona użytkownika.

Użycie atrybutu **-p** w komendzie **setmqaut** nie powoduje nadania dostępu wszystkim użytkownikom w tej samej grupie podstawowej, jeśli autoryzacje oparte na użytkownikach są włączone w pliku `qm.ini` zgodnie z opisem w sekcji Service pliku qm.ini.

Jeśli użytkownik zacznie korzystać z autoryzacji opartej na użytkownikach i będzie miał wielu użytkowników, prawdopodobnie będzie więcej rekordów przechowywanych 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. Oczekuje się, że wzrost ten nie będzie znaczący. W razie potrzeby można użyć kombinacji uprawnień użytkownika i grupy.

Uwagi dotyczące migracji

Zmiana modelu z grupy na użytkownika dla istniejącego menedżera kolejek nie ma natychmiastowego skutku. Autoryzacje, które zostały już wprowadzone, będą nadal stosowane. Każdy użytkownik, który nawiązuje połączenie z menedżerem kolejek, otrzymuje te same uprawnienia, co poprzednio: połączenie wszystkich grup, do których należy jego identyfikator. Nowe komendy systemu **setmqaut** wydawane dla identyfikatorów użytkowników zaczynają obowiązywać natychmiast.

W przypadku tworzenia nowego menedżera kolejek przy użyciu strategii użytkownika, ten menedżer kolejek ma uprawnienia tylko dla użytkownika, który go utworzył (zwykle jest to identyfikator użytkownika `mqm`). Istnieją również uprawnienia, które są automatycznie nadawane grupie `mqm` . Jeśli jednak grupa `mqm` nie jest grupą podstawową, grupa `mqm` nie zostanie dołączona do początkowego zestawu autoryzacji.

W przypadku przejścia ze strategii użytkownika do strategii grupy autoryzacje oparte na użytkownikach nie są automatycznie usuwane. 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 jest on teraz menedżerem kolejek opartym na grupach, w efekcie reguły identyfikatorów użytkowników są przechowywane w oparciu o grupę podstawową.

Pojęcia pokrewne

menedżer uprawnień obiektu (OAM)

“Nazwy użytkowników i grupy w systemie AIX, Linux, and Windows” na stronie 451

Użytkownicy mogą należeć do grup. Nadając dostęp do zasobów grupom, a nie poszczególnym osobom, można zmniejszyć liczbę wymaganych czynności administracyjnych. Listy kontroli dostępu (ACL) są oparte zarówno na grupach, jak i na identyfikatorach użytkowników.

Odsyłacze pokrewne

Sekcja service pliku qm.ini

crtmqm (tworzenie menedżera kolejek-create queue manager), komenda

ALW Nadawanie dostępu do obiektu IBM MQ w systemie AIX, Linux, and Windows

Użyj komendy sterującej **setmqaut** , komendy **SET AUTHREC** MQSC lub komendy **MQCMD_SET_AUTH_REC** PCF, aby nadać użytkownikom i grupom użytkowników dostęp do obiektów IBM MQ . Należy zauważyć, że w urządzeniu IBM MQ Appliance można używać tylko komendy **SET AUTHREC** .

Pełną definicję komendy sterującej **setmqaut** i jej składnię zawiera opis komendy setmqaut.

Pełną definicję komendy **SET AUTHREC** MQSC i jej składni zawiera sekcja SET AUTHREC.

Pełną definicję komendy **MQCMD_SET_AUTH_REC** PCF i jej składnię zawiera sekcja Ustawianie rekordu uprawnień.

Aby można było użyć tej komendy, menedżer kolejek musi być uruchomiony. Po zmianie dostępu dla nazwy użytkownika zmiany są natychmiast odzwierciedlane przez OAM.

Aby nadać użytkownikom dostęp do obiektu, należy określić:

- Nazwa menedżera kolejek, który jest właścicielem obiektów, z którymi pracuje użytkownik. Jeśli nazwa menedżera kolejek nie zostanie określona, przyjmowany jest domyślny menedżer kolejek.
- Nazwa i typ obiektu (w celu jednoznacznego zidentyfikowania obiektu). Nazwę określa się jako *profil* ; Jest to jawna nazwa obiektu lub nazwa ogólna zawierająca znaki wieloznaczne. Szczegółowy opis profili ogólnych oraz użycie w nich znaków wieloznacznych zawiera sekcja “Korzystanie z profili ogólnych OAM w systemie AIX, Linux, and Windows” na stronie 400.
- Jedna lub więcej nazw użytkowników i grup, do których ma zastosowanie uprawnienie.

  Jeśli identyfikator użytkownika zawiera spacje, należy go ująć w cudzysłów podczas używania tej komendy. W systemach Windows można kwalifikować identyfikator użytkownika za pomocą nazwy domeny. Jeśli rzeczywisty identyfikator użytkownika zawiera znak @, należy go zastąpić znakiem @ @, aby pokazać, że jest on częścią identyfikatora użytkownika, a nie separatorem między identyfikatorem użytkownika a nazwą domeny.
- Lista autoryzacji. Każdy element na liście określa typ dostępu, który ma zostać nadany temu obiektowi (lub odebrany). Każda autoryzacja na liście jest określona jako słowo kluczowe, poprzedzone znakiem plus (+) lub znakiem minus (-). Użyj znaku plus, aby dodać określoną autoryzację, lub znaku minus, aby usunąć autoryzację. Między znakiem + lub-a słowem kluczowym nie mogą występować spacje.

  W pojedynczej komendzie można podać dowolną liczbę autoryzacji. Na przykład lista autoryzacji umożliwiających użytkownikowi lub grupie umieszczanie komunikatów w kolejce i przeglądanie ich, ale odbierających dostęp 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 używania 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 jest identyfikatorem grupy z autoryzacjami, które mają zostać zmienione.
- +browse -get +put jest listą autoryzacji dla określonej kolejki
  - +browse dodaje autoryzację do przeglądania komunikatów w kolejce (w celu wydania komendy **MQGET** z opcją przeglądania)
  - -get usuwa autoryzację do pobierania (**MQGET**) komunikatów z kolejki
  - +put dodaje uprawnienia do umieszczania (**MQPUT**) komunikatów w kolejce

Poniższa komenda odbiera uprawnienie do umieszczania w kolejce MyQueue użytkownikowi fvuser oraz grupom groupa i groupb. W systemach AIX and Linux ta komenda odbiera również uprawnienie 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
```

Używanie komendy setmqaut z inną usługą autoryzacji

Jeśli zamiast usługi OAM używana jest własna usługa autoryzacji, można podać nazwę tej usługi w komendzie **setmqaut** , aby skierować komendę do tej usługi. Ten parametr należy określić, jeśli w tym samym czasie uruchomionych jest wiele instalowalnych komponentów; w przeciwnym razie zostanie wykonana aktualizacja pierwszego instalowalnego komponentu dla usługi autoryzacji. Domyślnie jest to podany 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.

ALW Korzystanie z profili ogólnych OAM w systemie AIX, 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 AIX and 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: Chociaż użytkownicy w systemie AIX and Linux mogą używać opcji `-p` dla komendy **dmpmqaut** , 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
```

ALW *Używanie znaków wieloznacznych w profilach OAM w systemie AIX, Linux, and Windows*

Użyj znaków wieloznacznych w nazwie profilu menedżera uprawnień do obiektów (OAM), aby profil ten mógł być stosowany do więcej niż jednego obiektu.

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.

Uwaga: Jeśli w systemach AIX and Linux używane są znaki wieloznaczne, **należy** ująć nazwę profilu w pojedynczy cudzysłów.

ALW *Priorytety profili w systemie AIX, 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 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
```

Pierwsza nadaje uprawnienie do wszystkich kolejek 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 konkretne**. 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. **

Informacje na temat używania tej komendy MQSC znajdują się w sekcji SET AUTHREC .

ALW *Zrzucanie ustawień profilu w systemie AIX, Linux, and Windows*

Użyj komendy sterującej **dmpmqaut** , komendy **DISPLAY AUTHREC** MQSC lub komendy **MQCMD_INQUIRE_AUTH_RECS** PCF, aby zrzucić bieżące autoryzacje powiązane z określonym profilem. Należy zauważyć, że w urządzeniu IBM MQ Appliance można używać tylko komendy **DISPLAY AUTHREC** .

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 podobnie jak w poniższym przykładzie:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Uwaga: Użytkownicy systemu AIX and Linux nie mogą używać opcji `-p` ; zamiast niej 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 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 zrzuca wszystkie rekordy uprawnień dla profilu a.b. *, typu kolejka.

```
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 zrzuca się 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 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
```

ALW Wyświetlanie ustawień dostępu w systemie AIX, Linux, and Windows

Użyj komendy sterującej **dspmqaut** , komendy **DISPLAY AUTHREC** MQSC lub komendy **MQCMD_INQUIRE_ENTITY_AUTH** PCF, aby wyświetlić autoryzacje, które konkretna nazwa użytkownika lub grupa ma dla konkretnego obiektu. Należy zauważyć, że w urządzeniu IBM MQ Appliance można używać tylko komendy **DISPLAY AUTHREC** .

Aby można było użyć tej komendy, menedżer kolejek musi być uruchomiony. W przypadku zmiany dostępu dla nazwy użytkownika zmiany są natychmiast odzwierciedlane przez system OAM. Autoryzacja może być wyświetlana tylko dla jednej grupy lub nazwy użytkownika w danym momencie.

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.

W poniższym przykładzie przedstawiono użycie komendy sterującej **dspmqaut** do wyświetlenia uprawnień grupy GpAdmin do definicji procesu o nazwie Annuities , która znajduje się w menedżerze kolejek QueueMan1.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

ALW Zmienianie i odbieranie dostępu do obiektu IBM MQ w systemie AIX, 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 zauważyć, że w urządzeniu IBM MQ Appliance można używać tylko komendy **DELETE AUTHREC** .

Proces usuwania użytkownika z grupy opisano w następujących sekcjach:

- Windows “Tworzenie grup i zarządzanie nimi w systemie Windows” na stronie 155
- AIX “Tworzenie grup i zarządzanie nimi w systemie AIX” na stronie 154
- Linux “Tworzenie grup i zarządzanie nimi w systemie Linux” na stronie 155

.

ID użytkownika, który tworzy obiekt IBM MQ , otrzymuje pełne uprawnienia 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. Po usunięciu obiektu

z grupy mqm lub grupy administratorów należy użyć komendy sterującej **setmqaut** lub komendy **MQCMD_DELETE_AUTH_REC** PCF, aby odebrać dostęp do obiektu ID użytkownika, który go utworzył.

Pełną definicję komendy sterującej setmqaut i jej składnię zawiera sekcja setmqaut.

Pełną definicję komendy **DELETE AUTHREC** MQSC i jej składni zawiera sekcja DELETE AUTHREC.

Pełną definicję komendy **MQCMD_DELETE_AUTH_REC** PCF i jej składnię zawiera sekcja Usuwanie rekordu uprawnień.

Windows W systemie Windowsz poziomu systemu IBM MQ 8.0można w dowolnym momencie usunąć wpisy OAM odpowiadające konkretnemu koncie użytkownika Windows , korzystając z parametru **-u** *SID* o wartości **setmqaut**.

W wersjach wcześniejszych niż IBM MQ 8.0przed usunięciem profilu użytkownika trzeba było usunąć pozycje OAM odpowiadające konkretnemu koncie użytkownika Windows . Po usunięciu konta użytkownika nie można było usunąć pozycji OAM.

ALW Zapobieganie sprawdzaniu dostępu do zabezpieczeń w systemach AIX, Linux, and Windows

Uwaga: W tej sekcji opisano funkcje, których włączenie nie jest zalecane. Aby wyłączyć sprawdzanie zabezpieczeń, można wyłączyć menedżera uprawnień do obiektów (OAM). Może to być odpowiednie dla środowiska testowego. Jeśli ta opcja jest wyłączona, menedżer kolejek nie może już wykonywać sprawdzania autoryzacji ani uwierzytelniania połączenia. Nadal można używać protokołów TLS, rekordów uwierzytelniania kanału i wyjść zabezpieczeń. 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 środowiskowej **MQSNOAUT** oraz sposobu ustawienia zmiennej **MQSNOAUT** w systemie AIX, Linux, and Windowszawiera sekcja Opisy zmiennych środowiskowych.
- Edytuj plik konfiguracyjny menedżera kolejek, aby usunąć usługę.

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.

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.
- Żadne informacje autoryzacyjne przekazane do modułu OAM na potrzeby sprawdzania uwierzytelniania nie są sprawdzane.

Pojęcia pokrewne

Usługi i komponenty, które można zainstalować w systemie AIX, Linux, and Windows

Zadania pokrewne

Konfigurowanie instalowalnych usług

Odsyłacze pokrewne

Informacje uzupełniające o usługach instalowalnych

Nadawanie wymaganego dostępu do zasobów

Ten temat zawiera informacje dotyczące zadań, które należy wykonać w celu zastosowania ochrony w systemie IBM MQ .

O tym zadaniu

Podczas wykonywania tego zadania użytkownik decyduje, jakie działania są niezbędne do zastosowania odpowiedniego poziomu zabezpieczeń do elementów instalacji produktu IBM MQ . Każde zadanie, do którego się odwołuje, zawiera szczegółowe instrukcje dla wszystkich platform.

Procedura

1. Czy konieczne jest ograniczenie dostępu do menedżera kolejek do określonych użytkowników?
   a) Nie: Nie podejmuj 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 częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek” na stronie 408.
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 418.
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 424.
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 425.
6. Czy do nawiązania połączenia z menedżerem kolejek potrzebne są aplikacje użytkownika?
   a) Nie: wyłącz połączenia zgodnie z opisem w sekcji “Usuwanie połączenia z menedżerem kolejek” na stronie 427
   b) Tak: Patrz “Zezwalanie aplikacjom użytkownika na nawiązywanie połączeń z menedżerem kolejek” na stronie 427.

Multi z/OS Nadawanie częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek

Niektórym użytkownikom należy przyznać częściowy dostęp administracyjny do niektórych, ale nie wszystkich, zasobów menedżera kolejek. Ta tabela służy do określenia działań, które należy wykonać.

Tabela 72. Nadawanie częściowego dostępu administracyjnego do podzbioru zasobów menedżera kolejek	
Użytkownicy muszą administrować obiektami tego typu	**Wykonaj to działanie**
Kolejki	Nadaj częściowy dostęp administracyjny do wymaganych kolejek, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych kolejek” na stronie 409
Tematy	Nadaj częściowy dostęp administracyjny do wymaganych tematów zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych tematów” na stronie 411
Kanały	Nadaj częściowy dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych kanałów” na stronie 412
Menedżer kolejek	Nadaj częściowy dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji “Nadawanie ograniczonego dostępu administracyjnego do menedżera kolejek” na stronie 413
Procesy	Nadaj częściowy dostęp administracyjny do wymaganych procesów, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych procesów” na stronie 414
Listy nazw	Nadaj częściowy dostęp administracyjny do wymaganych list nazw, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych list nazw” na stronie 415
Usługi	Nadaj częściowy dostęp administracyjny do wymaganych usług, zgodnie z opisem w sekcji “Przyznawanie ograniczonego dostępu administracyjnego do niektórych usług” na stronie 416

Przyznawanie ograniczonego dostępu administracyjnego do niektórych kolejek

Przyznaj częściowy dostęp administracyjny do niektórych kolejek w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać niektórym działaniom ograniczony dostęp administracyjny do niektórych kolejek, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
```

- IBM i
  W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS W systemie z/OSnależy wydać następujące komendy, aby nadać dostęp 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, wprowadź 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 wydać 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

  ReqdAction
  Działanie, które ma zostać wykonane przez grupę:

  – ALW W systemach AIX, Linux, and Windows : dowolna kombinacja następujących autoryzacji: + chg, + clr, + dlt, + dsp. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.

  – IBM i W systemie IBM i: dowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.

  – z/OS W systemie z/OSjest to jedna z następujących wartości: ALTER, CLEAR, DELETE lub MOVE.

Uwaga: Nadanie + crt dla kolejek pośrednio powoduje, że użytkownik lub grupa staje się administratorem. Nie należy używać uprawnienia + crt do nadawania ograniczonego dostępu administracyjnego do niektórych kolejek.

QTYPE

Dla komendy DISPLAY: jedna z wartości: QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE lub QCLUSTER.

W przypadku innych wartości parametru *ReqdAction*należy podać jedną z następujących wartości: QLOCAL, QALIAS, QMODEL lub QREMOTE.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych tematów

Przyznaj częściowy dostęp administracyjny do niektórych tematów w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać niektórym działaniom ograniczony dostęp administracyjny do niektórych tematów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW

  W systemach AIX, Linux, and Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
  ```

- IBM i

  W systemie IBM iwprowadź następującą komendę:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS W systemie z/OSwydaj następujące komendy:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Te komendy umożliwiają dostęp do określonego tematu. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w tym temacie, należy wydać 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 wydać 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

ReqdAction
Działanie, które ma zostać wykonane przez grupę:

- ALW W systemach AIX, Linux, and Windows : dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.
- IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.
- z/OS W systemie z/OS: jedna z wartości ALTER, CLEAR, DEFINE, DELETE lub MOVE.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych kanałów

Nadaj częściowy dostęp administracyjny do niektórych kanałów w menedżerze kolejek każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać niektórym kanałom ograniczony dostęp administracyjny do niektórych działań, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 umożliwiają dostęp do określonego kanału. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w kanale, wprowadź następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby umożliwić użytkownikowi korzystanie z komendy DISPLAY CHANNEL, należy wydać 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

ReqdAction
Działanie, które ma zostać wykonane przez grupę:

- ALW W systemie AIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.
- IBM i W systemie IBM i: dowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLx. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.
- z/OS W systemie z/OS: jedna z wartości ALTER, CLEAR, DEFINE, DELETE lub MOVE.

Nadawanie ograniczonego dostępu administracyjnego do menedżera kolejek

Przyznaj częściowy dostęp administracyjny do menedżera kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać ograniczony dostęp administracyjny do wykonywania niektórych działań w menedżerze kolejek, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 można wykonać w menedżerze kolejek, wprowadź następujące komendy dla każdej komendy MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName. ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Aby umożliwić użytkownikowi użycie komendy DISPLAY QMGR, należy wydać 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, której ma zostać nadany dostęp.

ReqdAction
Działanie, które ma zostać wykonane przez grupę:

- ALW W systemie AIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.

  Chociaż uprawnienie + set jest autoryzacją MQI i zwykle nie jest uznawane za administracyjne, nadanie uprawnienia + set w menedżerze kolejek może pośrednio prowadzić do pełnego uprawnienia administracyjnego. Nie należy nadawać + set zwykłym użytkownikom i aplikacjom.
- IBM i W systemie IBM i: dowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych procesów

Nadaj częściowy dostęp administracyjny do niektórych procesów w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać niektórym działaniom ograniczony dostęp administracyjny do niektórych procesów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 umożliwiają dostęp do określonego kanału. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika w kanale, wprowadź 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 wydać 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

ReqdAction
Działanie, które ma zostać wykonane przez grupę:

- ALW W systemie AIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + dsp. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.
- IBM i W systemie IBM i: dowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.
- z/OS W systemie z/OS: jedna z wartości ALTER, CLEAR, DEFINE, DELETE lub MOVE.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych list nazw

Nadaj częściowy dostęp administracyjny do niektórych list nazw w menedżerze kolejek każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać niektórym działaniom ograniczony dostęp administracyjny do niektórych list nazw, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 umożliwiają dostęp do określonej listy nazw. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika na liście nazw, wprowadź 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, wydaj 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

  ReqdAction
  Działanie, które ma zostać wykonane przez grupę:

  - ALW W systemie AIX, Linux, and Windowsdowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.
  - IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.
  - z/OS W systemie z/OS: jedna z wartości ALTER, CLEAR, DEFINE, DELETE lub MOVE.

Przyznawanie ograniczonego dostępu administracyjnego do niektórych usług

Nadaj częściowy dostęp administracyjny do niektórych usług w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać niektórym usługom ograniczony dostęp administracyjny do niektórych usług, należy użyć komend odpowiednich dla danego systemu operacyjnego. z/OS Należy zauważyć, że obiekty usług nie istnieją w systemie z/OS.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 umożliwiają dostęp do określonej usługi. Aby określić, które komendy MQSC mogą być wykonywane przez użytkownika na usłudze, należy wydać 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 wydać 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, której ma zostać nadany dostęp.

  ReqdAction
  Działanie, które ma zostać wykonane przez grupę:

  – ALW W systemach AIX, Linux, and Windows dowolna kombinacja następujących autoryzacji: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. Autoryzacja + alladm jest równoważna + chg + clr + dlt + dsp.

  – IBM i W systemie IBM idowolna kombinacja następujących autoryzacji: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. Uprawnienie *ALLADM jest równoważne wszystkim autoryzacjom indywidualnym.

Nadawanie pełnego dostępu administracyjnego do podzbioru zasobów menedżera kolejek

Niektórym użytkownikom należy przyznać pełny dostęp administracyjny do niektórych, ale nie wszystkich, zasobów menedżera kolejek. Poniższe tabele umożliwiają określenie działań, które należy wykonać.

Tabela 73. 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 pełnego dostępu administracyjnego do niektórych kolejek” na stronie 418
Tematy	Nadaj pełny dostęp administracyjny do wymaganych tematów zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do niektórych tematów” na stronie 419
Kanały	Nadaj pełny dostęp administracyjny do wymaganych kanałów, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do niektórych kanałów” na stronie 420
Menedżer kolejek	Nadaj pełny dostęp administracyjny do menedżera kolejek zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do menedżera kolejek” na stronie 421
Procesy	Nadaj pełny dostęp administracyjny do wymaganych procesów zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do niektórych procesów” na stronie 421
Listy nazw	Nadaj pełny dostęp administracyjny do wymaganych list nazw, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do niektórych list nazw” na stronie 422
Usługi	Nadaj pełny dostęp administracyjny do wymaganych usług, zgodnie z opisem w sekcji “Nadawanie pełnego dostępu administracyjnego do niektórych usług” na stronie 423

Nadawanie pełnego dostępu administracyjnego do niektórych kolejek

Nadaj pełny dostęp administracyjny do niektórych kolejek w menedżerze kolejek, każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych kolejek, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do niektórych tematów

Nadaj pełny dostęp administracyjny do niektórych tematów w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać niektórym działaniom pełny dostęp administracyjny do niektórych tematów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do niektórych kanałów

Nadaj pełny dostęp administracyjny do niektórych kanałów w menedżerze kolejek każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych kanałów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW

  W systemie AIX, 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do menedżera kolejek

Nadaj pełny dostęp administracyjny do menedżera kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do menedżera kolejek, należy użyć komend odpowiednich dla używanego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do niektórych procesów

Nadaj pełny dostęp administracyjny do niektórych procesów w menedżerze kolejek każdej grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych procesów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do niektórych list nazw

Nadaj pełny dostęp administracyjny do niektórych list nazw w menedżerze kolejek każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych list nazw, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do niektórych usług

Nadaj pełny dostęp administracyjny do niektórych usług w menedżerze kolejek każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać pełny dostęp administracyjny do niektórych usług, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemie AIX, 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie dostępu tylko do odczytu do wszystkich zasobów w menedżerze kolejek

Przyznaj dostęp tylko do odczytu do wszystkich zasobów w menedżerze kolejek każdemu użytkownikowi lub grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Użyj kreatora dodawania uprawnień opartych na rolach lub komend odpowiednich dla używanego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Po zmianie szczegółów autoryzacji należy wykonać odświeżanie zabezpieczeń za pomocą komendy REFRESH SECURITY .

Procedura

- Przy użyciu kreatora:
  a) W panelu IBM MQ Explorer Navigator kliknij prawym przyciskiem myszy menedżer kolejek, a następnie kliknij opcję **Uprawnienia do obiektów** > **Dodaj uprawnienia oparte na rolach**
  Zostanie otwarty kreator dodawania uprawnień opartych na rolach.
- ALW
  W systemach AIX, Linux, and Windows wydaj 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
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 niezbędny tylko wtedy, gdy ma być używany IBM MQ Explorer.
- IBM i
  W systemie IBM iwydaj 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 systemie z/OSwydaj 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 kolejek.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie pełnego dostępu administracyjnego do wszystkich zasobów w menedżerze kolejek

Nadaj pełny dostęp administracyjny do wszystkich zasobów w menedżerze kolejek każdemu użytkownikowi lub grupie użytkowników z potrzebą biznesową.

O tym zadaniu

Można użyć kreatora dodawania uprawnień opartych na rolach lub komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Uwagi: ALW

1. Jeśli do administrowania menedżerem kolejek używany jest program **runmqsc** , a nie program IBM MQ Explorer, należy nadać uprawnienie do tworzenia zapytań o system SYSTEM.MQSC.REPLY.QUEUEi nie trzeba nadawać żadnych uprawnień w systemie SYSTEM.MQEXPLORER.REPLY.MODEL .
2. Podczas nadawania użytkownikowi dostępu do wszystkich zasobów w menedżerze kolejek istnieją pewne komendy, których użytkownik nie może uruchomić, chyba że ma on prawo do odczytu pliku `qm.ini` . Jest to spowodowane ograniczeniami dotyczącymi użytkowników innych niż `mqm` , którzy mogą odczytać plik `qm.ini` .

   Użytkownik nie może wydać następujących komend, jeśli nie nadano mu prawa do odczytu pliku qm.ini :

- Definiowanie kanału skonfigurowanego do używania protokołu TLS
- Definiowanie kanału przy użyciu zmiennych wstawiania automatycznej konfiguracji zdefiniowanych w pliku `qm.ini`

Procedura

- Jeśli używany jest kreator, w panelu IBM MQ Explorer Navigator kliknij prawym przyciskiem myszy menedżer kolejek, a następnie kliknij opcję **Uprawnienia do obiektów** > **Dodaj uprawnienia oparte na rolach**.

  Zostanie otwarty kreator dodawania uprawnień opartych na rolach.

- Linux AIX

  W systemach AIX and Linux wydaj 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 ten temat zawiera sekcja **setmqaut** . `@class`

- Windows

  W systemach Windows wydaj te same komendy, co w systemach AIX and Linux , ale używając nazwy profilu @CLASS zamiast @class.

- IBM i

  W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- z/OS

  W systemie z/OSwydaj 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 kolejek.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Usuwanie połączenia z menedżerem kolejek

Jeśli aplikacje użytkownika nie mają nawiązywać połączenia z menedżerem kolejek, należy usunąć ich uprawnienia do nawiązywania połączenia z menedżerem kolejek.

O tym zadaniu

Uprawnienia wszystkich użytkowników do nawiązywania połączeń z menedżerem kolejek należy odebrać za pomocą komendy odpowiedniej dla danego systemu operacyjnego.

W systemie Wiele platformmożna również użyć komendy DELETE AUTHREC .

Uwaga: W urządzeniu IBM MQ Appliance można używać tylko komendy **DELETE AUTHREC** .

Procedura

- ALW

  W systemach AIX, Linux, and Windows wydaj następującą komendę:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName -connect
  ```

- IBM i

  W systemie IBM iwprowadź następującą komendę:

  ```
  RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
  ```

- z/OS

  W systemie z/OSwydaj 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/OSW systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejek.

  GroupName
  Nazwa grupy, której dostęp ma zostać zabroniony.

Zezwalanie aplikacjom użytkownika na nawiązywanie połączeń z menedżerem kolejek

Użytkownik chce zezwolić aplikacji użytkownika na nawiązywanie połączenia z menedżerem kolejek. Tabele 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 będą nawiązywać połączenie z menedżerem kolejek, nie jest aplikacją kliencką, należy wyłączyć zdalny dostęp zgodnie z opisem w sekcji “Wyłączanie zdalnego dostępu do menedżera kolejek” na stronie 435.

Jeśli co najmniej jedna aplikacja, która będzie nawiązywać połączenie z menedżerem kolejek, jest aplikacją kliencką, należy zabezpieczyć połączenia zdalne zgodnie z opisem w sekcji “Zabezpieczanie połączeń zdalnych z menedżerem kolejek” na stronie 428.

W obu przypadkach należy skonfigurować zabezpieczenia połączenia zgodnie z opisem w sekcji “Konfigurowanie zabezpieczeń połączenia” na stronie 435 .

Aby kontrolować dostęp do zasobów dla każdego użytkownika łączącego się z menedżerem kolejek, należy zapoznać się z poniższą tabelą. Jeśli instrukcja w pierwszej kolumnie jest prawdziwa, wykonaj działanie wymienione w drugiej kolumnie.

Instrukcja	**Wykonaj to działanie**
Istnieją aplikacje, które korzystają z kolejek	Więcej informacji znajduje się w sekcji “Kontrolowanie dostępu użytkowników do kolejek” na stronie 436
Istnieją aplikacje, które korzystają z tematów	Patrz “Kontrolowanie dostępu użytkowników do tematów” na stronie 442.
Istnieją aplikacje, które sprawdzają obiekt menedżera kolejek	Patrz “Nadawanie uprawnień do uzyskiwania informacji o menedżerze kolejek” na stronie 444.
Istnieją aplikacje, które używają obiektów procesu	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień dostępu do procesów” na stronie 444
Istnieją aplikacje, które korzystają z list nazw	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień dostępu do list nazw” na stronie 445

Zabezpieczanie połączeń zdalnych z menedżerem kolejek

Połączenia zdalne z menedżerem kolejek można zabezpieczyć za pomocą protokołu TLS, wyjścia zabezpieczeń, rekordów uwierzytelniania kanału lub kombinacji tych metod.

O tym zadaniu

Połączenie klienta z menedżerem kolejek jest nawiązywane przy użyciu kanału połączenia klienta na stacji roboczej klienta i kanału połączenia serwera na serwerze. Zabezpiecz takie połączenia w jeden z następujących sposobów.

Procedura

1. Używanie protokołu TLS z rekordami uwierzytelniania kanału:
   a) Zablokuj możliwość otwierania kanału przez nazwę wyróżniającą (DN) za pomocą rekordu uwierzytelniania kanału SSLPEERMAP w celu odwzorowania wszystkich nazw wyróżniających na USERSRC (NOACCESS).
   b) Zezwalaj na otwieranie kanału przez konkretne nazwy wyróżniające lub zestawy nazw wyróżniających przy użyciu rekordu uwierzytelniania kanału SSLPEERMAP w celu odwzorowania ich na USERSRC (CHANNEL).
2. Używanie protokołu TLS z wyjściem zabezpieczeń:
   a) Ustaw parametr MCAUSER w kanale połączenia z serwerem na identyfikator użytkownika bez uprawnień.
   b) Napisz wyjście zabezpieczeń, aby przypisać wartość MCAUSER w zależności od wartości nazwy wyróżniającej TLS otrzymanej w polach SSLPeerNamePtr i SSLPeerNameLength przekazanych do wyjścia w strukturze MQCD.
3. Używanie protokołu TLS ze stałymi wartościami definicji kanału:
   a) Ustaw parametr SSLPEER w kanale połączenia z serwerem na konkretną wartość lub wąski zakres wartości.
   b) Ustaw wartość MCAUSER w kanale połączenia z serwerem na identyfikator użytkownika, z którym kanał ma być uruchamiany.
4. Korzystanie z rekordów uwierzytelniania kanału w kanałach, które nie korzystają z protokołu TLS:

a) Zablokuj otwieranie kanałów przez adres IP, używając rekordu uwierzytelniania kanału odwzorowania adresu z adresami ADDRESS (*) i USERSRC (NOACCESS).

b) Zezwól na otwieranie kanałów dla konkretnych adresów IP, używając rekordów uwierzytelniania kanału odwzorowania adresów dla tych adresów z USERSRC (CHANNEL).

5. Korzystanie z wyjścia zabezpieczeń:

   a) Napisz wyjście zabezpieczeń, aby autoryzować połączenia na podstawie wybranej właściwości, na przykład początkowego adresu IP.

6. Możliwe jest również użycie rekordów uwierzytelniania kanału z wyjściem zabezpieczeń lub użycie wszystkich trzech metod, jeśli wymagają tego konkretne okoliczności.

Blokowanie konkretnych adresów IP
Używając rekordu uwierzytelniania kanału, można zapobiec zaakceptowaniu przez określony kanał połączenia przychodzącego z adresu IP lub zezwolić całemu menedżerowi kolejek na dostęp z adresu IP.

Zanim rozpoczniesz

Włącz rekordy uwierzytelniania kanału, uruchamiając następującą komendę:

```
ALTER QMGR CHLAUTH(ENABLED)
```

O tym zadaniu

Aby uniemożliwić konkretnym kanałom akceptowanie połączeń przychodzących 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 uniemożliwić dostęp adresu IP do całego menedżera kolejek, zwykle należy użyć firewalla w celu jego trwałego zablokowania. Można jednak użyć innego typu reguły, aby tymczasowo zablokować kilka adresów, na przykład podczas oczekiwania na aktualizację firewalla.

Procedura

- Aby zablokować adresy IP dla 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)
```

Komenda składa się z trzech części:

SET CHLAUTH (*nazwa_kanału_ogólnego*)
Ta część komendy służy do sterowania blokowaniem połączenia dla całego menedżera kolejek, pojedynczego kanału lub zakresu kanałów. To, co tu umieściłeś, określa, które obszary są pokryte.

Na przykład:

– SET CHLAUTH('*') -blokuje każdy kanał w menedżerze kolejek, czyli cały menedżer kolejek.
– SET CHLAUTH ('SYSTEM. *')-blokuje każdy kanał rozpoczynający się łańcuchem SYSTEM.
– SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-blokuje kanał SYSTEM.DEF.SVRCONN DEF.SVRCONN

Typ reguły CHLAUTH
Ta część komendy służy do określenia typu komendy i określenia, czy ma zostać podany pojedynczy adres, czy lista adresów.

Na przykład:

– TYPE(ADDRESSMAP) -użyj ADDRESSMAP, jeśli chcesz podać pojedynczy adres lub znak wieloznaczny. Na przykład komenda ADDRESS('192.168.*') blokuje wszystkie połączenia przychodzące z adresu IP rozpoczynającego się od łańcucha 192.168.

Więcej informacji na temat filtrowania adresów IP za pomocą wzorców zawiera sekcja Ogólne adresy IP.

– TYPE(BLOCKADDR) -użyj parametru BLOCKADDR, aby podać listę adresów do zablokowania.

Parametry dodatkowe

Parametry te zależą od typu reguły użytej w drugiej części komendy:

– W przypadku systemu TYPE(ADDRESSMAP) należy użyć parametru ADDRESS

– W systemie TYPE(BLOCKADDR) należy użyć komendy ADDRLIST.

Odsyłacze pokrewne

USTAW CHLAURA

Tymczasowe blokowanie konkretnych adresów IP, jeśli menedżer kolejek nie jest uruchomiony

Jeśli menedżer kolejek nie jest uruchomiony i dlatego nie można wydawać komend MQSC, może być konieczne zablokowanie określonych adresów IP lub zakresów adresów. Adresy IP można tymczasowo zablokować w wyjątkowych sytuacjach, modyfikując plik `blockaddr.ini` .

O tym zadaniu

Plik `blockaddr.ini` zawiera kopię definicji BLOCKADDR, które są używane przez menedżer kolejek. Ten plik jest odczytywany przez program nasłuchujący, jeśli program nasłuchujący został uruchomiony przed menedżerem kolejek. W takiej sytuacji program nasłuchujący używa wartości, które zostały ręcznie dodane do pliku `blockaddr.ini` .

Należy jednak pamiętać, że po uruchomieniu menedżer kolejek zapisuje zestaw definicji BLOCKADDR w pliku `blockaddr.ini` , nadpisując w ten sposób dowolną ręczną edycję, która mogła zostać wykonana. Podobnie za każdym razem, gdy definicja parametru BLOCKADDR jest dodawana lub usuwana za pomocą komendy **SET CHLAUTH** , plik `blockaddr.ini` jest aktualizowany. Z tego powodu trwałe zmiany w definicjach BLOCKADDR można wprowadzać tylko za pomocą komendy **SET CHLAUTH** podczas działania menedżera kolejek.

Procedura

1. Otwórz plik `blockaddr.ini` w edytorze tekstu.

   Plik znajduje się w katalogu danych menedżera kolejek.

2. Dodaj adresy IP jako proste pary słowo klucz-wartość, gdzie słowo kluczowe to `Addr`.

   Informacje na temat filtrowania adresów IP za pomocą wzorców 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 429

Używając rekordu uwierzytelniania kanału, można zapobiec zaakceptowaniu przez określony kanał połączenia przychodzącego z adresu IP lub zezwolić całemu menedżerowi kolejek na dostęp z adresu IP.

Odsyłacze pokrewne

USTAW CHLAURA

Blokowanie konkretnych identyfikatorów użytkowników

Można uniemożliwić konkretnym użytkownikom korzystanie z kanału, określając identyfikatory użytkowników, które po potwierdzeniu spowodują 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)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.

Lista użytkowników podana w pliku TYPE(BLOCKUSER) ma zastosowanie tylko do kanałów SVRCONN, a nie do kanałów menedżera kolejek.

userID1 i *userID2* to identyfikatory użytkowników, którym należy uniemożliwić korzystanie z kanału. Można również podać wartość specjalną *MQADMIN , aby odnosić się do uprzywilejowanych użytkowników administracyjnych. Więcej informacji na temat użytkowników uprzywilejowanych zawiera sekcja “Użytkownicy uprzywilejowani” na stronie 365. Więcej informacji na temat komendy *MQADMINzawiera sekcja SET CHLAUTH.

Odsyłacze pokrewne

USTAW CHLAURA

Odwzorowanie zdalnego menedżera kolejek na ID użytkownika MCAUSER

Za pomocą rekordu uwierzytelniania kanału można ustawić atrybut MCAUSER kanału zgodnie z menedżerem kolejek, z którego kanał się łączy.

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 reguła ma zastosowanie.

Należy zauważyć, że ta technika nie ma zastosowania do kanałów połączenia z serwerem. Jeśli w poniższych komendach zostanie podana nazwa kanału połączenia z serwerem, nie będzie ona działać.

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)
  ```

  ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.

  ogólna-partner-qmgr-name jest nazwą menedżera kolejek lub wzorcem zawierającym 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 dołączyć 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)
```

  ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
  generic-ip-address to pojedynczy adres lub wzorzec z symbolem gwiazdki (*) jako znakiem wieloznacznym lub łącznikiem (-) oznaczającym zakres, który jest zgodny z adresem. Więcej informacji na temat ogólnych adresów IP zawiera sekcja Ogólne adresy IP.

Odsyłacze pokrewne
USTAW CHLAURA

Odwzorowanie identyfikatora użytkownika klienta na identyfikator użytkownika MCAUSER
Za pomocą rekordu uwierzytelniania kanału można zmienić atrybut MCAUSER kanału połączenia z serwerem zgodnie z identyfikatorem użytkownika odebranym od klienta.

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 ma zastosowanie tylko do kanałów połączenia z serwerem. Nie ma to 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)
```

  ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
  nazwa-użytkownika-klienta to identyfikator użytkownika powiązany z połączeniem klienta. Wartość ta może zostać potwierdzona przez aplikację kliencką i zmieniona przez uwierzytelnianie połączenia przy użyciu wczesnego adoptowania lub ustawiona za pomocą wyjścia kanału.
  użytkownik jest identyfikatorem użytkownika, który ma być używany zamiast nazwy użytkownika klienta.

Odsyłacze pokrewne
USTAW CHLAURA
Atrybuty sekcji kanałów (ChlauthEarlyAdopt)

Odwzorowanie 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)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
generic-ssl-peer-name to łańcuch zgodny ze standardowymi regułami języka IBM MQ dotyczącymi wartości parametru SSLPEER. Patrz sekcja Reguły dotyczące wartości SSLPEER w systemie IBM MQ.
użytkownik to identyfikator użytkownika, który ma być używany dla wszystkich połączeń korzystających z podanej nazwy wyróżniającej.
ogólna-nazwa-wystawcy odnosi się do nazwy wyróżniającej wystawcy certyfikatu, który ma być zgodny. Ten parametr jest opcjonalny, ale należy go używać, aby uniknąć błędnego dopasowania certyfikatu, jeśli używanych jest wiele ośrodków certyfikacji.

Odsyłacze pokrewne
USTAW CHLAURA

Blokowanie dostępu ze zdalnego menedżera kolejek
Aby zapobiec uruchamianiu kanałów przez zdalny menedżer kolejek, można użyć rekordu uwierzytelniania kanału.

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 w poniższej komendzie zostanie podana nazwa kanału połączenia z serwerem, nie będzie ona działać.

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)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
ogólna-partner-qmgr-name jest nazwą menedżera kolejek lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą menedżera kolejek.

Odsyłacze pokrewne
USTAW CHLAURA

Blokowanie dostępu dla ID użytkownika klienta
Można użyć rekordu uwierzytelniania kanału, aby zapobiec nawiązywaniu połączenia kanału przez identyfikator użytkownika klienta.

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 ma zastosowanie tylko do kanałów połączenia z serwerem. Nie ma to 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)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
nazwa-użytkownika-klienta to identyfikator użytkownika powiązany z połączeniem klienta. Wartość ta może zostać potwierdzona przez aplikację kliencką i zmieniona przez uwierzytelnianie połączenia przy użyciu wczesnego adoptowania lub ustawiona za pomocą wyjścia kanału.

Odsyłacze pokrewne
USTAW CHLAURA

Blokowanie dostępu dla nazwy wyróżniającej SSL lub TLS
Można użyć rekordu uwierzytelniania kanału, aby zapobiec uruchamianiu kanałów przez nazwę wyróżniającą TLS (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(NOACCESS)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
generic-ssl-peer-name to łańcuch zgodny ze standardowymi regułami języka IBM MQ dotyczącymi wartości parametru SSLPEER. Patrz sekcja Reguły dotyczące wartości SSLPEER w systemie IBM MQ.
ogólna-nazwa-wystawcy odnosi się do nazwy wyróżniającej wystawcy certyfikatu, który ma być zgodny. Ten parametr jest opcjonalny, ale należy go używać, aby uniknąć błędnego dopasowania certyfikatu, jeśli używanych jest wiele ośrodków certyfikacji.

Odsyłacze pokrewne
USTAW CHLAURA

Odwzorowanie 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)
```

ogólna-nazwa-kanału jest nazwą kanału, do którego ma być kontrolowany dostęp, lub wzorcem zawierającym symbol gwiazdki (*) jako znak wieloznaczny, który jest zgodny z nazwą kanału.
użytkownik to identyfikator użytkownika, który ma być używany dla wszystkich połączeń korzystających z podanej nazwy wyróżniającej.
generic-ip-address to adres, z którego nawiązywane jest połączenie, lub wzorzec zawierający gwiazdkę (*) jako znak wieloznaczny lub myślnik (-) wskazujący zakres, który jest zgodny z adresem.

Odsyłacze pokrewne
USTAW CHLAURA

Wyłączanie zdalnego dostępu do menedżera kolejek
Jeśli aplikacje klienckie nie mają nawiązywać połączenia z menedżerem kolejek, należy wyłączyć zdalny dostęp do tego menedżera.

O tym zadaniu
Zapobiegaj nawiązywaniu przez aplikacje klienckie połączeń z menedżerem kolejek w jeden z następujących sposobów:

Procedura
- Usuń wszystkie kanały połączenia z serwerem za pomocą komendy MQSC **DELETE CHANNEL**.
- Za pomocą komendy MQSC **ALTER CHANNEL**ustaw identyfikator użytkownika agenta kanału komunikatów (MCAUSER) dla kanału na identyfikator użytkownika bez uprawnień dostępu.

Konfigurowanie zabezpieczeń połączenia
Nadaj uprawnienie do nawiązywania połączenia z menedżerem kolejek dla każdego użytkownika lub grupy użytkowników, którzy mają taką potrzebę biznesową.

O tym zadaniu
Aby skonfigurować ochronę połączenia, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW

  W systemie AIX, 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 nadają uprawnienia do nawiązywania połączeń dla zadań wsadowych, CICS, IMS i inicjatora kanału (CHIN). Jeśli nie jest używany konkretny typ połączenia, należy pominąć odpowiednie komendy.

  Nazwy zmiennych mają następujące znaczenie:

  QMgrName
  Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Pojęcia pokrewne

“Profile zabezpieczeń połączenia dla inicjatora kanału” na stronie 211
Profile sprawdzania połączeń z inicjatora kanału składają się z nazwy menedżera kolejek lub grupy współużytkowania kolejek, po której następuje słowo *CHIN*. Nadaj ID użytkownika używany przez przestrzeń adresową uruchomionego zadania inicjatora kanału prawo do odczytu profilu połączenia.

Kontrolowanie dostępu użytkowników do kolejek

Użytkownik chce kontrolować dostęp aplikacji do kolejek. W tej sekcji opisano działania, które należy wykonać.

Dla każdej prawdziwej instrukcji w pierwszej kolumnie wykonaj 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 437
Kontekst zestawu aplikacji	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do ustawiania kontekstu” na stronie 438

Instrukcja	Działanie
Aplikacja przekazuje kontekst	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do przekazywania kontekstu” na stronie 439
Aplikacja umieszcza komunikaty w kolejce klastrowej	Więcej informacji znajduje się w sekcji “Autoryzowanie umieszczania komunikatów w zdalnych kolejkach klastra” na stronie 527
Aplikacja umieszcza komunikaty w kolejce lokalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 440
Aplikacja umieszcza komunikaty w kolejce modelowej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w kolejce modelowej” na stronie 440
Aplikacja umieszcza komunikaty w kolejce zdalnej	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra” na stronie 441

Nadawanie uprawnień do pobierania komunikatów z kolejek
Nadaj uprawnienie do pobierania komunikatów z kolejki lub zestawu kolejek dla każdej grupy użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia do pobierania komunikatów z niektórych kolejek, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- W systemie z/OSwydaj 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do ustawiania kontekstu
Nadaj uprawnienie do ustawiania kontekstu dla komunikatu, który jest umieszczany, dla każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać uprawnienie do ustawiania kontekstu w niektórych kolejkach, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, 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 użyć uprawnienia `setid` lub `setall` , należy nadać uprawnienia zarówno do odpowiedniego obiektu kolejki, jak i do obiektu menedżera kolejek.
- W przypadku systemu IBM inależy wydać jedną z następujących komend:
  - Aby ustawić tylko kontekst tożsamości:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('
    QMgrName ')
    ```

  - Aby ustawić cały kontekst:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME('
    QMgrName ')
    ```

- W systemie z/OSwykonaj 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do przekazywania kontekstu
Nadaj uprawnienie do przekazywania kontekstu z pobranego komunikatu do umieszczanego komunikatu dla każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać uprawnienie do przekazywania kontekstu w niektórych kolejkach, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- ALW
  W systemach AIX, 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 systemu IBM inaleźy wydać 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 systemie z/OSnależy wydać 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej
Nadaj uprawnienia do umieszczania komunikatów w kolejce lokalnej lub zestawie kolejek dla każdej grupy użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia do umieszczania komunikatów w niektórych kolejkach lokalnych, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- W systemie z/OSwydaj 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w kolejce modelowej
Nadaj uprawnienia do umieszczania komunikatów w kolejce modelowej lub zestawie kolejek modelowych dla każdej grupy użytkowników, którzy tego potrzebują.

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 komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następujące komendy:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- W systemie IBM iwydaj następujące komendy:

```
GRTMQMAUT OBJ(' ModelQueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- W systemie z/OSwydaj 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 kolejek.

Nazwa kolejki ModelQueue
Nazwa kolejki modelowej, na której oparte są kolejki dynamiczne.

ObjectProfile
Nazwa kolejki dynamicznej lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra
Nadaj uprawnienie do umieszczania komunikatów w zdalnej kolejce klastra lub zestawie kolejek dla każdej grupy użytkowników, którzy tego potrzebują.

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 jest uprawnienie do umieszczania w obiekcie lokalnym: patrz sekcja “Nadawanie uprawnień do umieszczania komunikatów w kolejce lokalnej” na stronie 440. Jeśli używana jest pełna kolejka zdalna, wymagane jest uprawnienie do umieszczania w kolejce zdalnej. Należy nadać to uprawnienie za pomocą komend odpowiednich dla danego systemu operacyjnego.

Domyślnym zachowaniem jest wykonywanie kontroli dostępu do serwera SYSTEM.CLUSTER.TRANSMIT.QUEUE. Należy zauważyć, że to zachowanie ma zastosowanie nawet wtedy, gdy używanych jest wiele kolejek transmisji.

Specyficzne zachowanie opisane w tym temacie ma zastosowanie tylko wtedy, gdy atrybut **ClusterQueueAccessControl** w pliku qm.ini został skonfigurowany jako *RQMName*(zgodnie z opisem w sekcji Bezpieczeństwo), a menedżer kolejek został zrestartowany.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

Należy zauważyć, że obiektu *rqmname* można używać tylko dla zdalnych kolejek klastra.

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
```

```
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

Należy zauważyć, że obiektu RMTMQMNAME można używać tylko dla zdalnych kolejek klastra.

- W systemie z/OSwydaj następujące komendy:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Należy zauważyć, że nazwy zdalnego menedżera kolejek (lub grupy współużytkowania kolejek) można używać tylko dla zdalnych kolejek klastra.

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejek.

ObjectProfile
Nazwa zdalnego menedżera kolejek lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Kontrolowanie dostępu użytkowników do tematów

Należy kontrolować dostęp aplikacji do tematów. W tej sekcji opisano działania, które należy wykonać.

Dla każdej prawdziwej instrukcji w pierwszej kolumnie wykonaj działanie wskazane w drugiej kolumnie.

Tabela 74. 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 442
Aplikacja subskrybuje temat	Więcej informacji znajduje się w sekcji “Nadawanie uprawnień do subskrybowania tematów” na stronie 443

Nadawanie uprawnień do publikowania komunikatów w temacie
Nadaj uprawnienie do publikowania komunikatów w temacie lub zestawie tematów dla każdej grupy użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia do publikowania komunikatów w niektórych tematach, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('
QMgrName ')
```

- W systemie z/OSwydaj 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do subskrybowania tematów
Nadaj uprawnienie do subskrybowania tematu lub zestawu tematów dla każdej grupy użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia do subskrybowania niektórych tematów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('
QMgrName ')
```

- W systemie z/OSwydaj 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień do uzyskiwania informacji o menedżerze kolejek

Nadaj uprawnienie do tworzenia zapytań o menedżer kolejek dla każdej grupy użytkowników z potrzebą biznesową.

O tym zadaniu

Aby nadać uprawnienie do uzyskiwania informacji o menedżerze kolejek, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName
')
```

- W systemie z/OSwydaj następujące komendy:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

  Te komendy umożliwiają dostęp do określonego menedżera kolejek. Aby zezwolić użytkownikowi na użycie komendy MQINQ, należy wydać 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 kolejek.

  ObjectProfile
  Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

  GroupName
  Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień dostępu do procesów

Nadaj uprawnienia dostępu do procesu lub zestawu procesów każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia dostępu do niektórych procesów, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName
')
```

- W systemie z/OSwydaj 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

Nadawanie uprawnień dostępu do list nazw

Nadaj uprawnienie dostępu do listy nazw lub zestawu list nazw każdej grupie użytkowników, którzy tego potrzebują.

O tym zadaniu

Aby nadać uprawnienia dostępu do niektórych list nazw, należy użyć komend odpowiednich dla danego systemu operacyjnego.

Na platformach wieloplatformowych można również użyć komendy SET AUTHREC .

Uwaga: MQ Appliance W systemie IBM MQ Appliance można użyć tylko komendy **SET AUTHREC** .

Procedura

- W systemach AIX, Linux, and Windows wydaj następującą komendę:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
+all
```

- W systemie IBM iwprowadź następującą komendę:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- W systemie z/OSwydaj 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 kolejek.

ObjectProfile
Nazwa obiektu lub profilu ogólnego, dla którego mają zostać zmienione autoryzacje.

GroupName
Nazwa grupy, której ma zostać nadany dostęp.

ALW Uprawnienia do administrowania systemem IBM MQ w systemie AIX, Linux, and Windows

Administratorzy IBM MQ mogą używać wszystkich komend IBM MQ i nadawać uprawnienia innym użytkownikom. Gdy administratorzy wydają komendy zdalnym menedżerom kolejek, muszą mieć wymagane uprawnienia do zdalnego menedżera kolejek. Dalsze uwagi dotyczą systemów Windows .

Administratorzy IBM MQ mają uprawnienia do używania wszystkich komend IBM MQ (w tym komend nadających uprawnienia IBM MQ innym użytkownikom).

Aby być administratorem systemu IBM MQ , należy być członkiem specjalnej grupy o nazwie **mqm** .

Windows Alternatywnie, tylko w systemie Windows , konta lokalne mogą administrować systemem IBM MQ , jeśli są członkami grupy Administratorzy w systemach Windows .

Ostrzeżenie: Aby dodać użytkownika Azure AD do grupy mqm, należy użyć komendy administratora. Na przykład użyj komendy `net localgroup mqm AzureAD\<your userID> /add`. Następnie uruchom komendy administracyjne IBM MQ lub użyj komendy IBM MQ Explorer.

Grupa **mqm** jest tworzona automatycznie podczas instalowania produktu IBM MQ . Można dodać kolejnych użytkowników do grupy, aby umożliwić im administrowanie. Wszyscy członkowie tej grupy mają dostęp do wszystkich zasobów. Dostęp ten można odebrać 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 komenda **setmqaut**, która służy do nadawania uprawnień innym użytkownikom, aby umożliwić im dostęp do zasobów IBM MQ lub sterowanie nimi. Komendy PCF służące do zarządzania rekordami uprawnień są dostępne dla użytkowników innych niż administratorzy, którym nadano uprawnienia dsp i chg w menedżerze kolejek. Więcej informacji na temat zarządzania uprawnieniami za pomocą komend PCF zawiera sekcja Formaty komend programowalnych.

Administratorzy muszą mieć uprawnienia wymagane do przetwarzania komend MQSC przez zdalny menedżer kolejek. Program IBM MQ Explorer wydaje komendy PCF w celu wykonania zadań administracyjnych. Administratorzy nie wymagają dodatkowych uprawnień, aby używać programu IBM MQ Explorer do administrowania menedżerem kolejek w systemie lokalnym. Jeśli program IBM MQ Explorer jest używany do administrowania menedżerem kolejek w innym systemie, administratorzy muszą mieć uprawnienia wymagane do przetwarzania komend PCF przez zdalny menedżer kolejek.

Ostrzeżenie: W systemie IBM MQ 8.0nie trzeba być administratorem, aby użyć komendy sterującej **runmqsc**, która wywołuje komendy skryptowe IBM MQ (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.

Więcej informacji na temat sprawdzania uprawnień podczas przetwarzania komend PCF i MQSC zawierają następujące tematy:

- Informacje na temat komend PCF, które działają na menedżerach kolejek, kolejkach, procesach, listach nazw i obiektach informacji uwierzytelniającej, zawiera sekcja Uprawnienia do pracy z obiektami

systemu IBM MQ. W tej sekcji znajdują się równoważne komendy MQSC hermetyzowane w komendach Escape PCF.

- Informacje na temat komend PCF, które działają na kanałach, inicjatorach kanałów, programach nasłuchujących i klastrach, zawiera sekcja 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 przetwarzanych przez serwer komend w systemie IBM MQ for z/OSzawiera sekcja Bezpieczeństwo komend i bezpieczeństwo zasobów komend w systemie z/OS .

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

Na platformach AIX and Linux tworzony jest również specjalny identyfikator użytkownika **mqm** , który może być używany tylko przez produkt. Nie może być ona nigdy dostępna dla użytkowników nieuprzywilejowanych. Wszystkie obiekty IBM MQ należą do ID użytkownika **mqm**.

W systemach Windows członkowie grupy Administratorzy mogą również administrować dowolnym menedżerem kolejek, podobnie jak konto SYSTEM. Można również utworzyć grupę domeny **mqm** w kontrolerze domeny, która zawiera wszystkie identyfikatory użytkowników uprzywilejowanych aktywnych w domenie, i dodać ją do lokalnej grupy **mqm** . Niektóre komendy, na przykład **crtmqm**, służą do manipulowania uprawnieniami do obiektów IBM MQ i wymagają uprawnień do pracy z tymi obiektami (zgodnie z opisem w poniższych sekcjach). Członkowie grupy **mqm** mają uprawnienia do pracy ze wszystkimi obiektami, ale w systemach Windows mogą wystąpić okoliczności, w których uprawnienia są odmówione, jeśli użytkownik jest użytkownikiem lokalnym i użytkownikiem uwierzytelnionym w domenie o takiej samej nazwie. Zostało to opisane w sekcji “Nazwy użytkowników i grupy w systemie AIX, Linux, and Windows” na stronie 451.

Wersje systemu Windows z funkcją Kontrola konta użytkownika (UAC) ograniczają działania, które użytkownicy mogą wykonywać na niektórych systemach operacyjnych, nawet jeśli należą do grupy Administratorzy. Jeśli identyfikator użytkownika należy do grupy Administratorzy, ale nie do grupy **mqm** , należy użyć wiersza komend z podwyższonym poziomem uprawnień, aby wywołać komendy administracyjne IBM MQ , takie jak **crtmqm**. W przeciwnym razie zostanie wygenerowany błąd `AMQ7077: Brak uprawnień do wykonania żądanej operacji .` Aby otworzyć wiersz komend z podwyższonym poziomem uprawnień, kliknij prawym przyciskiem myszy element menu Start lub ikonę wiersza komend i wybierz opcję **Uruchom jako administrator**.

Aby wykonać następujące działania, nie trzeba być członkiem grupy **mqm** :

- Wydaj komendy z programu użytkowego, który wydaje komendy PCF lub komendy MQSC w komendzie Escape PCF, chyba że komendy te manipulują inicjatorami kanałów. (Komendy te zostały opisane w sekcji “Zabezpieczanie definicji inicjatora kanału” na stronie 123).
- Wykonaj wywołania MQI z aplikacji (chyba że w wywołaniu `MQCONNX` mają być używane powiązania krótkiej ścieżki).
- Komenda `crtmqcvx` służy do tworzenia fragmentu kodu, który wykonuje konwersję danych na strukturach typów danych.
- Użyj komendy `dspmq` , aby wyświetlić menedżery kolejek.
- Użyj komendy `dspmqtrc` , aby wyświetlić sformatowane dane wyjściowe śledzenia IBM MQ .

Ograniczenie do 12 znaków dotyczy zarówno identyfikatorów grup, jak i użytkowników.

Platformy UNIX and Linux zwykle ograniczają długość identyfikatora użytkownika do 12 znaków. System AIX 5.3 zwiększył ten limit, ale system IBM MQ nadal przestrzega ograniczenia dotyczącego 12 znaków na wszystkich platformach UNIX and Linux . Jeśli ID użytkownika ma więcej niż 12 znaków, IBM MQ zastępuje go wartością `UNKNOWN`. Nie należy definiować identyfikatora użytkownika o wartości `UNKNOWN`.

ALW Zarządzanie grupą mqm w systemie AIX, Linux, and Windows

Użytkownicy należący do grupy mqm mają pełne uprawnienia administracyjne względem produktu IBM MQ. Z tego powodu nie należy rejestrować aplikacji i zwykłych użytkowników w grupie mqm. Grupa mqm powinna zawierać tylko konta administratorów IBM MQ .

Zadania te zostały opisane w następujących sekcjach:

- Windows Tworzenie grup i zarządzanie nimi w systemie Windows
- AIX Tworzenie grup i zarządzanie nimi w systemie AIX
- Linux Tworzenie grup i zarządzanie nimi w systemie Linux

Windows Jeśli kontroler domeny działa w systemie Windows 2000 lub Windows 2003 albo w nowszej wersji, może być konieczne skonfigurowanie przez administratora domeny specjalnego konta dla systemu IBM MQ . Więcej informacji na ten temat zawiera sekcja Konfigurowanie IBM MQ z produktem Prepare IBM MQ Wizard oraz sekcja Tworzenie i konfigurowanie kont domeny Windows dla produktu IBM MQ.

ALW Uprawnienia do pracy z obiektami IBM MQ w systemie AIX, Linux, and Windows

Wszystkie obiekty są chronione przez IBM MQ, a użytkownicy muszą mieć odpowiednie uprawnienia, aby uzyskać do nich dostęp. Różne nazwy użytkowników wymagają różnych praw dostępu do różnych obiektów.

Dostęp do menedżerów kolejek, kolejek, definicji procesów, list nazw, kanałów, kanałów połączenia klienckiego, obiektów nasłuchiwania, usług i informacji uwierzytelniających można uzyskać z poziomu aplikacji, które używają wywołań MQI lub komend PCF. Wszystkie te zasoby są chronione przez produkt IBM MQ, a aplikacje muszą mieć nadane uprawnienia dostępu do nich. Jednostką wysyłającą żądanie może być użytkownik, aplikacja wywołująca wywołanie MQI lub program administracyjny wydający komendę PCF. Identyfikator requestera jest określany jako *jednostka główna*.

Różnym grupom użytkowników można nadać różne typy uprawnień dostępu do tego samego obiektu. Na przykład dla konkretnej kolejki jedna grupa może mieć uprawnienia do wykonywania operacji umieszczania i pobierania, a inna grupa może mieć uprawnienia tylko do przeglądania kolejki (komenda MQGET z opcją przeglądania). Podobnie niektóre grupy mogą mieć uprawnienia do umieszczania i pobierania w kolejce, ale nie mogą zmieniać ani usuwać atrybutów kolejki.

Niektóre operacje są szczególnie wrażliwe i powinny być ograniczone do użytkowników uprzywilejowanych. Na przykład:

- Uzyskiwanie dostępu do niektórych kolejek specjalnych, takich jak kolejki transmisji lub kolejka komend SYSTEM.ADMIN.COMMAND.QUEUE
- Uruchomione programy, 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 administratorów w systemach Windows).

Pojęcia pokrewne

“Uprawnienia do administrowania systemem IBM MQ w systemie AIX, Linux, and Windows” na stronie 446

Administratorzy IBM MQ mogą używać wszystkich komend IBM MQ i nadawać uprawnienia innym użytkownikom. Gdy administratorzy wydają komendy zdalnym menedżerom kolejek, muszą mieć wymagane uprawnienia do zdalnego menedżera kolejek. Dalsze uwagi dotyczą systemów Windows .

ALW Podczas sprawdzania zabezpieczeń w systemie AIX, Linux, and Windows

Sprawdzenia zabezpieczeń są zwykle wykonywane podczas nawiązywania połączenia z menedżerem kolejek, otwierania lub zamykania obiektów oraz umieszczania lub pobierania komunikatów.

Kontrole bezpieczeństwa wykonywane dla typowej aplikacji są następujące:

Nawiązywanie połączenia z menedżerem kolejek (wywołania MQCONN lub MQCONNX)
Jest to pierwszy raz, gdy aplikacja jest powiązana z konkretnym menedżerem kolejek. Menedżer kolejek odpytuje środowisko operacyjne w celu wykrycia identyfikatora użytkownika powiązanego z aplikacją. Następnie program IBM MQ sprawdza, czy ID użytkownika jest autoryzowany do nawiązania połączenia z menedżerem kolejek i zachowuje ID użytkownika na potrzeby przyszłych sprawdzeń.

Użytkownicy nie muszą logować się do IBM MQ; IBM MQ zakłada, że użytkownicy wpisali się do bazowego systemu operacyjnego i zostali przez to uwierzytelnieni.

Otwieranie obiektu (wywołania MQOPEN lub MQPUT1)
Dostęp do obiektów IBM MQ można uzyskać, otwierając obiekt i wydając dla niego komendy. Wszystkie operacje sprawdzania zasobów są wykonywane po otwarciu obiektu, a nie po uzyskaniu do niego dostępu. Oznacza to, że żądanie **MQOPEN** musi określać typ wymaganego dostępu (na przykład, czy użytkownik chce tylko przeglądać obiekt lub wykonywać aktualizację, taką jak umieszczanie komunikatów w kolejce).

Program IBM MQ sprawdza zasób, który jest wymieniony w żądaniu **MQOPEN** . W przypadku aliasu lub obiektu kolejki zdalnej używana jest autoryzacja samego obiektu, a nie kolejki, na którą rozstrzygany jest alias lub kolejka zdalna. Oznacza to, że użytkownik nie potrzebuje uprawnień, aby uzyskać do niego dostęp. Ogranicz uprawnienia do tworzenia kolejek do użytkowników uprzywilejowanych. W przeciwnym razie użytkownicy mogą pominąć zwykłą kontrolę dostępu, tworząc alias. Jeśli kolejka zdalna jest przywoływana jawnie z nazwami kolejki i menedżera kolejek, sprawdzana jest kolejka transmisji powiązana ze zdalnym menedżerem kolejek.

Uprawnienia do kolejki dynamicznej są oparte na uprawnieniach kolejki modelowej, z której pochodzi, ale nie muszą być takie same. Zostało to opisane w uwadze “1” na stronie 142.

ID użytkownika używany przez menedżer kolejek do sprawdzania dostępu to ID użytkownika uzyskany ze środowiska operacyjnego aplikacji połączonej z menedżerem kolejek. Odpowiednio autoryzowana aplikacja może wywołać funkcję **MQOPEN** , określając alternatywny identyfikator użytkownika. Następnie wykonywane są sprawdzenia kontroli dostępu dla alternatywnego identyfikatora użytkownika. Nie zmienia to identyfikatora użytkownika powiązanego z aplikacją, tylko tego, który był używany 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, chyba że **MQCLOSE** spowoduje usunięcie kolejki dynamicznej. W takim przypadku należy sprawdzić, czy ID użytkownika ma uprawnienia do usuwania kolejki.

Subskrybowanie tematu (MQSUB)
Gdy aplikacja subskrybuje temat, określa typ operacji, która ma zostać wykonana. Jest to utworzenie nowej subskrypcji, zmiana istniejącej subskrypcji lub wznowienie istniejącej subskrypcji bez jej zmiany. Dla każdego typu operacji menedżer kolejek sprawdza, czy ID użytkownika powiązany z aplikacją ma uprawnienia do wykonania tej operacji.

Gdy aplikacja subskrybuje temat, operacje sprawdzania uprawnień są wykonywane względem obiektów tematu, które znajdują się w drzewie tematów w miejscu lub powyżej punktu w drzewie tematów, w którym aplikacja zasubskrybowała. Sprawdzanie uprawnień może obejmować sprawdzanie więcej niż jednego obiektu tematu.

Identyfikator użytkownika używany przez menedżer kolejek na potrzeby sprawdzania uprawnień jest identyfikatorem użytkownika uzyskanym z systemu operacyjnego, gdy aplikacja nawiązuje połączenie z menedżerem kolejek.

Menedżer kolejek sprawdza uprawnienia w kolejkach subskrybentów, ale nie w kolejkach zarządzanych.

ALW Sposób implementowania kontroli dostępu przez produkt IBM MQ w systemie AIX, Linux, and Windows

Program IBM MQ korzysta z usług bezpieczeństwa udostępnianych przez bazowy system operacyjny przy użyciu menedżera uprawnień do obiektów. Program IBM MQ udostępnia komendy służące do tworzenia i obsługi list kontroli dostępu.

Interfejs kontroli dostępu nazywany interfejsem usługi autoryzacji jest częścią produktu IBM MQ. IBM MQ dostarcza implementację menedżera kontroli dostępu (zgodnego z interfejsem usługi autoryzacji), znanego jako *menedżer uprawnień do obiektów (object authority manager-OAM)*. Jest ona automatycznie instalowana i włączana dla każdego utworzonego menedżera kolejek, chyba że określono inaczej (zgodnie z opisem w sekcji “Zapobieganie sprawdzaniu dostępu do zabezpieczeń w systemach AIX, Linux, and Windows” na stronie 407). OAM można zastąpić dowolnym komponentem napisanym przez użytkownika lub dostawcę, który jest zgodny z interfejsem usługi autoryzacji.

OAM wykorzystuje opcje zabezpieczające bazowego systemu operacyjnego, używając 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 AIX, Linux, and Windows” na stronie 397 opisuje sposób nadawania i odbierania tego uprawnienia.

OAM utrzymuje listę kontroli dostępu (ACL) dla każdego zasobu, który kontroluje. Dane autoryzacji są przechowywane w kolejce lokalnej o nazwie SYSTEM.AUTH.DATA.QUEUE. Dostęp do tej kolejki jest ograniczony do użytkowników w grupie mqm, a dodatkowo w systemie Windowsdo użytkowników w grupie Administratorzy oraz do użytkowników zalogowanych przy użyciu identyfikatora SYSTEM. Nie można zmienić dostępu użytkownika do kolejki.

Program 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 AIX, Linux, and Windows” na stronie 397.

IBM MQ przekazuje OAM żądanie zawierające nazwę użytkownika, nazwę zasobu i typ dostępu. Moduł OAM nadaje lub odrzuca dostęp na podstawie listy ACL, którą obsługuje. IBM MQ następuje po decyzji OAM; jeśli OAM nie może podjąć decyzji, IBM MQ nie zezwala na dostęp.

ALW Identyfikowanie identyfikatora użytkownika w systemie AIX, Linux, and Windows

Menedżer uprawnień do obiektu identyfikuje nazwę użytkownika, który żąda dostępu do zasobu. Identyfikator użytkownika używany jako nazwa użytkownika różni się w zależności od kontekstu.

Menedżer uprawnień do obiektów (object authority manager-OAM) musi być w stanie zidentyfikować, kto żąda dostępu do określonego zasobu. W produkcie IBM MQ do odwoływania się do tego identyfikatora używany jest termin *nazwa użytkownika* . Element główny jest ustanawiany podczas pierwszego połączenia aplikacji z menedżerem kolejek. Jest on określany przez menedżer kolejek na podstawie identyfikatora użytkownika powiązanego z aplikacją nawiązującą połączenie. (Jeśli aplikacja wysyła wywołania XA bez nawiązywania połączenia z menedżerem kolejek, do sprawdzania uprawnień przez menedżer kolejek używany jest identyfikator użytkownika powiązany z aplikacją wywołującą wywołanie xa_open).

W systemach AIX and Linux procedury autoryzacji sprawdzają rzeczywisty (zalogowany) identyfikator użytkownika lub efektywny identyfikator użytkownika powiązany z aplikacją. Sprawdzany ID użytkownika może być zależny od typu powiązania. Szczegółowe informacje na ten temat zawiera sekcja Usługi instalowalne.

Produkt IBM MQ propaguje identyfikator użytkownika odebrany z systemu w nagłówku komunikatu (struktura MQMD) każdego komunikatu jako identyfikator użytkownika. Ten identyfikator jest częścią informacji o kontekście komunikatu i jest opisany w sekcji “Uprawnienie kontekstowe w systemie AIX, Linux, and Windows” na stronie 454. Aplikacje nie mogą zmieniać tych informacji, jeśli nie zostały autoryzowane do zmiany informacji o kontekście.

ALW *Nazwy użytkowników i grupy w systemie AIX, Linux, and Windows*

Użytkownicy mogą należeć do grup. Nadając dostęp do zasobów grupom, a nie poszczególnym osobom, można zmniejszyć liczbę wymaganych czynności administracyjnych. Listy kontroli dostępu (ACL) są oparte zarówno na grupach, jak i na identyfikatorach użytkowników.

Na przykład można zdefiniować grupę składającą się z użytkowników, którzy chcą uruchomić określoną aplikację. Inni użytkownicy mogą uzyskać dostęp do wszystkich zasobów, których potrzebują, dodając swój identyfikator użytkownika do odpowiedniej grupy.

Ten proces definiowania grup i zarządzania nimi jest opisany dla poszczególnych platform:

- AIX Tworzenie grup i zarządzanie nimi w systemie AIX
- Linux Tworzenie grup i zarządzanie nimi w systemie Linux
- Windows Tworzenie grup i zarządzanie nimi w systemie Windows

Jednostka główna może należeć do więcej niż jednej grupy (jej zestawu grup). Posiada on sumę wszystkich uprawnień przyznanych każdej grupie w jej zestawie grup. Te uprawnienia są buforowane, dlatego wszelkie zmiany wprowadzone w przypisaniu nazwy użytkownika do grupy nie są rozpoznawane do czasu zrestartowania menedżera kolejek, chyba że zostanie wywołana komenda MQSC **REFRESH SECURITY** (lub jej odpowiednik PCF).

Linux AIX Systemy AIX and Linux

W systemie IBM MQ 8.0listy kontroli dostępu (ACL) są oparte zarówno na identyfikatorach użytkowników, jak i na grupach i można ich użyć do autoryzacji, ustawiając atrybut **SecurityPolicy** na odpowiednią wartość zgodnie z opisem w sekcji Service pliku qm.ini oraz w sekcji Configuring authorization service on AIX and Linux.

W produkcie IBM MQ 8.0do autoryzacji można użyć *modelu opartego na użytkownikach* , co pozwala na użycie zarówno użytkowników, jak i grup. Jeśli jednak użytkownik zostanie określony w komendzie setmqaut , nowe uprawnienia będą miały zastosowanie tylko do tego użytkownika, a nie do grup, do których ten użytkownik należy. Więcej informacji na ten temat zawiera sekcja “Uprawnienia OAM oparte na użytkownikach w systemie AIX and Linux” na stronie 397.

Jeśli do autoryzacji używany jest *model oparty na grupach* , grupa podstawowa, do której należy ID użytkownika, jest dołączana do listy ACL. Identyfikator użytkownika nie jest uwzględniany, a uprawnienia są nadawane wszystkim członkom tej grupy. Z tego powodu należy pamiętać, że można przypadkowo zmienić uprawnienia jednostki głównej, zmieniając uprawnienia innej jednostki głównej w tej samej grupie.

Wszyscy użytkownicy są nominalnie przypisani do domyślnej grupy użytkowników nobody (nikt) i domyślnie tej grupie nie są nadawane żadne autoryzacje. Można zmienić autoryzację w grupie nobody (nikt), aby nadać dostęp do zasobów IBM MQ użytkownikom bez konkretnych autoryzacji.

V 9.3.0 W produkcie IBM MQ 9.3.0można użyć opcji `UserExternal` atrybutu **SecurityPolicy** , aby utworzyć nazwę użytkownika w systemie innym niż system operacyjny. Jeśli zostanie utworzona nazwa użytkownika systemu innego niż system operacyjny, użytkownik ten będzie traktowany jako nie należący do żadnych grup, z wyjątkiem grupy nobody . Więcej informacji na temat tej opcji zawierają sekcje crtmqm i Usługa w pliku qm.ini.

Nie należy definiować identyfikatora użytkownika o wartości `UNKNOWN`. Wartość `UNKNOWN` jest używana, gdy identyfikator użytkownika jest zbyt długi, więc dowolne identyfikatory użytkowników będą używać uprawnień dostępu `UNKNOWN`.

Więcej informacji na temat korzystania z protokołu LDAP zawiera sekcja “Ustawianie autoryzacji” na stronie 460 .

ID użytkowników mogą zawierać do 12 znaków, a nazwy grup do 12 znaków.

Windows Systemy Windows

Listy ACL są oparte zarówno na identyfikatorach użytkowników, jak i na grupach. Sprawdzenia są takie same, jak w przypadku AIX and Linux. W różnych domenach mogą istnieć różni użytkownicy o tym samym identyfikatorze. Produkt IBM MQ zezwala na kwalifikowanie identyfikatorów użytkowników za pomocą nazwy domeny, dzięki czemu tym użytkownikom można nadawać różne poziomy dostępu.

Nazwa grupy może opcjonalnie zawierać nazwę domeny, określoną 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 ustawienie: `GroupModel=GlobalGroups`. Patrz Zabezpieczanie.
2. Menedżer kolejek używa alternatywnej grupy dostępu zabezpieczeń. Patrz **crtmqm** .

Identyfikatory użytkowników mogą zawierać do 20 znaków, nazwy domen do 15 znaków i nazwy grup do 64 znaków.

OAM najpierw sprawdza lokalną bazę danych zabezpieczeń, następnie bazę danych domeny podstawowej, a na końcu bazę danych wszystkich zaufanych domen. Pierwszy napotkany ID użytkownika jest używany przez OAM do sprawdzania. Każdy z tych identyfikatorów użytkowników może mieć inne przypisania do grup na konkretnym komputerze.

Niektóre komendy sterujące (na przykład **crtmqm**) zmieniają uprawnienia do obiektów IBM MQ za pomocą menedżera uprawnień do obiektów (object authority manager-OAM). OAM przeszukuje bazy danych zabezpieczeń w kolejności podanej w poprzednim akapicie, aby określić prawa uprawnień dla konkretnego ID użytkownika. W rezultacie uprawnienia określone przez OAM mogą przesłonić fakt, że ID użytkownika jest członkiem lokalnej grupy mqm. Jeśli na przykład komenda **crtmqm** zostanie wywołana z ID użytkownika uwierzytelnionego przez kontroler domeny, który jest członkiem lokalnej grupy mqm z grupy globalnej, wykonanie komendy nie powiedzie się, jeśli w systemie znajduje się użytkownik lokalny o tej samej nazwie, który nie należy do lokalnej grupy mqm.

Więcej informacji na temat ustawiania atrybutu **SecurityPolicy** w systemie Windowszawierają sekcje Usługi instalowalne i Konfigurowanie usług autoryzacji w systemie Windows.

Windows *Identyfikatory zabezpieczeń (SID) Windows*

IBM MQ w systemie Windows używa identyfikatora SID, tam gdzie jest on dostępny. Jeśli identyfikator Windows SID nie został dostarczony z żądaniem autoryzacji, IBM MQ identyfikuje użytkownika na podstawie samej nazwy użytkownika, ale może to spowodować nadanie niewłaściwego uprawnienia.

W systemach Windows identyfikator bezpieczeństwa (SID) jest używany jako uzupełnienie identyfikatora użytkownika. Identyfikator SID zawiera informacje identyfikujące pełne szczegóły konta użytkownika w bazie danych SAM (Security Account Manager) systemu Windows , w której zdefiniowano użytkownika. Gdy komunikat jest tworzony w systemie IBM MQ for Windows, IBM MQ zapisuje identyfikator SID w deskryptorze komunikatu. Gdy system IBM MQ w systemie Windows wykonuje sprawdzenia autoryzacji, używa identyfikatora SID do wysłania zapytania o pełne informacje z bazy danych SAM. (Baza danych SAM, w której jest zdefiniowany użytkownik, musi być dostępna, aby to zapytanie powiodło się).

Domyślnie, jeśli identyfikator Windows SID nie jest dostarczany z żądaniem autoryzacji, IBM MQ identyfikuje użytkownika na podstawie samej nazwy użytkownika. W tym celu należy przeszukać bazy danych zabezpieczeń w następującej kolejności:

1. Lokalna baza danych zabezpieczeń
2. Baza danych zabezpieczeń domeny podstawowej
3. Baza danych zabezpieczeń zaufanych domen

Jeśli nazwa użytkownika nie jest unikalna, może zostać nadane niepoprawne uprawnienie IBM MQ . Aby zapobiec temu problemowi, należy dołączyć identyfikator SID do każdego żądania 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 identyfikatora **regedit**. Ustaw właściwość SecurityPolicy na wartość NTSIDsRequired.

ALW Alternatywne uprawnienia użytkownika w systemie AIX, Linux, and Windows

Można określić, że ID użytkownika może korzystać z uprawnień innego użytkownika podczas uzyskiwania dostępu do obiektu IBM MQ . Jest to nazywane *alternatywnym uprawnieniem użytkownika*i można go użyć dla dowolnego obiektu IBM MQ .

Alternatywne uprawnienia użytkownika są niezbędne, gdy serwer odbiera żądania z programu i 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 załóżmy, że program serwera działający z ID użytkownika PAYSERV pobiera komunikat żądania z kolejki, która została umieszczona w kolejce przez ID 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 identyfikatora użytkownika (PAYSERV) do autoryzowania otwierania kolejki odpowiedzi, serwer może określić inny identyfikator użytkownika, w tym przypadku USER1. W tym przykładzie można użyć uprawnienia alternatywnego użytkownika do określenia, czy PAYSERV może określić USER1 jako alternatywny identyfikator użytkownika podczas otwierania kolejki odpowiedzi.

Alternatywny identyfikator użytkownika jest określony w polu **AlternateUserId** deskryptora obiektu.

Linux Rozwiązywanie niektórych problemów z przypisaniem do grup w systemie Linux

Niektóre systemy wolno zwracają informacje o grupach za pośrednictwem zwykłych serii wywołań funkcji API systemu operacyjnego **getgrent** , a jeśli w przedsiębiorstwie istnieją tysiące grup do wyszukania, w poszukiwaniu grup, w których znajduje się użytkownik produktu `mqm` , powolna odpowiedź może spowodować przekroczenie limitu czasu wewnętrznego menedżera kolejek. Aby obejść ten problem, istnieje alternatywny interfejs API systemu operacyjnego.

Aby użyć alternatywnego interfejsu API, który jest szybszy i zwraca wszystkie grupy z jednego wywołania, należy ustawić zmienną środowiskową MQS_GETGROUPLIST_API.

Być może wystąpił błąd RC2035 podczas nadawania dostępu do grupy dodatkowej użytkownika i włączania zmiennej MQS_GETGROUPLIST_API rozwiązuje problem.

Następnie program IBM MQ używa interfejsu API języka **getgrouplist** zamiast interfejsu API języka **getgrent** .

Aby włączyć funkcję **getgrouplist**:

1. Zatrzymaj menedżer kolejek
2. Uruchom komendę export MQS_GETGROUPLIST_API=1
3. Zrestartuj menedżer kolejek

Ponów scenariusz, który się nie powiódł i jeśli problem został rozwiązany, można rozważyć zmodyfikowanie pliku `.bashrc / .profile` dla użytkownika `mqm` w celu dodania tej zmiennej środowiskowej lub dodanie zmiennej środowiskowej do skryptu używanego do uruchamiania menedżera kolejek.

Jeśli system scala informacje o użytkownikach lub grupach dla systemu operacyjnego z wielu repozytoriów, takich jak NIS lub LDAP, upewnij się, że identyfikator grupy lub użytkownika jest spójny we wszystkich repozytoriach, w tym w repozytorium lokalnym, ponieważ są one używane do instalowania i ustawiania uprawnień na poziomie systemu operacyjnego.

ALW Uprawnienie kontekstowe w systemie AIX, 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 Sterowanie informacjami o kontekście zawiera informacje o opcjach kontekstu, a sekcja MQMD-deskryptor komunikatu zawiera opisy pól deskryptora komunikatu związanych z kontekstem.

Implementowanie kontroli dostępu w wyjściach zabezpieczeń

Kontrolę dostępu można zaimplementować w wyjściu zabezpieczeń za pomocą MCAUserIdentifier lub menedżera uprawnień do obiektów.

MCAUserIdentifier

Każda instancja kanału, która jest bieżąca, ma powiązaną strukturę definicji kanału MQCD. Początkowe wartości pól w MQCD są określane przez definicję kanału utworzoną przez administratora produktu IBM MQ . W szczególności początkowa wartość jednego z pól, *MCAUserIdentifier*, jest określana przez wartość parametru MCAUSER w komendzie DEFINE CHANNEL lub przez odpowiednik MCAUSER, jeśli definicja kanału została utworzona w inny sposób.

Struktura MQCD jest przekazywana do programu obsługi wyjścia kanału, gdy jest wywoływana przez agent MCA. Gdy wyjście zabezpieczeń jest wywoływane przez agent MCA, wyjście zabezpieczeń może zmienić wartość parametru *MCAUserIdentifier*, zastępując dowolną wartość określoną w definicji kanału.

Multi W systemie Wiele platform, jeśli wartość parametru *MCAUserIdentifier* nie jest pusta, menedżer kolejek używa wartości *MCAUserIdentifier* jako identyfikatora użytkownika na potrzeby sprawdzania uprawnień, gdy agent MCA próbuje uzyskać dostęp do zasobów menedżera kolejek po nawiązaniu połączenia z menedżerem kolejek. Jeśli wartość parametru *MCAUserIdentifier* jest pusta, menedżer kolejek używa domyślnego identyfikatora użytkownika agenta MCA. Dotyczy to kanałów RCVR, RQSTR, CLUSRCVR i SVRCONN. Przy wysyłaniu agentów MCA do sprawdzania uprawnień zawsze jest używany domyślny identyfikator użytkownika, nawet jeśli wartość *MCAUserIdentifier* nie jest pusta.

z/OS W systemie z/OSmenedżer kolejek może używać wartości *MCAUserIdentifier* do sprawdzania uprawnień, pod warunkiem, że nie jest ona pusta. To, czy menedżer kolejek używa do sprawdzania uprawnień wartości *MCAUserIdentifier* , aby odbierać adaptery MCA i połączenia z serwerem, zależy od tego, czy:

- Wartość parametru PUTAUT w definicji kanału
- Profil RACF używany do sprawdzania

- Poziom dostępu ID użytkownika przestrzeni adresowej inicjatora kanału do profilu RESLEVEL

W przypadku wysyłania MCA zależy to od:

- Określa, czy wysyłający agent MCA jest programem wywołującym, czy odpowiadającym
- Poziom dostępu ID użytkownika przestrzeni adresowej inicjatora kanału do profilu RESLEVEL

Identyfikator użytkownika, który jest przechowywany przez program zewnętrzny zabezpieczeń w konsoli *MCAUserIdentifier* , można uzyskać na różne sposoby. Poniżej przedstawiono kilka przykładów:

- Jeśli na końcu kanału MQI po stronie klienta nie ma wyjścia zabezpieczeń, identyfikator użytkownika powiązany z aplikacją kliencką IBM MQ przepływa od agenta MCA połączenia klienckiego do agenta MCA połączenia serwera, gdy aplikacja kliencka wysyła wywołanie MQCONN.Agent MCA połączenia serwera zapisuje ten identyfikator użytkownika w polu *RemoteUserIdentyfikator* w strukturze definicji kanału (MQCD). Jeśli wartość *MCAUserIdentifier* jest obecnie pusta, agent MCA zapisuje ten sam identyfikator użytkownika w pliku *MCAUserIdentifier*. Jeśli agent MCA nie przechowuje identyfikatora użytkownika w programie *MCAUserIdentifier*, wyjście zabezpieczeń może to zrobić później, ustawiając parametr *MCAUserIdentifier* na wartość *RemoteUserIdentifier*.

  Jeśli ID użytkownika, który przepływa z systemu klienta, wprowadza nową domenę zabezpieczeń i nie jest poprawny w systemie serwera, wyjście zabezpieczeń może zastąpić ID użytkownika, który jest poprawny, i zapisać podstawiony ID użytkownika w *MCAUserIdentifier*.
- Identyfikator użytkownika może zostać wysłany przez wyjście zabezpieczeń partnera w komunikacie bezpieczeństwa.

  W przypadku kanału komunikatów wyjście zabezpieczeń wywoływane przez wysyłający agent MCA może wysłać identyfikator użytkownika, w ramach którego działa wysyłający agent MCA. Wyjście zabezpieczeń wywoływane przez odbierający agent MCA może następnie zapisać identyfikator użytkownika w programie *MCAUserIdentifier*. Podobnie w przypadku kanału MQI wyjście zabezpieczeń po stronie klienta kanału może wysłać identyfikator użytkownika powiązany z aplikacją IBM MQ MQI client . Wyjście zabezpieczeń po stronie serwera kanału może następnie zapisać identyfikator użytkownika w *MCAUserIdentifier*. Podobnie jak w poprzednim przykładzie, jeśli ID użytkownika nie jest poprawny w systemie docelowym, wyjście zabezpieczeń może zastąpić ID użytkownika, który jest poprawny, i zapisać go w *MCAUserIdentifier*.

  Jeśli certyfikat cyfrowy zostanie odebrany 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 zapisać identyfikator użytkownika w *MCAUserIdentifier*.
- Jeśli w kanale jest używany protokół TLS, nazwa wyróżniająca partnera jest przekazywana do wyjścia w polu SSLPeerNamePtr 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, struktury MQCD i struktury parametru wyjścia kanału, MQCXP, zawiera sekcja Wywołania wyjścia kanału i struktury danych. Więcej informacji na temat identyfikatora użytkownika, który przepływa z systemu klienta przez kanał 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 IBM MQ

W przypadku połączeń IBM MQ MQI client wyjścia zabezpieczeń mogą być używane do modyfikowania lub tworzenia struktury MQCSP używanej w uwierzytelnianiu użytkownika menedżera OAM (object authority manager). Zostało 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 ID użytkownika innym ID.

Rozważmy aplikację kliencką, która wysyła komunikat do aplikacji serwera. Aplikacja serwera może wyodrębnić identyfikator użytkownika z pola *UserIdentifier* w deskryptorze komunikatu i, jeśli ma on alternatywne uprawnienie użytkownika, może poprosić menedżera kolejek o użycie tego identyfikatora użytkownika do sprawdzania uprawnień podczas uzyskiwania dostępu 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 na potrzeby sprawdzania uprawnień, gdy agent MCA otwiera kolejkę docelową.

W pewnych okolicznościach, gdy generowany jest komunikat raportu, jest on umieszczany przy użyciu uprawnień ID użytkownika w polu *UserIdentifier* komunikatu będącego źródłem raportu. W szczególności raporty dotyczące potwierdzania dostarczenia (COD) i raporty dotyczące wygaśnięcia są zawsze umieszczane w tym organie.

Ze względu na te sytuacje może być konieczne zastąpienie jednego identyfikatora użytkownika innym w polu *UserIdentifier* , gdy komunikat zostanie wprowadzony do nowej domeny zabezpieczeń. Można to zrobić za pomocą wyjścia 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, która wysłała komunikat, program zewnętrzny komunikatu może sprawdzić poprawność certyfikatu i odwzorować nazwę wyróżniającą w certyfikacie na ID użytkownika, który jest poprawny w systemie odbierającym. Następnie może ustawić ten identyfikator użytkownika w polu *UserIdentifier* w deskryptorze komunikatu.

Jeśli konieczne jest, aby wyjście komunikatu zmieniło wartość pola *UserIdentifier* w komunikacie przychodzącym, może być konieczne, aby wyjście komunikatu uwierzytelniało nadawcę komunikatu w tym samym czasie. Szczegółowe informacje na ten temat zawiera sekcja “Odwzorowanie tożsamości w wyjściach komunikatów” na stronie 369.

Implementowanie kontroli dostępu w wyjściu funkcji API i wyjściu funkcji API

Interfejs API lub wyjście przekraczania funkcji API może zapewnić kontrolę dostępu uzupełniającą te, które są udostępniane 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, funkcja API lub wyjście przekraczające API może sprawdzić, czy łączna wartość zamówienia jest mniejsza niż określony limit.
- Komunikaty są przesyłane do kolejki docelowej ze zdalnych menedżerów kolejek. Gdy aplikacja próbuje pobrać komunikat z kolejki, funkcja API lub wyjście przekraczające API może sprawdzić, czy nadawca komunikatu jest uprawniony do wysłania komunikatu do kolejki.

V 9.3.0 Multi Bezpieczeństwo kolejek strumieniowych

Funkcja kolejek strumieniowych umożliwia administratorowi skonfigurowanie kolejki lokalnej (lub modelowej) z kolejką dodatkową, w której umieszczane są zduplikowane komunikaty, za każdym razem, gdy komunikat jest umieszczany w oryginalnej kolejce. Istnieją dwa aspekty, które należy wziąć pod uwagę w odniesieniu do uprawnień do przesyłania strumieniowego kolejki.

Uprawnienie do konfigurowania kolejki na potrzeby przetwarzania strumieniowego zduplikowanych komunikatów

Aby włączyć strumieniowanie zduplikowanych komunikatów z jednej kolejki do kolejki dodatkowej, należy mieć odpowiednie uprawnienia. Uprawnienie do konfigurowania atrybutu **STREAMQ** kolejki wymaga posiadania następujących uprawnień:

1. Uprawnienie CHG do kolejki, dla której zmieniany jest atrybut **STREAMQ**
2. Uprawnienie CHG do kolejki, do której mają być umieszczane komunikaty duplikacji

Kombinacja tych dwóch sprawdzeń uprawnień w czasie konfiguracji zapewnia, że użytkownik, który ma tylko uprawnienie CHG w oryginalnej kolejce, nie może spowodować umieszczenia komunikatów w innej kolejce, do której nie ma uprawnień.

Uprawnienia do otwierania kolejki lub kolejek i umieszczania komunikatów

Gdy aplikacja otwiera kolejkę, która została skonfigurowana z kolejką dodatkową, za pomocą jej atrybutu **STREAMQ** wykonywane jest sprawdzenie, czy użytkownik aplikacji ma uprawnienie PUT do oryginalnej kolejki.

Uwaga: Nie jest wykonywane dodatkowe sprawdzanie uprawnień dla użytkownika aplikacji w kolejce dodatkowej, która jest podobna do modelu uprawnień używanego dla kolejek aliasowych.

Aplikacje korzystające z komunikatów z oryginalnej lub dodatkowej kolejki wymagają uprawnienia GET lub BROWSE tylko w kolejce, z której korzystają.

Podczas operacji put lub get nie są wykonywane żadne dodatkowe operacje sprawdzania uprawnień.

Przykład

W poniższym przykładzie przedstawiono ustawienie poprawnych uprawnień umożliwiających użytkownikowi `admin` skonfigurowanie oryginalnej kolejki INQUIRIES.QUEUEw celu strumieniowania zduplikowanych komunikatów do kolejki lokalnej ANALYTICS.QUEUE, ale uniemożliwiające produktowi `admin` duplikowanie komunikatów do kolejki PURCHASES.QUEUE:

```
SET AUTHREC PROFILE(INQUIRIES.QUEUE) PRINCIPAL('admin') AUTHADD(CHG)
SET AUTHREC PROFILE(ANALYTICS.QUEUE) PRINCIPAL('admin') AUTHADD(CHG)
SET AUTHREC PROFILE(PURCHASES.QUEUE) PRINCIPAL('admin') AUTHRMV(CHG)
```

Użytkownik `admin` może następnie wydać następującą komendę:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(ANALYTICS.QUEUE)
```

ale jeśli ten sam użytkownik wyda następującą komendę:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(PURCHASES.QUEUE)
```

, aby skonfigurować zapytania INQUIRIES.QUEUE , aby umieścić zduplikowane komunikaty w PURCHASES.QUEUE, otrzymują następujący błąd:

```
AMQ8135E Brak uprawnień
```

Z ZAPYTANIAMI INQUIRIES.QUEUE skonfigurowana do duplikowania komunikatów do ANALYTICS.QUEUE, następujące rekordy uprawnień są używane, aby umożliwić aplikacji działającej jako użytkownik `appuser` umieszczanie komunikatów w INQUIRIES.QUEUEi duplikowanie komunikatów do produktu ANALYTICS.QUEUE:

```
SET AUTHREC PROFILE(INQUIRIES.QUEUE) PRINCIPAL('appuser') AUTHADD(PUT)
```

Uwaga: `appuser` nie wymaga rekordu uprawnień do produktu ANALYTICS.QUEUE. Zduplikowane komunikaty są umieszczane w kolejce przez menedżer kolejek.

Pojęcia pokrewne

Kolejki przetwarzania strumieniowego

z/OS V 9.3.0 Bezpieczeństwo kolejek strumieniowych w systemie z/OS

Funkcja kolejek strumieniowych umożliwia administratorowi skonfigurowanie kolejki lokalnej (lub modelowej) z kolejką dodatkową, w której umieszczane są zduplikowane komunikaty, za każdym razem, gdy komunikat jest umieszczany w oryginalnej kolejce. Istnieją dwa aspekty, które należy wziąć pod uwagę w odniesieniu do uprawnień do przesyłania strumieniowego kolejki.

Uprawnienie do konfigurowania kolejki na potrzeby przetwarzania strumieniowego zduplikowanych komunikatów

Aby włączyć strumieniowanie zduplikowanych komunikatów z jednej kolejki do kolejki dodatkowej, należy mieć odpowiednie uprawnienia. Uprawnienie do konfigurowania atrybutu **STREAMQ** kolejki wymaga skonfigurowania następujących profili:

1. Poziom dostępu ALTER na poziomie MQADMIN lub MXADMIN dla kolejki, dla której zmieniany jest atrybut **STREAMQ** dla
2. Poziom dostępu ALTER do MQADMIN lub MXADMIN dla kolejki, do której mają być przesyłane komunikaty

Kombinacja tych sprawdzeń bezpieczeństwa w czasie konfiguracji zapewnia, że użytkownik, który ma tylko dostęp typu ALTER do oryginalnej kolejki, nie może spowodować umieszczenia komunikatów w innej kolejce, do której nie ma uprawnień.

Uprawnienia do otwierania kolejki lub kolejek i umieszczania komunikatów

Gdy aplikacja otwiera kolejkę, która została skonfigurowana z kolejką dodatkową, za pomocą jej atrybutu **STREAMQ** wykonywane jest sprawdzenie uprawnień, czy użytkownik aplikacji ma uprawnienie UPDATE do oryginalnej kolejki.

Uwaga: Nie jest wykonywane dodatkowe sprawdzanie uprawnień dla użytkownika aplikacji w kolejce dodatkowej, która jest podobna do modelu uprawnień używanego dla kolejek aliasowych.

Aplikacje korzystające z komunikatów z oryginalnej lub dodatkowej kolejki wymagają uprawnienia UPDATE lub READ tylko w kolejce, z której korzystają.

Podczas operacji put lub get nie są wykonywane żadne dodatkowe operacje sprawdzania uprawnień.

Przykład

W poniższym przykładzie przedstawiono poprawne profile, które są ustawiane w celu umożliwienia użytkownikowi ADMIN skonfigurowania oryginalnej kolejki, zapytań INQUIRIES.QUEUE, aby przesyłać komunikaty do kolejki lokalnej ANALYTICS.QUEUE przy użyciu RACF:

```
RDEFINE MQCMDS <QMGR>.ALTER.QLOCAL UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.ALTER.QLOCAL CLASS(MQCMDS) ID(ADMIN) ACCESS(ALTER)

RDEFINE MQADMIN <QMGR>.QUEUE.INQUIRIES.QUEUE UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.QUEUE.INQUIRIES.QUEUE CLASS(MQADMIN) ID(ADMIN) ACCESS(ALTER)

RDEFINE MQADMIN <QMGR>.QUEUE.ANALYTICS.QUEUE UACC(NONE) OWNER(<OWNER>)
PERMIT <QMGR>.QUEUE.ANALYTICS.QUEUE CLASS(MQADMIN) ID(ADMIN) ACCESS(ALTER)
```

Użytkownik ADMIN może następnie wydać następującą komendę:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(ANALYTICS.QUEUE)
```

ale jeśli ten sam użytkownik wyda następującą komendę bez konfigurowania poprawnych profili zabezpieczeń:

```
ALTER QLOCAL(INQUIRIES.QUEUE) STREAMQ(PURCHASES.QUEUE)
```

, aby skonfigurować zapytania INQUIRIES.QUEUE , aby umieścić zduplikowane komunikaty w PURCHASES.QUEUE, otrzymują następujący błąd:

```
CSQM166I <QMGR> CSQMAQLC QLOCAL (ZAPYTANIAINQUIRIES.QUEUE) NIE JEST AUTORYZOWANA
```

Pojęcia pokrewne

Kolejki przetwarzania strumieniowego

Multi Autoryzacja LDAP

Można użyć autoryzacji LDAP, aby usunąć potrzebę posiadania identyfikatora użytkownika lokalnego.

Dostępność autoryzacji LDAP na obsługiwanych platformach

Autoryzacja LDAP jest dostępna na wielu platformach:

Ostrzeżenie:

W przypadku ogólnej dostępności produktu IBM MQ 9.0 ta funkcja jest dostępna we wszystkich menedżerach kolejek, niezależnie od tego, czy były to nowe, czy migrowane z wcześniejszej wersji.

Przegląd autoryzacji LDAP

W przypadku autoryzacji LDAP komendy, które obsługują konfigurację autoryzacji, takie jak **setmqaut** i **DISPLAY AUTHREC**, mogą przetwarzać nazwy wyróżniające. Poprzednio użytkownicy byli uwierzytelniani przez porównanie ich referencji z maksymalną liczbą znaków dostępnych 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 poda identyfikator użytkownika, a nie nazwę wyróżniającą, zostanie on przetworzony. Jeśli na przykład w kanale występuje komunikat przychodzący z wartością PUTAUT (CTX), znaki w ID użytkownika są odwzorowywane na nazwę wyróżniającą LDAP i wykonywane są odpowiednie sprawdzenia autoryzacji.

Inne komendy, takie jak **DISPLAY CONN**, kontynuują pracę i wyświetlają rzeczywistą wartość dla ID użytkownika, nawet jeśli ID użytkownika nie istnieje w lokalnym systemie operacyjnym.

Linux AIX Jeśli istnieje autoryzacja LDAP, menedżer kolejek zawsze używa modelu użytkownika zabezpieczeń na platformach AIX and Linux , niezależnie od atrybutu **SecurityPolicy** w pliku `qm.ini` . Dlatego ustawienie uprawnień dla pojedynczego użytkownika ma wpływ tylko na tego użytkownika, a nie na nikogo innego, kto należy do żadnej z grup tego użytkownika.

Podobnie jak w przypadku modelu systemu operacyjnego, użytkownik nadal ma połączone uprawnienia, które zostały przypisane zarówno do osoby, jak i do wszystkich grup (jeśli istnieją), do których użytkownik należy.

Załóżmy na przykład, że w repozytorium LDAP zdefiniowano następujące rekordy.

- 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 korzystający z tego serwera LDAP musi być zdefiniowany w taki sposób, aby jego wartość **CONNAUTH** wskazywała na obiekt **AUTHINFO** typu IDPWLDAP, którego odpowiednie atrybuty tłumaczenia nazw są prawdopodobnie ustawione w następujący sposób:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Przy takiej konfiguracji na potrzeby 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".

Multi

Ustawianie autoryzacji

Sposób użycia nazwy skróconej lub nazwy **USRFIELD** do ustawienia autoryzacji.

Sposób pracy z wieloma formatami, opisany w sekcji “Autoryzacja LDAP” na stronie 459, jest kontynuowany w komendach autoryzacji z kolejnym rozszerzeniem, które może być używane jako plik shortname lub USRFIELD w sposób nieautoryzowany.

Łańcuch znaków określa konkretny atrybut w rekordzie LDAP podczas nadawania nazw użytkownikom (użytkownikom) na potrzeby autoryzacji.

Ważne: Łańcuch znaków nie może zawierać znaku = , ponieważ znak ten nie może być używany w ID użytkownika systemu operacyjnego.

Jeśli nazwa użytkownika zostanie przekazana do modułu OAM w celu autoryzacji, która może być shortname, łańcuch znaków musi mieścić się w 12 znakach. Algorytm odwzorowania najpierw próbuje przetłumaczyć nazwę wyróżniającą przy użyciu atrybutu SHORTUSR w zapytaniu LDAP.

Jeśli wystąpi błąd UNKNOWN_ENTITY lub jeśli podany łańcuch nie może być łańcuchem shortname, podejmowana jest kolejna próba użycia atrybutu USRFIELD do utworzenia zapytania LDAP.

Ostrzeżenie: Jeśli została uruchomiona komenda DEFINE AUTHINFO, należy zrestartować menedżer kolejek. Jeśli menedżer kolejek nie zostanie zrestartowany, komenda setmqaut nie zwróci poprawnego wyniku.

W przypadku przetwarzania autoryzacji użytkowników wszystkie poniższe ustawienia komendy setmqaut są równoważne.

Tabela 75. Ustawienia autoryzacji użytkownika

Komenda	**Uwaga**
`setmqaut -m QM -t qmgr -p jodoe +connect`	Jest to płaska, niekwalifikowana nazwa, tłumaczona przez SHORTUSR.
`setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect`	Również płaska, niekwalifikowana nazwa, tłumaczona przez USRFIELD na tę samą jednostkę.
`setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect`	Użycie nazwanego atrybutu.

Tabela 75. Ustawienia autoryzacji użytkownika (kontynuacja)	
Komenda	**Uwaga**
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	Użycie innego nazwanego atrybutu, który nie musi być żadnym z atrybutów skonfigurowanych w obiekcie AUTHINFO.

Zamiast komendy **setmqaut** można użyć komendy MQSC SET AUTHREC :

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

lub Set Authority Record (MQCMD_SET_AUTH_REC) PCF z elementem MQCACF_PRINCIPAL_ENTITY_NAMES zawierającym łańcuch:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Podczas przetwarzania grup nie ma dwuznaczności w przetwarzaniu `shortname` , ponieważ nie ma potrzeby dopasowania jakiejkolwiek formy nazwy grupy do 12 znaków. Dlatego nie ma odpowiednika atrybutu SHORTUSR dla grup.

Oznacza to, że przykłady składni opisane w sekcji Tabela 76 na stronie 461 są poprawne, przy założeniu, że obiekt AUTHINFO został skonfigurowany z atrybutami rozszerzonymi i ma ustawioną wartość:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabela 76. Ustawienia autoryzacji grupy	
Komenda	**Uwaga**
`setmqaut -m QM -t qmgr -g ApplicationGroupA +connect`	Używanie GRPFIELD do rozstrzygania
`setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect`	Nadawanie nazwy pojedynczemu atrybutowi
`setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect`	Używanie pełnej nazwy wyróżniającej

Zamiast poprzedniej komendy **setmqaut** można użyć komendy MQSC SET AUTHREC :

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

lub komendę PCF Set Authority Record (MQCMD_SET_AUTH_REC) z elementem MQCACF_GROUP_ENTITY_NAMES zawierającym łańcuch:

```
 "ApplicationGroupA"
```

Ważne:

Niezależnie od tego, który format jest używany do odwoływania się do nazwy, niezależnie od tego, czy jest to nazwa użytkownika, czy grupy, musi być możliwe uzyskanie unikalnej nazwy wyróżniającej.

Dlatego na przykład nie mogą istnieć dwa odrębne rekordy, które zawierają "`shortu=jodoe`".

Jeśli nie można określić pojedynczej unikalnej nazwy wyróżniającej, funkcja OAM zwraca MQRC_UNKNOWN_ENTITY.

Multi Wyświetlanie autoryzacji

Różne metody wyświetlania autoryzacji użytkowników lub grup.

Komenda dspmqaut

Najprostszą metodą wyświetlania autoryzacji dostępnych dla użytkownika lub grupy jest użycie komendy dspmqaut .

Do identyfikacji użytkownika lub grupy można użyć zapytania dotyczącego dowolnej odmiany składni. Należy zauważyć, że dane wyjściowe komendy powtarzają tożsamość w formacie podanym w wierszu komend. Dane wyjściowe nie zawierają pełnej przetłumaczonych nazw wyróżniających.

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 i jej odpowiedniki MQSC lub PCF mogą określać nazwę użytkownika lub grupę w dowolnym z obsługiwanych formatów, na przykład w tabelach **setmqaut** opisanych w sekcji “Ustawianie autoryzacji” na stronie 460. Jednak w przeciwieństwie do komendy **dspmqaut**komenda **dmpmqaut** zawsze zgłasza pełną nazwę wyróżniającą (DN).

```
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 dla wybranych rekordów, zawsze wyświetla pełną nazwę wyróżniającą w formacie, który można odtworzyć później.

```
dmpmqcfg -m QM -x authrec
------------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

Multi Inne uwagi dotyczące używania autoryzacji LDAP

Krótki opis zmian w interfejsie MQI (Message Queue Interface) oraz innych komendach MQSC i PCF, o których należy pamiętać podczas korzystania z autoryzacji LDAP z produktu IBM MQ 9.0.0.

ADOPTCTX

Nie jest wymagane, aby aplikacje udostępniły informacje uwierzytelniania lub aby atrybut ADOPTCTX był ustawiony na wartość YES.

Jeśli aplikacja nie uwierzytelnia się jawnie lub jeśli parametr **ADOPTCTX** ma wartość NO dla aktywnego obiektu CONNAUTH, kontekst tożsamości powiązany z aplikacją jest pobierany z identyfikatora użytkownika systemu operacyjnego.

Gdy wymagane jest zastosowanie autoryzacji, ten kontekst jest odwzorowywany na tożsamość LDAP przy użyciu tych samych reguł, co w przypadku komend setmqaut .

Parametry wejściowe wywołań MQI

MQOPEN, MQPUT1i MQSUB mają struktury umożliwiające określenie alternatywnego ID użytkownika.

Jeśli te pola są używane, 12-znakowy identyfikator użytkownika jest odwzorowywany na nazwę wyróżniającą przy użyciu tych samych reguł, co w komendach **setmqaut**, **dmpmqaut**i **dspmqaut** .

Komendy MQPUT i MQPUT1 umożliwiają również odpowiednio autoryzowanym programom ustawianie pola UserIdentifier deskryptora MQMD. Wartość tego pola nie jest określana podczas procesu PUT i można ją ustawić na dowolną wartość.

Zwykle jednak wartość **UserIdentifier** może być używana do autoryzacji na późniejszych etapach przetwarzania komunikatu, na przykład gdy w kanale odbiorczym jest zdefiniowana wartość PUTAUT (CTX).

W tym momencie identyfikator zostanie sprawdzony pod kątem autoryzacji przy użyciu konfiguracji odbierającego menedżera kolejek, który może być oparty na protokole LDAP lub systemie operacyjnym.

Parametry wyjściowe wywołań MQI

Za każdym razem, gdy identyfikator użytkownika jest udostępniany programowi w strukturze MQI, jest to 12-znakowa wersja nazwy skróconej powiązana z połączeniem.

Na przykład wartość **MQAXC.UserId** dla wyjść funkcji API jest nazwą skróconą zwróconą z odwzorowania LDAP.

Inne administracyjne komendy MQSC i PCF

Komendy wyświetlające 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 umożliwiające 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).

Składnia nie ulega zmianie. Jeśli dla tej tożsamości jest wymagana autoryzacja, jest ona wewnętrznie odwzorowywana na nazwę wyróżniającą przy użyciu tych samych reguł, co w przypadku komend **setmqaut**, **dmpmqaut**i **dspmqaut** .

Oznacza to, że wartość 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 komenda DISPLAY CHSTATUS (*) ALL wyświetla wartość SHORTUSR, *MCAUSER (jodoe)* dla wszystkich połączeń.

Multi Przełączanie między modelami autoryzacji systemu operacyjnego i LDAP

Sposób przełączania się między różnymi metodami autoryzacji na różnych platformach.

Atrybut CONNAUTH menedżera kolejek wskazuje na obiekt AUTHINFO. Jeśli obiekt jest typu IDPWLDAP, do uwierzytelniania używane jest repozytorium LDAP.

Teraz można zastosować metodę autoryzacji do tego samego obiektu, co umożliwia kontynuowanie autoryzacji opartej na systemie operacyjnym lub pracę z autoryzacją LDAP.

IBM i, AIX and Linux

Linux IBM i AIX

Menedżer kolejek może być przełączany w dowolnym momencie między modelami systemu operacyjnego i LDAP. Konfigurację tę można zmienić i aktywować 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, należy zrestartować menedżer kolejek, aby zmiana odniosła skutek. W przeciwnym razie można aktywować zmianę za pomocą komendy REFRESH SECURITY TYPE (CONNAUTH) .

Reguły przetwarzania

Podczas przełączania 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, po przełączeniu z LDAP na OS, wszystkie zdefiniowane autoryzacje LDAP stają się nieaktywne i niewidoczne, przywracając oryginalne reguły systemu operacyjnego.

Aby z dowolnej przyczyny utworzyć kopię zapasową definicji menedżera kolejek przy użyciu komendy **dmpmqcfg** , ta kopia zapasowa będzie zawierać tylko te reguły, które są zdefiniowane dla metody autoryzacji w momencie tworzenia kopii zapasowej.

Multi Administrowanie LDAP

Przegląd sposobu, w jaki każda platforma administruje serwerem LDAP.

Jeśli używana jest autoryzacja LDAP, członkostwo w grupie mqm (lub jej odpowiedniku) w systemie operacyjnym nie jest tak ważne. Przynależność do tej grupy decyduje tylko o tym, czy niektóre komendy wiersza komend mogą być przetwarzane.

W szczególności użytkownik musi należeć do tej grupy, aby mógł wydawać komendy strmqm i endmqm .

Po uruchomieniu menedżera kolejek istnieją obecnie limity dla konta z pełnym uprawnieniu. Oprócz identyfikatora użytkownika, który uruchomił komendę **strmqm** , inni użytkownicy należący do grupy systemu operacyjnego mqm (lub jej odpowiedników) nie mają specjalnych uprawnień.

Autoryzacje innych użytkowników są oparte na grupach LDAP, do których należą. Niekwalifikowana nazwa grupy `mqm` w komendach, takich jak **setmqaut** , nie może być odwzorowana na żadną grupę LDAP.

AIX and Linux

Po uruchomieniu menedżera kolejek 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 automatycznie mógł wykonywać zadań administracyjnych sterowanych przez moduł OAM.

Windows

W systemie Windowskonta automatycznie w pełni uprzywilejowane to użytkownik systemu operacyjnego, który uruchomił menedżer kolejek, a także użytkownik uruchamiający podstawowe procesy menedżera kolejek, na przykład MUSR_MQADMIN, jeśli menedżer kolejek został uruchomiony jako usługa systemu Windows .

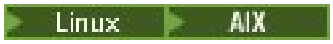
W przypadku uruchamiania w trybie autoryzacji LDAP produkt Windows zachowuje się podobnie do platform AIX and Linux . Zajmuje się 12 znakowymi skróconymi nazwami i pełnymi nazwami wyróżniającymi.

IBM i

W systemie IBM iautomatycznie uprzywilejowane konta to konta, które uruchamiają menedżer kolejek i identyfikator QMQM.

Wymagane są oba identyfikatory, ponieważ identyfikator użytkownika uruchamiającego menedżer kolejek jest wymagany tylko do uruchomienia systemu. Po uruchomieniu procesy menedżera kolejek mają tylko uprawnienie QMQM.

Przykładowy skrypt udostępniający uprawnienia MQADMIN



Ponieważ grupa może wykonywać pełne czynności administracyjne w menedżerze kolejek, przykładowy skrypt jest dostarczany na platformach AIX and Linux w następujący sposób:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

W tym przykładzie używane są dwa parametry:

- Nazwa menedżera kolejek
- Nazwa grupy LDAP

Przykład przetwarza komendy setmqaut , nadając pełne uprawnienia do wszystkich obiektów. Jest to ten sam skrypt, który jest generowany przez kreator IBM MQ Explorer OAM dla ról administracyjnych. Na przykład kod rozpoczyna się od:

```
setmqaut -t q -m qmgr -n "**" +alladm -g
      groupname
```

Poufność komunikatów

Szyfrowanie komunikatów zapewnia, że ich treść pozostaje poufna. W zależności od potrzeb istnieją różne metody szyfrowania komunikatów w produkcie IBM MQ .

Jeśli potrzebna jest kompleksowa ochrona danych na poziomie aplikacji dla infrastruktury przesyłania komunikatów między punktami, można użyć Advanced Message Security do zaszyfrowania komunikatów lub napisać własne wyjście funkcji API lub wyjście funkcji API.

Najbezpieczniejszym rozwiązaniem jest zapewnienie szyfrowania na całej trasie przez szyfrowanie komunikatu od punktu, w którym jest on umieszczany przez aplikację, do punktu, w którym jest otrzymywany przez aplikację konsumującą. Można to zrobić za pomocą serwera “Planowanie Advanced Message Security” na stronie 115 (AMS) lub przez napisanie własnego wyjścia funkcji API lub wyjścia przez funkcję API; więcej informacji na ten temat zawiera sekcja “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 515 .

Jeśli komunikaty mają być szyfrowane tylko wtedy, gdy są przesyłane przez sieć, można użyć protokołu TLS. Więcej informacji na ten temat zawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24 . Można też napisać własne wyjście zabezpieczeń, wyjście komunikatów lub programy obsługi wyjścia wysyłania i odbierania w celu przeprowadzenia szyfrowania.

z/OS Aby zaszyfrować komunikaty w spoczynku w menedżerze kolejek, można użyć szyfrowania zestawu danych produktu z/OS w tym menedżerze kolejek. Więcej informacji na ten temat zawiera sekcja “Poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych” na stronie 517 .

Zadania pokrewne

Łączenie dwóch menedżerów kolejek przy użyciu protokołu TLS

Bezpieczne łączenie klienta z menedżerem kolejek

Włączanie CipherSpecs

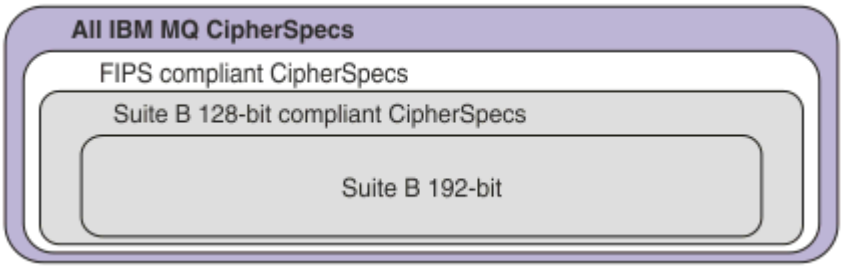
Włącz parametr CipherSpec , używając parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** lub **ALTER CHANNEL** MQSC.

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Niektóre CipherSpecs , których można użyć z produktem IBM MQ , są zgodne ze standardem FIPS. Niektóre CipherSpecs zgodne ze standardem FIPS są również zgodne ze standardem Suite B, ale inne, takie jak TLS_RSA_WITH_AES_256_CBC_SHA, nie są zgodne.

Wszystkie CipherSpecs zgodne ze standardem Suite B są również zgodne ze standardem FIPS. Wszystkie CipherSpecs zgodne ze standardem Suite B dzielą się na dwie grupy: 128 bitów (na przykład ECDHE_ECDSA_AES_128_GCM_SHA256) i 192 bity (na przykład ECDHE_ECDSA_AES_256_GCM_SHA384).

Na poniższym diagramie przedstawiono relacje między tymi podzbiorami:



Począwszy od wersji IBM MQ 9.2.0, produkt obsługuje protokół zabezpieczeń TLS 1.3 na wszystkich platformach.

CipherSpecs , których można użyć dla każdej z tych platform, są wymienione w sekcji Tabela 77 na stronie 467. Informacje na temat używania tych CipherSpecsznajdują się w sekcji "Korzystanie z protokołu TLS 1.3 w systemie IBM MQ" na stronie 471 i "IBM MQ MQI client i TLS 1.3" na stronie 471.

Aby ułatwić konfigurowanie i migrację w przyszłości, produkt IBM MQ udostępnia również zestaw aliasów CipherSpecs. Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia aliasu CipherSpec oznacza, że można dostosować się do dodanych i nieaktualnych algorytmów szyfrowania bez konieczności wprowadzania dalszych inwazyjnych zmian w konfiguracji w przyszłości. Te aliasy CipherSpecs są wymienione w sekcji CipherSpecs aliasu w pliku Tabela 77 na stronie 467. Więcej informacji na temat migrowania w celu użycia aliasu CipherSpeczawiera sekcja Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia aliasu CipherSpec.

Można skonfigurować domyślne CipherSpecs zgodnie z opisem w sekcji "Domyślne wartości parametru CipherSpec włączone w produkcie IBM MQ" na stronie 472. Można również udostępnić alternatywny zestaw CipherSpecs , które są włączone do użycia z kanałami w:

- Multi IBM MQ for Multiplatforms, zgodnie z opisem w sekcji "Udostępnianie niestandardowej listy uporządkowanych i włączonych CipherSpecs w systemie IBM MQ for Multiplatforms" na stronie 480.
- z/OS IBM MQ for z/OS, zgodnie z opisem w sekcji "Udostępnianie niestandardowej listy uporządkowanych i włączonych CipherSpecs w systemie IBM MQ for z/OS" na stronie 481.

Nieaktualne CipherSpecs , które można ponownie włączyć w celu użycia z produktem IBM MQ , jeśli jest to konieczne, są wymienione w sekcji "Nieaktualne CipherSpecs" na stronie 482. Informacje na temat włączania nieaktualnych CipherSpecsmożna znaleźć w sekcji "Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie IBM MQ for Multiplatforms" na stronie 486 lub "Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie z/OS" na stronie 486.

CipherSpecs , których można używać z obsługą protokołu TLS produktu IBM MQ

CipherSpecs , których można używać automatycznie z menedżerem kolejek produktu IBM MQ , są wymienione w poniższej tabeli. Jeśli żądasz certyfikatu osobistego, należy podać wielkość klucza dla pary kluczy publicznego i prywatnego. Wielkość klucza, która jest używana podczas uzgadniania TLS, to wielkość przechowywana w certyfikacie, chyba że jest ona określona przez specyfikację szyfrowania CipherSpec(zgodnie z opisem w tabeli).

Tabela 77. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ

Obsługa platformy "1" na stronie 470	**Nazwa specyfikacji szyfrowania**	**Kod szesnastkowy**	**Używany protokół**	**Algorytm MAC**	**Algorytm szyfrowania (bity szyfrowania)**	**FIPS** "2" na stronie 470	**Suite B**
Specyfikacje szyfrowania aliasów							
Wszystkie	ANY_TLS13_OR_HIGHER "3" na stronie 470 "4" na stronie 470	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY_TLS13 "4" na stronie 470 "5" na stronie 470	N/D	TLS 1.3	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY_TLS12_OR_HIGHER "4" na stronie 470 "6" na stronie 470	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane

Tabela 77. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 470	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Algorytm MAC	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 470	Suite B
Wszystkie	ANY_TLS12 "7" na stronie 470	N/D	TLS 1.2	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Wszystkie	ANY "8" na stronie 470	N/D	Negocjowane	Negocjowane	Negocjowane	Negocjowane	Negocjowane
Specyfikacje szyfrowania dla protokołu TLS 1.3							
Wszystkie	TLS_AES_128_GCM_SHA256	1301	TLS 1.3	GCM	AES-128 z GCM (128)	Tak	Nie
Wszystkie	TLS_AES_256_GCM_SHA384	1302	TLS 1.3	GCM	AES-256 z GCM (256)	Tak	Nie
Wszystkie	TLS_CHACHA20_POLY1305_SHA256	1303	TLS 1.3	POLY1305	CHACHA20 (256)	Nie	Nie
ALW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	AES-128 z funkcją CTR (128)	Tak	Nie
ALW	TLS_AES_128_CCM_8_SHA256 "10" na stronie 470	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 "9" na stronie 470	003C	TLS 1.2	SHA-256	AES (128)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_256_CBC_SHA256 "9" na stronie 470 "11" na stronie 470	003D	TLS 1.2	SHA-256	Algorytm AES (256)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_128_GCM_SHA256 "9" na stronie 470 "12" na stronie 470	009C	TLS 1.2	SHA-256 i AEAD GCM	AES (128)	Tak	Nie
Wszystkie	TLS_RSA_WITH_AES_256_GCM_SHA384 "9" na stronie 470 "11" na stronie 470 "12" na stronie 470	009D	TLS 1.2	SHA-384 i AEAD GCM	Algorytm AES (256)	Tak	Nie
Wszystkie	ECDHE_ECDSA_AES_128_CBC_SHA256 "9" na stronie 470	C023	TLS 1.2	SHA-256	AES (128)	Tak	Nie
Wszystkie	ECDHE_ECDSA_AES_256_CBC_SHA384 "9" na stronie 470 "11" na stronie 470	C024	TLS 1.2	SHA-384	Algorytm AES (256)	Tak	Nie
Wszystkie	ECDHE_RSA_AES_128_CBC_SHA256 "9" na stronie 470	C027	TLS 1.2	SHA-256	AES (128)	Tak	Nie

Tabela 77. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ (kontynuacja)

Obsługa platformy “1” na stronie 470	**Nazwa specyfikacji szyfrowania**	**Kod szesnastkowy**	**Używany protokół**	**Algorytm MAC**	**Algorytm szyfrowania (bity szyfrowania)**	**FIPS** “2” na stronie 470	**Suite B**
Wszystkie	ECDHE_RSA_AES_256_CBC_SHA384 “9” na stronie 470 “11” na stronie 470	C028	TLS 1.2	SHA-384	Algorytm AES (256)	Tak	Nie
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 “11” na stronie 470 “12” na stronie 470	C02B	TLS 1.2	SHA-256 i AEAD GCM	Algorytm AES (SHA384)	Tak	128 bitów
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 “11” na stronie 470 “12” na stronie 470	C02C	TLS 1.2	SHA-384 i AEAD GCM	Algorytm AES (SHA384)	Tak	192 bity
Wszystkie	ECDHE_RSA_AES_128_GCM_SHA256 “12” na stronie 470	C02F	TLS 1.2	SHA-256 i AEAD GCM	AES (128)	Tak	Nie
Wszystkie	ECDHE_RSA_AES_256_GCM_SHA384 “11” na stronie 470 “12” na stronie 470	C030	TLS 1.2	AEAD AES-128 GCM	Algorytm AES (SHA384)	Tak	Nie

Tabela 77. Specyfikacje szyfrowania, których można użyć z obsługą protokołu TLS produktu IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 470	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Algorytm MAC	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 470	Suite B

Uwagi:

1. Listę platform obsługiwanych przez poszczególne ikony znajdują się w sekcji Ikony używane 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. ALW 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. 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.
5. ALW 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.
6. ALW 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.
7. 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.
8. ALW Specyfikacja szyfrowania aliasów ANY negocjuje najwyższy poziom zabezpieczeń, który umożliwia zdalny element końcowy połączenia.
9. IBM i Następujące specyfikacje szyfrowania nie są włączone w systemach IBM i 7.4 i mają wartość systemową QSSLCSLCTL ustawioną na *OPSSYS.
10. ALW Te specyfikacje szyfrowania korzystają z wartości sprawdzania integralności (Integrity Check Value – ICV) złożonej z 8 oktetów, a nie z 16.
11. 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.
12. ALW 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.

    To ograniczenie nie obowiązuje w przypadku programu IBM MQ for z/OS.

Korzystanie z protokołu TLS 1.3 w systemie IBM MQ

Począwszy od wersji IBM MQ 9.2.0, produkt obsługuje protokół TLS 1.3 na wszystkich platformach. W wersjach wcześniejszych niż IBM MQ 9.2.0obsługa protokołu TLS 1.3 w produkcie AIX, Linux, and Windows dla systemu Continuous Delivery była dostępna w serwisie IBM MQ 9.1.4.

Menedżery kolejek utworzone w wersji IBM MQ 9.2.0 lub nowszej domyślnie obsługują protokół TLS 1.3 . Menedżery kolejek poddane migracji z wcześniejszych wersji produktu IBM MQ muszą mieć włączoną obsługę protokołu TLS 1.3 . Protokół TLS 1.3 można włączyć w migrowanych menedżerach kolejek, ustawiając właściwość **AllowTLSV13**=TRUE :

- Multi W przypadku menedżerów kolejek systemu IBM MQ for Multiplatforms zmodyfikuj plik qm.ini i dodaj właściwość **AllowTLSV13**=TRUE w sekcji SSL (odsyłacz do

```
SSL:
  AllowTLSV13=TRUE
```

- z/OS W przypadku menedżerów kolejek systemu IBM MQ for z/OS należy dokonać edycji zestawu danych QMINI określonego w JCL uruchamiania menedżera kolejek i dodać właściwość **AllowTLSV13**=TRUE w sekcji TransportSecurity .

```
TransportSecurity:
    AllowTLSV13=TRUE
```

Jeśli włączona jest obsługa protokołu TLS 1.3 i zgodnie ze specyfikacją TLS 1.3, każda próba nawiązania komunikacji ze słabą specyfikacją szyfrowania CipherSpec, niezależnie od tego, czy są one włączone w produkcie IBM MQ , czy nie, jest odrzucana. CipherSpecs , które protokół TLS 1.3 uważa za słabe, to CipherSpecs , które spełniają co najmniej jedno z następujących kryteriów:

- Używa protokołu SSL 3.0 .
- Używa algorytmu szyfrowania RC4 lub RC2 .
- Ma wielkość klucza szyfrowania (bit) równą lub mniejszą niż 112.

Te ograniczenia są oznaczone uwagą [3] w Tabeli 1 nieaktualnych specyfikacji szyfrowania CipherSpecs.

Jeśli konieczne jest kontynuowanie korzystania z takich CipherSpecs, należy wyłączyć tryb TLS 1.3 :

- ALW Dokonaj edycji pliku qm.ini menedżera kolejek i zmień ustawienie właściwości **AllowTLSV13** na:

```
SSL:
  AllowTLSV13=FALSE
```

- z/OS Edytuj zestaw danych QMINI menedżera kolejek i zmień ustawienie właściwości **AllowTLSV13** na:

```
TransportSecurity:
    AllowTLSV13=FALSE
```

IBM MQ MQI client i TLS 1.3

ALW

Jeśli używany jest IBM MQ MQI client, wartość **AllowTLSV13** jest określana, chyba że została jawnie określona w sekcji SSL pliku mqclient.ini , który jest używany przez aplikację.

- Jeśli włączone są słabe CipherSpecs , parametr **AllowTLSV13** ma wartość FALSE i nie można używać protokołu TLS 1.3 CipherSpecs .
- W przeciwnym razie dla parametru **AllowTLSV13** zostanie ustawiona wartość TRUE i będzie można użyć nowej specyfikacji szyfrowania TLS 1.3 CipherSpecs i aliasu CipherSpecs .

Domyślne wartości parametru CipherSpec włączone w produkcie IBM MQ

W domyślnej konfiguracji dla nowego menedżera kolejek systemu IBM MQ produkt IBM MQ zapewnia obsługę protokołów TLS 1.2 i TLS 1.3 oraz różnych algorytmów szyfrowania korzystających z CipherSpecs. Ze względu na kompatybilność produkt IBM MQ można również skonfigurować do używania protokołów SSL 3.0 i TLS 1.0 oraz wielu algorytmów szyfrowania, o których wiadomo, że są słabe lub podatne na słabe punkty zabezpieczeń. Lista CipherSpecs , które są włączone w konfiguracji domyślnej, może ulec zmianie po zastosowaniu konserwacji.

Produkt IBM MQ można skonfigurować w taki sposób, aby ograniczał lub zezwalał na użycie CipherSpecs przy użyciu następujących elementów sterujących:

- Dozwolone są tylko CipherSpecs zgodne ze standardem FIPS 140-2, jeśli używany jest protokół SSLFIPS.
- ALW Zezwalaj tylko na CipherSpecs zgodne z pakietem NSA Suite B przy użyciu elementu SUITEB.
- Multi Zezwalaj na niestandardową listę CipherSpecs przy użyciu **AllowedCipherSpecs**.
- ALW Zezwalaj na niestandardową listę CipherSpecs przy użyciu zmiennej środowiskowej **AMQ_ALLOWED_CIPHERS** .
- ALW Zezwala na użycie nieaktualnych CipherSpecs przy użyciu zmiennej środowiskowej **AllowWeakCipher** lub **AMQ_SSL_WEAK_CIPHER_ENABLE** .
- z/OS Zezwalaj na użycie nieaktualnych CipherSpecs przy użyciu instrukcji DD w kodzie JCL CHINIT.

Uwaga: Jeśli zostanie określona niestandardowa lista CipherSpecs przy użyciu parametru **AllowedCipherSpecs** lub **AMQ_ALLOWED_CIPHERS** , przesłania to włączenie wszystkich nieaktualnych CipherSpecs. Należy pamiętać, że w przypadku używania ograniczeń 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.

Pojęcia pokrewne

“Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48
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 22
Szyfrujące protokoły bezpieczeństwa muszą być zgodne z algorytmami używanymi przez bezpieczne połączenie. CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

“Konfigurowanie produktu IBM MQ dla pakietu B” na stronie 45
Produkt IBM MQ można skonfigurować do działania zgodnie ze standardem NSA Suite B na platformach AIX, Linux, and Windows .

“Standardy FIPS (Federal Information Processing Standards)” na stronie 35
W tym temacie przedstawiono program sprawdzania poprawności Cryptomodule FIPS (Federal Information Processing Standards) dla National Institute of Standards and Technology oraz funkcje kryptograficzne, które mogą być używane w kanałach TLS.

Zadania pokrewne

Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia aliasu CipherSpe

Odsyłacze pokrewne

Zdefiniowanie kanału

ZMIEŃ KANAŁ

Zmiana, kopiowanie i tworzenie kanału

ALW 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 IBM Global Security Kit (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 działanie, 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.

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 CipherSpecs” na stronie 466.

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.

Kolejność w specyfikacji szyfrowania CipherSpec podczas uzgadniania TLS

Kolejność w polu CipherSpecs jest używana podczas wyboru spośród wielu możliwych CipherSpecs, na przykład w przypadku korzystania z jednej ze specyfikacji szyfrowania ANY* CipherSpecs.

Podczas uzgadniania TLS klient i serwer wymieniają CipherSpecs i obsługiwane przez nie protokoły w kolejności określonej przez ich preferencje. Wspólna specyfikacja szyfrowania CipherSpec , która jest po obu stronach priorytetyzowana, jest wybierana i używana na potrzeby komunikacji TLS. Jeśli zostanie wybrany protokół CipherSpec , wersja jest również brana pod uwagę, na przykład jeśli serwer wyświetla listę specyfikacji szyfrowania TLS 1.2 CipherSpecs przed protokołem TLS 1.3 CipherSpecs , nadal będzie nadawał priorytet protokołowi TLS 1.3 , o ile klient może go obsługiwać i ma wspólną specyfikację szyfrowania TLS 1.3 CipherSpec , która może być używana.

W produkcie IBM MQ 9.2.0, gdy produkt IBM MQ jest skonfigurowany na potrzeby protokołu TLS, parametr CipherSpecs jest ustawiany w kolejności przedstawionej w poniższej tabeli (od najbardziej preferowanego do najmniej preferowanego).

Uwaga: Jeśli atrybut CipherSpec nie jest włączony za pomocą atrybutu **AllowedCipherSpecs** , nie zostanie skonfigurowany do użycia podczas uzgadniania TLS.

Jeśli atrybut **AllowedCipherSpecs** nie jest określony, używana jest domyślna lista włączonych szyfrów, wskazana w poniższej tabeli.

Tabela 78. CipherSpecs (specyfikacje szyfrowania), kolejność od IBM MQ 9.2.0

Platforma	CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
Wszystkie	TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Tak
Wszystkie	TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Tak

Tabela 78. CipherSpecs (specyfikacje szyfrowania), kolejność od IBM MQ 9.2.0 (kontynuacja)				
Platforma	**CipherSpec**	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
Wszystkie	TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Tak
ALW	TLS_AES_128_CCM_SHA256	TLS 1.3	1304	Tak
ALW	TLS_AES_128_CCM_8_SHA256	TLS 1.3	1305	Tak
Wszystkie	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Tak
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384	TLS 1.2	C02C	Tak
Wszystkie	ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Tak
Wszystkie	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Tak
Wszystkie	ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Tak
Wszystkie	ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Tak
Wszystkie	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Tak
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256	TLS 1.2	C02B	Tak
Wszystkie	ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Tak
Wszystkie	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Tak
Wszystkie	ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Tak
Wszystkie	ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Tak
ALW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	TLS 1.2	C008	Nie

Tabela 78. CipherSpecs (specyfikacje szyfrowania), kolejność od IBM MQ 9.2.0 (kontynuacja)				
Platforma	**CipherSpec**	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
Multi	ECDHE_RSA_3DES_EDE_CBC_SHA256	TLS 1.2	C012	Nie
ALW	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	0005	Nie
ALW	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	C007	Nie
Multi	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	C011	Nie
Wszystkie	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Nie
ALW	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	C006	Nie
Multi	ECDHE_RSA_NULL_SHA256	TLS 1.2	C010	Nie
ALW	TLS_RSA_WITH_NULL_NULL	TLS 1.2	0000	Nie
ALW z/OS	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Nie
ALW z/OS	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Nie
IBM i	AES_SHA_US	TLS 1.0	002E	Nie
Wszystkie	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Nie
Wszystkie	TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Nie
IBM i	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	0004	Nie
Wszystkie	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0009	Nie
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0	0003	Nie
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5	TLS 1.0	0006	Nie

Tabela 78. CipherSpecs (specyfikacje szyfrowania), kolejność od IBM MQ 9.2.0 (kontynuacja)				
Platforma	**CipherSpec**	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
IBM i	TLS_RSA_WITH_NULL_SHA	TLS 1.0	0002	Nie
IBM i	TLS_RSA_WITH_NULL_MD5	TLS 1.0	0001	Nie
Wszystkie	TRIPLE_DES_SHA_US	SSL 3	000A	Nie
Wszystkie	RC4_SHA_US	SSL 3	0005	Nie
Wszystkie	RC4_MD5_US	SSL 3	0004	Nie
Wszystkie	DES_SHA_EXPORT	SSL 3	0009	Nie
Wszystkie	RC4_MD5_EXPORT	SSL 3	0003	Nie
Wszystkie	RC2_MD5_EXPORT	SSL 3	0006	Nie
Wszystkie	NULL_SHA	SSL 3	0002	Nie
Wszystkie	NULL_MD5	SSL 3	0001	Nie
ALW	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3	FEFF	Nie
ALW	RC4_56_SHA_EXPORT1024	SSL 3	0064	Nie
ALW	DES_SHA_EXPORT1024	SSL 3	0062	Nie
ALW	FIPS_WITH_DES_CBC_SHA	SSL 3	FEFE	Nie

Ta lista została utworzona przez uporządkowanie protokołów z domyślną listą dostarczoną przez bibliotekę szyfrującą używaną przez IBM MQ w systemie z/OS i jest spójna na wszystkich platformach z/OS i platformach rozproszonych.

zmiana kolejności

Jeśli wymagana jest inna kolejność, można podać nową kolejność w polu CipherSpecs (Specyfikacje szyfrowania), używając atrybutu **AllowedCipherSpecs** w sekcji SSL w produkcie IBM MQ for Multiplatforms z/OS lub sekcji TransportSecurity w systemie IBM MQ for z/OS( ) z następującymi regułami:

- Zawsze używane są wyższe wersje protokołu, niezależnie od ich pozycji na liście.
- Wszystkie wyłączone CipherSpecs zostaną ponownie włączone, jeśli zostaną podane na liście.
- Kolejność listy serwerów TLS ma wyższy priorytet niż klient TLS.
- Jeśli włączono protokół TLS 1.3 , niektóre CipherSpecs nie są obsługiwane.

Na przykład w systemie IBM MQ for Multiplatforms, jeśli w menedżerze kolejek skonfigurowano następujące elementy:

```
SSL:
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA
```

z/OS i w systemie IBM MQ for z/OS, jeśli w menedżerze kolejek skonfigurowano następujące elementy:

```
TransportSecurity:
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_AES_128_GCM_SHA256,
TLS_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA
```

Następnie:

- Klient łączący się z serwerem ANY_TLS12 prawdopodobnie użyje protokołu TLS 1.2 CipherSpec TLS_RSA_WITH_AES_128_GCM_SHA256.
- Klient łączący się z opcją ANY_TLS12_OR_HIGHER prawdopodobnie użyje protokołu TLS 1.3 CipherSpec TLS_AES_128_GCM_SHA256 (przy założeniu, że klient obsługuje protokół TLS 1.3).
- Klient łączący się z protokołem TLS 1.0 CipherSpec TLS_RSA_WITH_AES_256_CBC_SHA użyje tej specyfikacji CipherSpec.

Poprzednie wersje programu IBM MQ

Przed produktem IBM MQ 9.2.0była używana następująca kolejność CipherSpecs :

Tabela 79. CipherSpecs przed IBM MQ 9.2.0

Platforma	CipherSpec	Protokół	Domyślnie włączone
ALW z/OS	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	Nie
IBM i	AES_SHA_US	TLS 1.0	Nie
ALW z/OS	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	Nie
Wszystkie	RC4_SHA_US	SSL 3	Nie
Wszystkie	TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	Nie
Wszystkie	RC4_MD5_US	SSL 3	Nie
IBM i	TLS_RSA_WITH_RC4_128_MD5	TLS 1.0	Nie
Wszystkie	TRIPLE_DES_SHA_US	SSL 3	Nie
Wszystkie	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	Nie
ALW	DES_SHA_EXPORT1024	SSL 3	Nie
Wszystkie	RC4_56_SHA_EXPORT1024	SSL 3	Nie
Wszystkie	RC4_MD5_EXPORT	SSL 3	Nie
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS 1.0	Nie
Wszystkie	RC2_MD5_EXPORT	SSL 3	Nie

Tabela 79. CipherSpecs przed IBM MQ 9.2.0 (kontynuacja)			
Platforma	**CipherSpec**	**Protokół**	**Domyślnie włączone**
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5	TLS 1.0	Nie
Wszystkie	DES_SHA_EXPORT	SSL 3	Nie
Wszystkie	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	Nie
Wszystkie	NULL_SHA	SSL 3	Nie
IBM i	TLS_RSA_WITH_NULL_SHA	TLS 1.0	Nie
Wszystkie	NULL_MD5	SSL 3	Nie
IBM i	TLS_RSA_WITH_NULL_MD5	TLS 1.0	Nie
ALW	FIPS_WITH_DES_CBC_SHA	SSL 3	Nie
ALW	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3	Nie
Wszystkie	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	Tak
Wszystkie	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	Tak
Wszystkie	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	Nie
Wszystkie	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	Tak
Wszystkie	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	Tak
ALW	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	Nie
ALW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	TLS 1.2	Nie
Multi	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	Nie
Multi	ECDHE_RSA_3DES_EDE_CBC_SHA256	TLS 1.2	Nie
Wszystkie	ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	Tak
Wszystkie	ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	Tak
Wszystkie	ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	Tak
Wszystkie	ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	Tak

Tabela 79. CipherSpecs przed IBM MQ 9.2.0 (kontynuacja)			
Platforma	**CipherSpec**	**Protokół**	**Domyślnie włączone**
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256	TLS 1.2	Tak
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384	TLS 1.2	Tak
Wszystkie	ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	Tak
Wszystkie	ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	Tak
Multi	ECDHE_RSA_NULL_SHA256	TLS 1.2	Nie
ALW	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	Nie
ALW	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Nie
ALW	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	Nie
Multi	TLS_AES_128_GCM_SHA256	TLS 1.3	Tak
Multi	TLS_AES_256_GCM_SHA384	TLS 1.3	Tak
Multi	TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	Tak
ALW	TLS_AES_128_CCM_SHA256	TLS 1.3	Tak
ALW	TLS_AES_128_CCM_8_SHA256	TLS 1.3	Tak

Ważne: Od dnia 23rd lipca 2020 r. następujący atrybut specyfikacji AllowedCipherwłącza tylko specyfikacje szyfrowania CipherSpecs , które są obecnie domyślnie włączone. Należy jednak sprawdzić, czy parametr CipherSpecs włączony przez następujący atrybut AllowedCipherSpecs z bieżącymi danymi, aby upewnić się, że parametr CipherSpecs , który jest nieaktualny od tej daty, nie zostanie przypadkowo ponownie włączony.

Aby powrócić do tej kolejności CipherSpecs, można użyć następującej wartości atrybutu sekcji **AllowedCipherSpecs** SSL/TransportSecurity :

```
AllowedCipherSpecs=TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,ECDHE_ECDSA_AES_128_CBC_SHA256,
ECDHE_ECDSA_AES_256_CBC_SHA384,ECDHE_RSA_AES_128_CBC_SHA256,ECDHE_RSA_AES_256_CBC_SHA384,
ECDHE_ECDSA_AES_128_GCM_SHA256,ECDHE_ECDSA_AES_256_GCM_SHA384,ECDHE_RSA_AES_128_GCM_SHA256,
ECDHE_RSA_AES_256_GCM_SHA384
```

Udostępnianie niestandardowej listy uporządkowanych i włączonych CipherSpecs w systemie IBM MQ for Multiplatforms

Multi

Można udostępnić alternatywny zestaw CipherSpecs , który jest włączony, w preferowanej kolejności, do użycia z kanałami IBM MQ , za pomocą atrybutu sekcji SSL ALW Zmienna środowiskowa **AMQ_ALLOWED_CIPHERS** lub **AllowedCipherSpecs** w pliku `.ini` . Tego ustawienia można użyć z jednej z następujących przyczyn:

- Ograniczenie akceptowania przychodzących żądań uruchomienia kanału przez procesy nasłuchujące produktu IBM MQ , chyba że używają one jednej z nazwanych CipherSpecs.
- Umożliwia zmianę kolejności priorytetów CipherSpecs używanych podczas uzgadniania TLS.

Ta funkcja może być używana do sterowania CipherSpecs , które są zawarte w specyfikacji szyfrowania ANY* CipherSpecs.

Zmienna środowiskowa **AMQ_ALLOWED_CIPHERS** lub atrybut sekcji SSL systemu **AllowedCipherSpecs** akceptuje następujące wartości:

- Pojedyncza nazwa CipherSpec .
- Rozdzielana przecinkami lista nazw CipherSpec do ponownego włączenia.
- Wartość specjalna `ALL`reprezentująca wszystkie CipherSpecs.

Uwaga: Nie należy włączać opcji **ALL** CipherSpecs, ponieważ spowoduje to włączenie protokołów SSL 3.0 i TLS 1.0 oraz dużej liczby słabych algorytmów szyfrowania.

Jeśli to ustawienie jest skonfigurowane, przesłania ono domyślną listę CipherSpec i powoduje, że produkt IBM MQ ignoruje ustawienia słabego dezaktualizacji szyfru (patrz poniżej):

- Obiekty nasłuchiwania systemu IBM MQ akceptują tylko te propozycje protokołu SSL/TLS, które używają jednej z wymienionych CipherSpecs.
- Kanały IBM MQ zezwalają tylko na pustą wartość SSLCIPH lub na jedną z nazwanych CipherSpecs.
- Zakończenie wartości SSLCIPH na karcie **runmqsc** ogranicza wartości zakończenia do jednej z nazw CipherSpecs.

Na przykład, aby umożliwić definiowanie/zmianę kanałów i akceptowanie przez procesy nasłuchujące ECDHE_RSA_AES_128_GCM_SHA256 lub ECDHE_ECDSA_AES_256_GCM_SHA384 , w pliku `qm.ini` można ustawić następujące wartości:

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

Ponadto do określenia priorytetu CipherSpecs używanych podczas uzgadniania TLS zostanie użyta opcja CipherSpecs z tej listy. Na przykład, jeśli zostanie podana lista `TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256` , podczas uzgadniania wartość TLS_RSA_WITH_AES_128_CBC_SHA256 CipherSpec zostanie wybrana zamiast wartości TLS_RSA_WITH_AES_256_CBC_SHA256 CipherSpec , jeśli klient nawiąże połączenie, podając obie te wartości CipherSpecs, to znaczy klienta łączącego się z wartością ANY_TLS12.

Należy zauważyć, że szyfry używane przez kanały AMQP lub MQTT można ograniczyć przy użyciu ustawień pliku java.security .

Udostępnianie niestandardowej listy uporządkowanych i włączonych CipherSpecs w systemie IBM MQ for z/OS

z/OS

Możliwe jest udostępnienie alternatywnego zestawu CipherSpecs , które są włączone i w preferowanej kolejności, do użycia z kanałami IBM MQ , za pomocą atrybutu sekcji **AllowedCipherSpecs** TransportSecurity w sekcji Zestaw danych QMINI. Można to zrobić z jednej z następujących przyczyn:

- Ograniczenie akceptowania przychodzących żądań uruchomienia kanału przez procesy nasłuchujące produktu IBM MQ , chyba że używają one jednej z nazwanych CipherSpecs.
- Umożliwia zmianę kolejności priorytetów CipherSpecs używanych podczas uzgadniania TLS.

Tej funkcji można użyć do sterowania CipherSpecs , które są uwzględnione w specyfikacji szyfrowania ANY* CipherSpecs. Atrybut **AllowedCipherSpecs** akceptuje następujące wartości:

- Pojedyncza nazwa CipherSpec .
- Rozdzielana przecinkami lista nazw CipherSpec do ponownego włączenia.
- Wartość specjalna ALLreprezentująca wszystkie CipherSpecs.

  Uwaga: Nie należy włączać opcji **ALL** CipherSpecs, ponieważ spowoduje to włączenie protokołów SSL 3.0 i TLS 1.0 oraz dużej liczby słabych algorytmów szyfrowania. Jeśli to ustawienie zostanie skonfigurowane, przesłania ono domyślną listę CipherSpec i powoduje, że produkt IBM MQ ignoruje ustawienia słabego dezaktualizacji szyfrów (patrz sekcja "Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie z/OS" na stronie 486).

Obiekty nasłuchiwania systemu IBM MQ akceptują tylko te propozycje protokołu SSL/TLS, które używają jednego z nazwanych kanałów CipherSpecs i IBM MQ zezwalają tylko na pustą wartość SSLCIPH lub jedną z nazwanych CipherSpecs.

Na przykład, aby umożliwić definiowanie/zmianę kanałów i akceptowanie przez procesy nasłuchujące ECDHE_RSA_AES_128_GCM_SHA256 lub ECDHE_RSA_AES_256_GCM_SHA384 , można ustawić następujące wartości:

```
TransportSecurity:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256,
                     ECDHE_RSA_AES_256_GCM_SHA384
```

Ponadto CipherSpecs na tej liście są używane do określenia priorytetu CipherSpecs używanych podczas uzgadniania TLS. Na przykład, jeśli zostanie podana lista TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256 podczas uzgadniania będzie prawdopodobnie wybrana opcja TLS_RSA_WITH_AES_128_CBC_SHA256 CipherSpec dla opcji TLS_RSA_WITH_AES_256_CBC_SHA256 CipherSpec , jeśli klient nawiąże połączenie z opcją CipherSpecs, która jest klientem łączącym się, tzn.

Deprecated Nieaktualne CipherSpecs

Lista nieaktualnych CipherSpecs , których można używać w razie potrzeby z produktem IBM MQ .

Uwaga: W systemie AIX, Linux, and Windows IBM MQ zapewnia zgodność ze standardem FIPS 140-2 za pośrednictwem modułu szyfrującego IBM Crypto for C (ICC) . Certyfikat dla tego modułu został przeniesiony do statusu historycznego. Klienci powinni zapoznać się z informacjami w sekcji Certyfikat IBM Crypto for C (ICC) i zapoznać się z poradami NIST. Zastępczy moduł FIPS 140-3 jest obecnie w toku, a jego status można wyświetlić, wyszukując go na liście Moduły NIST CMVP na liście procesów.

Informacje na temat włączania nieaktualnych specyfikacji szyfrowania CipherSpecsmożna znaleźć w sekcji "Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie IBM MQ for Multiplatforms" na stronie 486 lub "Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie z/OS" na stronie 486.

W poniższej tabeli wymieniono nieaktualne CipherSpecs , których można używać z obsługą protokołu TLS produktu IBM MQ .

Tabela 80. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ

Obsługa platformy "1" na stronie 485	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 485	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Specyfikacje szyfrowania dla protokołu SSL 3.0								

Tabela 80. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 485	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 485	Suite B	Aktualizacja, w której uznano ją za nieaktualną
IBM i	AES_SHA_US "3" na stronie 485	002F	SSL 3.0	SHA-1	AES (128)	Nie	Nie	9.0.0.0
Wszystkie	DES_SHA_EXPORT "3" na stronie 485 "4" na stronie 485 "5" na stronie 485	0009	SSL 3.0	SHA-1	DES (56)	Nie	Nie	9.0.0.0
ALW	DES_SHA_EXPORT1024 "3" na stronie 485 "6" na stronie 485	0062	SSL 3.0	SHA-1	DES (56)	Nie	Nie	9.0.0.0
ALW	FIPS_WITH_DES_CBC_SHA "3" na stronie 485	FEFE	SSL 3.0	SHA-1	DES (56)	Nie "7" na stronie 485	Nie	9.0.0.0
ALW	FIPS_WITH_3DES_EDE_CBC_SHA "3" na stronie 485	FEFF	SSL 3.0	SHA-1	3DES (168)	Nie "8" na stronie 485	Nie	9.0.0.1 i 9.0.1
Wszystkie	NULL_MD5 "3" na stronie 485	0001	SSL 3.0	MD5	Brak	Nie	Nie	9.0.0.1
Wszystkie	NULL_SHA "3" na stronie 485	0002	SSL 3.0	SHA-1	Brak	Nie	Nie	9.0.0.1
Wszystkie	RC2_MD5_EXPORT "3" na stronie 485 "4" na stronie 485 "5" na stronie 485	0006	SSL 3.0	MD5	RC2 (40)	Nie	Nie	9.0.0.0
Wszystkie	RC4_MD5_EXPORT "4" na stronie 485 "3" na stronie 485	0003	SSL 3.0	MD5	RC4 (40)	Nie	Nie	9.0.0.0
Wszystkie	RC4_MD5_US "3" na stronie 485	0004	SSL 3.0	MD5	RC4 (128)	Nie	Nie	9.0.0.0
Wszystkie	RC4_SHA_US "3" na stronie 485 "5" na stronie 485	0005	SSL 3.0	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ALW	RC4_56_SHA_EXPORT1024 "3" na stronie 485 "6" na stronie 485	0064	SSL 3.0	SHA-1	RC4 (56)	Nie	Nie	9.0.0.0
Wszystkie	TRIPLE_DES_SHA_US "3" na stronie 485 "5" na stronie 485	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 485	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 485 "4" na stronie 485	0003	TLS 1.0	MD5	RC4 (40)	Nie	Nie	9.0.0.0

Tabela 80. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 485	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 485	Suite B	Aktualizacja, w której uznano ją za nieaktualną
Wszystkie	TLS_RSA_WITH_DES_CBC_SHA "3" na stronie 485	0009	TLS 1.0	SHA-1	DES (56)	Nie "9" na stronie 485	Nie	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" na stronie 485	0001	TLS 1.0	MD5	Brak	Nie	Nie	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" na stronie 485	0002	TLS 1.0	SHA-1	Brak	Nie	Nie	9.0.0.1
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" na stronie 485	0004	TLS 1.0	MD5	RC4 (128)	Nie	Nie	9.0.0.0
z/OS ALW	TLS_RSA_WITH_AES_128_CBC_SHA "10" na stronie 485	002F	TLS 1.0	SHA-1	AES (128)	Tak	Nie	9.0.5
z/OS ALW	TLS_RSA_WITH_AES_256_CBC_SHA "6" na stronie 485 "10" na stronie 485	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								
ALW	ECDHE_ECDSA_NULL_SHA256 "3" na stronie 485	C006	TLS 1.2	SHA-1	Brak	Nie	Nie	9.0.0.1
ALW	ECDHE_ECDSA_RC4_128_SHA256 "3" na stronie 485	C007	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ALW IBM i	ECDHE_RSA_NULL_SHA256 "3" na stronie 485	C010	TLS 1.2	SHA-1	Brak	Nie	Nie	9.0.0.1
ALW IBM i	ECDHE_RSA_RC4_128_SHA256 "3" na stronie 485	C011	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ALW	TLS_RSA_WITH_NULL_NULL "3" na stronie 485	0000	TLS 1.2	Brak	Brak	Nie	Nie	9.0.0.1
Wszystkie	TLS_RSA_WITH_NULL_SHA256 "3" na stronie 485	003B	TLS 1.2	SHA-256	Brak	Nie	Nie	9.0.0.1
ALW	TLS_RSA_WITH_RC4_128_SHA256 "3" na stronie 485	0005	TLS 1.2	SHA-1	RC4 (128)	Nie	Nie	9.0.0.0
ALW	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 80. Nieaktualne specyfikacje szyfrowania, które można ponownie włączyć w produkcie IBM MQ (kontynuacja)

Obsługa platformy "1" na stronie 485	Nazwa specyfikacji szyfrowania	Kod szesnastkowy	Używany protokół	Integralność danych	Algorytm szyfrowania (bity szyfrowania)	FIPS "2" na stronie 485	Suite B	Aktualizacja, w której uznano ją za nieaktualną
ALW IBM i	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 poszczególne ikony znajdują się w sekcji Ikony używane 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. ALW 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 późniejszej domyślnie włączają protokół TLS 1.3, co powoduje wyłączenie tych specyfikacji szyfrów. 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 poddane migracji do wersji IBM MQ for z/OS 9.2.0 z wcześniejszej wersji nie mają domyślnie włączonego protokołu TLS 1.3, zatem te specyfikacje szyfrów są w nich włączone.
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. Deprecated 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. Deprecated 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.

Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie IBM MQ for Multiplatforms

Multi

Domyślnie nie jest dozwolone określanie nieaktualnej specyfikacji szyfrowania CipherSpec w definicji kanału. W przypadku próby określenia nieaktualnej specyfikacji szyfrowania CipherSpec w systemie IBM MQ for Multiplatformszostanie wyświetlony komunikat AMQ8242: Niepoprawna definicja SSLCIPH, a program PCF zwróci wartość MQRCCF_SSL_CIPHER_SPEC_ERROR.

Nie można uruchomić kanału z nieaktualną CipherSpec. W przypadku podjęcia takiej próby z nieaktualną wartością CipherSpecsystem zwróci do klienta kod MQCC_FAILED (2) wraz z wartością **Reason** MQRC_SSL_INITIALIZATION_ERROR (2393) .

Aby ponownie włączyć jedną lub więcej nieaktualnych CipherSpecs na potrzeby definiowania kanałów w czasie wykonywania na serwerze, należy ustawić zmienną środowiskową **AMQ_SSL_WEAK_CIPHER_ENABLE**.

Zmienna środowiskowa **AMQ_SSL_WEAK_CIPHER_ENABLE** przyjmuje następujące wartości:

- Pojedyncza nazwa CipherSpec lub
- Rozdzielana przecinkami lista nazw CipherSpec do ponownego włączenia lub
- Wartość specjalna ALLreprezentująca wszystkie CipherSpecs.

Ostrzeżenie: Chociaż opcja ALL jest poprawna, należy jej używać **tylko** w konkretnej sytuacji, która jest wymagana w przedsiębiorstwie, ponieważ ponowne włączenie opcji ALL CipherSpecs powoduje włączenie protokołów SSL 3.0 i TLS 1.0 , a także dużej liczby słabych algorytmów szyfrowania.

Na przykład, aby ponownie włączyć opcję ECDHE_RSA_RC4_128_SHA256, należy ustawić następującą zmienną środowiskową:

```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

lub zmień sekcję SSL w pliku qm.ini , ustawiając:

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

Włączanie nieaktualnych specyfikacji szyfrowania produktu CipherSpecs w systemie z/OS

z/OS

Domyślnie nie jest dozwolone określanie nieaktualnej specyfikacji szyfrowania CipherSpec w definicji kanału. W przypadku próby określenia nieaktualnej specyfikacji szyfrowania CipherSpec w systemie z/OSzostanie wyświetlony komunikat CSQM102E, komunikat CSQX616Elub CSQX674E.

Należy postępować zgodnie z instrukcjami podanymi w tej sekcji, jeśli zostanie odebrany jeden z tych komunikatów, a przedsiębiorstwo musi ponownie włączyć używanie słabych CipherSpecs.

Ostrzeżenie: W poniższych instrukcjach, aby instrukcje definicji fikcyjnej (DD) zostały zastosowane, wartość SSLTASKS musi być różna od zera. Jeśli wymaga to zmiany w SSLTASKS, należy zrestartować inicjator kanału.

W systemie IBM MQ for z/OSbieżąca metoda kontrolowania słabych lub zerwanych CipherSpecs jest następująca:

- Aby ponownie włączyć używanie słabych CipherSpecs, należy dodać do kodu JCL inicjatora kanału instrukcję definicji danych (DD) o nazwie CSQXWEAK . Podanie samej wartości powoduje włączenie tylko słabych CipherSpecs powiązanych z protokołem TLS 1.2 , na przykład:

  ```
  //CSQXWEAK DD DUMMY
  ```

  Uwaga: Nie wszystkie nieaktualne CipherSpecs wymagają użycia tej instrukcji DD. Patrz uwaga 10 w powyższej tabeli.
- Aby ponownie włączyć użycie CipherSpecsprotokołu SSLv3 , należy dodać do kodu JCL inicjatora kanału fikcyjną instrukcję DD o nazwie CSQXSSL3 . Wszystkie CipherSpecs protokołu SSLv3 są traktowane jako **słaba**, dlatego należy również podać wartość CSQXWEAK:

  ```
  //CSQXSSL3 DD DUMMY
  ```
- Aby ponownie włączyć nieaktualny protokół TLS V1 CipherSpecs, należy dodać do kodu JCL inicjatora kanału fikcyjną instrukcję DD o nazwie TLS10ON (należy włączyć protokół TLS V1.0 ON). Podanie samej wartości powoduje włączenie silnych CipherSpecs powiązanych z protokołem TLS 1.0 :

  ```
  //TLS10ON DD DUMMY
  ```

  Jeśli ta opcja zostanie określona z parametrem CSQXWEAK , zostanie również włączone ustawienie **Słabe specyfikacje szyfrowania** CipherSpecs powiązane z protokołem TLS 1.0.
- Aby jawnie wyłączyć nieaktualne specyfikacje szyfrowania TLS V1 CipherSpecs, należy dodać fikcyjną instrukcję DD o nazwie TLS10OFF (wyłącz TLS V1.0) do kodu JCL inicjatora kanału, na przykład:

  ```
  //TLS10OFF DD DUMMY
  ```

Aby negocjować tylko z programem nasłuchującym przy użyciu specyfikacji szyfrów wymienionych na domyślnej liście specyfikacji szyfrów **`System SSL`** , należy zdefiniować następującą instrukcję DD w JCL CHINIT:

```
JCL: //GSKDCIPS DD DUMMY
```

Ważne: W przypadku systemu IBM MQ for z/OS 9.2.0 i nowszych wersji podczas wyświetlania komunikatów podczas uruchamiania inicjatora kanału są brane pod uwagę wymienione wcześniej karty DD i wartość **`AllowTLSV13`** , aby wskazać, które protokoły są włączone, a które nie. Tak więc, nawet jeśli jedna z wymienionych wcześniej kart DD jest określona, może to oznaczać, że ze względu na połączenie tych ustawień, pewien protokół nie może być włączony z innym protokołem. Na przykład protokół SSL 3.0 nie jest dozwolony, jeśli włączony jest protokół TLS 1.3 .

Istnieją alternatywne mechanizmy, których można użyć do wymuszenia ponownego włączenia słabych CipherSpecsi obsługi protokołu SSLv3 , jeśli zmiana definicji danych nie jest odpowiednia. Aby uzyskać więcej informacji, skontaktuj się z serwisem IBM .

Pojęcia pokrewne

“Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48

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 CipherSpec aliasu

Te informacje opisują oczekiwane zachowanie w przypadku różnych kombinacji aliasów CipherSpecs w konfiguracjach klienta i serwera. W tym przypadku klient odwołuje się do jednostki inicjującej komunikację, na przykład do aplikacji klienckiej lub kanału nadawczego menedżera kolejek, a serwer

odwołuje się do jednostki odbierającej komunikację od klienta, na przykład do kanału połączenia z serwerem lub kanału odbiorczego.

Minimalna liczba protokołów a stała liczba protokołów CipherSpecs

Produkt IBM MQ obsługuje dwa różne typy CipherSpecs:

Protokół minimalny
Minimalne wartości protokołu CipherSpecs to te, które nie ustawiają górnej granicy, na przykład ANY, ANY_TLS12_OR_HIGHER lub ANY_TLS13_OR_HIGHER.

Stały protokół
CipherSpecs protokołu stałego to te, które identyfikują konkretny protokół, na przykład ANY_TLS12 i ANY_TLS13lub konkretny algorytm, taki jak ECDHE_ECDSA_3DES_EDE_CBC_SHA256.

Od wersji IBM MQ 9.2.0minimalne i stałe CipherSpecs protokołu są obsługiwane na wszystkich platformach.

Aby zmaksymalizować prostotę konfiguracji przy zachowaniu bezpieczeństwa, zaleca się użycie **minimalnego protokołu** CipherSpecs po obu stronach kanału. Dzięki temu komunikacja może automatycznie obsługiwać i używać wyższej wersji protokołu TLS, gdy obie strony obsługują nową wersję bez konieczności zmiany konfiguracji obu stron.

Użycie **minimalnego protokołu** CipherSpec po stronie inicjującej, ale **ustalony protokół** CipherSpec po stronie odbierającej może spowodować odrzucenie połączenia.

- Multi Wysyłane są komunikaty AMQ9631 i AMQ9641 .
- z/OS Wysyłane są komunikaty CSQX631E i CSQX641E .

W poniższych tabelach przedstawiono relację między różnymi ustawieniami CipherSpec aliasu i oczekiwanym wynikiem. Tabela 81 na stronie 488 przedstawia oczekiwane zachowanie, gdy protokół TLS 1.3 nie jest włączony ani na kliencie, ani na serwerze, ani na obu tych serwerach. Tabela 82 na stronie 489 przedstawia 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 CipherSpecs dla serwera są wyświetlane na osi X tabeli.

Uwaga: W poniższych tabelach komórki oznaczone jako *Prawdopodobna awaria* wskazują na możliwość wystąpienia konfliktu, gdy dla jednej części połączenia zostanie określony **minimalny protokół** CipherSpec , a dla innej-konkretny (**ustalony protokół**) CipherSpec .

Na przykład załóżmy, że klient i serwer mają ustawioną wartość ANY CipherSpec, a kanał serwera ma ustawioną wartość CipherSpec:

- Jeśli najsilniejsza obsługiwana specyfikacja szyfrowania CipherSpec dla klienta i serwera jest zgodna z konkretną specyfikacją szyfrowania CipherSpec skonfigurowaną w kanale, uzgadnianie TLS zakończy się pomyślnie.
- Jeśli jednak istnieje silniejsza wartość atrybutu CipherSpec , która jest obsługiwana zarówno przez klienta, jak i serwer, uzgadnianie TLS jest rozstrzygane na podstawie tego atrybutu, nawet jeśli nie jest zgodne ze specyfikacją CipherSpec określoną w kanale, a uzgadnianie TLS kończy się niepowodzeniem.

Tabela 81. Oczekiwane zachowanie, gdy protokół TLS 1.3 nie jest włączony ani na kliencie, ani na serwerze, ani na obu tych serwerach

	Serwer			
Klient	**Specyficzny dla protokołu TLS 1.2 CipherSpec**	**ANY**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
Specyficzny protokół TLS 1.2 CipherSpec	Połączenia	Połączenia	Połączenia	Połączenia

Tabela 81. Oczekiwane zachowanie, gdy protokół TLS 1.3 nie jest włączony ani na kliencie, ani na serwerze, ani na obu tych serwerach (kontynuacja)				
	Serwer			
Klient	**Specyficzny dla protokołu TLS 1.2 CipherSpec**	**ANY**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
any	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia
ANY_ TLS12	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia
ANY_TLS12_ NOWY_WYŻSZY	*Prawdopodobna awaria*	Połączenia	Połączenia	Połączenia

Tabela 82. Oczekiwane zachowanie, gdy protokół TLS 1.3 jest włączony zarówno na kliencie, jak i na serwerze							
	Serwer						
Klient	**Specyficzny dla protokołu TLS 1.2 CipherSpec**	**Specyficzny dla protokołu TLS 1.3 CipherSpec**	**ANY**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ WYSOKI**	**ANY_TLS13_ WYSOKI**
Specyficzny protokół TLS 1.2 CipherSpec	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	**Niepowodzenie**	Połączenia	**Niepowodzenie**
Konkretne TLS 1.3 CipherSpec	**Niepowodzenie**	Połączenia	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	Połączenia
any	**Niepowodzenie**	*Prawdopodobna awaria*	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	Połączenia
ANY_TLS12	*Prawdopodobna awaria*	**Niepowodzenie**	Połączenia	Połączenia	**Niepowodzenie**	Połączenia	**Niepowodzenie**
ANY_TLS13	**Niepowodzenie**	*Prawdopodobna awaria*	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	Połączenia
ANY_TLS12_ WYSOKI	**Niepowodzenie**	*Prawdopodobna awaria*	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	Połączenia
ANY_TLS13_ WYSOKI	**Niepowodzenie**	*Prawdopodobna awaria*	Połączenia	**Niepowodzenie**	Połączenia	Połączenia	Połączenia

Pojęcia pokrewne

“Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48

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 22

Szyfrujące protokoły bezpieczeństwa muszą być zgodne z algorytmami używanymi przez bezpieczne połączenie. CipherSpecs i CipherSuites definiują konkretne kombinacje algorytmów.

“Włączanie CipherSpecs” na stronie 466
Włącz parametr CipherSpec , używając parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** lub **ALTER CHANNEL** MQSC.

Zadania pokrewne

Migrowanie istniejących konfiguracji zabezpieczeń w celu użycia atrybutu ANY_TLS12_OR_HIGHER CipherSpec

Uzyskiwanie informacji na temat CipherSpecs przy użyciu produktu IBM MQ Explorer

Aby wyświetlić opisy CipherSpecs, można użyć parametru IBM MQ Explorer .

Aby uzyskać informacje na temat CipherSpecs w pliku “Włączanie CipherSpecs” na stronie 466, wykonaj 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, i 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 specyfikację szyfrowania CipherSpec , z którą chcesz pracować. Opis jest wyświetlany w oknie poniżej listy.

z/OS IBM i Alternatywne sposoby określania CipherSpecs

W przypadku platform, na których system operacyjny udostępnia obsługę protokołu TLS, system może obsługiwać nowe CipherSpecs , które nie są uwzględnione w produkcie “Włączanie CipherSpecs” na stronie 466.

W parametrze SSLCIPH można podać nową CipherSpec , ale podana wartość zależy od platformy. We wszystkich przypadkach specyfikacja musi odpowiadać specyfikacji szyfrowania TLS CipherSpec , która jest poprawna i obsługiwana przez wersję protokołu TLS działającą w systemie.

Uwaga: Ta sekcja nie dotyczy systemów AIX, Linux, and Windows , ponieważ CipherSpecs są dostarczane z produktem IBM MQ , więc nowe CipherSpecs nie są dostępne po wysyłce.

IBM i IBM i

Dwuznakowy łańcuch reprezentujący wartość szesnastkową.

Więcej informacji na temat dozwolonych wartości zawiera punkt trzeci w sekcji Uwagi dotyczące używania w sekcji Ustawianie informacji o znakach dla sesji chronionej.

Ostrzeżenie: Nie należy podawać szesnastkowych wartości szyfru w **SSLCIPH**, ponieważ nie jest jasne, która wartość szyfru będzie używana, a wybór protokołu, który ma być używany, jest nieokreślony. Użycie szesnastkowych wartości szyfru może prowadzić do błędów niezgodności specyfikacji szyfrowania CipherSpec .

Do określenia wartości można użyć komendy **CHGMQMCHL** lub **CRTMQMCHL** , na przykład:

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

Do ustawienia parametru **SSLCIPH** można także użyć komendy **ALTER QMGR** MQSC.

z/OS z/OS

Łańcuch czteroznakowy reprezentujący wartość szesnastkową. Kody szesnastkowe odpowiadają wartościom zdefiniowanym w protokole TLS.

Więcej informacji na ten temat zawiera sekcja Definicje zestawów algorytmów szyfrowania , w której znajduje się lista wszystkich obsługiwanych specyfikacji szyfrów TLS 1.0, TLS 1.2i TLS 1.3 w postaci 4-cyfrowych kodów szesnastkowych.

Uwaga: Deprecated Aby użyć słabej wartości atrybutu CipherSpeclub CipherSpec należącego do nieaktualnego protokołu, takiego jak SSL V3.0 lub TLS 1.0, należy określić odpowiednią kartę DD w kodzie JCL uruchamiania inicjatora kanału. Więcej informacji zawiera sekcja "Nieaktualne CipherSpecs" na stronie 482.

Uwagi dotyczące klastrów IBM MQ

W przypadku klastrów IBM MQ najbezpieczniej jest używać nazw CipherSpec w produkcie "Włączanie CipherSpecs" na stronie 466. 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 530.

Określanie CipherSpec dla IBM MQ MQI client

Istnieją trzy opcje określania parametru CipherSpec dla IBM MQ MQI client.

Dostępne są następujące opcje:

- Korzystanie z tabeli definicji kanału
- Użycie pola SSLCipherSpec w strukturze MQCD w wersji MQCD_VERSION_7 lub nowszej w wywołaniu MQCONNX.
- Korzystanie z usługi Active Directory (w systemach Windows z obsługą Active Directory)

Określanie CipherSuite z IBM MQ classes for Java i IBM MQ classes for JMS

IBM MQ classes for Java i IBM MQ classes for JMS określają CipherSuites inaczej niż na innych platformach.

Informacje na temat określania CipherSuite z produktem IBM MQ classes for Javazawiera sekcja Obsługa protokołu TLS (Transport Layer Security) w produkcie Java .

Informacje na temat określania opcji CipherSuite z produktem IBM MQ classes for JMSzawiera sekcja Używanie protokołu TLS (Transport Layer Security) z produktem IBM MQ classes for JMS .

Określanie parametru CipherSpec dla produktu IBM MQ.NET

W przypadku produktu IBM MQ.NET parametr CipherSpec można określić za pomocą klasy MQEnvironment lub za pomocą właściwości MQC.SSL_CIPHER_SPEC_PROPERTY w tabeli mieszającej właściwości połączenia.

Informacje na temat określania atrybutu CipherSpec dla niezarządzanego klienta .NET zawiera sekcja Włączanie protokołu TLS dla niezarządzanego klienta .NET .

Informacje na temat określania atrybutu CipherSpec dla zarządzanego klienta .NET zawiera sekcja Obsługa atrybutuCipherSpec dla zarządzanego klienta .NET .

z/OS Używanie protokołu AT-TLS z produktem IBM MQ for z/OS

Application Transparent Transport Layer Security (AT-TLS) zapewnia obsługę protokołu TLS dla aplikacji z/OS bez konieczności implementowania obsługi TLS przez te aplikacje, a nawet bez względu na to, że używany jest protokół TLS. Protokół AT-TLS jest dostępny tylko w systemie z/OS.

Protokół AT-TLS może być używany ze wszystkimi wersjami programu IBM MQ for z/OS.

Przed użyciem protokołu AT-TLS z produktem IBM MQ for z/OSnależy zapoznać się z informacjami zawartymi w sekcji "Ograniczenia" na stronie 495 .

Aby użyć opcji Application Transparent Transport Layer Security , należy zdefiniować instrukcje strategii zawierające zestaw reguł, które są używane przez serwer z/OS Communications Server do 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 z obsługiwaną CipherSpec.

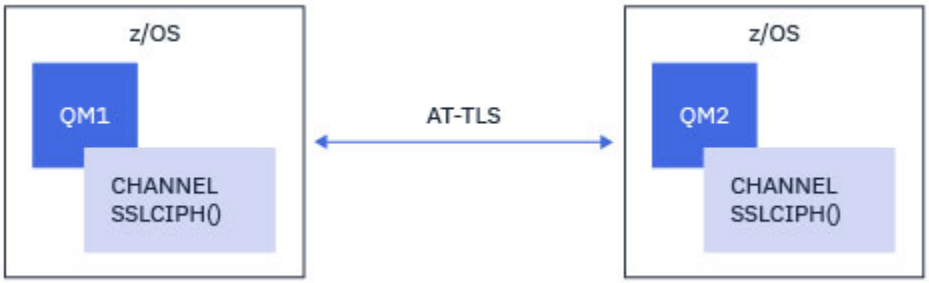
Decydując się na włączenie protokołu TLS w kanale, administrator produktu IBM MQ może zdecydować o użyciu protokołu AT-TLS lub IBM MQ TLS. Decyzja jest często podejmowana w zależności od tego, czy mechanizm AT-TLS jest używany dla innego oprogramowania pośredniego, czy też ze względu na wpływ na wydajność. Podstawowe porównanie wydajności protokołów AT-TLS i IBM MQ TLS zawiera dokument MP16: Capacity Planning and Tuning for IBM MQ for z/OS.

Scenariusze

Użycie mechanizmu AT-TLS z produktem IBM MQ jest obsługiwane w następujących scenariuszach:

Scenariusz 1

Między dwoma menedżerami kolejek systemu IBM MQ for z/OS , w których po obu stronach kanału jest używany protokół AT-TLS. Oznacza to, że żaden z kanałów nie określa atrybutu SSLCIPH. Tego podejścia można używać z dowolnym kanałem komunikatów.



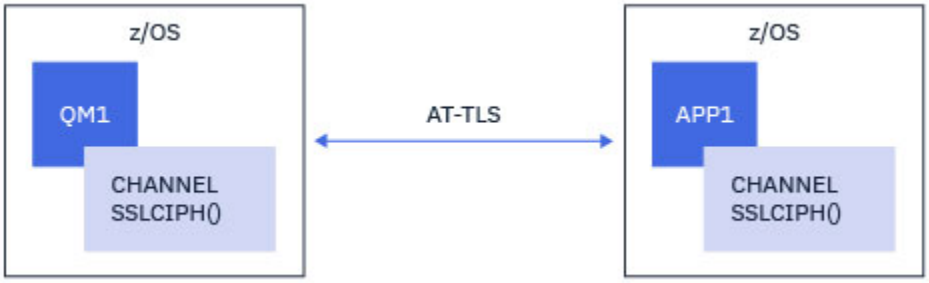
Implementacja tego scenariusza obejmuje zdefiniowanie dwóch strategii AT-TLS, po jednej dla każdej strony kanału. Strategie te są takie same, jak te używane w przypadku Scenariusza 3 lub Scenariusza 4.

Jeśli na przykład kanał został zmieniony z używania pojedynczej specyfikacji szyfrowania o nazwie CipherSpec na używanie protokołu AT-TLS, kanał wychodzący użyje 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 496 , a kanał przychodzący użyje 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 505.

Jeśli kanał został zmieniony z użycia aliasu CipherSpec na użycie AT-TLS, kanał wychodzący użyje strategii z produktu "Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpecs" na stronie 500 , a kanał przychodzący użyje strategii z produktu "Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec" na stronie 509.

Scenariusz2

Między menedżerem kolejek systemu IBM MQ for z/OS a aplikacją kliencką systemu IBM MQ Java działającą w systemie z/OS , w którym po obu stronach kanału używany jest protokół AT-TLS. Oznacza to, że ani kanał połączenia z serwerem, ani kanał połączenia z klientem nie określają atrybutu SSLCIPH.



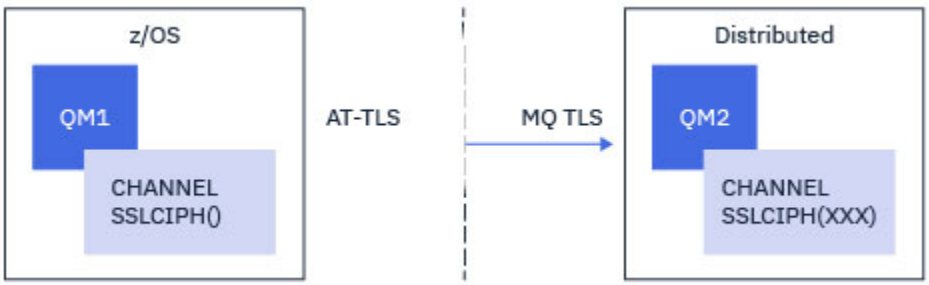
Implementacja tego scenariusza obejmuje zdefiniowanie dwóch strategii AT-TLS, po jednej dla każdej strony kanału. Strategie te są takie same, jak te używane w przypadku Scenariusza 3 lub Scenariusza 4.

Na przykład, jeśli kanał został zmieniony z używania pojedynczej, o nazwie CipherSpec na używanie protokołu AT-TLS, kanał połączenia klienckiego będzie używał 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 496 , a kanał połączenia z serwerem będzie używał 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 505.

Jeśli kanał był zmieniany z używania aliasu CipherSpec na używanie mechanizmu AT-TLS, kanał połączenia z klientem będzie używał strategii z produktu “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpecs” na stronie 500 , a kanał połączenia z serwerem będzie używał strategii z produktu “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec” na stronie 509.

Scenariusz 3

Między menedżerem kolejek systemu IBM MQ for z/OS a menedżerem kolejek działającym w systemie IBM MQ for Multiplatforms, w którym menedżer kolejek systemu IBM MQ for z/OS używa protokołu AT-TLS, a menedżer kolejek systemu IBM MQ for Multiplatforms używa protokołu IBM MQ TLS, określając atrybut SSLCIPH z pojedynczą nazwą CipherSpec. Dotyczy to wszystkich typów kanałów komunikatów innych niż cluster-sender i cluster-receiver.

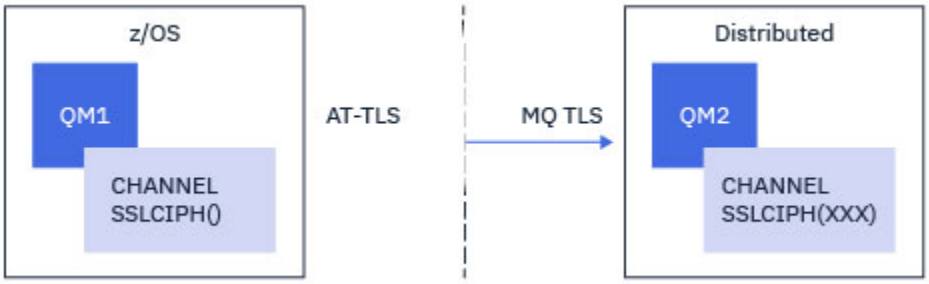


Sekcja “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek produktu IBM MQ for Multiplatforms przy użyciu pojedynczej, nazwanej CipherSpec” na stronie 496 zawiera przykładową konfigurację AT-TLS dla kanałów wychodzących z menedżera kolejek IBM MQ for z/OS do menedżera kolejek IBM 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 505 przykładową konfigurację AT-TLS dla kanałów przychodzących z menedżera kolejek IBM MQ for Multiplatforms do menedżera kolejek IBM MQ for z/OS .

Tej samej konfiguracji mechanizmu AT-TLS można użyć, gdy oba menedżery kolejek znajdują się w systemie z/OS, ale menedżer kolejek po prawej stronie nie został skonfigurowany do używania mechanizmu AT-TLS.

Scenariusz 4

Między menedżerem kolejek produktu IBM MQ for z/OS a menedżerem kolejek działającym w systemie IBM MQ for Multiplatforms, gdzie menedżer kolejek produktu IBM MQ for z/OS używa protokołu AT-TLS, a menedżer kolejek produktu IBM MQ for Multiplatforms używa protokołu TLS produktu IBM MQ , określając atrybut SSLCIPH z aliasem CipherSpec. Dotyczy to wszystkich typów kanałów komunikatów innych niż cluster-sender i cluster-receiver.

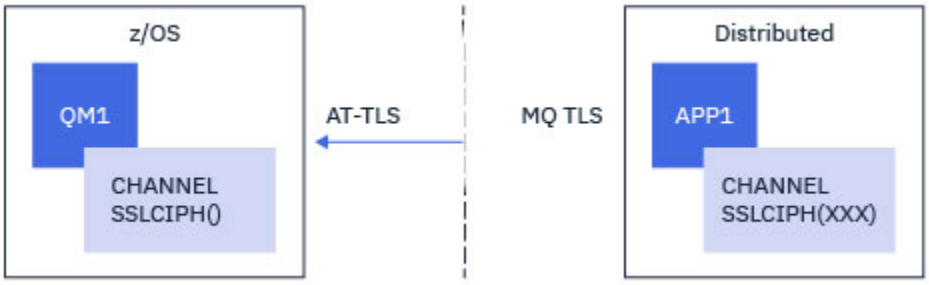


Przykład konfiguracji AT-TLS dla kanałów wychodzących z menedżera kolejek IBM MQ for z/OS do menedżera kolejek IBM MQ for Multiplatforms oraz “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec” na stronie 509i “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec” na stronie 509 dla przykładowej konfiguracji AT-TLS dla kanałów przychodzących z menedżera kolejek IBM MQ for Multiplatforms do menedżera kolejek IBM MQ for z/OS zawiera sekcja “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpecs” na stronie 500 .

Tej samej konfiguracji mechanizmu AT-TLS można użyć, gdy oba menedżery kolejek znajdują się w systemie z/OS, ale menedżer kolejek po prawej stronie nie został skonfigurowany do używania mechanizmu AT-TLS.

Scenariusz 5

Między menedżerem kolejek produktu IBM MQ for z/OS a 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 TLS produktu IBM MQ , określając atrybut SSLCIPH z pojedynczym atrybutem o nazwie CipherSpec.

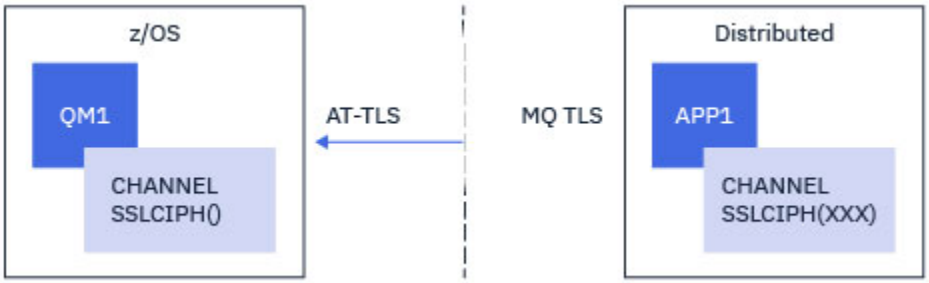


W tym scenariuszu wymagana jest jedna strategia AT-TLS, która spełnia te same wymagania, co strategia używana przez kanał komunikatów przychodzących (patrz sekcja “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu pojedynczej specyfikacji szyfrowania o nazwie CipherSpec” na stronie 505).

Ta sama konfiguracja mechanizmu AT-TLS może być używana, gdy aplikacja kliencka jest aplikacją Java i działa również w systemie z/OS, ale nie została skonfigurowana do używania mechanizmu AT-TLS.

Scenariusz 6

Między menedżerem kolejek produktu IBM MQ for z/OS a 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 TLS produktu IBM MQ , określając atrybut SSLCIPH z aliasem CipherSpec.



W tym scenariuszu wymagana jest jedna strategia AT-TLS, która spełnia te same wymagania, co strategia używana przez kanał komunikatów przychodzących (patrz sekcja “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec” na stronie 509).

Ta sama konfiguracja mechanizmu AT-TLS może być używana, gdy aplikacja kliencka jest aplikacją Java i działa również w systemie z/OS, ale nie została skonfigurowana do używania mechanizmu AT-TLS.

Ograniczenia

IBM MQ for z/OS nie rozpoznaje mechanizmu AT-TLS, dlatego istnieje kilka ograniczeń, które mają zastosowanie w poprzednich scenariuszach:

- Protokół AT-TLS w połączeniu z protokołem IBM MQ TLS nie działa w przypadku kanałów nadawczych i odbierających klastry.
- Menedżery kolejek systemu IBM MQ for z/OS nie mają informacji o użyciu protokołu AT-TLS i nie otrzymują żadnych informacji o certyfikacie od partnerskiego menedżera kolejek lub klienta. Dlatego następujące atrybuty nie mają wpływu na stronę kanału z/OS korzystającą z mechanizmu AT-TLS:
  - Atrybuty kanału SSLCAUTH i SSLPEER
  - Atrybut menedżera kolejek SSLRKEYC
  - Atrybuty SSLPEERMAP reguł CHLAUTH
- Ponowne negocjowanie klucza tajnego TLS wymaga, aby obie strony kanału używały protokołu TLS produktu IBM MQ . Dlatego w przypadku nawiązywania połączenia z menedżerem kolejek produktu IBM MQ for z/OS przy użyciu protokołu AT-TLS nie należy włączać renegocjacji klucza tajnego TLS w przypadku menedżera kolejek produktu IBM MQ for Multiplatforms lub klienta.

  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 na ten temat zawiera sekcja “Resetowanie kluczy tajnych SSL i TLS” na stronie 514.

Instrukcje konfiguracyjne AT-TLS

Protokół AT-TLS jest konfigurowany przy użyciu zestawu instrukcji. W scenariuszach opisanych w tym temacie używane są następujące elementy:

TTLSRule (opcja 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.

TTLSEnvironmentAction
Określa szczegółową konfigurację odwołania TTLSRule i odwołuje się do wielu innych instrukcji.

TTLSKeyringParms
Odwołuje się do pliku kluczy, który ma być używany przez mechanizm AT-TLS.

TTLSCipherParms
Definiuje zestawy algorytmów szyfrowania, które mają być używane.

TTLSEnvironmentAdvancedParms
Definiuje, które protokoły TLS lub SSL są włączone.

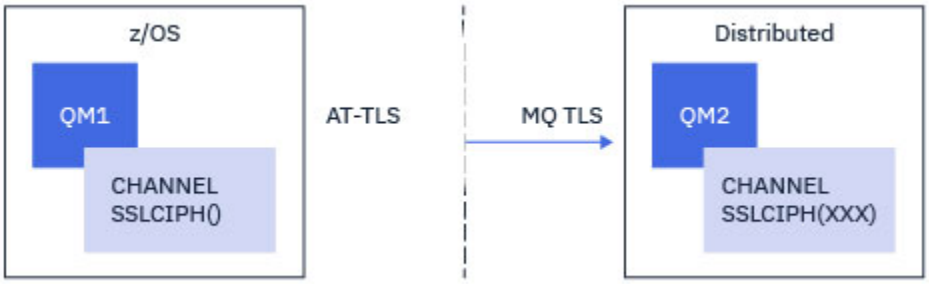
Ostrzeżenie: Istnieją inne instrukcje strategii AT-TLS z AT-TLS, które nie zostały opisane w tej sekcji i mogą być używane z produktem IBM MQ w zależności od potrzeb. Jednak produkt IBM MQ został przetestowany tylko ze strategiami opisanymi w tym temacie.

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.

Przykład użycia aliasu CipherSpeczawiera sekcja “Konfigurowanie protokołu AT-TLS w kanale wychodzącym do menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpecs” na stronie 500 .

W tym przykładzie istniejąca para kanałów nadawczych i odbiorczych, która używa protokołu TLS 1.3 TLS_AES_256_GCM_SHA384 CipherSpec , zostanie dopasowana w taki sposób, aby kanał nadawczy używał protokołu AT-TLS zamiast 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 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 272.

```
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 kolumny kodu szesnastkowego z rozszerzoną kolumną znaków z tabeli 2 w temacie dotyczącym instrukcji TTLSCipherParms .

Tabela 83. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0			
CipherSpec	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Tak
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Tak
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Tak
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Tak
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Tak
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Tak
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Tak
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Tak
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Tak
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Tak
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Tak
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Tak
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Tak
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Nie
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Nie
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Nie
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Nie
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Nie
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0009	Nie
TRIPLE_DES_SHA_US	SSL 3	000A	Nie
RC4_SHA_US	SSL 3	0005	Nie
RC4_MD5_US	SSL 3	0004	Nie

Tabela 83. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0 (kontynuacja)			
CipherSpec	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
DES_SHA_EXPORT	SSL 3	0009	N
RC4_MD5_EXPORT	SSL 3	0003	Nie
RC2_MD5_EXPORT	SSL 3	0006	Nie
NULL_SHA	SSL 3	0002	Nie
NULL_MD5	SSL 3	0001	Nie

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_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         OFF
  TLSv1.3         ON
}
```

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_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(SDR) SSLCIPH(' ')
```

Krok 4: Uruchamianie kanału

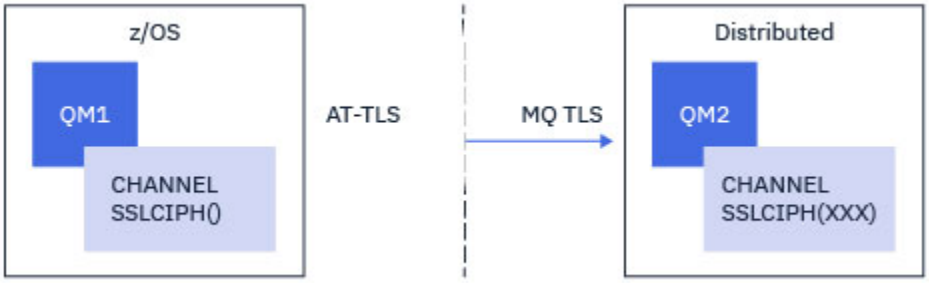
Po uruchomieniu kanału zostanie użyta kombinacja protokołów AT-TLS i IBM MQ TLS.

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 protokołu AT-TLS w kanale wychodzącym do menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpecs

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 z atrybutem SSLCIPH ustawionym na alias CipherSpec .

W tym przykładzie istniejąca para kanałów nadawca-odbiorca, która używa aliasu ANY_TLS13 CipherSpec , zostanie dopasowana w taki sposób, aby kanał nadawczy używał protokołu AT-TLS zamiast IBM MQ TLS.



Innych protokołów TLS i CiperSpecs 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 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 272.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Instrukcja TTLSCipherParms powiązana z `TTLSEnvironmentAction` przez właściwość **TTLSCipherParmsRef** .

   Ta instrukcja musi zawierać jedną lub więcej nazw zestawów algorytmów szyfrowania, z których co najmniej jedna powinna być zgodna z zestawem CipherSpecs określonym przez alias CipherSpec używany 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 kolumny kodu szesnastkowego z rozszerzoną kolumną znaków z tabeli 2 w temacie TTLSCipherParms .

Tabela 84. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0

CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Tak
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Tak
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Tak
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Tak
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Tak
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Tak
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Tak
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Tak
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Tak

Tabela 84. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0 (kontynuacja)			
CipherSpec	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Tak
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Tak
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Tak
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Tak
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Nie
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Nie
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Nie
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Nie
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Nie
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0009	Nie
TRIPLE_DES_SHA_US	SSL 3	000A	Nie
RC4_SHA_US	SSL 3	0005	Nie
RC4_MD5_US	SSL 3	0004	Nie
DES_SHA_EXPORT	SSL 3	0009	N
RC4_MD5_EXPORT	SSL 3	0003	Nie
RC2_MD5_EXPORT	SSL 3	0006	Nie
NULL_SHA	SSL 3	0002	Nie
NULL_MD5	SSL 3	0001	Nie

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256
}
```

Ostrzeżenie: Jeśli zarówno menedżer kolejek, jak i strategia AT-TLS obsługują protokół TLS 1.3, tylko alias CipherSpecs , który zawiera co najmniej jedną specyfikację TLS 1.3 CipherSpec , umożliwia uruchomienie kanału. Na przykład użycie opcji ANY_TLS12 powoduje, że uruchomienie kanału nie powiedzie się, nawet jeśli parametr TTLSCipherParms zawiera TLS 1.2 CipherSpecs, ale użycie opcji ANY_TLS12_OR_HIGHER lub ANY_TLS13 umożliwia uruchomienie kanału. Wyjaśnienie znajduje się w sekcji “Relacja między ustawieniami CipherSpec aliasu” na stronie 487 .

6. Instrukcja TTLSEnvironmentAdvancedParms jest powiązana z TTLSEnvironmentAction przez właściwość **TTLSEnvironmentAdvancedParmsRef** .

   Tej instrukcji można użyć do określenia, które protokoły SSL i TLS są włączone i powinny być spójne z zestawami algorytmów szyfrowania w instrukcji TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

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_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256

}

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(SDR) SSLCIPH(' ')
```

Krok 4: Uruchamianie kanału

Po uruchomieniu kanału zostanie użyta kombinacja protokołów AT-TLS i IBM MQ TLS.

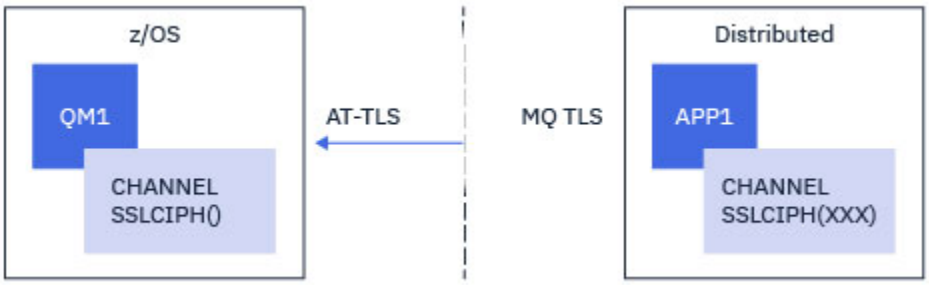
Ostrzeżenie: Wcześniejsze instrukcje AT-TLS są tylko minimalną konfiguracją. Istnieją inne instrukcje strategii AT-TLS z AT-TLS, które nie zostały opisane w tej sekcji i mogą być używane z produktem IBM MQ w zależności od potrzeb. Jednak produkt IBM MQ został przetestowany tylko z opisanymi strategiami.

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.

Przykład użycia aliasu CipherSpeczawiera sekcja “Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu CipherSpec” na stronie 509 .

W tym przykładzie istniejąca para kanałów nadawczych i odbiorczych, która używa protokołu TLS 1.3 TLS_AES_256_GCM_SHA384 CipherSpec , zostanie dopasowana w taki sposób, aby kanał odbiorczy używał protokołu AT-TLS zamiast 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 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 272.

```
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 kolumny kodu szesnastkowego z rozszerzoną kolumną znaków z tabeli 2 w temacie dotyczącym instrukcji TTLSCipherParms .

Tabela 85. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0

CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Tak
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Tak

Tabela 85. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0 (kontynuacja)

CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Tak
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Tak
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Tak
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Tak
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Tak
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Tak
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Tak
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Tak
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Tak
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Tak
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Tak
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Nie
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Nie
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Nie
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Nie
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Nie
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0009	Nie
TRIPLE_DES_SHA_US	SSL 3	000A	Nie
RC4_SHA_US	SSL 3	0005	Nie
RC4_MD5_US	SSL 3	0004	Nie
DES_SHA_EXPORT	SSL 3	0009	N
RC4_MD5_EXPORT	SSL 3	0003	Nie
RC2_MD5_EXPORT	SSL 3	0006	Nie

Tabela 85. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0 (kontynuacja)			
CipherSpec	**Protokół**	**Kod szesnastkowy**	**Domyślnie włączone**
NULL_SHA	SSL 3	0002	Nie
NULL_MD5	SSL 3	0001	Nie

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_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         OFF
  TLSv1.3         ON
}
```

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                   SERVER
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_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

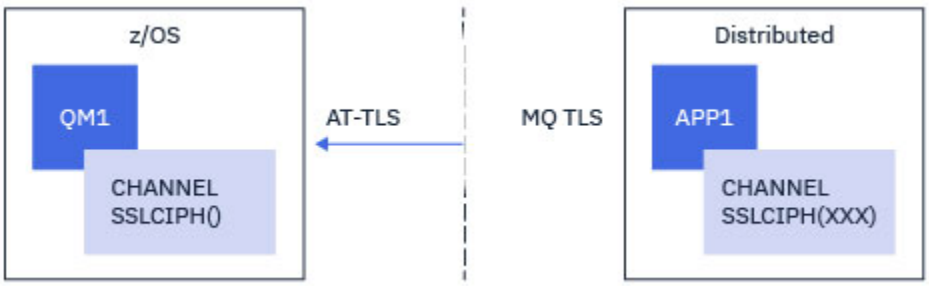
Po uruchomieniu kanału zostanie użyta kombinacja protokołów AT-TLS i IBM MQ TLS.

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.

Konfigurowanie mechanizmu AT-TLS w kanale przychodzącym z menedżera kolejek systemu IBM MQ for Multiplatforms przy użyciu aliasu 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 alias CipherSpec.

W tym przykładzie istniejąca para kanałów nadawca-odbiorca, która używa dowolnej CipherSpec protokołu TLS 1.3 , zostanie dopasowana w taki sposób, aby kanał odbiorczy używał protokołu AT-TLS zamiast IBM MQ TLS.



Innych protokołów TLS i CiperSpecs 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 272.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Instrukcja TTLSCipherParms powiązana z TTLSEnvironmentAction przez właściwość **TTLSCipherParmsRef** .

   Ta instrukcja musi zawierać co najmniej jedną nazwę zestawu algorytmów szyfrowania, która jest zawarta w aliasie CipherSpec ustawionym 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 kolumny kodu szesnastkowego z rozszerzoną kolumną znaków z tabeli 2 w temacie dotyczącym instrukcji TTLSCipherParms .

Tabela 86. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0

CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
TLS_CHACHA20_POLY1305_SHA256	TLS 1.3	1303	Tak
TLS_AES_256_GCM_SHA384	TLS 1.3	1302	Tak
TLS_AES_128_GCM_SHA256	TLS 1.3	1301	Tak
TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2	009D	Tak
ECDHE_RSA_AES_256_GCM_SHA384	TLS 1.2	C030	Tak
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2	003D	Tak
ECDHE_ECDSA_AES_256_CBC_SHA384	TLS 1.2	C024	Tak
ECDHE_RSA_AES_256_CBC_SHA384	TLS 1.2	C028	Tak

Tabela 86. CipherSpecs w systemie z/OS z serwisu IBM MQ for z/OS 9.2.0 (kontynuacja)

CipherSpec	Protokół	Kod szesnastkowy	Domyślnie włączone
TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2	009C	Tak
ECDHE_RSA_AES_128_GCM_SHA256	TLS 1.2	C02F	Tak
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2	003C	Tak
ECDHE_ECDSA_AES_128_CBC_SHA256	TLS 1.2	C023	Tak
ECDHE_RSA_AES_128_CBC_SHA256	TLS 1.2	C027	Tak
TLS_RSA_WITH_NULL_SHA256	TLS 1.2	003B	Nie
TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0	0035	Nie
TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0	002F	Nie
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0	000A	Nie
TLS_RSA_WITH_RC4_128_SHA	TLS 1.0	0005	Nie
TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	0009	Nie
TRIPLE_DES_SHA_US	SSL 3	000A	Nie
RC4_SHA_US	SSL 3	0005	Nie
RC4_MD5_US	SSL 3	0004	Nie
DES_SHA_EXPORT	SSL 3	0009	N
RC4_MD5_EXPORT	SSL 3	0003	Nie
RC2_MD5_EXPORT	SSL 3	0006	Nie
NULL_SHA	SSL 3	0002	Nie
NULL_MD5	SSL 3	0001	Nie

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256
}
```

Ostrzeżenie: Jeśli zarówno menedżer kolejek, jak i strategia AT-TLS obsługują protokół TLS 1.3, tylko alias CipherSpecs , który zawiera co najmniej jedną specyfikację TLS 1.3 CipherSpec , umożliwia uruchomienie kanału. Na przykład użycie opcji ANY_TLS12 powoduje, że uruchomienie kanału nie powiedzie się, nawet jeśli parametr TTLSCipherParms zawiera TLS 1.2 CipherSpecs, ale użycie opcji ANY_TLS12_OR_HIGHER lub ANY_TLS13 umożliwia

uruchomienie kanału. Wyjaśnienie znajduje się w sekcji “Relacja między ustawieniami CipherSpec aliasu” na stronie 487 .

6. Instrukcja TTLSEnvironmentAdvancedParms jest powiązana z TTLSEnvironmentAction przez właściwość **TTLSEnvironmentAdvancedParmsRef** .

   Tej instrukcji można użyć do określenia, które protokoły SSL i TLS są włączone i powinny być spójne z zestawami algorytmów szyfrowania w instrukcji TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

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                   SERVER
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_CHACHA20_POLY1305_SHA256
  V3CipherSuites            TLS_AES_256_GCM_SHA384
  V3CipherSuites            TLS_AES_128_GCM_SHA256

}

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(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.

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.

IBM i W systemie IBM inależy użyć komendy **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 KeyResetLicznik w strukturze MQSCO wywołania MQCONNX.
2. Za pomocą zmiennej środowiskowej **MQSSLRESET**.
3. Przez ustawienie atrybutu **SSLKeyResetCount** w sekcji SSL pliku konfiguracyjnego klienta.

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.

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 .NET klientów niezarządzanych właściwość liczby całkowitej **SSLKeyResetCount** wskazuje liczbę niezaszyfrowanych bajtów wysłanych i odebranych w ramach konwersacji TLS przed renegocjacją 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 w celu zachowania spójności z innymi klientami IBM MQ IBM MQ zarządzany klient .NET umożliwia aplikacjom ustawianie wartości parametru **SSLKeyResetCount**. 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)

WYŚWIETLANY MENEDŻER KOLEJEK

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 bezpieczeństwa

Wyjścia zabezpieczeń mogą odgrywać rolę w usłudze poufności, generując i dystrybuując klucz symetryczny na potrzeby szyfrowania i deszyfrowania danych, które przepływają przez kanał. W tym celu stosuje się powszechnie stosowaną technikę PKI.

Jedno wyjście zabezpieczeń generuje losową wartość danych, szyfruje ją za pomocą klucza publicznego menedżera kolejek lub użytkownika reprezentowanego przez partnerskie wyjście zabezpieczeń i wysyła zaszyfrowane dane do swojego partnera w komunikacie bezpieczeństwa. Program zewnętrzny zabezpieczeń partnera deszyfruje losową wartość danych przy użyciu klucza prywatnego reprezentowanego przez niego menedżera kolejek lub użytkownika. Każde wyjście zabezpieczeń może teraz korzystać z losowej wartości danych w celu uzyskania klucza symetrycznego niezależnie od drugiego za pomocą algorytmu znanego obu z nich. Alternatywnie mogą one użyć losowej wartości danych jako klucza.

Jeśli do tego czasu pierwsze wyjście zabezpieczeń nie uwierzytelnia swojego partnera, następny komunikat zabezpieczeń wysłany przez partnera może zawierać oczekiwaną wartość zaszyfrowaną za pomocą klucza symetrycznego. Pierwsze wyjście zabezpieczeń może teraz uwierzytelnić swojego partnera, sprawdzając, czy było w stanie poprawnie zaszyfrować oczekiwaną wartość.

Wyjścia zabezpieczeń mogą również użyć tej możliwości, aby uzgodnić algorytm szyfrowania i deszyfrowania danych, które przepływają przez kanał, jeśli dostępny jest więcej niż jeden algorytm.

Implementowanie poufności w wyjściach komunikatów

Wyjście komunikatu na wysyłającym końcu kanału może zaszyfrować 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 w tym celu. Więcej informacji na temat sposobu generowania i dystrybuowania klucza symetrycznego zawiera sekcja “Implementowanie poufności w programach obsługi wyjścia użytkownika” na stronie 515.

Nagłówki w komunikacie, takie jak nagłówek kolejki transmisji MQXQH, który zawiera osadzony deskryptor komunikatu, nie mogą być szyfrowane przez wyjście komunikatu. Jest to spowodowane tym, że konwersja danych nagłówków komunikatów odbywa się po wywołaniu wyjścia komunikatu na końcu wysyłającym lub przed wywołaniem wyjścia komunikatu na końcu odbierającym. Jeśli nagłówki są zaszyfrowane, konwersja danych nie powiedzie się i kanał zostanie zatrzymany.

Implementowanie poufności w wyjściach wysyłania i odbierania

Wyjścia nadawcze i odbiorcze mogą być używane do szyfrowania i deszyfrowania danych przepływających przez kanał. Są one bardziej odpowiednie niż wyjścia komunikatów do obsługi tej usługi z następujących powodów:

- W kanale komunikatów nagłówki komunikatów mogą być szyfrowane, a także dane aplikacji w komunikatach.
- Wyjścia nadawcze i odbiorcze mogą być używane zarówno w kanałach MQI, jak i w kanałach komunikatów. Parametry wywołań MQI mogą zawierać wrażliwe dane aplikacji, które muszą być chronione podczas przepływu w kanale MQI. Dlatego w obu kanałach można używać tych samych wyjść wysyłania i odbierania.

Implementowanie poufności w wyjściu funkcji API i wyjściu funkcji API

Dane aplikacji w komunikacie mogą być szyfrowane przez interfejs API lub wyjście przekraczające API, gdy komunikat jest umieszczany przez aplikację wysyłającą, i deszyfrowane 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, gdzie wielu użytkowników może wysyłać komunikaty do siebie, problem polega na tym, jak zapewnić, że tylko zamierzony odbiorca komunikatu jest w stanie zdeszyfrować komunikat. Jednym z rozwiązań jest użycie innego klucza symetrycznego dla każdej pary użytkowników, którzy wysyłają do siebie komunikaty. Jednak administrowanie tym rozwiązaniem może być trudne i czasochłonne, zwłaszcza jeśli użytkownicy należą

do różnych organizacji. Standardowym sposobem rozwiązania tego problemu jest użycie technologii PKI (*digital envelope oping*).

Gdy aplikacja umieszcza komunikat w kolejce, funkcja API lub wyjście przekraczające API generuje losowy klucz symetryczny i używa tego klucza do szyfrowania danych aplikacji w komunikacie. Wyjście szyfruje klucz symetryczny za pomocą klucza publicznego zamierzonego odbiornika. Następnie dane aplikacji w komunikacie są zastępowane zaszyfrowanymi danymi aplikacji i zaszyfrowanym kluczem symetrycznym. W ten sposób tylko zamierzony odbiorca może deszyfrować klucz symetryczny, a tym samym dane aplikacji. Jeśli zaszyfrowany komunikat ma więcej niż jeden potencjalny zamierzony odbiornik, wyjście może zaszyfrować kopię klucza symetrycznego dla każdego zamierzonego odbiorcy.

Jeśli dostępne są różne algorytmy szyfrowania i deszyfrowania danych aplikacji, wyjście może zawierać nazwę używanego algorytmu.

z/OS Poufność danych przechowywanych w systemie IBM MQ for z/OS z szyfrowaniem zestawu danych

Produkt IBM MQ for z/OS może zatwardzić dane klienta i dane konfiguracyjne, zapisując dane w zestawach danych aktywnego dziennika, zestawach danych dziennika archiwalnego, zestawach stron, zestawach danych programu startowego (BSDS) i zestawach danych współużytkowanego komunikatu (SMDS).

Produkt z/OS zapewnia wydajne, oparte na strategiach szyfrowanie zestawów danych. IBM MQ for z/OS obsługuje szyfrowanie zestawu danych z/OS dla:

- Aktywne zestawy danych dziennika; patrz uwaga “1” na stronie 517
- Archiwalne zestawy danych dziennika; patrz uwaga “2” na stronie 517
- Zestawy stron; patrz uwaga “1” na stronie 517
- BSDS; patrz uwaga “2” na stronie 517
- Zestawy danych CSQINP*; patrz uwaga “2” na stronie 517
- SMDS; patrz uwaga “1” na stronie 517

Zapewnia to poufność danych przechowywanych w pojedynczym menedżerze kolejek systemu z/OS .

Uwagi:

1. W produkcie IBM MQ for z/OS 9.2.0szyfrowanie zestawu danych z/OS dla aktywnych dzienników. obsługiwane są zestawy stron i zestawy SMDS.
2. Szyfrowanie zestawów danych dla dzienników archiwalnych, zestawów danych BSDS i CSQINP* jest obsługiwane we wszystkich wersjach systemu IBM MQ for z/OS.
3. IBM MQ Advanced Message Security udostępnia alternatywny mechanizm ochrony danych w spoczynku. Ponadto produkt AMS chroni również dane w pamięci i w trakcie przesyłania.

Więcej informacji na temat szyfrowania zestawu danych z/OS zawiera sekcja Korzystanie z rozszerzeń szyfrowania zestawu danych systemu z/OS .

Konfiguracja szyfrowania zestawu danych z/OS jest poza kontrolą produktu IBM MQ for z/OS. Ustawienia szyfrowania są uwzględniane podczas tworzenia zestawu danych.

Oznacza to, że wszystkie istniejące zestawy danych muszą zostać ponownie utworzone przed użyciem nowej strategii szyfrowania zestawu danych.

Produkt IBM MQ for z/OS może działać z kombinacją zaszyfrowanych i niezaszyfrowanych zestawów danych, ale standardowa konfiguracja zaszyfruje wszystkie używane zestawy danych lub nie zaszyfruje żadnego z nich.

z/OS Przegląd kroków szyfrowania zestawu danych IBM MQ for z/OS

Sposób szyfrowania zestawu danych IBM MQ for z/OS .

Zanim rozpoczniesz

Należy upewnić się, że w przedsiębiorstwie poprawnie skonfigurowano szyfrowanie zestawu danych z/OS . Jeśli szyfrowanie zestawu danych jest konfigurowane w grupie współużytkowania kolejek, należy skonfigurować szyfrowanie zestawu danych z/OS na potrzeby współużytkowania danych.

Uwaga: Zaszyfrowany zestaw danych z/OS musi być zestawem danych w formacie rozszerzonym.

Procedura

1. Skonfiguruj klucz szyfrowania i `key-label` w RACF do szyfrowania zestawu danych.
2. Utwórz profil dla `key-label` w klasie RACF CSFKEYS.
3. Nadaj prawo do odczytu identyfikatora użytkownika menedżera kolejek i wszystkich innych identyfikatorów użytkowników, które wymagają dostępu do zaszyfrowanych danych.

   Może to obejmować identyfikatory użytkowników, które są używane do uruchamiania programów narzędziowych do drukowania dla zestawu danych. Na przykład użytkownik uruchamiający program CSQUTIL SCOPY będzie musiał zdeszyfrować odpowiedni zestaw stron.
4. Powiąż szyfrowanie `key-label` z nazwą zestawu danych.

   Można to zrobić za pomocą klasy danych SMS lub segmentu DFP RACF dla nazwy zestawu danych lub kwalifikatora wysokiego poziomu.

   Można również powiązać `key-label` z zestawem danych po przydzieleniu zestawu danych.
5. Zmień nazwę istniejącego zestawu danych za pomocą IDCAMS ALTER.
6. Ponownie przydziel zestaw danych z odpowiednimi atrybutami.
7. Skopiuj zawartość zestawu danych o zmienionej nazwie do nowego zestawu danych za pomocą IDCAMS REPRO.

   Dane są szyfrowane przez działanie kopiowania ich do zestawu danych.
8. Powtórz kroki od “4” na stronie 518 do “6” na stronie 518 dla wszystkich innych zestawów danych, które wymagają szyfrowania.

z/OS 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 dla 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.DS002itd.
- Środowisko sprzętowe i programowe może korzystać z szyfrowania zestawu danych z/OS .
- Narzędzie RACF jest używane jako narzędzie SAF.
- Menedżer kolejek został zatrzymany

Procedurę należy przeprowadzić w następującej kolejności:

1. “Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek” na stronie 518
2. “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 519

z/OS Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek

Sposób konfigurowania klucza szyfrowania zestawu danych dla menedżera kolejek.

O tym zadaniu

To zadanie jest wymaganiem wstępnym dla produktu “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 519.

Procedura

1. Skonfiguruj klucz DATA szyfrowania bitowego AES-256 z etykietą, na przykład CSQ1DSKY, używając z/OS program narzędziowy generatora kluczy (key generator utility program-KGUP).
2. Zdefiniuj profil RACF CSFKEYS dla klucza szyfrowania CSQ1DSKY , wydając następującą komendę:

   ```
   RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
   ```

3. Skonfiguruj segment ICSF profilu, aby umożliwić użycie klucza jako klucza zabezpieczonego, wprowadzając następującą komendę:

   ```
   RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
   ```

4. Zezwól menedżerowi kolejek na użycie klucza szyfrowania, nadając użytkownikowi QMCSQ1 dostęp do odczytu do profilu, wprowadzając następującą komendę:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Przyznaj te same prawa dostępu każdemu użytkownikowi administracyjnemu, który musi odczytać lub zapisać zaszyfrowany zestaw danych.
5. Odśwież klasę CSFKEYS, wydając następującą komendę.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Co dalej

Skonfiguruj szyfrowanie zestawów danych zgodnie z opisem w sekcji “Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika” na stronie 519

z/OS Konfigurowanie szyfrowania zestawu danych dla zestawów danych dziennika

Sposób konfigurowania szyfrowania w zestawach danych dziennika.

Zanim rozpoczniesz

Należy zapoznać się z następującymi informacjami:

Przegląd kroków szyfrowania IBM MQ for z/OS zestawu danychi wykonanie procedury w “Konfigurowanie klucza szyfrowania zestawu danych dla menedżera kolejek” na stronie 518

O tym zadaniu

W tej metodzie używany jest segment DFP profilu ogólnego RACF , dzięki czemu można używać klucza szyfrowania dla wszystkich nowych zestawów danych zgodnych z profilem.

Alternatywnie można skonfigurować i użyć klasy danych SMS lub bezpośrednio określić etykietę klucza podczas przydzielania zestawu danych.

Jak opisano wcześniej, w tym przykładzie menedżer kolejek CSQ1 jest uruchamiany dla użytkownika QMCSQ1i ma aktywne zestawy danych dziennika CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002itd.

Procedura

1. Utwórz profil ogólny, jeśli nie istnieje, wydając następującą komendę:

```
ADDSD 'CSQ1.LOGS.*' UACC(NONE)
```

2. Zezwól użytkownikowi menedżera kolejek na zmianę dostępu do profilu, wydając następującą komendę:

```
PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
```

   Należy również zezwolić każdemu użytkownikowi administracyjnemu na odpowiedni dostęp.

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 był używany podczas konfigurowania 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 przy użyciu programu IDCAMS. Następujący fragment JCL przekształca CSQ1.LOGS.LOGCOPY1.DS001:

   a) Zmień nazwę zestawu danych na kopię zapasową

```
//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) Ponownie zdefiniuj zestaw danych.

   Nowy zestaw danych zostanie zaszyfrowany z powodu profilu RACF .

   Uwaga: Zastąp + + EXTDCLASS + + nazwą klasy danych w formacie rozszerzonym, 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 utworzonego zestawu danych.

   W tym kroku dane są szyfrowane:

```
//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 520 dla wszystkich zestawów danych aktywnego dziennika.

Wymagany jest tylko jeden klucz szyfrowania, a wszystkie zestawy danych mogą być powiązane z tą samą etykietą klucza.

Zrestartuj menedżer kolejek CSQ1. Użyj danych wyjściowych komendy DISPLAY LOG , aby sprawdzić, czy zestawy danych dziennika zostały zaszyfrowane.

z/OS Uwagi dotyczące szyfrowania zestawu danych z/OS w grupie współużytkowania kolejek

Każdy menedżer kolejek w grupie współużytkowania kolejek (QSG) musi mieć możliwość odczytu protokołów, BSDS i współużytkowanych zestawów danych komunikatów (SMDS) każdego innego menedżera kolejek w grupie QSG.

Oznacza to, że każdy system, w którym może działać element grupy QSG, musi spełniać wymagania dotyczące szyfrowania zestawu danych z/OS , a wszystkie etykiety kluczy i klucze szyfrowania używane do ochrony zestawów danych dla każdego menedżera kolejek w grupie QSG muszą być dostępne w każdym systemie.

Menedżer kolejek w wersjach wcześniejszych niż IBM MQ for z/OS 9.1.4 nie może uzyskać dostępu do zaszyfrowanego zestawu danych aktywnego dziennika.

Menedżer kolejek w wersjach wcześniejszych niż IBM MQ for z/OS 9.1.5 nie może uzyskać dostępu do zaszyfrowanego zestawu SMDS.

Przed użyciem szyfrowania zestawu danych z/OS należy przeprowadzić migrację wszystkich menedżerów kolejek w grupie QSG do co najmniej IBM MQ for z/OS 9.1.5.

Jeśli menedżer kolejek w systemie QSG został uruchomiony z dowolnym szyfrowanym aktywnym zestawem danych dziennika, a inny menedżer kolejek w systemie QSG został uruchomiony, ale nie został ostatnio uruchomiony z wersją programu IBM MQ for z/OS , która obsługuje szyfrowane aktywne dzienniki, menedżer kolejek z szyfrowanym aktywnym dziennikiem zostanie nieprawidłowo zakończony z kodem nieprawidłowego zakończenia 5C6-00F50033.

Można przekształcić QSG, aby używać szyfrowanych protokołów aktywnych i SMDS bez pełnego wyłączenia, poprzez:

1. Migracja każdego menedżera kolejek do co najmniej IBM MQ for z/OS 9.1.5 po kolei.
2. Kolejno przekształcanie aktywnych dzienników w zaszyfrowane zestawy danych dla każdego menedżera kolejek. Wymaga to zamknięcia i zrestartowania menedżera kolejek.

   Jednocześnie jest prawdopodobne, że zestawy stron i dzienniki archiwalne również będą włączone dla szyfrowanych zestawów danych, ale nie ma to wpływu na migrację QSG.

   Procedura przekształcania poszczególnych zestawów danych została opisana w sekcji “Przykład szyfrowania aktywnych dzienników menedżera kolejek” na stronie 518
3. Przekształcanie zestawów SMDS w szyfrowane zestawy danych dla każdej struktury CF w następujący sposób:
   a. Wprowadzenie komendy RESET SMDS (*) ACCESS (DISABLED) CFSTRUCT (nazwa struktury) w celu zawieszenia dostępu menedżera kolejek do SMDS.

      Należy zauważyć, że w tym czasie dane we współużytkowanych kolejkach powiązanych z SMDS są tymczasowo niedostępne.
   b. Przekształcenie każdego zestawu danych, który składa się na zestaw SMDS, w szyfrowane zestawy danych, przy użyciu procedury opisanej w sekcji “Przykład szyfrowania aktywnych dzienników menedżera kolejek” na stronie 518.
   c. Wprowadzenie komendy RESET SMDS (*) ACCESS (ENABLED) CFSTRUCT (nazwa struktury) w celu wznowienia dostępu menedżera kolejek do SMDS.

Ostrzeżenie: Przed przekształceniem dzienników należy całkowicie wyłączyć menedżer kolejek, a odtwarzanie struktury narzędzia CF może nie być możliwe podczas konwersji, ponieważ aktywne zestawy danych dziennika będą tymczasowo niedostępne.

z/OS 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
- 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:

- SMDS
- Zestaw stron i
- Aktywny dziennik

Zestawy danych, ponieważ są one używane z szyfrowaniem zestawu danych z/OS , nie są obsługiwane w produkcie IBM MQ for z/OS 9.1.0i wcześniejszych wersjach obsługi długoterminowej.

Przed migracją wsteczną wszystkie strategie szyfrowania dla zestawów SMDS, zestawów stron i zestawów danych dziennika aktywnego muszą zostać usunięte, a dane zdeszyfrowane. Ten proces jest opisany w sekcji “Usuwanie szyfrowania zestawu danych z zestawu danych” na stronie 522.

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 524 .

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 SMDS i zestawów stron.

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 poddany migracji wstecznej do wersji produktu IBM MQ for z/OS , która nie obsługuje szyfrowania zestawu danych, wszystkie aktywne zestawy danych dziennika i zestaw SMDS wszystkich menedżerów kolejek w grupie QSG muszą zostać usunięte strategie szyfrowania zestawu danych, a ich dane 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 522.

   Jeśli menedżer kolejek ma być migrowany wstecz, jego zestaw stron również powinien zostać zdeszyfrowany w tym momencie. Następnie zrestartuj menedżer kolejek.
2. 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 522 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 522 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

Zestaw danych	Błąd, jeśli menedżer kolejek nie obsługuje szyfrowania zestawu danych systemu z/OS
SMDS	Komunikat IEC161I-122 został zarejestrowany w dzienniku "Zestaw danych ma etykietę KEYLABEL, ale użytkownik nie określił, że aplikacja może obsługiwać szyfrowanie". SMDS oznaczył AVAIL (BŁĄD).

Integralność danych komunikatów

W celu zachowania integralności danych można użyć różnych typów programu obsługi wyjścia użytkownika, aby udostępnić dla komunikatów skróty komunikatów lub podpisy cyfrowe.

Integralność danych

Implementowanie integralności danych w komunikatach

Jeśli używany jest protokół TLS, wybór opcji CipherSpec określa poziom integralności danych w przedsiębiorstwie. Jeśli używana jest usługa AMS (IBM MQ Advanced Message Service), można określić integralność dla unikalnego komunikatu.

Implementowanie integralności danych w wyjściach komunikatów

Komunikat może być podpisany cyfrowo przez wyjście komunikatu na wysyłającym końcu kanału. Podpis cyfrowy może być następnie sprawdzany przez wyjście komunikatu na odbierającym końcu kanału w celu wykrycia, czy komunikat został celowo zmodyfikowany.

Niektóre zabezpieczenia można zapewnić za pomocą skrótu wiadomości zamiast podpisu cyfrowego. Skrót wiadomości może być skuteczny w przypadku nieformalnych lub niedyskryminujących manipulacji, ale nie uniemożliwia bardziej poinformowanym osobom zmiany lub wymiany wiadomości i generowania dla niej zupełnie nowego streszczenia. Jest to szczególnie istotne, jeśli algorytm używany do generowania streszczenia komunikatu jest dobrze znany.

Implementowanie integralności danych w wyjściach wysyłania i odbierania

W kanale komunikatów wyjścia komunikatów są bardziej odpowiednie do udostępniania tej usługi, ponieważ wyjście komunikatów ma dostęp do całego komunikatu. W przypadku kanału MQI parametry w wywołaniach MQI mogą zawierać dane aplikacji, które muszą być chronione i tylko wyjścia nadawcze i odbiorcze mogą zapewnić tę ochronę.

Implementowanie integralności danych w wyjściu funkcji API lub wyjściu funkcji API

Komunikat może być podpisany cyfrowo przez funkcję API lub wyjście przekraczające funkcję API, gdy komunikat jest umieszczany przez aplikację wysyłającą. Podpis cyfrowy może być następnie sprawdzany przez drugie wyjście podczas pobierania komunikatu przez aplikację odbierającą w celu wykrycia, czy komunikat został celowo zmodyfikowany.

Niektóre zabezpieczenia można zapewnić za pomocą skrótu wiadomości zamiast podpisu cyfrowego. Skrót wiadomości może być skuteczny w przypadku nieformalnych lub niedyskryminujących manipulacji, ale nie uniemożliwia bardziej poinformowanym osobom zmiany lub wymiany wiadomości i generowania dla niej zupełnie nowego streszczenia. Jest to szczególnie istotne, jeśli algorytm używany do generowania streszczenia komunikatu jest dobrze znany,

Więcej informacji

Więcej informacji na temat zapewniania integralności danych zawiera sekcja “Włączanie CipherSpecs” na stronie 466 .

Zadania pokrewne

Łączenie dwóch menedżerów kolejek przy użyciu protokołu TLS

Bezpieczne łączenie klienta z menedżerem kolejek

Kontrola

Za pomocą komunikatów o zdarzeniach można sprawdzić, czy nie wystąpiły włamania lub próby włamania. Bezpieczeństwo systemu można również sprawdzić za pomocą konsoli IBM MQ Explorer.

Aby wykryć próby wykonania nieautoryzowanych działań, takich jak nawiązanie połączenia z menedżerem kolejek lub umieszczenie komunikatu w kolejce, należy sprawdzić komunikaty zdarzeń wygenerowane przez menedżery kolejek, w szczególności komunikaty zdarzeń uprawnień. Więcej informacji na temat komunikatów zdarzeń menedżera kolejek zawiera sekcja Zdarzenia menedżera kolejek, a więcej informacji na temat monitorowania zdarzeń zawiera sekcja Monitorowanie zdarzeń.

Zabezpieczanie klastrów

Autoryzuj lub zablokuj dołączanie menedżerów kolejek do klastrów lub umieszczanie komunikatów w kolejkach klastrów. Wymuś opuszczenie klastra przez menedżer kolejek. Podczas konfigurowania protokołu TLS dla klastrów należy wziąć pod uwagę pewne dodatkowe zagadnienia.

Zatrzymywanie nieautoryzowanych menedżerów kolejek wysyłających komunikaty

Należy uniemożliwić nieautoryzowanym menedżerom kolejek wysyłanie komunikatów do menedżera kolejek przy użyciu wyjścia zabezpieczeń kanału.

Zanim rozpoczniesz

Łączenie w klastry 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

Zapobiegaj wysyłaniu komunikatów do menedżera kolejek przez wybrane menedżery kolejek:

Procedura

1. Zdefiniuj program obsługi wyjścia zabezpieczeń kanału w definicji kanału CLUSRCVR .
2. Napisz program, który uwierzytelnia menedżery kolejek próbujące wysyłać komunikaty w kanale odbiorczym klastra i odmawia im dostępu, jeśli nie są autoryzowane.

Co dalej

Programy obsługi wyjścia zabezpieczeń kanału są wywoływane podczas inicjowania i kończenia MCA.

Zatrzymywanie nieautoryzowanych menedżerów kolejek umieszczanych w kolejkach

Użyj atrybutu uprawnienia do umieszczania kanału w kanale odbiorczym klastra, aby zatrzymać nieautoryzowane menedżery kolejek, które umieszczają komunikaty w kolejkach. Autoryzuj zdalny menedżer kolejek, sprawdzając identyfikator użytkownika w komunikacie przy użyciu programu RACF w systemie z/OSlub programu OAM na innych platformach.

O tym zadaniu

Dostęp do kolejek można kontrolować za pomocą narzędzi bezpieczeństwa platformy oraz mechanizmu kontroli dostępu w produkcie IBM MQ .

Procedura

1. Aby uniemożliwić niektórym menedżerom kolejek umieszczanie komunikatów w kolejce, należy użyć narzędzi bezpieczeństwa 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 atrybutu uprawnienia do umieszczania (put) PUTAUTw definicji kanału CLUSRCVR .

   Atrybut PUTAUT umożliwia określenie identyfikatorów użytkowników, które mają być używane do ustanawiania uprawnień do umieszczania komunikatów w kolejce.

   Dostępne są następujące opcje atrybutu PUTAUT :

   DEF
   Użyj domyślnego identyfikatora użytkownika. W systemie z/OSsprawdzenie może wymagać użycia zarówno identyfikatora użytkownika odebranego z sieci, jak i identyfikatora pochodzącego od użytkownika MCAUSER.

   CTX (CTX)
   Użyj identyfikatora użytkownika w informacjach o kontekście powiązanych z komunikatem. W systemie z/OS sprawdzenie może wymagać użycia identyfikatora użytkownika odebranego z sieci, identyfikatora pochodzącego od użytkownika MCAUSERlub obu tych elementów. Tej opcji należy użyć, jeśli odsyłacz jest zaufany i uwierzytelniony.

   ONLYMCA (tylko w systemie z/OS)
   Podobnie jak w przypadku DEF, ale żaden ID użytkownika odebrany z sieci nie jest używany. Tej opcji należy użyć, jeśli odsyłacz nie jest zaufany. Użytkownik chce zezwolić tylko na konkretny zestaw działań, które są zdefiniowane dla użytkownika MCAUSER.

   ALTMCA (tylko z/OS)
   Podobnie jak w przypadku CTX, ale żaden identyfikator użytkownika odebrany z sieci nie jest używany.

Autoryzowanie umieszczania komunikatów w zdalnych kolejkach klastra

W systemie z/OS należy skonfigurować autoryzację do umieszczania w kolejce klastra za pomocą komendy RACF. Na innych platformach autoryzuj dostęp do połączeń z menedżerami kolejek i umieszczaj je w kolejkach w tych menedżerach kolejek.

O tym zadaniu

Domyślnym zachowaniem jest wykonywanie kontroli dostępu do serwera SYSTEM.CLUSTER.TRANSMIT.QUEUE. Należy zauważyć, że to zachowanie ma zastosowanie nawet wtedy, gdy używanych jest wiele kolejek transmisji.

Specyficzne zachowanie opisane w tym temacie ma zastosowanie tylko wtedy, gdy atrybut **ClusterQueueAccessControl** w pliku qm.ini został skonfigurowany jako *RQMName*(zgodnie z opisem w sekcji Bezpieczeństwo), a menedżer kolejek został zrestartowany.

Procedura

- W systemie z/OSwydaj następujące komendy:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- W systemach AIX, Linux, and Windows wydaj następujące komendy:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- W systemie IBM iwydaj 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, a nie w innych kolejkach klastra.

Nazwy zmiennych mają następujące znaczenie:

QMgrName
Nazwa menedżera kolejek. W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejek.

GroupName
Nazwa grupy, której ma zostać nadany 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. Ustaw to uprawnienie, wykonując instrukcje podane w sekcji “Nadawanie uprawnień do umieszczania komunikatów w zdalnej kolejce klastra” na stronie 441.

Pojęcia pokrewne
Sekcja zabezpieczeń w pliku qm.ini

Blokowanie dołączania menedżerów kolejek do klastra

Jeśli obcy menedżer kolejek dołącza do klastra, trudno jest zapobiec odbieraniu komunikatów, które nie mają być odbierane.

Procedura

Aby upewnić się, że tylko niektóre autoryzowane menedżery kolejek dołączą do klastra, należy wybrać jedną z trzech technik:

- Korzystając z rekordów uwierzytelniania kanału, można zablokować połączenie kanału klastra na podstawie zdalnego adresu IP, nazwy zdalnego menedżera kolejek lub nazwy wyróżniającej TLS udostępnianej przez system zdalny.
- Napisz program obsługi wyjścia, aby uniemożliwić nieautoryzowanym menedżerom kolejek zapisywanie w programie SYSTEM.CLUSTER.COMMAND.QUEUE. Nie należy ograniczać dostępu do produktu SYSTEM.CLUSTER.COMMAND.QUEUE w taki sposób, aby żaden menedżer kolejek nie mógł do niego zapisywać, lub należy uniemożliwić dołączanie menedżera kolejek do klastra.
- Program obsługi wyjścia zabezpieczeń w definicji kanału CLUSRCVR .

Wyjścia zabezpieczeń w kanałach klastra

Dodatkowe uwagi dotyczące używania 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 pobiera on atrybuty

z odpowiedniej definicji kanału odbierającego klastry. Oryginalna definicja kanału nadawczego klastra zostanie nadpisana nowymi atrybutami, w tym atrybutem `SecurityExit` .

Procedura

1. Należy zdefiniować wyjście zabezpieczeń zarówno na końcu nadajnika klastra, jak i na końcu odbiornika klastra kanału.

   Początkowe połączenie musi zostać nawiązane z uzgadnianiem wyjścia zabezpieczeń, nawet jeśli nazwa wyjścia zabezpieczeń jest przesyłana z definicji odbiorcy klastra.
2. Sprawdź poprawność atrybutu `PartnerName` w strukturze `MQCXP` w wyjściu zabezpieczeń.

   Wyjście musi zezwalać na uruchomienie kanału tylko wtedy, gdy partnerski menedżer kolejek jest autoryzowany.
3. Zaprojektuj wyjście zabezpieczeń w definicji odbiornika klastra, które ma być inicjowane przez odbiorcę.
4. Jeśli zostanie on zaprojektowany jako inicjowany przez nadawcę, nieautoryzowany menedżer kolejek bez wyjścia zabezpieczeń może dołączyć do klastra, ponieważ nie są wykonywane żadne sprawdzenia zabezpieczeń.

   Przed zatrzymaniem i zrestartowaniem kanału można wysłać nazwę SCYEXIT z definicji odbiornika klastra i wykonać 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 odbiornika klastra.
6. Aby wyświetlić pierwotną definicję, użyj komendy:

   ```
   DISPLAY CHANNEL( channel name ) ALL
   ```
7. Może być konieczne zdefiniowanie wyjścia automatycznej definicji kanału `CHADEXIT`w menedżerze kolejek nadawcy klastra, jeśli menedżery kolejek znajdują się na różnych platformach.

   Użyj automatycznego wyjścia definicji kanału, aby ustawić atrybut `SecurityExit` na odpowiedni format dla platformy docelowej.
8. Wdróż i skonfiguruj program security-exit.

   z/OS **z/OS**

   Moduł ładujący wyjścia zabezpieczeń musi znajdować się w zestawie danych określonym w instrukcji `CSQXLIB DD` procedury przestrzeni adresowej inicjatora kanału.

   ALW **Systemy AIX, Linux, and Windows**

   - Biblioteka dołączana dynamicznie wyjścia zabezpieczeń musi znajdować się w ścieżce określonej w atrybucie SCYEXIT definicji kanału.
   - Biblioteka dołączana dynamicznie wyjścia automatycznego definiowania kanału musi znajdować się w ścieżce określonej w atrybucie `CHADEXIT` definicji menedżera kolejek.

Wymuszanie opuszczenia klastra przez niechciane menedżery kolejek

Wymuś, aby niepotrzebny menedżer kolejek opuścił klaster, wprowadzając komendę `RESET CLUSTER` w menedżerze kolejek repozytorium pełnego.

O tym zadaniu

Istnieje możliwość wymuszenia opuszczenia klastra przez niepożądanego menedżera kolejek. Jeśli na przykład menedżer kolejek został usunięty, ale jego kanały odbiorcze klastra są nadal zdefiniowane w klastrze. Możesz chcieć posprzątać.

Tylko menedżery kolejek pełnego repozytorium mają uprawnienia do wysuwania menedżera kolejek z klastra.

Uwaga: Chociaż użycie komendy RESET CLUSTER powoduje wymuszenie usunięcia menedżera kolejek z klastra, użycie samej komendy RESET CLUSTER nie uniemożliwia późniejszego ponownego dołączania menedżera kolejek do klastra. Aby upewnić się, że menedżer kolejek nie przyłączy się ponownie do klastra, należy wykonać kroki opisane w sekcji "Blokowanie dołączania menedżerów kolejek do klastra" na stronie 528.

Aby wysunąć menedżer kolejek OSLO z klastra NORWAY, wykonaj następującą procedurę:

Procedura

1. W menedżerze kolejek pełnego repozytorium wprowadź komendę:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Zamiast wartości QMNAME w komendzie można również 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

Menedżer kolejek, który został usunięty z wymuszenia, nie ulega zmianie. Jego definicje klastra lokalnego wskazują, że znajduje się on w klastrze. Definicje we wszystkich innych menedżerach kolejek nie są wyświetlane w klastrze.

Blokowanie odbierania komunikatów przez menedżery kolejek

Można uniemożliwić menedżerowi kolejek klastra odbieranie komunikatów, które nie są autoryzowane do odbierania, za pomocą programów obsługi wyjścia.

O tym zadaniu

Trudno jest zatrzymać definiowanie kolejki przez menedżera kolejek, który jest elementem klastra. Istnieje niebezpieczeństwo, że zbuntowany menedżer kolejek dołączy do klastra i zdefiniuje własną instancję jednej z kolejek w klastrze. Może teraz odbierać komunikaty, do których nie ma uprawnień. Aby uniemożliwić menedżerowi kolejek odbieranie komunikatów, 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 do określenia, czy docelowy menedżer kolejek ma wysyłać komunikaty.
- Program obsługi wyjścia obciążenia klastra, który używa rekordów docelowych do określenia przydatności kolejki docelowej i menedżera kolejek do wysyłania 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 używa protokołu TLS, należy skonfigurować protokół TLS we wszystkich menedżerach kolejek, które komunikują się za pomocą tego kanału.

Więcej informacji na temat protokołu TLS zawiera sekcja “Protokoły zabezpieczeń TLS w produkcie IBM MQ” na stronie 24. Ta porada ma ogólne zastosowanie do kanałów klastra, ale warto zwrócić szczególną uwagę na następujące kwestie:

W klastrze IBM MQ konkretna definicja kanału CLUSRCVR jest często propagowana do wielu innych menedżerów kolejek, w których jest transformowana w automatycznie definiowany produkt CLUSSDR. Następnie automatycznie zdefiniowana wartość CLUSSDR jest używana do uruchamiania kanału dla CLUSRCVR. Jeśli serwer CLUSRCVR jest skonfigurowany do obsługi połączeń TLS, mają zastosowanie następujące uwagi:

- Wszystkie menedżery kolejek, które mają komunikować się z tym produktem CLUSRCVR , muszą mieć dostęp do obsługi protokołu TLS. Ta obsługa protokołu TLS musi obsługiwać specyfikację szyfrowania CipherSpec dla kanału.
- Różne menedżery kolejek, do których zostały propagowane automatycznie zdefiniowane kanały nadawcze klastra, będą miały powiązaną inną nazwę wyróżniającą. Jeśli sprawdzanie nazwy wyróżniającej węzła sieci ma być używane w systemie CLUSRCVR , musi być skonfigurowane tak, aby wszystkie nazwy wyróżniające, które mogą być odebrane, były pomyślnie zgodne.

  Załóżmy na przykład, że wszystkie menedżery kolejek, które będą udostępniały kanały nadawcze klastra łączące się z określonym serwerem CLUSRCVR, mają powiązane certyfikaty. Załóżmy również, że nazwy wyróżniające we wszystkich tych certyfikatach definiują kraj jako Wielka Brytania, organizację jako IBM, jednostkę organizacyjną jako IBM MQ Development i wszystkie mają nazwy wspólne w postaci DEVT.QMnnn, gdzie nnn jest liczbą.

  W takim przypadku wartość C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM* parametru SSLPEER w systemie CLUSRCVR umożliwi pomyślne nawiązanie połączenia przez wszystkie wymagane kanały nadawcze klastra, ale uniemożliwi nawiązanie połączenia przez niechciane kanały nadawcze klastra.
- Jeśli używane są niestandardowe łańcuchy CipherSpec , należy pamiętać, że niestandardowe formaty łańcuchów nie są dozwolone na wszystkich platformach. Na przykład parametr CipherSpec łańcuch RC4_SHA_US ma wartość 05 w systemie IBM i , ale nie jest poprawną specyfikacją w systemach AIX, Linux, and Windows . Jeśli więc niestandardowe parametry SSLCIPH są używane w systemie CLUSRCVR, wszystkie wynikowe automatycznie definiowane kanały nadawcze klastra powinny znajdować się na platformach, na których bazowa obsługa protokołu TLS implementuje tę CipherSpec i na których można ją określić przy użyciu wartości niestandardowej. Jeśli nie można wybrać wartości parametru SSLCIPH , która będzie zrozumiała dla całego klastra, konieczne będzie użycie wyjścia automatycznej definicji kanału w celu zmiany go na wartość zrozumiałą dla używanych platform. Tam, gdzie jest to możliwe, należy używać tekstowych łańcuchów CipherSpec (na przykład TLS_RSA_WITH_AES_128_CBC_SHA).

Parametr SSLCRLNL ma zastosowanie do pojedynczego menedżera kolejek i nie jest propagowany do innych menedżerów kolejek w klastrze.

Aktualizowanie klastrowych menedżerów kolejek i kanałów do protokołu SSL/TLS

Zaktualizuj kanały klastra pojedynczo, zmieniając wszystkie kanały CLUSRCVR przed kanałami CLUSSDR .

Zanim rozpoczniesz

Należy rozważyć następujące uwagi, ponieważ mogą one mieć wpływ na wybór opcji CipherSpec dla klastra:

- Niektóre CipherSpecs nie są dostępne na wszystkich platformach. Należy zwrócić uwagę na wybór CipherSpec , która jest obsługiwana przez wszystkie menedżery kolejek w klastrze.

- Niektóre 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 CipherSpecs obsługiwanych przez każdą wersję.

  Aby użyć nowej CipherSpec w klastrze, należy najpierw przeprowadzić migrację wszystkich menedżerów kolejek klastra do wersji bieżącej.
- Niektóre CipherSpecs wymagają użycia konkretnego typu certyfikatu cyfrowego, zwłaszcza takiego, który używa szyfrowania z krzywą eliptyczną.

  Ostrzeżenie: W menedżerach kolejek, które mają zostać połączone jako część klastra, nie można używać kombinacji certyfikatów podpisanych przez Elliptic Curve i certyfikatów podpisanych przez RSA.

  Wszystkie menedżery kolejek w klastrze muszą używać certyfikatów podpisanych przez RSA lub wszystkich certyfikatów podpisanych przez EC, a nie obu tych rodzajów certyfikatów.

  Więcej informacji zawiera sekcja “Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48.

Zaktualizuj wszystkie menedżery kolejek w klastrze do wersji IBM MQ V8 lub nowszej, jeśli nie są one jeszcze na tych poziomach. Dystrybuuj certyfikaty i klucze, aby protokół TLS działał z każdym z nich.

Aby wykonać aktualizację lub użyć dowolnego z aliasów CipherSpecs (ANY_TLS13, ANY_TLS13_OR_HIGHER, ANY_TLS12, ANY_TLS12_OR_HIGHERitd.), należy zaktualizować wszystkie menedżery kolejek produktu IBM MQ for Multiplatforms w klastrze do wersji IBM MQ 9.1.4 lub nowszej, a wszystkie menedżery kolejek produktu IBM MQ for z/OS w klastrze do wersji IBM MQ for z/OS 9.2.0 lub nowszej.

O tym zadaniu

Zmień kanały CLUSRCVR przed kanałami CLUSSDR .

Procedura

1. Zmień kanały CLUSRCVR na TLS w dowolnej kolejności, zmieniając jednocześnie jeden CLUSRCVR i pozwól, aby zmiany przepływały przez klaster przed zmianą następnego.

   Ważne: Należy upewnić się, że ścieżka odwrotna nie zostanie zmieniona, dopóki zmiany dla bieżącego kanału nie zostaną rozdystrybuowane w klastrze.
2. Opcjonalne: Przełącz wszystkie ręczne kanały CLUSSDR na TLS.

   Nie ma to wpływu na działanie klastra, chyba że zostanie użyta komenda REFRESH CLUSTER z opcją REPOS(YES) .

   Uwaga: W przypadku dużych klastrów użycie komendy **REFRESH CLUSTER** może być zakłócające dla klastra w trakcie jego działania, a następnie może być wykonywane co 27 dni, gdy 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 klastrze.
4. Zrestartuj kanały, aby użyć protokołu TLS, i uruchom REFRESH SECURITY (SSL).

Pojęcia pokrewne

“Włączanie CipherSpecs” na stronie 466
Włącz parametr CipherSpec , używając parametru **SSLCIPH** w komendzie **DEFINE CHANNEL** lub **ALTER CHANNEL** MQSC.

“Zgodność certyfikatów cyfrowych i specyfikacji szyfrowania CipherSpec w produkcie IBM MQ” na stronie 48
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 klastrowych menedżerach kolejek i kanałach

Aby wyłączyć protokół TLS, należy nadać parametrowi SSLCIPH wartość ' '. Należy wyłączyć protokół TLS dla poszczególnych kanałów klastra, zmieniając wszystkie kanały odbiorcy klastra przed kanałami nadawcy klastra.

O tym zadaniu

Zmień jeden kanał odbiorczy klastra na raz i zezwól na przepływ zmian przez klaster przed zmianą następnego.

Ważne: Należy upewnić się, że ścieżka odwrotna nie zostanie zmieniona, dopóki zmiany dla bieżącego kanału nie zostaną rozdystrybuowane w klastrze.

Procedura

1. Ustaw wartość parametru SSLCIPH na ' ', pusty łańcuch w pojedynczym cudzysłowie IBM i lub *NONE w systemie IBM i .

   Protokół TLS można wyłączyć w kanałach odbiorczych klastra w dowolnej kolejności.

   Należy zauważyć, że zmiany są wprowadzane w odwrotnym kierunku w kanałach, w których protokół TLS jest aktywny.
2. Za pomocą komendy **DISPLAY CLUSQMGR(*)** ALLsprawdź, czy nowa wartość została odzwierciedlona we wszystkich pozostałych menedżerach kolejek.
3. Wyłącz protokół TLS we wszystkich ręcznych kanałach nadawczych klastra.

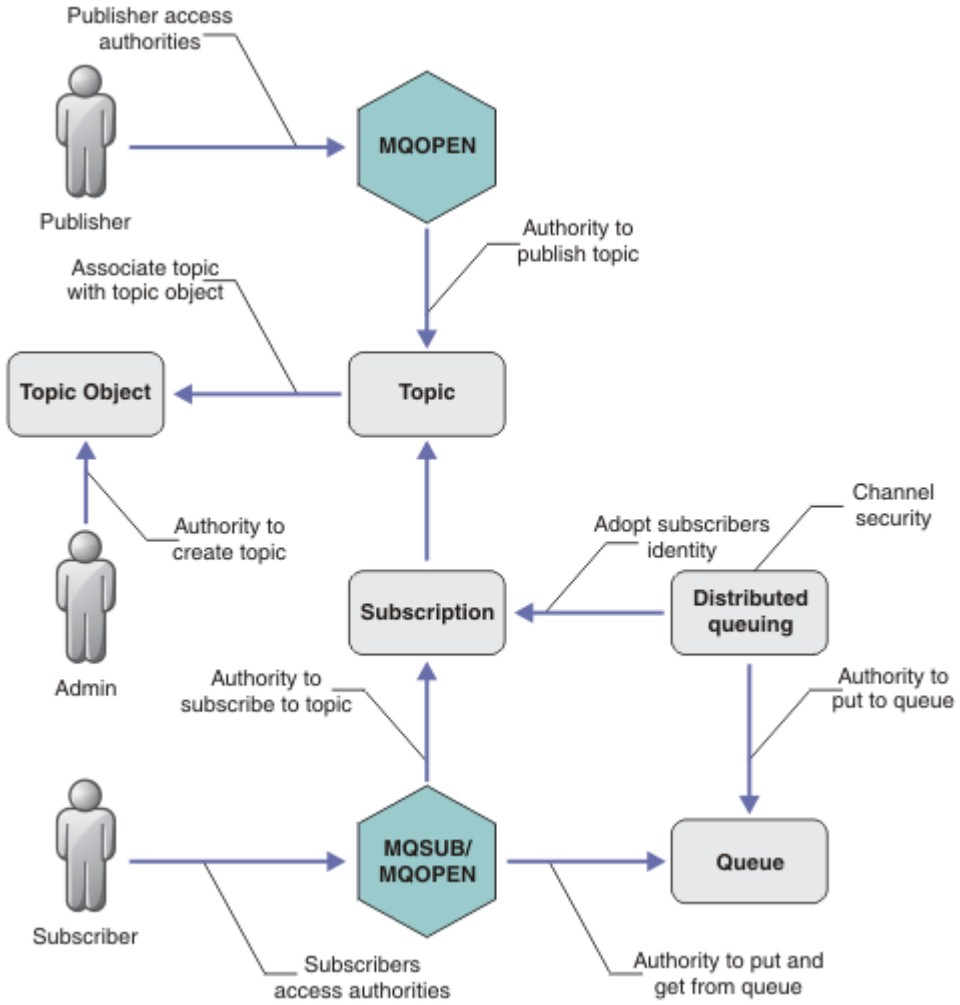
   Nie ma to wpływu na działanie klastra, chyba że zostanie użyta komenda **REFRESH CLUSTER** z opcją REPOS (YES).

   W przypadku dużych klastrów użycie komendy **REFRESH CLUSTER** może być zakłócające dla klastra w trakcie jego działania, a następnie w regularnych odstępach czasu, gdy obiekty klastra automatycznie wysyłają aktualizacje statusu do wszystkich zainteresowanych menedżerów kolejek. Więcej informacji na ten temat zawiera sekcja Odświeżanie dużego klastra może mieć wpływ na wydajność i dostępność klastra .
4. Zatrzymaj i zrestartuj kanały nadawcze klastra.

Zabezpieczenia publikowania/subskrypcji

Komponenty i interakcje, które są związane z publikowaniem/subskrybowaniem, są opisane jako wprowadzenie do bardziej szczegółowych wyjaśnień i przykładów, które znajdują się poniżej.

W publikowanie i subskrybowanie tematu zaangażowanych jest wiele komponentów. Niektóre relacje bezpieczeństwa między nimi zostały zilustrowane w sekcji Rysunek 22 na stronie 534 i opisane w poniższym przykładzie.



Rysunek 22. Relacje zabezpieczeń publikowania/subskrypcji między różnymi komponentami

Tematy

Tematy są identyfikowane przez łańcuchy tematów i zwykle są zorganizowane w postaci drzew. Więcej informacji na ten temat zawiera sekcja Drzewa tematów. Aby sterować dostępem do tematu, należy powiązać temat z obiektem tematu. W sekcji “Model zabezpieczeń tematu” na stronie 536 opisano sposób zabezpieczania tematów przy użyciu obiektów tematu.

Obiekty tematów administracyjnych

Za pomocą komendy **setmqaut** z listą obiektów tematów administracyjnych można kontrolować, kto ma dostęp do tematu i w jakim celu. Patrz przykłady: “Nadawanie użytkownikowi dostępu do subskrybowania tematu” na stronie 541 i “Przyznaj użytkownikowi dostęp do publikowania w temacie” na stronie 548. z/OS Aby kontrolować dostęp do obiektów tematu w systemie z/OS, należy zapoznać się z sekcją Profile zabezpieczeń tematu.

Subskrypcje

Subskrybowanie jednego lub większej liczby tematów przez utworzenie subskrypcji udostępniającej łańcuch tematu, który może zawierać znaki wieloznaczne, w celu dopasowania go do łańcuchów tematów publikacji. Więcej informacji na ten temat można znaleźć w następujących sekcjach:

Subskrybuj przy użyciu obiektu tematu

“Subskrybowanie przy użyciu nazwy obiektu tematu” na stronie 537

Subskrybuj przy użyciu tematu
"Subskrybowanie przy użyciu łańcucha tematu, w którym węzeł tematu nie istnieje" na stronie 538

Subskrybuj przy użyciu tematu ze znakami wieloznacznymi
"Subskrybowanie przy użyciu łańcucha tematu zawierającego znaki wieloznaczne" na stronie 539

Subskrypcja zawiera informacje o tożsamości subskrybenta i tożsamości kolejki docelowej, w której mają zostać umieszczone publikacje. Zawiera również informacje o tym, w jaki sposób publikacja ma zostać umieszczona w kolejce docelowej.

Oprócz określenia, którzy subskrybenci mają uprawnienia do subskrybowania określonych tematów, można ograniczyć subskrypcje do używania przez pojedynczego subskrybenta. Można również sterować informacjami o subskrybencie, które są używane przez menedżer kolejek podczas umieszczania publikacji w kolejce docelowej. Patrz "Zabezpieczenia subskrypcji" na stronie 554.

Kolejki

Kolejka docelowa jest ważną kolejką do zabezpieczenia. Jest on lokalny względem subskrybenta, a publikacje zgodne z subskrypcją są w nim umieszczane. Należy rozważyć 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 udostępnionej przez subskrybent. Subskrybent lub program, któremu delegowano zadanie pobierania publikacji, pobiera komunikaty z kolejki. Patrz "Uprawnienia do kolejek docelowych" na stronie 539.

Nie ma aliasów obiektów tematów, ale można użyć kolejki aliasowej jako aliasu dla obiektu tematu. W takim przypadku, a także podczas sprawdzania uprawnień do używania tematu do publikowania lub subskrybowania, menedżer kolejek sprawdza uprawnienia do używania kolejki.

"Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek" na stronie 556

Uprawnienie do publikowania lub subskrybowania tematu jest sprawdzane w lokalnym menedżerze kolejek przy użyciu lokalnych tożsamości i autoryzacji. Autoryzacja nie zależy od tego, czy temat jest zdefiniowany, czy nie, ani od tego, gdzie jest 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 można uzyskać dla kolejek, definiując alias kolejki lokalnie dla każdej kolejki klastrowej.

Menedżery kolejek wymieniają subskrypcje w klastrze. W większości konfiguracji klastra IBM MQ kanały są konfigurowane przy użyciu parametru PUTAUT=DEF w celu umieszczania komunikatów w kolejkach docelowych przy użyciu uprawnień procesu kanału. Konfigurację kanału można zmodyfikować w taki sposób, aby produkt PUTAUT=CTX wymagał od użytkownika subskrybującego uprawnienia do propagowania subskrypcji do innego menedżera kolejek w klastrze.

W sekcji "Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek" na stronie 556 opisano sposób zmiany definicji kanałów w celu określenia, kto może propagować subskrypcje na inne serwery w klastrze.

Autoryzacja

Autoryzację można zastosować do obiektów tematu, podobnie jak w przypadku kolejek i innych obiektów. Istnieją trzy operacje autoryzacji: `pub`, `subi` `resume` , które można zastosować tylko do tematów. Szczegółowe informacje zawiera sekcja Określanie uprawnień dla różnych typów obiektów.

Wywołania funkcji

W programach publikowania i subskrypcji, podobnie jak w programach kolejkowanych, sprawdzanie autoryzacji jest wykonywane, gdy obiekty są otwierane, tworzone, zmieniane lub usuwane. Sprawdzenia nie są wykonywane, jeśli wywołania MQI produktu `MQPUT` lub `MQGET` są wykonywane w celu umieszczania i pobierania publikacji.

Aby opublikować temat, należy wykonać na nim operację MQOPEN , która wykonuje sprawdzenia autoryzacji. Publikowanie komunikatów w uchwycie tematu za pomocą komendy MQPUT , która nie sprawdza autoryzacji.

Aby zasubskrybować temat, zwykle należy wykonać komendę MQSUB w celu utworzenia lub wznowienia subskrypcji, a także w celu otwarcia kolejki docelowej na potrzeby odbierania publikacji. Alternatywnie można wykonać osobną operację MQOPEN , aby otworzyć kolejkę docelową, a następnie wykonać operację MQSUB , aby utworzyć lub wznowić subskrypcję.

Niezależnie od tego, które wywołania są używane, menedżer kolejek sprawdza, czy można zasubskrybować temat i pobrać wynikowe publikacje z kolejki docelowej. Jeśli kolejka docelowa jest niezarządzana, wykonywane są również sprawdzenia autoryzacji, czy menedżer kolejek może umieszczać publikacje w kolejce docelowej. Używa on tożsamości, którą zaadoptował ze zgodnej subskrypcji. Zakłada się, że menedżer kolejek zawsze może umieszczać publikacje w zarządzanych kolejkach docelowych.

Rola

Użytkownicy pełnią cztery role w uruchamianiu aplikacji publikowania/subskrybowania:

1. Publikator
2. Subskrybent
3. Administrator tematu
4. IBM MQ Administrator-członek grupy mqm

Zdefiniuj grupy z odpowiednimi autoryzacjami odpowiadającymi rolom administracyjnym publikowania, subskrybowania i tematu. Następnie można przypisać nazwy użytkowników do tych grup, autoryzując je do wykonywania określonych zadań publikowania i subskrypcji.

Ponadto należy rozszerzyć uprawnienia do operacji administracyjnych na administratora kolejek i kanałów odpowiedzialnych za przenoszenie publikacji i subskrypcji.

Model zabezpieczeń tematu

Tylko zdefiniowane obiekty tematu mogą mieć powiązane atrybuty bezpieczeństwa. Opis obiektów tematu zawiera sekcja Obiekty tematu administracyjnego. Atrybuty zabezpieczeń określają, czy określony identyfikator użytkownika lub grupa uprawnień może wykonywać operacje subskrybowania lub publikowania na każdym obiekcie tematu.

Atrybuty zabezpieczeń są powiązane z odpowiednim węzłem administracyjnym w drzewie tematów. Jeśli podczas operacji subskrybowania lub publikowania wykonywane jest sprawdzanie uprawnień dla określonego identyfikatora użytkownika, nadawane uprawnienie jest oparte na atrybutach zabezpieczeń powiązanego węzła drzewa tematów.

Atrybuty bezpieczeństwa są listą kontroli dostępu wskazującą, jakie uprawnienia ma określony ID użytkownika systemu operacyjnego lub grupa uprawnień do obiektu tematu.

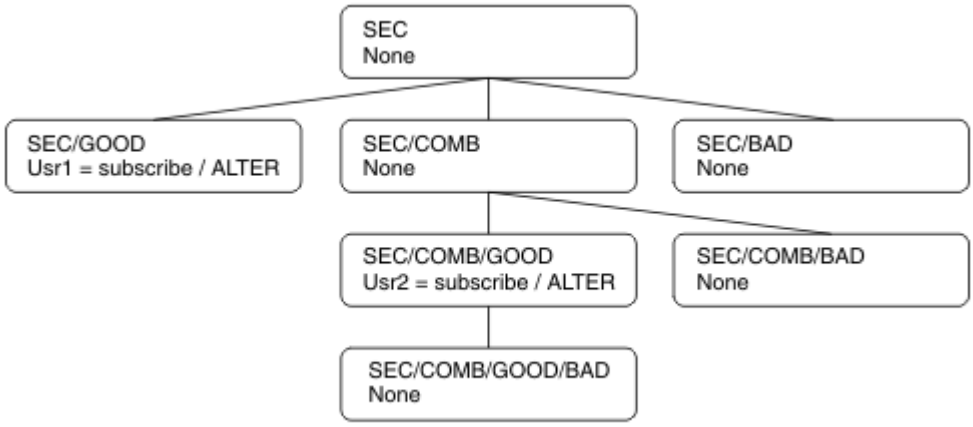
Rozważmy następujący przykład, w którym obiekty tematu zostały zdefiniowane z atrybutami bezpieczeństwa lub pokazanymi uprawnieniami:

Tabela 87. 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 87. 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 z powiązanymi atrybutami zabezpieczeń w każdym węźle może być reprezentowane w następujący sposób:



Podane przykłady zawierają następujące autoryzacje:

- W węźle głównym drzewa /SECżaden użytkownik nie ma uprawnień do tego węzła.
- usr1 nadano uprawnienie do subskrybowania obiektu /SEC/GOOD
- usr2 nadano uprawnienie do subskrybowania obiektu /SEC/COMB/GOOD

Subskrybowanie przy użyciu nazwy obiektu tematu

Podczas subskrybowania obiektu tematu przez podanie nazwy MQCHAR48 znajduje się odpowiedni węzeł w drzewie tematów. Jeśli atrybuty bezpieczeństwa powiązane z węzłem wskazują, że użytkownik ma uprawnienia do subskrybowania, dostęp jest nadawany.

Jeśli użytkownikowi nie nadano dostępu, węzeł nadrzędny w drzewie określa, czy użytkownik ma uprawnienia do subskrybowania na poziomie węzła nadrzędnego. Jeśli tak, to dostęp jest przyznawany. Jeśli nie, zostanie wzięty pod uwagę element nadrzędny tego węzła. Rekurencja jest kontynuowana do momentu zlokalizowania węzła, który nadaje użytkownikowi uprawnienie do subskrybowania. Rekurencja zostanie zatrzymana, gdy węzeł główny zostanie uznany za węzeł bez nadanego uprawnienia. W tym drugim przypadku dostęp jest zabroniony.

Krótko mówiąc, jeśli dowolny węzeł w ścieżce nadaje uprawnienie do subskrybowania tego użytkownika lub aplikacji, subskrybent może subskrybować w tym węźle lub w dowolnym miejscu poniżej tego węzła w drzewie tematów.

Węzeł główny w przykładzie to SEC.

Użytkownik otrzymuje uprawnienie do subskrypcji, jeśli lista kontroli dostępu wskazuje, że sam identyfikator użytkownika ma uprawnienie lub że grupa zabezpieczeń systemu operacyjnego, do której należy dany identyfikator użytkownika, ma uprawnienie.

Tak więc, na przykład:

- Jeśli produkt `usr1` podejmie próbę subskrypcji przy użyciu łańcucha tematu `SEC/GOOD`, subskrypcja będzie dozwolona, ponieważ ID użytkownika będzie miał dostęp do węzła powiązanego z tym tematem. Jeśli jednak program `usr1` próbował zasubskrybować przy użyciu łańcucha tematu `SEC/COMB/GOOD` , subskrypcja nie byłaby dozwolona, ponieważ ID użytkownika nie ma dostępu do powiązanego z nim węzła.
- Jeśli produkt `usr2` podejmie próbę subskrybowania, przy użyciu łańcucha tematu `SEC/COMB/GOOD` subskrypcja będzie dozwolona, ponieważ ID użytkownika będzie miał dostęp do węzła powiązanego z tematem. Jeśli jednak program `usr2` próbował zasubskrybować `SEC/GOOD` , subskrypcja nie byłaby dozwolona, ponieważ ID użytkownika nie ma dostępu do powiązanego z nim węzła.
- Jeśli program `usr2` podejmie próbę zasubskrybowania przy użyciu łańcucha tematu `SEC/COMB/GOOD/BAD` , subskrypcja będzie dozwolona, ponieważ ID użytkownika ma dostęp do węzła nadrzędnego `SEC/COMB/GOOD`.
- Jeśli produkt `usr1` lub `usr2` próbuje zasubskrybować przy użyciu łańcucha tematu `/SEC/COMB/BAD`, nie jest to dozwolone, ponieważ nie mają oni dostępu do powiązanego z nim węzła tematu ani do węzłów nadrzędnych tego tematu.

Operacja subskrypcji określająca nazwę obiektu tematu, który nie istnieje, powoduje błąd MQRC_UNKNOWN_OBJECT_NAME.

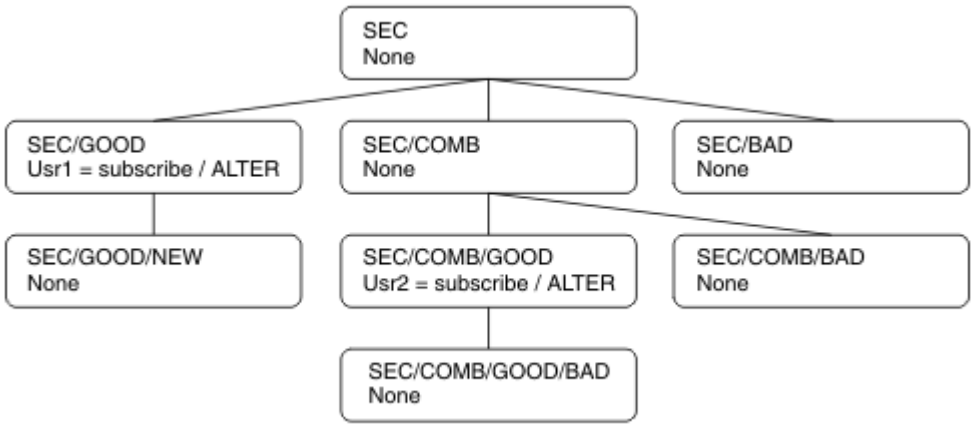
Subskrybowanie przy użyciu łańcucha tematu, w którym istnieje węzeł tematu

Zachowanie jest takie samo, jak w przypadku określania tematu za pomocą nazwy obiektu MQCHAR48 .

Subskrybowanie przy użyciu łańcucha tematu, w którym węzeł tematu nie istnieje

Należy rozważyć przypadek aplikacji subskrybującej, określając łańcuch tematu reprezentujący węzeł tematu, który aktualnie nie istnieje w drzewie tematów. Sprawdzanie uprawnień jest wykonywane zgodnie z opisem w poprzedniej sekcji. Sprawdzanie rozpoczyna się od węzła nadrzędnego względem tego, który jest reprezentowany przez łańcuch tematu. Jeśli uprawnienie zostanie nadane, w drzewie tematów zostanie utworzony nowy węzeł reprezentujący łańcuch tematu.

Na przykład program `usr1` próbuje zasubskrybować temat `SEC/GOOD/NEW`. Uprawnienie jest nadawane, ponieważ `usr1` ma dostęp do węzła nadrzędnego `SEC/GOOD`. W drzewie zostanie utworzony nowy węzeł tematu zgodnie z poniższym diagramem. Nowy węzeł tematu nie jest obiektem tematu, z którym nie są bezpośrednio powiązane żadne atrybuty zabezpieczeń. Atrybuty są dziedziczone z obiektu nadrzędnego.



Subskrybowanie przy użyciu łańcucha tematu zawierającego znaki wieloznaczne

Należy rozważyć możliwość subskrybowania 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.

Oznacza to, że jeśli aplikacja subskrybuje produkt SEC/COMB/GOOD/*, sprawdzanie uprawnień jest wykonywane zgodnie z opisem w dwóch poprzednich sekcjach w węźle SEC/COMB/GOOD w drzewie tematów.

Podobnie, jeśli aplikacja musi zasubskrybować produkt SEC/COMB/*/GOOD, w węźle SEC/COMBjest wykonywane sprawdzenie uprawnień.

Uprawnienia do kolejek docelowych

Podczas subskrybowania tematu jednym z parametrów jest uchwyt hobj kolejki, która została otwarta do wyprowadzania w celu odbierania publikacji.

Jeśli parametr hobj nie jest określony, ale jest pusty, tworzona jest kolejka zarządzana, jeśli spełnione są następujące warunki:

- Podano opcję MQSO_MANAGED .
- Subskrypcja nie istnieje.
- Określono tworzenie.

Jeśli parametr hobj jest pusty, a istniejąca subskrypcja jest zmieniana lub wznawiana, poprzednio podana kolejka docelowa może być zarządzana lub niezarządzana.

Aplikacja lub użytkownik wysyłający żądanie MQSUB musi mieć uprawnienie do umieszczania komunikatów w kolejce docelowej, którą udostępnił. W rezultacie musi mieć uprawnienie do umieszczania komunikatów opublikowanych w tej kolejce. Sprawdzanie uprawnień odbywa się zgodnie z istniejącymi regułami sprawdzania bezpieczeństwa kolejki.

W razie potrzeby sprawdzanie zabezpieczeń obejmuje alternatywny identyfikator użytkownika i sprawdzanie zabezpieczeń kontekstu. Aby można było ustawić dowolne z pól kontekstu tożsamości, należy podać opcję MQSO_SET_IDENTITY_CONTEXT oraz opcję MQSO_CREATE lub MQSO_ALTER . Nie można ustawić żadnego z pól kontekstu tożsamości dla żądania MQSO_RESUME .

Jeśli miejsce docelowe jest kolejką zarządzaną, nie są wykonywane żadne sprawdzenia zabezpieczeń w odniesieniu do zarządzanego miejsca docelowego. Jeśli użytkownik ma uprawnienia do subskrybowania tematu, zakłada się, że można używać zarządzanych miejsc docelowych.

Publikowanie przy użyciu nazwy tematu lub łańcucha tematu, w którym istnieje węzeł tematu

Model zabezpieczeń publikowania jest taki sam, jak w przypadku subskrybowania, z wyjątkiem znaków wieloznacznych. Publikacje nie zawierają znaków wieloznacznych, dlatego nie jest rozróżniana wielkość liter w łańcuchu tematu zawierającym znaki wieloznaczne.

Uprawnienia do publikowania i subskrybowania są różne. Użytkownik lub grupa może mieć uprawnienia do wykonania jednej z nich bez konieczności wykonywania drugiej.

Podczas publikowania do obiektu tematu przez określenie nazwy MQCHAR48 lub łańcucha tematu znajduje się odpowiedni węzeł w drzewie tematów. Jeśli atrybuty zabezpieczeń powiązane z węzłem tematu wskazują, że użytkownik ma uprawnienia do publikowania, dostęp jest nadawany.

Jeśli dostęp nie zostanie nadany, węzeł nadrzędny w drzewie określa, czy użytkownik ma uprawnienia do publikowania na tym poziomie. Jeśli tak, to dostęp jest przyznawany. Jeśli nie, rekurencja będzie kontynuowana do momentu zlokalizowania węzła, który nadaje użytkownikowi uprawnienie do publikowania. Rekurencja zostanie zatrzymana, gdy węzeł główny zostanie uznany za węzeł bez nadanego uprawnienia. W tym drugim przypadku dostęp jest zabroniony.

Krótko mówiąc, jeśli dowolny węzeł w ścieżce nadaje uprawnienie do publikowania dla tego użytkownika 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, podając łańcuch tematu reprezentujący węzeł tematu, który aktualnie nie istnieje w drzewie tematów, sprawdzanie uprawnień jest wykonywane, począwszy od elementu nadrzędnego węzła reprezentowanego przez łańcuch tematu. Jeśli uprawnienie zostanie nadane, 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, na który jest tłumaczona.

Sprawdzenie zabezpieczeń w kolejce aliasowej sprawdza, czy użytkownik ma uprawnienia do umieszczania komunikatów w tej kolejce aliasowej, a sprawdzenie zabezpieczeń w temacie sprawdza, czy użytkownik może publikować w tym temacie. Gdy kolejka aliasowa jest tłumaczona na inną kolejkę, sprawdzenia nie są wykonywane w kolejce bazowej. Sprawdzanie uprawnień jest wykonywane inaczej dla tematów i kolejek.

Zamykanie subskrypcji

W przypadku zamknięcia subskrypcji za pomocą opcji `MQCO_REMOVE_SUB` , jeśli subskrypcja nie została utworzona przy użyciu tego uchwytu, istnieje dodatkowe sprawdzanie zabezpieczeń.

Wykonywane jest sprawdzenie zabezpieczeń w celu upewnienia się, że użytkownik ma odpowiednie uprawnienia do wykonania tej czynności, ponieważ powoduje ona usunięcie subskrypcji. Jeśli atrybuty bezpieczeństwa powiązane z węzłem tematu wskazują, że użytkownik ma uprawnienia, nadawany jest dostęp. Jeśli nie, węzeł nadrzędny w drzewie jest brany pod uwagę w celu określenia, czy użytkownik ma uprawnienia do zamknięcia subskrypcji. Rekurencja jest kontynuowana do momentu przyznania uprawnień lub osiągnięcia węzła głównego.

Definiowanie, modyfikowanie i usuwanie subskrypcji

Jeśli subskrypcja jest tworzona administracyjnie, a nie przy użyciu żądania interfejsu API `MQSUB` , nie są wykonywane żadne sprawdzenia zabezpieczeń subskrypcji. Administrator otrzymał już to uprawnienie za pomocą komendy.

Wykonywane są sprawdzenia zabezpieczeń w celu upewnienia się, że publikacje mogą być umieszczane w kolejce docelowej powiązanej z subskrypcją. Sprawdzenia są wykonywane w taki sam sposób, jak w przypadku żądania `MQSUB` .

ID użytkownika, który jest używany do tych sprawdzeń bezpieczeństwa, zależy od wydawanej komendy. Jeśli podano parametr **SUBUSER** , ma on wpływ na sposób sprawdzania, jak to pokazano na rysunku (Tabela 88 na stronie 541):

Tabela 88. Identyfikatory użytkowników używane do sprawdzania bezpieczeństwa komend			
Komenda	**SUBUSER określone i puste**	**SUBUSER określone i zakończone**	**Nie określono SUBUSER**
	Użyj identyfikatora administratora		Użyj identyfikatora użytkownika z subskrypcji LIKE
	Użyj identyfikatora administratora		Użyj.DEFAULT.SU identyfikatoB -jeśli pole rajest puste, użytkowniknależy użyć a z systemuidentyfikator SYSTEMa administratora
	Użyj identyfikatora administratora		Użyj identyfikatora użytkownika z istniejącej subskrypcji

Jedyną kontrolą bezpieczeństwa wykonywaną podczas usuwania subskrypcji za pomocą komendy DELETE SUB jest kontrola bezpieczeństwa komendy.

Przykładowa konfiguracja zabezpieczeń publikowania/subskrypcji

W tej sekcji opisano scenariusz, w którym skonfigurowano kontrolę dostępu do tematów w sposób umożliwiający zastosowanie kontroli zabezpieczeń zgodnie z wymaganiami.

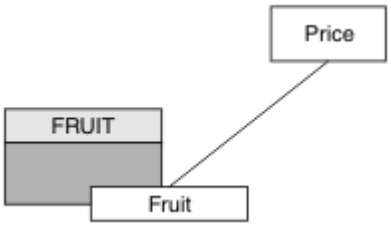
Nadawanie użytkownikowi dostępu do subskrybowania tematu

Ten temat jest pierwszym tematem na liście zadań, który informuje o sposobie nadawania dostępu do tematów przez więcej niż jednego użytkownika.

O tym zadaniu

W tej czynności przyjęto założenie, że nie istnieją żadne obiekty tematów administracyjnych ani nie zdefiniowano żadnych profili dla subskrypcji lub publikacji. Aplikacje tworzą nowe subskrypcje, a nie wznawiają istniejące, i robią to tylko przy użyciu łańcucha tematu.

Aplikacja może utworzyć subskrypcję, udostępniając obiekt tematu, łańcuch tematu lub kombinację obu tych elementów. Niezależnie od tego, w jaki sposób aplikacja wybiera, efektem jest subskrypcja w określonym miejscu w drzewie tematów. Jeśli ten punkt w drzewie tematów jest reprezentowany przez obiekt tematu administracyjnego, profil zabezpieczeń jest sprawdzany na podstawie nazwy tego obiektu tematu.



Rysunek 23. Przykład dostępu do obiektu tematu

Tabela 89. 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. Wydaj komendę MQSC `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Przyznaj dostęp w następujący sposób:

   - z/OS **z/OS** :

     Przyznaj dostęp do USER1 , aby zasubskrybować temat `"Price/Fruit"` , nadając użytkownikowi dostęp do profilu `hlq.SUBSCRIBE.FRUIT` . W tym celu należy użyć następujących komend RACF :

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
     PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - Inne platformy:

     Przyznaj dostęp do USER1 , aby zasubskrybować temat `"Price/Fruit"` , nadając użytkownikowi dostęp do obiektu FRUIT . W tym celu należy użyć komendy autoryzacji dla platformy:

     ALW **Systemy AIX, Linux, and Windows**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
     ```

Wyniki

Gdy USER1 próbuje zasubskrybować temat `"Price/Fruit"` , wynikiem jest powodzenie.

Gdy USER2 próbuje zasubskrybować temat `"Price/Fruit"` , wynikiem jest niepowodzenie z komunikatem `MQRC_NOT_AUTHORIZED` wraz z:

- z/OS W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- ALW Na innych platformach jest to 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 jest to następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Należy zauważyć, że jest to ilustracja przedstawiająca to, co widać, a nie wszystkie pola.

Przyznaj użytkownikowi dostęp do subskrybowania tematu znajdującego się głębiej w drzewie

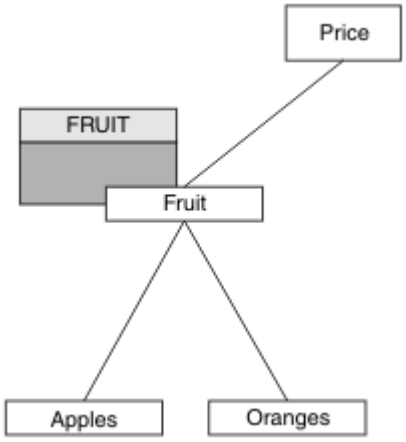
Ten temat jest drugim z listy zadań, które informują o sposobie nadawania dostępu do tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie używana jest konfiguracja opisana w sekcji “Nadawanie użytkownikowi dostępu do subskrybowania tematu” na stronie 541.

O tym zadaniu

Jeśli punkt w drzewie tematów, w którym aplikacja dokonuje subskrypcji, nie jest reprezentowany przez obiekt tematu administracyjnego, należy przenieść drzewo w górę, dopóki nie zostanie znaleziony najbliższy nadrzędny obiekt tematu administracyjnego. Profil zabezpieczeń jest sprawdzany na podstawie nazwy obiektu tematu.



Rysunek 24. Przykład nadawania dostępu do tematu w drzewie tematów

Tabela 90. Wymagania dotyczące dostępu do przykładowych tematów i obiektów tematów		
Temat	**Wymagany dostęp do subskrypcji**	**Obiekt tematu**
Cena	Brak użytkownika	Brak
Cena/owoce	USER1	fruit
Cena/Owoce/Jabłka	USER1	
Cena/Owoce/Pomarańcze	USER1	

W poprzedniej czynności USER1 nadano dostęp do subskrybowania tematu `"Price/Fruit"` , nadając mu dostęp do profilu `hlq.SUBSCRIBE.FRUIT` w systemie z/OS i do profilu FRUIT na innych platformach. Ten pojedynczy profil nadaje również USER1 dostęp do subskrypcji produktów `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` i `"Price/Fruit/#"`.

Gdy USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynikiem jest powodzenie.

Gdy USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynikiem jest niepowodzenie z komunikatem `MQRC_NOT_AUTHORIZED` wraz z:

- W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Na innych platformach jest to 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 otrzymywane w systemie z/OS są identyczne z komunikatami otrzymanymi w poprzednim zadaniu, jak te same obiekty tematu i profile kontrolujące dostęp.
- Komunikat zdarzenia odebrany na innych platformach jest podobny do komunikatu odebranego w poprzednim zadaniu, ale rzeczywisty łańcuch tematu jest inny.

Przyznaj innemu użytkownikowi dostęp do subskrybowania tylko tematu znajdującego się głębiej w drzewie

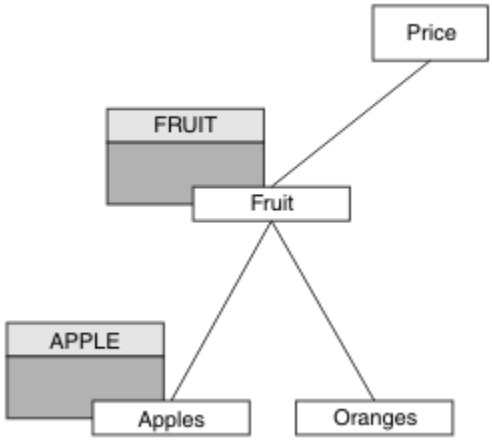
Ten temat jest trzecim tematem na liście zadań, który informuje o sposobie nadawania dostępu do subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie używana jest konfiguracja opisana w sekcji “Przyznaj użytkownikowi dostęp do subskrybowania tematu znajdującego się głębiej w drzewie” na stronie 543.

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 innych tematów.



Rysunek 25. Nadawanie dostępu do konkretnych tematów w drzewie tematów

Tabela 91. Wymagania dotyczące dostępu do 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. Wydaj komendę MQSC `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Przyznaj dostęp w następujący sposób:

- z/OS **z/OS** :

  W poprzedniej czynności USER1 nadano dostęp do subskrybowania tematu `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do profilu `hlq.SUBSCRIBE.FRUIT` .

  Ten pojedynczy profil nadał również USER1 dostęp do subskrybowania `"Price/Fruit/Oranges"` `"Price/Fruit/#"` , a dostęp ten pozostaje nawet po dodaniu nowego obiektu tematu i powiązanych z nim profili.

  Przyznaj dostęp do USER2 , aby zasubskrybować temat `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do profilu `hlq.SUBSCRIBE.APPLE` . W tym celu należy użyć następujących komend RACF :

```
RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
```

- Inne platformy:

  W poprzedniej czynności USER1 nadano dostęp do subskrybowania tematu `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do subskrybowania profilu FRUIT .

  Ten pojedynczy profil również nadał USER1 dostęp do subskrypcji produktów `"Price/Fruit/Oranges"` i `"Price/Fruit/#"`, a dostęp ten pozostaje nawet po dodaniu nowego obiektu tematu i powiązanych z nim profili.

  Nadaj dostęp do USER2 , aby subskrybować temat `"Price/Fruit/Apples"` , nadając użytkownikowi dostęp do subskrybowania profilu APPLE . W tym celu należy użyć komendy autoryzacji dla platformy:

  ALW **Systemy AIX, Linux, and Windows**

  ```
  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 produkt USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , pierwsze sprawdzenie zabezpieczeń profilu `hlq.SUBSCRIBE.APPLE` kończy się niepowodzeniem, ale podczas przenoszenia w górę drzewa profil `hlq.SUBSCRIBE.FRUIT` zezwala użytkownikowi USER1 na subskrybowanie, więc subskrypcja kończy się powodzeniem i kod powrotu nie jest wysyłany do wywołania MQSUB. Jednak dla pierwszego sprawdzenia generowany jest komunikat RACF `ICH` :

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Gdy USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynik jest pomyślany, ponieważ kontrola zabezpieczeń jest przekazywana do pierwszego profilu.

Gdy USER2 próbuje zasubskrybować temat `"Price/Fruit/Oranges"` , wynikiem jest niepowodzenie z komunikatem `MQRC_NOT_AUTHORIZED` wraz z:

- z/OS W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ALW Na platformach AIX, Linux, and Windows jest to 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 jest to 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 ICH . Można tego uniknąć, jeśli drzewo tematów jest zabezpieczone w inny sposób.

Zmień prawa dostępu, aby uniknąć dodatkowych komunikatów

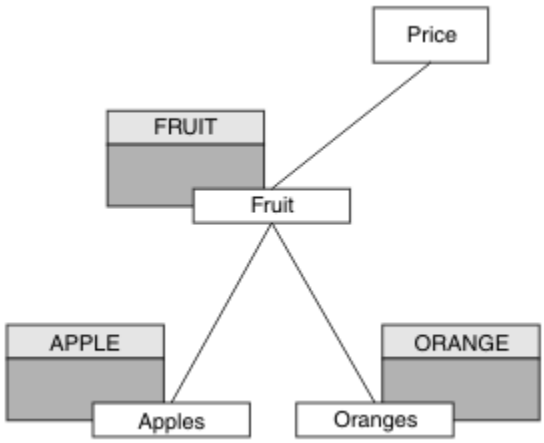
Ten temat jest czwartym tematem na liście zadań, który opisuje sposób nadawania dostępu do subskrybowania tematów przez więcej niż jednego użytkownika i unikania dodatkowych komunikatów RACF ICH408I w systemie z/OS.

Zanim rozpoczniesz

Ten temat rozszerza konfigurację opisaną w sekcji “Przyznaj innemu użytkownikowi dostęp do subskrybowania tylko tematu znajdującego się głębiej w drzewie” na stronie 544 , aby uniknąć dodatkowych komunikatów o błędach.

O tym zadaniu

W tym temacie opisano sposób nadawania dostępu do tematów znajdujących się głębiej w drzewie oraz sposób usuwania dostępu do tematu znajdującego się niżej w drzewie, gdy nie jest on wymagany przez żadnego użytkownika.



Rysunek 26. Przykład nadawania praw dostępu w celu uniknięcia dodatkowych komunikatów.

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Wydaj komendę MQSC `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Przyznaj dostęp w następujący sposób:
   - z/OS **z/OS** :

     Zdefiniuj nowy profil i dodaj dostęp do tego profilu oraz do istniejących profili. W tym celu należy użyć następujących komend 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 równoważny dostęp przy użyciu komend autoryzacji dla platformy:

Systemy AIX, Linux, and Windows

```
setmqaut -t topic -n ORANGE -p USER1 +sub
setmqaut -t topic -n APPLE -p USER1 +sub
```

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 produkt USER1 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , pierwsze sprawdzenie zabezpieczeń w profilu `hlq.SUBSCRIBE.APPLE` powiedzie się.

Podobnie, gdy USER2 próbuje zasubskrybować temat `"Price/Fruit/Apples"` , wynik jest pomyślny, ponieważ kontrola zabezpieczeń przechodzi do pierwszego profilu.

Gdy USER2 próbuje zasubskrybować temat `"Price/Fruit/Oranges"` , wynikiem jest niepowodzenie z komunikatem `MQRC_NOT_AUTHORIZED` wraz z:

- W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Na innych platformach jest to następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

- W systemie IBMi jest to następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

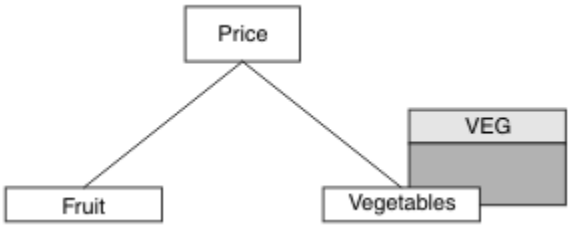
Przyznaj użytkownikowi dostęp do publikowania w temacie

Ten temat jest pierwszym tematem na liście zadań, który informuje o sposobie nadawania uprawnień do publikowania tematów przez więcej niż jednego użytkownika.

O tym zadaniu

W przypadku tej czynności przyjęto założenie, że po prawej stronie drzewa tematów nie istnieją żadne obiekty tematów administracyjnych, ani żadne profile nie zostały zdefiniowane na potrzeby publikowania. Przyjęto założenie, że publikatory używają tylko łańcucha tematu.

Aplikacja może publikować w temacie, udostępniając obiekt tematu, łańcuch tematu lub kombinację obu tych elementów. Niezależnie od tego, w jaki sposób aplikacja wybierze, efektem jest opublikowanie w określonym punkcie drzewa tematów. Jeśli ten punkt w drzewie tematów jest reprezentowany przez obiekt tematu administracyjnego, profil zabezpieczeń jest sprawdzany na podstawie nazwy tego obiektu tematu. Na przykład:



Rysunek 27. Nadawanie prawa do publikowania tematu

Tabela 92. Przykładowe wymagania dotyczące dostępu do publikowania

Temat	Wymagany dostęp do publikowania	Obiekt tematu
Cena	Brak użytkownika	Brak
Cena/Warzywa	USER1	VEG

Zdefiniuj nowy obiekt tematu w następujący sposób:

Procedura

1. Wydaj komendę MQSC `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Przyznaj dostęp w następujący sposób:

   - z/OS **z/OS** :

     Nadaj użytkownikowi USER1 dostęp do publikowania w temacie `"Price/Vegetables"` , nadając mu dostęp do profilu `hlq.PUBLISH.VEG` . W tym celu należy użyć następujących komend RACF :

     ```
     RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
     PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
     ```

   - Inne platformy:

     Nadaj użytkownikowi USER1 dostęp do publikowania w temacie `"Price/Vegetables"` , nadając mu dostęp do profilu VEG . W tym celu należy użyć komendy autoryzacji dla platformy:

     ALW **Systemy AIX, Linux, and Windows**

     ```
     setmqaut -t topic -n VEG -p USER1 +pub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
     ```

Wyniki

Gdy USER1 podejmuje próbę opublikowania w temacie `"Price/Vegetables"` , wynik jest pomyślny, tzn. wywołanie MQOPEN kończy się powodzeniem.

Gdy USER2 podejmuje próbę opublikowania w temacie `"Price/Vegetables"` , wywołanie MQOPEN kończy się niepowodzeniem z komunikatem `MQRC_NOT_AUTHORIZED` wraz z następującymi komunikatami:

- z/OS W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ALW Na innych platformach jest to 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 jest to następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Należy zauważyć, że jest to ilustracja przedstawiająca to, co widać, a nie wszystkie pola.

Przyznaj użytkownikowi dostęp do publikowania w temacie znajdującym się głębiej w drzewie

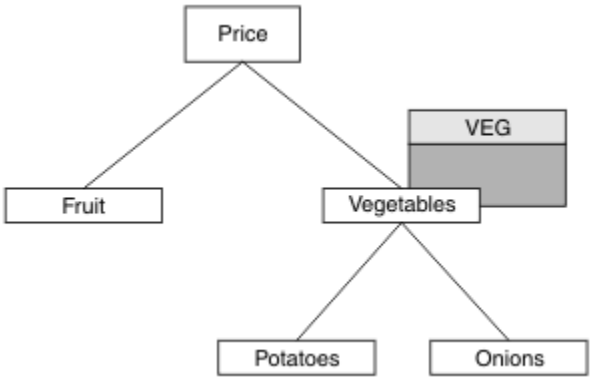
Ten temat jest drugim tematem na liście zadań, który informuje o sposobie nadawania dostępu do publikowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie używana jest konfiguracja opisana w sekcji “Przyznaj użytkownikowi dostęp do publikowania w temacie” na stronie 548.

O tym zadaniu

Jeśli punkt w drzewie tematów, w którym publikowana jest aplikacja, nie jest reprezentowany przez obiekt tematu administracyjnego, należy przenieść drzewo w górę, dopóki nie zostanie znaleziony najbliższy nadrzędny obiekt tematu administracyjnego. Profil zabezpieczeń jest sprawdzany na podstawie nazwy obiektu tematu.



Rysunek 28. Nadawanie prawa do publikowania tematu w drzewie tematów

Tabela 93. 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 poprzedniej czynności USER1 nadano dostęp do tematu publikowania `"Price/Vegetables/Potatoes"` , nadając mu dostęp do profilu `hlq.PUBLISH.VEG` w systemie z/OS lub dostęp do profilu VEG na innych platformach. Ten pojedynczy profil nadaje również USER1 dostęp do publikowania w `"Price/Vegetables/Onions"`.

Gdy USER1 próby publikowania w temacie `"Price/Vegetables/Potatoes"` zakończą się powodzeniem, czyli wywołanie MQOPEN zakończy się powodzeniem.

Gdy funkcja USER2 próbuje zasubskrybować temat `"Price/Vegetables/Potatoes"` , wynikiem jest niepowodzenie. Oznacza to, że wywołanie MQOPEN kończy się niepowodzeniem i wyświetlany jest komunikat `MQRC_NOT_AUTHORIZED` wraz z:

- W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Na innych platformach jest to 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 otrzymywane w systemie z/OS są identyczne z komunikatami otrzymanymi w poprzednim zadaniu, jak te same obiekty tematu i profile kontrolujące dostęp.
- Komunikat zdarzenia odebrany na innych platformach jest podobny do komunikatu odebranego w poprzednim zadaniu, ale rzeczywisty łańcuch tematu jest inny.

Przyznaj dostęp do publikowania i subskrybowania

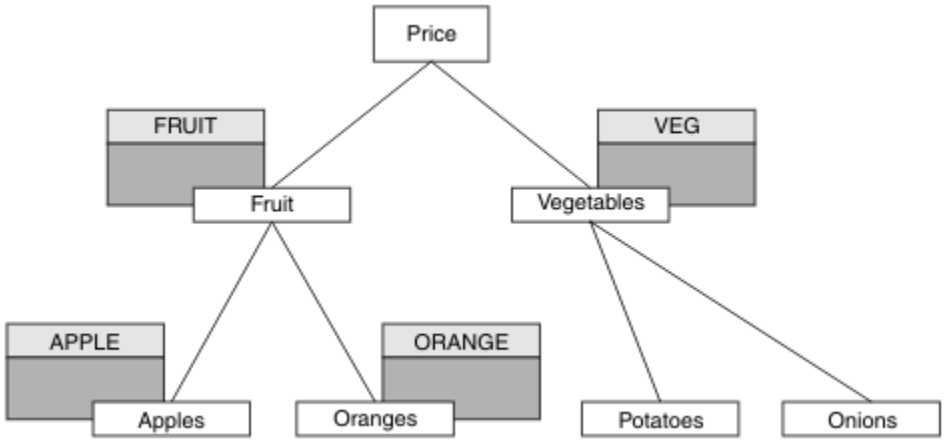
Ten temat jest ostatnim tematem na liście zadań, który informuje o sposobie nadawania dostępu do publikowania i subskrybowania tematów przez więcej niż jednego użytkownika.

Zanim rozpoczniesz

W tym temacie używana jest konfiguracja opisana w sekcji “Przyznaj użytkownikowi dostęp do publikowania w temacie znajdującym się głębiej w drzewie” na stronie 550.

O tym zadaniu

W poprzedniej czynności USER1 nadano dostęp do subskrybowania tematu `"Price/Fruit"`. W tym temacie opisano, w jaki sposób nadać temu użytkownikowi dostęp do publikowania w tym temacie.



Rysunek 29. Nadawanie dostępu do publikowania i subskrybowania

Tabela 94. Przykładowe wymagania dotyczące dostępu do publikowania i subskrybowania

Temat	Wymagany dostęp do subskrypcji	Wymagany 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

Przyznaj dostęp w następujący sposób:

- z/OS **z/OS** :

  We wcześniejszej czynności USER1 nadano dostęp do subskrybowania tematu `"Price/Fruit"` przez nadanie użytkownikowi dostępu do profilu `hlq.SUBSCRIBE.FRUIT` .

  Aby opublikować w temacie `"Price/Fruit"` , nadaj dostęp do pliku USER1 profilowi `hlq.PUBLISH.FRUIT` . W tym celu należy użyć następujących komend RACF :

```
RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
```

- Inne platformy:

  Nadaj użytkownikowi dostęp do USER1 publikowania w temacie `"Price/Fruit"` , nadając mu dostęp do publikowania w profilu FRUIT . W tym celu należy użyć komendy autoryzacji dla platformy:

  ALW **Systemy AIX, Linux, and Windows**

```
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 produkt USER1 podejmuje próbę opublikowania w temacie `"Price/Fruit"` , przechodzi sprawdzanie zabezpieczeń wywołania MQOPEN.

Gdy USER2 podejmuje próbę opublikowania w temacie `"Price/Fruit"` , wynikiem jest niepowodzenie z komunikatem `MQRC_NOT_AUTHORIZED` wraz z:

- z/OS W systemie z/OSsą to następujące komunikaty wyświetlane w konsoli, które przedstawiają pełną ścieżkę zabezpieczeń w drzewie tematów, które próbowano wykonać:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ALW Na platformach AIX, Linux, and Windows jest to 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 IBM ijest to następujące zdarzenie autoryzacji:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Podążając za kompletnym zestawem tych zadań, należy nadać produktowi USER1 i USER2 następujące uprawnienia dostępu do publikowania i subskrybowania wymienionych tematów:

Tabela 95. Pełna lista uprawnień dostępu wynikających z przykładów ochrony

Temat	Wymagany dostęp do subskrypcji	Wymagany 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 istnieją różne wymagania dotyczące dostępu do zabezpieczeń na różnych poziomach w obrębie drzewa tematów, należy zachować ostrożność podczas planowania, aby w dzienniku konsoli z/OS nie pojawiły się dodatkowe ostrzeżenia dotyczące zabezpieczeń. Skonfigurowanie zabezpieczeń na odpowiednim poziomie w drzewie pozwala uniknąć wprowadzania w błąd komunikatów bezpieczeństwa.

Zabezpieczenia subskrypcji

MQSO_ALTERNATE_UPRAWNIENIA_UŻYTKOWNIKA

Pole identyfikatora AlternateUserzawiera identyfikator użytkownika używany do sprawdzania poprawności tego wywołania MQSUB. Wywołanie może zakończyć się powodzeniem tylko wtedy, gdy ten identyfikator AlternateUserjest autoryzowany do subskrybowania tematu z określonymi opcjami dostępu, niezależnie od tego, czy identyfikator użytkownika, pod którym działa aplikacja, jest do tego uprawniony.

MQSO_SET_IDENTITY_CONTEXT,

Subskrypcja ma używać tokenu rozliczania i danych tożsamości aplikacji podanych w polach PubAccountingToken i PubApplIdentityData .

Jeśli ta opcja jest określona, wykonywane jest takie samo sprawdzenie autoryzacji, jak w przypadku dostępu do kolejki docelowej za pomocą wywołania MQOPEN z opcją MQOO_SET_IDENTITY_CONTEXT, z wyjątkiem sytuacji, gdy opcja MQSO_MANAGED jest również używana, w której to przypadku nie ma sprawdzania autoryzacji w kolejce docelowej.

Jeśli ta opcja nie jest określona, publikacje wysyłane do tego subskrybenta mają powiązane domyślne informacje o kontekście w następujący sposób:

Tabela 96. Informacje o domyślnym kontekście publikacji	
Pole w strukturze MQMD	**Użyta wartość**
UserIdentifier	Identyfikator użytkownika powiązany z subskrypcją (patrz pole SUBUSER w DISPLAY SBSTATUS) w momencie publikowania.
AccountingToken	Określana na podstawie środowiska, jeśli jest to możliwe; w przeciwnym razie ustawiana jest wartość MQACT_NONE.
Dane_tożsamości_aplikacji	Ustaw na wartość pustą.

Ta opcja jest poprawna tylko z opcjami MQSO_CREATE i MQSO_ALTER. W przypadku użycia z opcją MQSO_RESUME pola PubAccountingToken i PubApplIdentityData są ignorowane, więc ta opcja nie ma zastosowania.

Jeśli subskrypcja zostanie zmieniona bez użycia tej opcji, gdy wcześniej subskrypcja dostarczyła informacje o kontekście tożsamości, dla zmienionej subskrypcji zostaną wygenerowane domyślne informacje o kontekście.

Jeśli subskrypcja zezwalająca różnym identyfikatorom użytkowników na korzystanie z niej z opcją MQSO_ANY_USERID jest wznawiana przez inny ID użytkownika, dla nowego ID użytkownika będącego właścicielem subskrypcji generowany jest domyślny kontekst tożsamości, a wszystkie kolejne publikacje są dostarczane z nowym kontekstem tożsamości.

Identyfikator AlternateSecurity

Jest to identyfikator bezpieczeństwa, który jest przekazywany z identyfikatorem AlternateUserdo usługi autoryzacji w celu umożliwienia przeprowadzenia odpowiednich sprawdzeń autoryzacji. AlternateSecurityIdentyfikator jest używany tylko wtedy, gdy określono wartość MQSO_ALTERNATE_USER_AUTHORITY, a pole identyfikatora AlternateUsernie jest całkowicie puste aż do pierwszego znaku o kodzie zero lub końca pola.

Opcja subskrypcji MQSO_ANY_USERID

Jeśli określono opcję MQSO_ANY_USERID, tożsamość subskrybenta nie jest ograniczona do pojedynczego identyfikatora użytkownika. Dzięki temu każdy użytkownik może zmienić lub wznowić subskrypcję, gdy ma odpowiednie uprawnienia. Subskrypcja może być dostępna tylko dla jednego użytkownika w danym momencie. Próba wznowienia korzystania z subskrypcji aktualnie używanej przez inną aplikację spowoduje, że wywołanie nie powiedzie się i zostanie użyta komenda MQRC_SUBSCRIPTION_IN_USE.

Aby dodać tę opcję do istniejącej subskrypcji, wywołanie MQSUB (przy użyciu MQSO_ALTER) musi pochodzić z tego samego identyfikatora użytkownika, co pierwotna subskrypcja.

Jeśli wywołanie MQSUB odwołuje się do istniejącej subskrypcji z ustawioną wartością MQSO_ANY_USERID, a identyfikator użytkownika różni się od oryginalnej subskrypcji, wywołanie powiedzie się tylko wtedy, gdy nowy identyfikator użytkownika ma uprawnienie do subskrybowania tematu. Po pomyślnym zakończeniu działania przyszłe publikacje dla tego subskrybenta są umieszczane w kolejce subskrybenta z nowym identyfikatorem użytkownika ustawionym w publikacji.

MQSO_FIXED_USERID (Identyfikator stałego użytkownika)

Jeśli określono parametr MQSO_FIXED_USERID, subskrypcja może być zmieniana lub wznawiana tylko przez jeden ID użytkownika będącego właścicielem. Ten ID użytkownika jest ostatnim ID użytkownika, który zmienił subskrypcję, która ustawiła tę opcję, usuwając w ten sposób opcję MQSO_ANY_USERID, lub jeśli nie zostały wykonane żadne zmiany, jest to ID użytkownika, który utworzył subskrypcję.

Jeśli komenda MQSUB odwołuje się do istniejącej subskrypcji z ustawionym identyfikatorem MQSO_ANY_USERID i modyfikuje subskrypcję (za pomocą komendy MQSO_ALTER) w celu użycia opcji MQSO_FIXED_USERID, identyfikator użytkownika subskrypcji jest teraz poprawiany przy użyciu tego nowego identyfikatora użytkownika. Wywołanie powiedzie się tylko wtedy, gdy nowy ID użytkownika ma uprawnienia do subskrybowania tematu.

Jeśli identyfikator użytkownika inny niż ten, który został zarejestrowany jako właściciel subskrypcji, ma możliwość wznowienia lub zmiany subskrypcji MQSO_FIXED_USERID, wywołanie nie powiedzie się z błędem MQRC_IDENTITY_MISMATCH. Identyfikator użytkownika będącego właścicielem subskrypcji można wyświetlić za pomocą komendy DISPLAY SBSTATUS.

Jeśli nie określono ani MQSO_ANY_USERID, ani MQSO_FIXED_USERID, wartością domyślną jest MQSO_FIXED_USERID.

Zabezpieczenia publikowania/subskrypcji między menedżerami kolejek

Wewnętrzne komunikaty publikowania/subskrypcji, takie jak subskrypcje proxy i publikacje, są umieszczane w kolejkach systemowych publikowania/subskrypcji przy użyciu zwykłych reguł zabezpieczeń kanału. Informacje i diagramy w tym temacie zawierają informacje o różnych procesach i identyfikatorach użytkowników uczestniczących w dostarczaniu tych komunikatów.

Lokalna kontrola dostępu

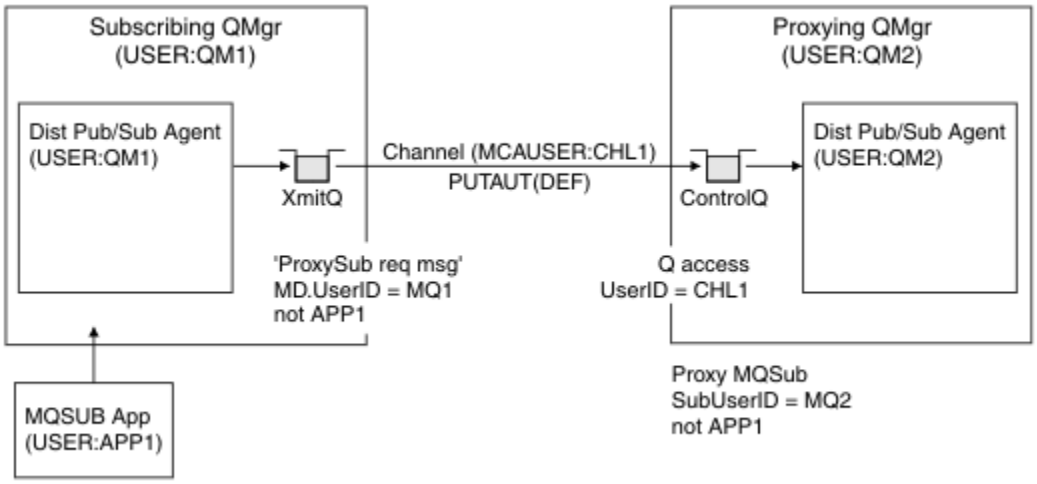
Dostęp do tematów związanych z publikowaniem i subskrypcjami jest zarządzany przez lokalne definicje zabezpieczeń i reguły opisane w sekcji Zabezpieczenia publikowania/subskrypcji. W systemie z/OSdo ustanowienia kontroli dostępu nie jest wymagany żaden lokalny obiekt tematu. Do kontroli dostępu na innych platformach nie jest wymagany żaden temat lokalny. Administratorzy mogą zastosować kontrolę dostępu do obiektów tematów w klastrze, bez względu na to, czy istnieją one jeszcze w klastrze.

Administratorzy systemu są odpowiedzialni za kontrolę dostępu w systemie lokalnym. Muszą oni ufać administratorom innych elementów hierarchii lub kolektywów klastra, którzy są odpowiedzialni za swoją strategię kontroli dostępu. Ponieważ kontrola dostępu jest definiowana dla każdego oddzielnego komputera, prawdopodobnie będzie uciążliwa, jeśli wymagana jest precyzyjna kontrola poziomu. Może nie być konieczne narzucanie jakiejkolwiek kontroli dostępu lub kontrola dostępu może być zdefiniowana dla obiektów wysokiego poziomu w drzewie tematów. Precyzyjną kontrolę dostępu można zdefiniować dla każdego podobszaru przestrzeni nazw tematów.

Tworzenie subskrypcji proxy

Zaufanie dla organizacji do połączenia swojego menedżera kolejek z menedżerem kolejek jest potwierdzane przez zwykłe uwierzytelnianie kanału. Jeśli ta zaufana organizacja może również wykonywać dystrybuowane publikowanie/subskrypcję, wykonywane jest sprawdzanie uprawnień. Sprawdzenie jest wykonywane, gdy kanał umieszcza komunikat w rozproszonej kolejce publikowania/subskrybowania. Na przykład, jeśli komunikat jest umieszczany w kolejce `SYSTEM.INTER.QMGR.CONTROL` . Identyfikator użytkownika dla sprawdzenia uprawnień do kolejki zależy od wartości `PUTAUT` kanału odbiorczego. Na przykład identyfikator użytkownika kanału, `MCAUSER`, kontekst komunikatu, w zależności od wartości i platformy. Więcej informacji na temat zabezpieczeń kanału zawiera sekcja Zabezpieczenia kanału.

Subskrypcje proxy są wykonywane przy użyciu identyfikatora użytkownika rozproszonego agenta publikowania/subskrypcji w zdalnym menedżerze kolejek. Na przykład `QM2` w pliku Rysunek 30 na stronie 557. Użytkownik może łatwo uzyskać dostęp do lokalnych profili obiektów tematu, ponieważ ten identyfikator użytkownika jest zdefiniowany w systemie i dlatego nie ma konfliktów domen.



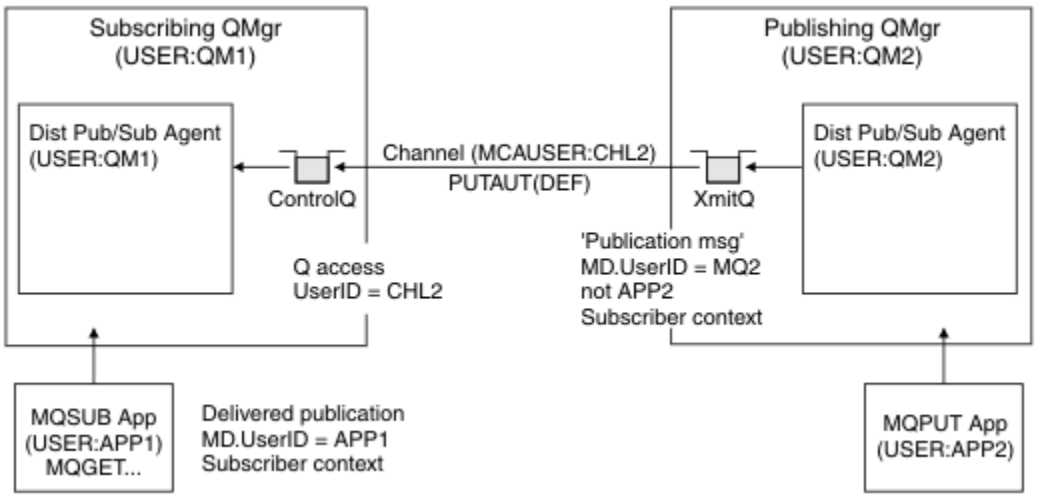
Rysunek 30. Zabezpieczenia subskrypcji proxy, tworzenie subskrypcji

Wysyłanie zdalnych publikacji

Gdy publikacja jest tworzona w menedżerze kolejek publikowania, dla każdej subskrypcji proxy tworzona jest kopia tej publikacji. Kontekst skopiowanej publikacji zawiera kontekst identyfikatora użytkownika, który dokonał subskrypcji; QM2 w programie Rysunek 31 na stronie 557. Subskrypcja proxy jest tworzona z kolejką docelową, która jest kolejką zdalną, dlatego komunikat publikacji jest tłumaczony na kolejkę transmisji.

Zaufanie organizacji do połączenia swojego menedżera kolejek QM2z innym menedżerem kolejek QM1jest potwierdzane przez zwykłe uwierzytelnianie kanału. Jeśli ta zaufana organizacja może wykonywać rozproszone publikowanie/subskrypcję, sprawdzanie uprawnień jest wykonywane, gdy kanał umieszcza komunikat publikacji w rozproszonej kolejce publikowania/subskrypcji SYSTEM.INTER.QMGR.PUBS. Identyfikator użytkownika dla sprawdzania uprawnień do kolejki zależy od wartości PUTAUT kanału odbiorczego (na przykład ID użytkownika kanału, MCAUSER, kontekst komunikatu i inne, w zależności od wartości i platformy). Więcej informacji na temat zabezpieczeń kanału zawiera sekcja Zabezpieczenia kanału.

Gdy komunikat publikacji dotrze do subskrybującego menedżera kolejek, kolejne wywołanie MQPUT do tematu jest wykonywane z uprawnieniami tego menedżera kolejek, a kontekst z komunikatem jest zastępowany przez kontekst każdego z lokalnych subskrybentów, ponieważ każdy z nich otrzymuje komunikat.



Rysunek 31. Zabezpieczenia subskrypcji proxy, przekazywanie publikacji

W systemie, w którym niewiele zostało rozważonych pod względem zabezpieczeń, rozproszone procesy publikowania/subskrypcji prawdopodobnie działają z 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 skonfigurowanie weryfikacji koncepcji w celu zademonstrowania rozproszonego publikowania i subskrybowania.

W systemie, w którym bezpieczeństwo jest poważniej brane pod uwagę, te wewnętrzne komunikaty podlegają tym samym mechanizmami ochrony, co każdy komunikat przesyłany przez kanał.

Jeśli kanał jest skonfigurowany z niepustą wartością `MCAUSER` i wartością `PUTAUT` określającą, że opcja `MCAUSER` musi być zaznaczona, należy nadać dostęp do kolejek `SYSTEM.INTER.QMGR.*` danemu `MCAUSER` . Jeśli istnieje wiele różnych zdalnych menedżerów kolejek z kanałami działającymi z różnymi identyfikatorami `MCAUSER` , wszystkim tym identyfikatorom użytkowników należy nadać dostęp do kolejek systemu `SYSTEM.INTER.QMGR.*` . Kanały działające z różnymi identyfikatorami `MCAUSER` mogą wystąpić na przykład wtedy, gdy w pojedynczym menedżerze kolejek skonfigurowano wiele połączeń hierarchicznych.

Jeśli kanał jest skonfigurowany przy użyciu wartości `PUTAUT` określającej, że używany jest kontekst komunikatu, dostęp do kolejek systemu `SYSTEM.INTER.QMGR.*` jest sprawdzany na podstawie identyfikatora użytkownika wewnątrz komunikatu wewnętrznego. Ponieważ wszystkie te komunikaty są umieszczane z identyfikatorem użytkownika rozproszonego agenta publikowania/subskrypcji z menedżera kolejek, który wysyła komunikat wewnętrzny lub komunikat publikacji (patrz sekcja Rysunek 31 na stronie 557), nie jest to zbyt duży zestaw identyfikatorów użytkowników, aby nadać dostęp do różnych kolejek systemowych (po jednej na zdalny menedżer kolejek), jeśli zabezpieczenia rozproszonego publikowania/subskrypcji mają zostać skonfigurowane w ten sposób. Nadal występują takie same problemy, jak w przypadku zabezpieczeń kontekstu kanału: różne domeny identyfikatorów użytkowników i fakt, że identyfikator użytkownika w komunikacie może nie być zdefiniowany w systemie odbierającym. Jest to jednak całkowicie akceptowalny sposób na uruchomienie w razie potrzeby.

z/OS Zabezpieczenia kolejki systemowej udostępniają listę kolejek i dostęp wymagany do bezpiecznego skonfigurowania rozproszonego środowiska publikowania/subskrypcji. Jeśli jakiekolwiek wewnętrzne komunikaty lub publikacje nie zostaną umieszczone z powodu naruszenia bezpieczeństwa, kanał zapisuje komunikat w dzienniku w normalny sposób, a komunikaty mogą zostać wysłane do kolejki niedostarczonych komunikatów zgodnie z normalnym przetwarzaniem błędów kanału.

Wszystkie funkcje przesyłania komunikatów między menedżerami kolejek na potrzeby rozproszonego publikowania/subskrypcji są uruchamiane przy użyciu zwykłych zabezpieczeń kanału.

Informacje na temat ograniczania publikowania i subskrypcji proxy na poziomie tematu zawiera sekcja Zabezpieczenia publikowania/subskrybowania.

Używanie domyślnych identyfikatorów użytkowników z hierarchią menedżera kolejek

Jeśli istnieje hierarchia menedżerów kolejek działających na różnych platformach i używane są domyślne identyfikatory użytkowników, należy zauważyć, że te domyślne identyfikatory użytkowników różnią się w zależności od platformy i mogą nie być znane na platformie docelowej. W wyniku tego menedżer kolejek działający na jednej platformie odrzuca komunikaty odebrane od menedżerów kolejek na innych platformach z kodem przyczyny `MQRC_NOT_AUTHORIZED`.

Aby uniknąć odrzucania komunikatów, należy dodać przynajmniej następujące uprawnienia do domyślnych identyfikatorów użytkowników używanych na innych platformach:

- Uprawnienie *PUT *GET w systemie SYSTEM.BROKER. kolejki
- *PUB Uprawnienie *SUB w systemie SYSTEM.BROKER. tematy
- Uprawnienia *ADMCRT *ADMDLT *ADMCHG w systemie SYSTEM.BROKER.CONTROL.QUEUE .

Domyślne identyfikatory użytkowników z hierarchią menedżera kolejek są następujące:

Platforma	Domyślny identyfikator użytkownika
Windows	`mqm`
Systemy AIX and Linux	`mqm`
IBM i	`QMQM`
z/OS	ID użytkownika przestrzeni adresowej inicjatora kanału

Utwórz i nadaj dostęp do identyfikatora użytkownika 'qmqm', jeśli jest on hierarchicznie przyłączony do menedżera kolejek w systemie IBM i dla menedżerów kolejek na platformach z/OSi AIX, Linux, and Windows .

W przypadku menedżerów kolejek na platformach IBM i i z/OS należy utworzyć i nadać dostęp do identyfikatora użytkownika mqm, jeśli jest on hierarchicznie przyłączony do menedżera kolejek w systemie AIX, Linux, and Windows .

Utwórz i nadaj użytkownikowi dostęp do ID użytkownika przestrzeni adresowej inicjatora kanału z/OS , jeśli jest on hierarchicznie przyłączony do menedżera kolejek w programie z/OS dla menedżerów kolejek w systemie Wiele platform.

W identyfikatorach użytkowników może być rozróżniana wielkość liter. Pierwotny menedżer kolejek (jeśli jest używany w systemie Wiele platform) wymusza używanie wielkich liter w ID użytkownika. Odbierający menedżer kolejek (jeśli jest w systemie AIX, Linux, and Windows) wymusza, aby identyfikator użytkownika był pisany małymi literami. Oznacza to, że wszystkie identyfikatory użytkowników utworzone w systemach AIX and Linux muszą być zapisane małymi literami. Jeśli program obsługi wyjścia komunikatów został zainstalowany, wymuszenie wprowadzenia wielkich lub małych liter w ID użytkownika nie ma miejsca. Należy zachować ostrożność, aby zrozumieć, w jaki sposób wyjście komunikatu przetwarza identyfikator użytkownika.

Aby uniknąć potencjalnych problemów z konwersją identyfikatorów użytkowników:

- W systemach AIX, Linux, and Windows należy upewnić się, że identyfikatory użytkowników zostały podane małymi literami.
- W systemach IBM i i z/OSnależy upewnić się, że identyfikatory użytkowników zostały podane wielkimi literami.

Bezpieczeństwo systemów IBM MQ Console i REST API

Zabezpieczenia produktów IBM MQ Console i REST API są konfigurowane przez edycję konfiguracji serwera mqweb w pliku `mqwebuser.xml` .

O tym zadaniu

Użytkownik może śledzić działania użytkownika i kontrolować użycie komend IBM MQ Console i REST API , sprawdzając pliki dziennika serwera mqweb.

Użytkownicy produktów IBM MQ Console i REST API mogą być uwierzytelniani za pomocą:

- Rejestr podstawowy
- Rejestr LDAP
- Rejestr lokalnego systemu operacyjnego
- SAF w systemie z/OS
- Dowolny inny typ rejestru obsługiwany przez WebSphere Liberty

Role można przypisać do użytkowników programu IBM MQ Console oraz do użytkowników programu REST API , aby określić poziom dostępu, jaki mają oni do obiektów programu IBM MQ . Aby na przykład wykonywać przesyłanie komunikatów, użytkownicy muszą mieć przypisaną rolę `MQWebUser` . Więcej informacji na temat dostępnych ról zawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

Po przypisaniu użytkownikowi roli istnieje wiele metod, których można użyć do uwierzytelnienia użytkownika. W programie IBM MQ Consoleużytkownicy mogą logować się przy użyciu nazwy użytkownika i hasła lub mogą używać uwierzytelniania przy użyciu certyfikatu klienta. W produkcie REST APIużytkownicy mogą używać podstawowego uwierzytelniania HTTP , uwierzytelniania opartego na znacznikach lub uwierzytelniania przy użyciu certyfikatu klienta.

Procedura

1. Zdefiniuj rejestr użytkowników, aby uwierzytelniać użytkowników, i przypisz każdemu użytkownikowi lub grupie rolę, aby autoryzować użytkowników i grupy do korzystania z IBM MQ Console lub REST API. Więcej informacji: “Konfigurowanie użytkowników i ról” na stronie 561
2. Wybierz sposób uwierzytelniania użytkowników produktu IBM MQ Console na serwerze mqweb. Nie trzeba używać tej samej metody dla wszystkich użytkowników:
   - Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować czas utraty ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
   - Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.
3. Wybierz sposób uwierzytelniania użytkowników produktu REST API na serwerze mqweb. Nie trzeba używać 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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
   - Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582.

     Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Jeśli jednak włączono połączenia HTTP , można zezwolić na używanie znacznika LTPA, który jest generowany dla połączenia HTTPS dla połączenia HTTP . Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
   - Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.
4. Opcjonalne: Skonfiguruj współużytkowanie zasobów między źródłami dla REST API.

   Domyślnie przeglądarka WWW nie zezwala skryptom, takim jak JavaScript, na wywoływanie skryptu REST API , gdy skrypt nie pochodzi z tego samego źródła co skrypt REST API. Oznacza to, że żądania z różnych źródeł nie są włączone. Można skonfigurować mechanizm CORS (Cross-Origin Resource Sharing), aby zezwolić na żądania między źródłami z określonych adresów URL. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie mechanizmu CORS dla serwera REST API” na stronie 585.
5. Opcjonalne: Skonfiguruj sprawdzanie poprawności nagłówka hosta dla IBM MQ Console i REST API.

Można skonfigurować sprawdzanie poprawności nagłówków hostów i utworzyć listę zaakceptowanych nazw hostów i portów, aby zapewnić, że tylko żądania zawierające konkretne nagłówki hostów będą przetwarzane przez IBM MQ Console i REST API. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie sprawdzania poprawności nagłówka hosta dla IBM MQ Console i REST API” na stronie 586.

Konfigurowanie użytkowników i ról

Aby użyć produktu IBM MQ Console lub produktu REST API, użytkownicy muszą uwierzytelnić 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. Należy je dodać, edytując plik `mqwebuser.xml` .

Podczas konfigurowania użytkowników i grup należy najpierw skonfigurować rejestr użytkowników na potrzeby uwierzytelniania użytkowników i grup. Ten rejestr użytkowników jest współużytkowany przez serwer IBM MQ Console i serwer REST API. Podczas konfigurowania ról dla użytkowników i grup można określić, czy użytkownicy i grupy mają mieć dostęp do IBM MQ Console, REST API, czy obu tych elementów.

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 produktu REST API for Managed File Transfer. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

Z serwerem mqweb udostępniono pewną liczbę przykładowych plików XML, aby uprościć konfigurację użytkowników i grup. Użytkownicy, którzy są zaznajomieni z konfigurowaniem zabezpieczeń w produkcie WebSphere Liberty (WLP), mogą nie korzystać z przykładów. WLP udostępnia inne możliwości autoryzacji oprócz tych opisanych w tym miejscu.

Procedura

- Skonfiguruj użytkowników i grupy z podstawowym rejestrem, używając 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 przy użyciu przykładowego pliku `basic_registry.xml` , należy zapoznać się z sekcją “Konfigurowanie rejestru podstawowego dla produktów IBM MQ Console i REST API” na stronie 562.
- Skonfiguruj użytkowników i grupy z rejestrem LDAP za pomocą pliku `ldap_registry.xml` .

  Nazwy użytkowników i hasła w rejestrze LDAP są używane do uwierzytelniania i autoryzowania użycia IBM MQ Console i REST API.

  Aby skonfigurować rejestr LDAP przy użyciu przykładowego pliku `ldap_registry.xml` , należy zapoznać się z sekcją “Konfigurowanie rejestru LDAP dla produktów IBM MQ Console i REST API” na stronie 567.
- ALW

  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 autoryzowania użytkowników produktów IBM MQ Console i REST API.

  Aby skonfigurować rejestr lokalnego systemu operacyjnego przy użyciu przykładowego pliku `local_os_registry.xml` , należy zapoznać się z sekcją “Konfigurowanie rejestru lokalnego systemu operacyjnego dla IBM MQ Console i REST API” na stronie 566.

- z/OS
  Konfigurowanie użytkowników i grup za pomocą interfejsu SAF (System Authorization Facility) w systemie z/OS przy użyciu pliku `zos_saf_registry.xml` .

  Profile RACFlub innego produktu zabezpieczania są używane do nadawania użytkownikom i grupom dostępu do ról. Nazwy i hasła użytkowników w bazie danych RACF są używane do uwierzytelniania i autoryzowania użytkowników produktów IBM MQ Console i REST API.

  Aby skonfigurować interfejs SAF przy użyciu przykładowego pliku `zos_saf_registry.xml` , należy zapoznać się z sekcją “Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API” na stronie 570.
- Za pomocą pliku `no_security.xml` należy wyłączyć zabezpieczenia, w tym możliwość uzyskania dostępu do serwera IBM MQ Consolelub serwera REST APIprzy użyciu protokołu HTTPS.

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować okres ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582. Można skonfigurować okres ważności znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

Konfigurowanie rejestru podstawowego dla produktów IBM MQ Console i REST API

Podstawowy rejestr można skonfigurować w pliku `mqwebuser.xml` . Nazwy użytkowników, hasła i role w pliku XML są używane do uwierzytelniania i autoryzowania użytkowników IBM MQ Console i REST API.

Zanim rozpoczniesz

- Konfigurując użytkowników w rejestrze podstawowym, należy przypisać każdemu użytkownikowi 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 podstawowego należy zapoznać się z tymi rolami. Więcej informacji na temat każdej z ról zawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.
- Aby wykonać tę czynność, użytkownik musi mieć uprawnienia wystarczające do edytowania pliku `mqwebuser.xml` :
  - z/OS W systemie z/OSwymagane jest uprawnienie do zapisu w pliku `mqwebuser.xml` .
  - Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.
  - V 9.3.5 Linux Jeśli serwer mqweb jest częścią autonomicznej instalacji produktu IBM MQ Web Server , użytkownik musi mieć dostęp do zapisu do pliku `mqwebuser.xml` w katalogu danych produktu IBM MQ Web Server .

Procedura

1. Skopiuj przykładowy plik XML `basic_registry.xml` z jednej z następujących ścieżek:
   - W przypadku instalacji w systemie IBM MQ :
     - ALW W systemie AIX, 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 for z/OS UNIX System Services Components .
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     gdzie *MQWEB_INSTALLATION_PATH* jest katalogiem, w którym zdekompresowano plik instalacyjny IBM MQ Web Server .
2. Umieść plik przykładowy w odpowiednim katalogu:
   - W przypadku instalacji w systemie IBM MQ :
     - Linux AIX W systemie AIX lub Linux: `/var/mqm/web/installations/`*installationName*`/servers/mqweb`
     - Windows W systemie Windows: *MQ_DATA_PATH*`\web\installations\`*installationName*`\servers\mqweb`, gdzie *MQ_DATA_PATH* jest ścieżką danych IBM MQ . Ta ścieżka jest ścieżką danych wybraną podczas instalowania produktu IBM MQ. Domyślna ścieżka to `C:\ProgramData\IBM\MQ`.
     - z/OS W systemie z/OS: *WLP_user_directory*`/servers/mqweb`

       gdzie *WLP_user_directory* to katalog określony podczas wykonywania skryptu **crtmqweb** w celu utworzenia definicji serwera mqweb.
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     gdzie *MQ_OVERRIDE_DATA_PATH* jest katalogiem danych produktu IBM MQ Web Server , na który wskazuje zmienna środowiskowa **MQ_OVERRIDE_DATA_PATH** .
3. Opcjonalne: Jeśli w pliku `mqwebuser.xml`zostały zmienione jakiekolwiek ustawienia konfiguracyjne, należy je skopiować do pliku przykładowego.

4. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę przykładowego pliku na `mqwebuser.xml`.
5. Zmodyfikuj nowy plik `mqwebuser.xml` , aby dodać użytkowników i grupy w obrębie znaczników **basicRegistry** .

   Należy pamiętać, że każdy użytkownik z rolą `MQWebUser` może wykonywać w menedżerze kolejek tylko te operacje, które zostały nadane identyfikatorowi użytkownika. Dlatego identyfikator użytkownika zdefiniowany w rejestrze musi mieć identyczny identyfikator użytkownika w systemie, w którym jest zainstalowany produkt IBM MQ . Te identyfikatory użytkowników muszą być w tym samym przypadku, w przeciwnym razie odwzorowanie między identyfikatorami użytkowników może się nie powieść.

   Więcej informacji na temat konfigurowania podstawowych rejestrów użytkowników zawiera sekcja Konfigurowanie podstawowego rejestru użytkowników dla serwera Liberty w dokumentacji serwera 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 IBM MQ Consolei REST API. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

   - Aby przypisać role i nadać dostęp do IBM MQ Console, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach **<enterpriseApplication id="com.ibm.mq.console">** .
   - Aby przypisać role i nadać dostęp do REST API, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach **<enterpriseApplication id="com.ibm.mq.rest">** .

   Aby uzyskać pomoc dotyczącą formatu informacji o użytkownikach i grupach w obrębie znaczników **security-role** , należy zapoznać się z przykładami.
7. Jeśli w pliku `mqwebuser.xml`podano hasła dla użytkowników, należy je zakodować, aby były bezpieczniejsze, za pomocą komendy **securityUtility encoding** udostępnianej przez WebSphere Liberty. Więcej informacji na ten temat zawiera sekcja Liberty:securityUtility w dokumentacji produktu WebSphere Liberty .

Przykład

W poniższym przykładzie grupie `MQWebAdminGroup` nadano dostęp do pliku IBM MQ Console z rolą `MQWebAdmin`. Użytkownik `reader`ma nadany dostęp z rolą `MQWebAdminRO`, a użytkownik `guest` ma nadany 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 użytkownikom `reader` i `guest` nadano dostęp do IBM MQ Console. Użytkownikowi `user` jest nadawany dostęp do pliku REST API, a wszyscy użytkownicy w grupie `MQAdmin` mają dostęp do pliku IBM MQ Console i pliku REST API. Użytkownik `mftadmin` ma nadany dostęp do pliku 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 tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować okres ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582. Można skonfigurować okres ważności znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

ALW Konfigurowanie rejestru lokalnego systemu operacyjnego dla IBM MQ Console i REST API

W pliku `mqwebuser.xml` można skonfigurować rejestr lokalnego systemu operacyjnego. Nazwy i hasła użytkowników w lokalnym systemie operacyjnym są używane do uwierzytelniania i autoryzowania użytkowników IBM MQ Console i REST API.

Zanim rozpoczniesz

- W przypadku uwierzytelniania przy użyciu certyfikatu klienta za pomocą funkcji 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 przy użyciu certyfikatu klienta nie powiedzie się i zostanie przywróone uwierzytelnianie oparte na haśle.
- Aby wykonać tę czynność, użytkownik musi mieć uprawnienia wystarczające do edytowania pliku `mqwebuser.xml` :
  - V 9.3.5 Linux Jeśli serwer mqweb jest częścią autonomicznej instalacji produktu IBM MQ Web Server , użytkownik musi mieć dostęp do zapisu do pliku `mqwebuser.xml` w katalogu danych produktu IBM MQ Web Server .
  - Jeśli serwer mqweb jest częścią instalacji produktu IBM MQ , użytkownik musi być użytkownikiem uprzywilejowanym.

O tym zadaniu

W przypadku rejestru lokalnego systemu operacyjnego użytkownicy i grupy są automatycznie przypisywani do roli:

- Każdemu użytkownikowi, który jest częścią grupy mqm lub grupy QMQMADM w systemie IBM i, nadawane są role `MQWebAdmin` i `MFTWebAdmin` .
- Wszystkim pozostałym użytkownikom zostanie nadana rola `MQWebUser` .

Więcej informacji na temat tych ról zawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

Rejestr lokalnego systemu operacyjnego może być używany tylko w systemie AIX, Linux, and Windows. Równoważna funkcja jest udostępniana w systemie z/OS przez skonfigurowanie rejestru SAF. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API” na stronie 570.

Procedura

1. Skopiuj przykładowy plik XML `local_os_registry.xml` z jednej z następujących ścieżek:
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     gdzie *MQWEB_INSTALLATION_PATH* jest katalogiem, w którym zdekompresowano plik instalacyjny IBM MQ Web Server .
   - W przypadku instalacji w systemie IBM MQ : *MQ_INSTALLATION_PATH*`/web/mq/samp/configuration`
2. Umieść plik przykładowy w jednym z następujących katalogów:
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     gdzie *MQ_OVERRIDE_DATA_PATH* jest katalogiem danych produktu IBM MQ Web Server , na który wskazuje zmienna środowiskowa **MQ_OVERRIDE_DATA_PATH** .

- W instalacji systemu IBM MQ : *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb

3. Opcjonalne: Jeśli w pliku mqwebuser.xmlzostały zmienione jakiekolwiek ustawienia konfiguracyjne, należy je skopiować do pliku przykładowego.
4. Usuń istniejący plik mqwebuser.xml i zmień nazwę przykładowego pliku na mqwebuser.xml.

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować okres ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API login za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582. Można skonfigurować okres ważności znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

Konfigurowanie rejestru LDAP dla produktów 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 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 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 systemach IBM MQ Console i REST API” na stronie 572.

Należy pamiętać, że każdy użytkownik z rolą `MQWebUser` może wykonywać w menedżerze kolejek tylko te operacje, które zostały nadane identyfikatorowi użytkownika. 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, w przeciwnym razie odwzorowanie między identyfikatorami użytkowników może się nie powieść.

- Aby wykonać tę czynność, użytkownik musi mieć uprawnienia wystarczające do edytowania pliku `mqwebuser.xml` :
  - z/OS W systemie z/OSwymagane jest uprawnienie do zapisu w pliku `mqwebuser.xml` .
  - Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.
  - V 9.3.5 Linux Jeśli serwer mqweb jest częścią autonomicznej instalacji produktu IBM MQ Web Server , użytkownik musi mieć dostęp do zapisu do pliku `mqwebuser.xml` w katalogu danych produktu IBM MQ Web Server .

Procedura

1. Skopiuj przykładowy plik XML `ldap_registry.xml` z jednej z następujących ścieżek:
   - W przypadku instalacji w systemie IBM MQ :
     - ALW W systemie AIX, 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 for z/OS UNIX System Services Components .
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQWEB_INSTALLATION_PATH*`/web/mq/samp/configuration`

     gdzie *MQWEB_INSTALLATION_PATH* jest katalogiem, w którym zdekompresowano plik instalacyjny IBM MQ Web Server .
2. Umieść plik przykładowy w odpowiednim katalogu:
   - W przypadku instalacji w systemie IBM MQ :
     - Linux AIX W systemie AIX lub Linux: `/var/mqm/web/installations/`*installationName*`/servers/mqweb`
     - Windows W systemie Windows: *MQ_DATA_PATH*`\web\installations\`*installationName*`\servers\mqweb`, gdzie *MQ_DATA_PATH* jest ścieżką danych IBM MQ . Ta ścieżka jest ścieżką danych wybraną podczas instalowania produktu IBM MQ. Domyślna ścieżka to `C:\ProgramData\IBM\MQ`.
     - z/OS W systemie z/OS: *WLP_user_directory*`/servers/mqweb`

       gdzie *WLP_user_directory* to katalog określony podczas wykonywania skryptu **crtmqweb** w celu utworzenia definicji serwera mqweb.
   - V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQ_OVERRIDE_DATA_PATH*`/web/installations/MQWEBINST/servers/mqweb`

     gdzie *MQ_OVERRIDE_DATA_PATH* jest katalogiem danych produktu IBM MQ Web Server , na który wskazuje zmienna środowiskowa **MQ_OVERRIDE_DATA_PATH** .
3. Opcjonalne: Jeśli w pliku `mqwebuser.xml`zostały zmienione jakiekolwiek ustawienia konfiguracyjne, należy je skopiować do pliku przykładowego.

4. Usuń istniejący plik `mqwebuser.xml` i zmień nazwę przykładowego pliku na `mqwebuser.xml`.
5. Zmodyfikuj 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 na serwerze Liberty w dokumentacji serwera 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 IBM MQ Consolei REST API. Każda rola nadaje inny poziom dostępu. Więcej informacji na ten tematzawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

   - Aby przypisać role i nadać dostęp do IBM MQ Console, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach **<enterpriseApplication id="com.ibm.mq.console">** .
   - Aby przypisać role i nadać dostęp do REST API, należy dodać użytkowników i grupy między odpowiednimi znacznikami **security-role** w znacznikach **<enterpriseApplication id="com.ibm.mq.rest">** .

Co dalej

Wybierz sposób uwierzytelniania użytkowników:

IBM MQ Console Opcje uwierzytelnienia

- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować okres ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582. Można skonfigurować okres ważności znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

z/OS 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 systemach IBM MQ Console i REST API” na stronie 572.
- 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 9.3.5 V 9.3.0.20 W produkcie IBM MQ 9.3.5 for Continuous Delivery i w produkcie IBM MQ 9.3.0 Fix Pack 20 for Long Term Supportprzykładowy plik konfiguracyjny `zos_saf_registry.xml` został zaktualizowany w celu usunięcia zduplikowanej pozycji safAuthorization .

Ta aktualizacja rozwiązuje problem polegający na tym, że może wystąpić błąd ICH408I , gdy produkt IBM MQ Console w systemie z/OS jest aktualizowany do wersji WebSphere Liberty Profile 22.0.0.12 lub nowszej: z produktu IBM MQ 9.3.0 Fix Pack 2 dla systemu Long Term Support oraz z produktu IBM MQ 9.3.1 CSU 1 i produktu IBM MQ 9.3.2 dla systemu Continuous Delivery. 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 IBM 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 katalogu z/OS UNIX System Services (z/OS UNIX), w którym są zainstalowane komponenty z/OS UNIX .

   W pliku `bbgzangl.jcl`zmień instrukcję SET ROOT, aby wskazywała na USS_ROOT`/web`, na przykład `/usr/lpp/mqm/V9R2M0/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 z/OS 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 MQWEB920 i MQWEB915.
   b. Ustaw wartość **unauthenticatedUser** na nazwę nieuwierzytelnionego użytkownika utworzonego w kroku “2” na stronie 570.
8. Zdefiniuj identyfikator APPLID serwera mqweb w pliku RACF.

   Nazwa zasobu APPLID jest wartością podaną w atrybucie **profilePrefix** w kroku “7” na stronie 571. 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 IBM 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 570. 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. Użyj komendy **SETROPTS** RACF , aby odświeżyć profile klas APPL w pamięci masowej RACLISTed:

    ```
    SETROPTS RACLIST(APPL) REFRESH
    ```
11. Zdefiniuj profile w klasie EJBROLE potrzebne do nadania użytkownikom dostępu do ról w systemach IBM 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 571.

```
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)
```

12. Nadaj użytkownikom dostęp do ról w IBM 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 “11” na stronie 571. Więcej informacji na temat ról zawiera sekcja “Role w systemach IBM MQ Console i REST API” na stronie 572.

    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 571.

```
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 tokenu. W takim przypadku użytkownik wprowadza identyfikator użytkownika i hasło na ekranie logowania do produktu IBM MQ Console . Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Aby użyć tej opcji uwierzytelniania, nie jest wymagana żadna dodatkowa konfiguracja, ale opcjonalnie można skonfigurować okres ważności dla znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie okresu ważności tokenu LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera IBM MQ Console, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

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 w celu uwierzytelnienia i autoryzowania użytkownika dla tego żądania. Aby to uwierzytelnianie było bezpieczne, należy użyć bezpiecznego połączenia. Oznacza to, że należy użyć protokołu HTTPS. Więcej informacji na ten temat zawiera sekcja “Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API” na stronie 581.
- Pozwól użytkownikom na uwierzytelnianie za pomocą tokenu. W takim przypadku użytkownik podaje identyfikator użytkownika i hasło do zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi pozostanie zalogowany i autoryzowany przez określony czas. Więcej informacji na ten tematzawiera sekcja “Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API” na stronie 582. Można skonfigurować okres ważności znacznika LTPA. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Pozwól użytkownikom na uwierzytelnianie przy użyciu certyfikatów klienta. W takim przypadku użytkownik nie używa identyfikatora ani hasła, aby zalogować się do serwera REST API, ale zamiast niego używa certyfikatu klienta. Więcej informacji na ten temat zawiera sekcja “Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console” na stronie 577.

Role w systemach IBM MQ Console i REST API

Podczas autoryzowania użytkowników i grup do korzystania z IBM MQ Console lub REST APInależy przypisać użytkownikom i grupom jedną z dostępnych ról: **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin**i **MFTWebAdminRO**. 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.

Uwaga: Z wyjątkiem roli **MQWebUser** w ID użytkownika nie jest rozróżniana wielkość liter. Szczegółowe wymagania dotyczące tej roli zawiera sekcja “MQWebUser” na stronie 573 .

MQWebAdmin
Użytkownik lub grupa z przypisaną tą rolą może wykonywać wszystkie operacje administracyjne 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 następujących usług REST:

- REST API dla MFT. Aby korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MFTWebAdmin** lub **MFTWebAdminRO** .
- messaging REST API. Aby użyć messaging REST API, użytkownik musi mieć przypisaną rolę **MQWebUser** .

MQWebAdminRO
Ta rola nadaje dostęp tylko do odczytu do IBM MQ Console lub REST API. Użytkownik lub grupa z przypisaną tą rolą może wykonywać następujące operacje:

- Wyświetlanie i uzyskiwanie informacji o operacjach na obiektach IBM MQ , takich jak kolejki i kanały.
- Przeglądanie komunikatów w kolejkach.

Użytkownik lub grupa z przypisaną tą rolą 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 korzystać z tych usług, użytkownik lub grupa musi również mieć przypisaną rolę **MFTWebAdmin** lub **MFTWebAdminRO** .
- messaging REST API. Aby użyć messaging REST API, użytkownik musi mieć przypisaną rolę **MQWebUser** .

MQWebUser
Użytkownik lub grupa, która ma przypisaną tę rolę, może wykonać dowolną operację, którą ID użytkownika może wykonać w menedżerze kolejek. Na przykład:

- Operacje uruchamiania i zatrzymywania obiektów IBM MQ , takich jak kanały.
- Definiowanie i ustawianie operacji na obiektach IBM MQ , takich jak kolejki i kanały.
- Wyświetlanie i uzyskiwanie informacji o operacjach na obiektach IBM MQ , takich jak kolejki i kanały.
- Umieszczanie i pobieranie komunikatów przy użyciu messaging REST API.

Użytkownik lub grupa, której przypisano tę rolę, działa w kontekście zabezpieczeń nazwy użytkownika i może wykonywać tylko te operacje, które zostały nadane identyfikatorowi użytkownika w menedżerze kolejek.

Oznacza to, że użytkownik lub grupa zdefiniowana w rejestrze użytkowników mqweb musi mieć nadane uprawnienie w produkcie IBM MQ , zanim będzie mógł wykonywać jakiekolwiek operacje. Za pomocą tej roli można precyzyjnie kontrolować, którzy użytkownicy mają typ dostępu do konkretnych zasobów IBM MQ , gdy korzystają z produktów IBM MQ Console i REST API.

Uwaga:

- Maksymalna długość identyfikatora użytkownika, któremu przypisano tę rolę, wynosi 12 znaków.
- Wielkość liter identyfikatora użytkownika musi być taka sama w rejestrze użytkowników mqweb i w systemie IBM MQ . Jeśli wielkość liter w ID użytkownika jest inna, użytkownik może zostać uwierzytelniony przez IBM MQ Console i REST API , ale nie ma uprawnień do korzystania z zasobów IBM MQ .

MFTWebAdmin
Użytkownik lub grupa z przypisaną tą rolą 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 mieć przypisaną rolę **MQWebAdmin**, **MQWebAdminRO**lub **MQWebUser** .

MFTWebAdminRO
Ta rola nadaje dostęp tylko do odczytu do REST API dla MFT . Użytkownik lub grupa z przypisaną tą rolą może wykonywać operacje tylko do odczytu (żądania GET), takie jak przesyłanie listy i wyświetlanie agentów.

Użytkownik lub grupa z przypisaną tą rolą 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 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 561.

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. Jeśli na przykład użytkownik z rolami **MQWebAdminRO** i **MQWebUser** wykonuje operację zapytania o kolejkę, używana jest rola **MQWebAdminRO** , a operacja jest podejmowana w kontekście identyfikatora użytkownika systemu, który uruchomił serwer WWW. Jeśli ten sam użytkownik wykonuje operację definiowania, używana jest rola **MQWebUser** i podejmowana jest próba wykonania tej operacji w kontekście nazwy użytkownika.

ALW Zmiana certyfikatu udostępnionego przez IBM MQ Console w przeglądarce

Program IBM MQ Console można skonfigurować w taki sposób, aby przedstawiał własny certyfikat podpisany przez ośrodek CA na potrzeby uwierzytelniania. Spowoduje to usunięcie ostrzeżenia o samopodpisanym certyfikacie, które jest wyświetlane przez przeglądarkę WWW podczas uzyskiwania dostępu do konsoli IBM MQ Console .

Zanim rozpoczniesz

Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do używania IBM MQ Console. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 561.

O tym zadaniu

Zabezpieczenia konsoli są udostępniane przez IBM WebSphere Application Server Liberty używane przez instalację produktu IBM MQ .

Aby zmienić certyfikat, który jest prezentowany w przeglądarce przez ten serwer, należy wykonać następujące czynności:

1. Dodaj certyfikat, który ma być obecny w magazynie kluczy serwera WWW.
2. Oznacz certyfikat etykietą.
3. Zmodyfikuj plik `mqwebuser.xml` , aby wyłączyć domyślną konfigurację zabezpieczeń.
4. Włącz własną konfigurację zabezpieczeń w pliku `mqwebuser.xml` i podaj certyfikat, który chcesz przedstawić.

W procedurze założono, że użytkownik:

- Korzystanie z systemu AIX, Linux, and Windows .
- Użytkownik uprzywilejowany.

Uwagi:

- W poniższym przykładzie jest tworzony i używany certyfikat samopodpisany przy użyciu komend wydanych na komputerze z systemem Linux , czyli **ls**, a nie **dir** na komputerze z systemem Windows .
- Spowoduje to wyświetlenie pojęcia, ale nie spowoduje usunięcia ostrzeżenia przeglądarki.
- Aby usunąć ostrzeżenie przeglądarki, należy podać certyfikat podpisany przez ośrodek CA.

Procedura

1. Jeśli serwer Liberty jest uruchomiony, zatrzymaj go, wprowadzając komendę **endmqweb** w wierszu komend.
2. Dodaj certyfikat do magazynu kluczy używanego przez serwer aplikacji Liberty , aby mógł on znaleźć i przedstawić certyfikat w przeglądarce WWW.

a) Przejdź do położenia magazynu kluczy, wydając następującą komendę i wyświetlając dane wyjściowe:

```
cd /var/mqm/web/installations/Installation1/servers/mqweb/resources/security
ls
```

Na przykład zostaną wyświetlone następujące dane wyjściowe, które zawierają magazyn kluczy o nazwie `key.jks`:

```
/var/mqm/web/installations/Installation1/servers/mqweb/resources/security$
ls key.jks ltpa.keys
```

b) Utwórz certyfikat samopodpisany:

Aby utworzyć certyfikat samopodpisany w celach edukacyjnych, który jest dodawany do `key.jks` za pomocą hasła `password`, należy wydać następującą komendę:

```
runmqckm -cert -create -db key.jks -pw password -dn
"cn=QueueManager,o=IBM,c=UK" -label myowncertificate
```

Opcja **-dn** umożliwia określenie wartości wyświetlanych w certyfikacie.

c) Sprawdź, czy certyfikat został pomyślnie dodany, wydając następującą komendę:

```
runmqckm -cert -list -db key.jks -pw password
```

Na przykład zostaną wyświetlone następujące dane wyjściowe, które wskazują, że certyfikat został dodany wraz z etykietą, wraz z certyfikatem o etykiecie `default` , który jest obecnie używany przez serwer:

```
/var/mqm/web/installations/Installation1/servers/mqweb/resources/security
$ runmqckm -cert -list -db key.jks -pw password
Certificates in database /var/mqm/web/installations/Installation1/servers/mqweb/resources/
security/key.jks
   default
   myown certificate
```

3. Zmodyfikuj plik `mqwebuser.xml` , aby serwer udostępniając nowy certyfikat.

a) Przejdź do położenia pliku `mqwebuser.xml` , a następnie otwórz go do edycji w edytorze tekstu (w tym przypadku jest to *nano*).

```
cd /var/mqm/web/installations/Installation1/servers/mqweb
nano mqwebuser.xml
```

b) Wyłącz domyślną konfigurację zabezpieczeń.

Przekształć w komentarz następujący wiersz, dodając łańcuch `<!--` na początku wiersza kodu i łańcuch `-->` na końcu wiersza kodu:

```
<!--
<sslDefault sslRef="mqDefaultSSLConfig"/>
-->
```

c) Włącz i określ własną konfigurację.

W tym celu wykonaj następującą procedurę:

i) Usuń znak komentarza z następujących wierszy kodu, usuwając znak `<!--` z początku bloku kodu i znak `-->` z końca bloku kodu.

```
<!--
<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"
serverKeyAlias="default" trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"/>
```

```
<sslDefault sslRef="thisSSLConfig"/>
-->
```

ii) **Nie zmieniaj pierwszego wiersza** bloku kodu, ponieważ ten wiersz określa magazyn kluczy używany przez konsolę do przechowywania certyfikatów osobistych.

iii) **Przekształć w komentarz drugi wiersz bloku kodu**, ponieważ ten wiersz określa magazyn zaufanych certyfikatów, w którym konsola będzie szukać certyfikatów klienta. Ponieważ używane jest uwierzytelnianie za pomocą znacznika, nie utworzono magazynu zaufanych certyfikatów, a pozostawienie w nim wiersza kodu spowodowałoby błąd podczas uruchamiania konsoli.

iv) **Zmień serverKeyAlias= "default" na serverKeyAlias= "myowncertificate"** w trzecim wierszu bloku kodu i pozostaw wszystko inne bez zmian.

v) **Nie zmieniaj ostatniego wiersza** bloku kodu, ponieważ spowoduje to, że serwer będzie używał podanej konfiguracji.

Blok kodu wygląda teraz następująco:

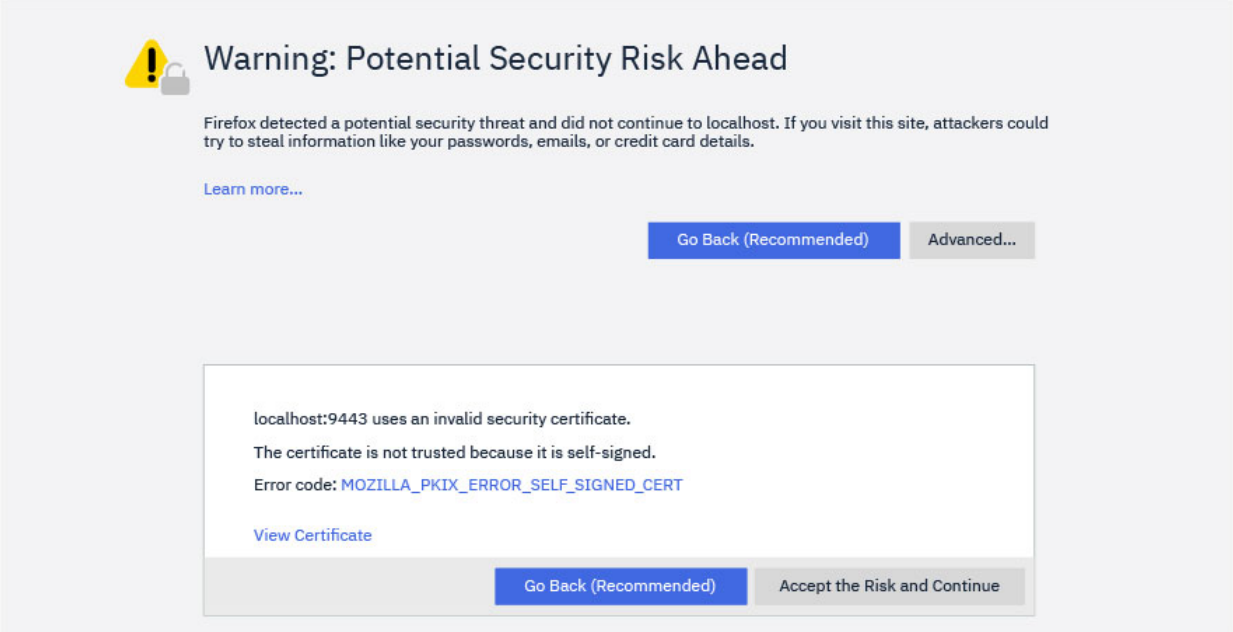
```
<keyStore id="defaultKeyStore" location="key.jks" type="JKS" password="password"/>
<!-- Commenting out the defaultTrustStore as otherwise we get errors (viewable in the messages.log file
in the logs folder) j
<keyStore id="defaultTrustStore" location="trust.jks" type="JKS" password="password"/>
-->
<ssl id="thisSSLConfig" clientAuthenticationSupported="true" keyStoreRef="defaultKeyStore"
serverKeyAlias="myowncertificate" trustStoreRef="defaultTrustStore" sslProtocol="TLSv1.2"/>
<sslDefault sslRef="thisSSLConfig"/>
```

4. Zrestartuj serwer WWW za pomocą komendy **strmqweb** .

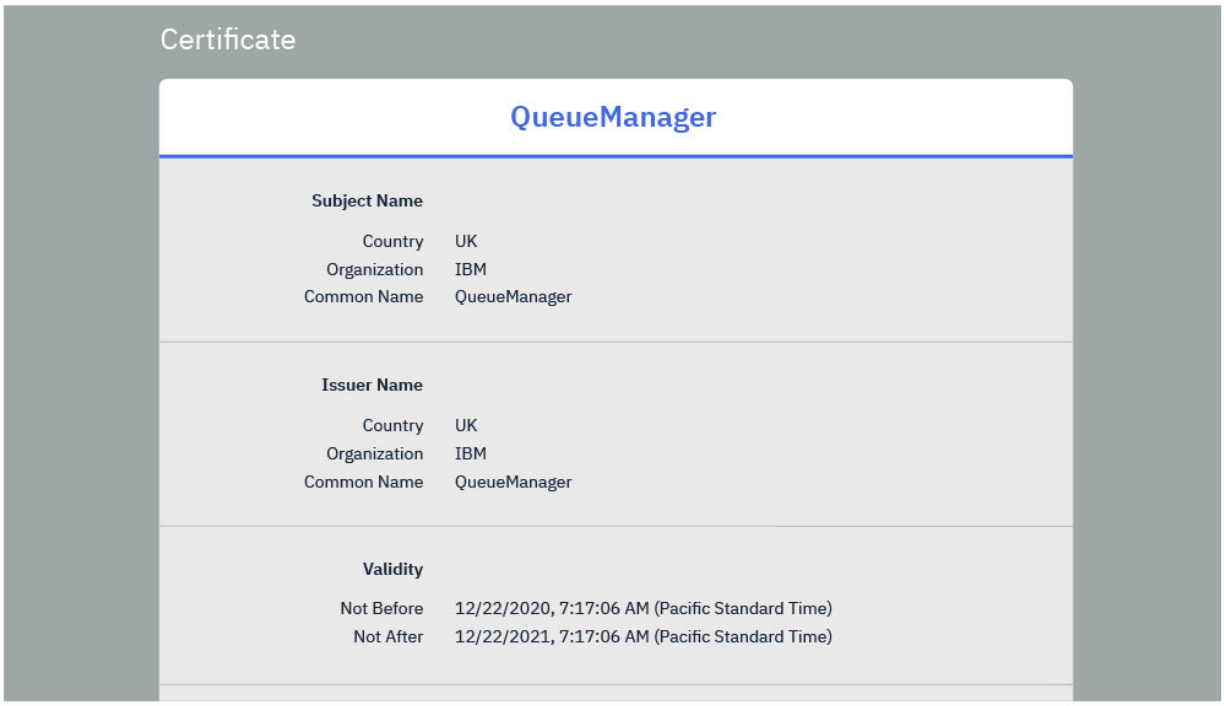
Wyniki

Po uruchomieniu serwera WWW przejdź do katalogu IBM MQ Console i odśwież go. Jeśli używany jest certyfikat samopodpisany, który został utworzony przy użyciu procedury opisanej w poprzednich krokach “2” na stronie 574 i “3” na stronie 575, zostanie wyświetlone ostrzeżenie systemu zabezpieczeń.

Należy zauważyć, że format tego ostrzeżenia zależy od używanej przeglądarki.



Po kliknięciu opcji **Wyświetl certyfikat**zostaną wyświetlone szczegóły podane w opcji **-dn** podczas tworzenia certyfikatu w kroku “2.b” na stronie 575.



Jeśli jednak używany jest certyfikat podpisany przez ośrodek CA, przeglądarka jest zaufana i została dodana za pomocą następującej komendy:

```
runmqckm -cert -add -db key.jks -pw password -label myCACertificate
```

gdzie `myCACertificate` jest ścieżką do pliku zawierającego certyfikat ośrodka CA, który został bezpośrednio wyświetlony na stronie logowania.

Ostrzeżenie: Jeśli używany jest certyfikat podpisany przez ośrodek CA, który jest częścią łańcucha certyfikatów, należy dodać wszystkie certyfikaty do łańcucha, rozpoczynając od certyfikatu głównego ośrodka CA. Więcej informacji zawiera sekcja “Dodawanie certyfikatu ośrodka CA lub publicznej części certyfikatu samopodpisanego do repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 338.

ALW Korzystanie z uwierzytelniania przy użyciu certyfikatu klienta w systemach REST API i IBM MQ Console

Certyfikaty klienta można odwzorować na nazwy użytkowników w celu uwierzytelnienia użytkowników IBM MQ Console i REST API .

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do korzystania z IBM MQ Console i REST API. Więcej informacji na ten tematzawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 561.
- W przypadku użycia REST APImożna wysłać zapytanie do referencji bieżącego użytkownika za pomocą metody GET HTTP dla zasobu `login` , udostępniając certyfikat klienta na potrzeby uwierzytelniania żądania. To żądanie zwraca informacje na temat nazwy użytkownika i przypisanych mu ról. Więcej informacji na ten temat zawiera sekcja GET `/login`.
- Gdy certyfikaty klienta są odwzorowywane na nazwy użytkowników w celu uwierzytelnienia użytkowników, nazwa wyróżniająca certyfikatu klienta jest używana do dopasowania do użytkowników w skonfigurowanym rejestrze użytkowników:

– W przypadku rejestru podstawowego nazwa zwykła (CN) jest porównywana z nazwą użytkownika. Na przykład wartość `CN=Fred, O=IBM, C=GB` jest porównywana z nazwą użytkownika `Fred`.
– W przypadku rejestru LDAP domyślnie pełna nazwa wyróżniająca jest dopasowywana do LDAP. Istnieje możliwość skonfigurowania filtrów i odwzorowania w celu dostosowania dopasowania. Więcej informacji na ten temat zawiera sekcja Tryb odwzorowania certyfikatu Liberty :LDAP w dokumentacji serwera WebSphere Liberty .

O tym zadaniu

Gdy użytkownik uwierzytelnia się przy użyciu certyfikatu klienta, certyfikat ten jest używany zamiast nazwy użytkownika i hasła. W przypadku serwera REST APIcertyfikat klienta jest dostarczany wraz z każdym żądaniem REST w celu uwierzytelnienia użytkownika. W przypadku serwera IBM MQ Console, gdy użytkownik loguje się przy użyciu certyfikatu, użytkownik nie może zostać wylogowany.

W procedurze przyjęto następujące informacje:

- Plik `mqwebuser.xml` jest oparty na jednym z następujących przykładów:
  – `basic_registry.xml`
  – `local_os_registry.xml`
  – `ldap_registry.xml`
- Używany jest system AIX, Linux, and Windows .
- Jesteś użytkownikiem uprzywilejowanym.

Aby skonfigurować uwierzytelnianie przy użyciu certyfikatu klienta za pomocą pliku kluczy RACF w systemie z/OS, należy wykonać procedurę opisaną w sekcji “Konfigurowanie protokołu TLS dla serwerów REST API i IBM MQ Console w systemie z/OS” na stronie 590.

Uwaga: Poniższa procedura przedstawia kroki, które należy wykonać, aby użyć certyfikatów klienta z IBM MQ Console i REST API. Dla wygody programisty kroki zawierają szczegółowe informacje na temat tworzenia i używania certyfikatów samopodpisanych. Jednak w środowisku produkcyjnym 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 **Plik bazy danych kluczy** w narzędziu IBM Key Management kliknij opcję **Nowy**.
      iii) Z listy **Typ bazy danych kluczy** wybierz pozycję **PKCS12** .
      iv) Wybierz położenie, w którym ma zostać zapisany magazyn kluczy, i wprowadź odpowiednią nazwę w polu **Nazwa pliku** . Na przykład: `user.p12`
      v) Po wyświetleniu zapytania ustaw hasło.
   b) Utwórz certyfikat, tworząc certyfikat samopodpisany lub uzyskując certyfikat z ośrodka certyfikacji:
      - Utwórz certyfikat samopodpisany:
        i) Kliknij opcję **Nowy samopodpisany**.
        ii) W polu **Key Label** (Etykieta klucza) wpisz `user` .
        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 upewnij 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 nazwie zwykłej (CN) w polu nazwy wyróżniającej (DN):

  i) Zażądaj nowego certyfikatu. W menu **Create** (Utwórz) kliknij opcję **New Certificate Request**(Nowe żądanie certyfikatu).

  ii) W polu **Key Label** (Etykieta klucza) wpisz etykietę certyfikatu.

  iii) Jeśli używany jest podstawowy rejestr użytkowników, w polu **Nazwa zwykła** wprowadź nazwę użytkownika, którego dotyczy certyfikat.

  Jeśli używany jest rejestr lokalnego systemu operacyjnego, pole **Nazwa zwykła** musi być zgodne z identyfikatorem użytkownika lokalnego systemu operacyjnego.

  W przypadku rejestru użytkowników LDAP upewnij się, że nazwa wyróżniająca certyfikatu jest zgodna z nazwą wyróżniającą w rejestrze LDAP.

  iv) Wpisz lub wybierz odpowiednie wartości dla pozostałych pól.

  v) Wybierz miejsce zapisania żądania certyfikatu i nazwę pliku dla żądania certyfikatu, a następnie kliknij przycisk **OK**.

  vi) Wyślij plik żądania certyfikatu do ośrodka certyfikacji (CA).

  vii) Po uzyskaniu certyfikatu z ośrodka CA otwórz narzędzie IBM Key Management, wprowadzając w wierszu komend komendę **strmqikm** .

  viii) W menu **Plik bazy danych kluczy** w narzędziu IBM Key Management kliknij opcję **Otwórz**.

  ix) Wybierz magazyn kluczy PKCS#12 , który zawiera certyfikat klienta. Na przykład `user.p12`

  x) Kliknij opcję **Receive**(Pobierz), wybierz odpowiedni certyfikat i kliknij przycisk **OK**.

3. Wyodrębnij publiczną część certyfikatu klienta:
   a) Otwórz narzędzie IBM Key Management, wprowadzając komendę **strmqikm** w wierszu komend.
   b) W menu **Plik bazy danych kluczy** w narzędziu IBM Key Management kliknij opcję **Otwórz**.
   c) Wybierz magazyn kluczy PKCS#12 , który zawiera 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 położenie, w którym ma zostać zapisany certyfikat, i wprowadź odpowiednią nazwę pliku w polu **Nazwa pliku certyfikatu** . Na przykład: `user.arm`.
4. Zaimportuj publiczną część certyfikatu klienta do magazynu zaufanych certyfikatów serwera mqweb jako certyfikat osoby podpisującej, aby serwer mógł sprawdzić poprawność certyfikatu klienta:
   a) Utwórz magazyn kluczy `trust.jks` do użycia przez serwer mqweb, jeśli jeszcze nie istnieje:

   i) W menu **Plik bazy danych kluczy** w narzędziu IBM Key Management kliknij opcję **Nowy**.

   ii) Z listy **Key database type** (Typ bazy danych kluczy) wybierz pozycję **JKS** .

   iii) Kliknij przycisk **Przeglądaj** i przejdź do katalogu: `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 zamiast go nadpisywać.

   iv) W polu **Nazwa pliku** wpisz `trust.jks` .

   v) Po wyświetleniu zapytania ustaw hasło.

   b) Z menu rozwijanego wybierz opcję **Certyfikaty osób podpisujących**.
   c) Kliknij przycisk **Add** (Dodaj).
   d) Wybierz odpowiedni plik arm i 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 katalogu *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb/resources/security .

d) Wybierz magazyn kluczy key.jks i kliknij przycisk **Otwórz**.

e) Po wyświetleniu zachęty 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 przy użyciu certyfikatu klienta w pliku mqwebuser.xml :

   Plik mqwebuser.xml można znaleźć w następującej ścieżce: *MQ_DATA_PATH*/web/installations/*installationName*/servers/mqweb

   a) Usuń oznaczenie komentarza z sekcji w pliku mqwebuser.xml , która umożliwia uwierzytelnianie przy użyciu 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) Sprawdź, czy wartość **serverKeyAlias** jest zgodna z nazwą certyfikatu serwera. Jeśli używany jest domyślny certyfikat serwera, wartość jest poprawna.

   c) Zmień wartość **password** dla defaultKeyStore na zakodowaną wersję hasła dla magazynu kluczy key.jks :

      i) W katalogu *MQ_INSTALLATION_PATH*/web/bin wprowadź następującą komendę w wierszu komend:

      ```
      securityUtility encode password
      ```

      ii) Umieść dane wyjściowe tej komendy w polu **password** dla defaultKeyStore.

   d) Zmień wartość **password** dla defaultTrustStore , aby była zgodna z hasłem dla magazynu kluczy trust.jks :

      i) W katalogu *MQ_INSTALLATION_PATH*/web/bin wprowadź następującą komendę w wierszu komend:

      ```
      securityUtility encode password
      ```

      ii) Umieść dane wyjściowe tej komendy w polu **password** dla defaultTrustStore.

   e) Usuń lub przekształć w komentarz 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 używać certyfikatu klienta z serwerem IBM MQ Console, zainstaluj certyfikat klienta w przeglądarce WWW, która jest używana do uzyskiwania dostępu do serwera IBM MQ Console. Na przykład zainstaluj certyfikat klienta user.p12 jako certyfikat osobisty.
   - Aby używać certyfikatu klienta z serwerem REST API, należy udostępnić certyfikat klienta dla każdego żądania REST. Jeśli używane są metody POST, PATCH lub DELETE protokołu HTTP , należy zapewnić dodatkowe uwierzytelnianie przy użyciu certyfikatu klienta, aby zapobiec atakom typu CSRF (Cross-Site Request Forgery). Oznacza to, że dodatkowe uwierzytelnianie jest używane do potwierdzenia, że referencje używane do uwierzytelniania żądania są używane przez właściciela referencji.

To dodatkowe uwierzytelnianie jest udostępniane przez nagłówek `ibm-mq-rest-csrf-token` HTTP . 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 certyfikaty samopodpisane, dlatego należy użyć implementacji cURL , która obsługuje tę implementację.

Poniższy przykład komendy cURL przedstawia sposób tworzenia nowej kolejki `Q1`w menedżerze kolejek `QM1`z uwierzytelnianiem przy użyciu certyfikatu klienta. Dokładna konfiguracja tej komendy cURL zależy od bibliotek, dla których zbudowano komendę cURL . Przykład jest oparty na systemie Windows z adresem cURL zbudowanym przy użyciu protokołu OpenSSL.

- Należy użyć metody HTTP POST z zasobem kolejki, uwierzytelniając się przy użyciu certyfikatu klienta i dołączając nagłówek `ibm-mq-rest-csrf-token` HTTP z dowolną wartością. Ta wartość może być dowolna, w tym pusta. Opcja `--cert-type` określa, że certyfikat jest certyfikatem PKCS#12 . Opcja `--cert` określa położenie certyfikatu, po którym następuje dwukropek, znak:, a następnie hasło 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\"}"
```

Korzystanie z podstawowego uwierzytelniania HTTP w systemie REST API

Użytkownicy serwera REST API mogą uwierzytelniać się, podając swój identyfikator i hasło w nagłówku HTTP . Aby użyć tej metody uwierzytelniania przy użyciu metod HTTP , takich jak POST, PATCH i DELETE, należy również podać nagłówek `ibm-mq-rest-csrf-token` HTTP , a także identyfikator użytkownika i hasło.

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do używania REST API. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 561.
- Upewnij się, że podstawowe uwierzytelnianie HTTP jest włączone. Sprawdź, czy w pliku `mqwebuser.xml` znajduje się następujący kod XML i czy nie jest on przekształcony w komentarz. Ten kod XML musi znajdować się w obrębie znaczników `<featureManager>` :

```
<feature>basicAuthenticationMQ-1.0</feature>
```

z/OS W systemie z/OS, aby edytować ten plik, należy być użytkownikiem, który ma uprawnienia do zapisu w pliku `mqwebuser.xml` .

Multi We wszystkich innych systemach operacyjnych, aby edytować plik `mqwebuser.xml` , należy być użytkownikiem uprzywilejowanym .

- Upewnij się, że podczas wysyłania żądań REST używane jest bezpieczne połączenie. Ponieważ kombinacja nazwy użytkownika i hasła jest zakodowana, ale nie jest zaszyfrowana, należy użyć bezpiecznego połączenia (HTTPS), jeśli z serwerem REST APIużywane jest podstawowe uwierzytelnianie HTTP .
- Informacje autoryzacyjne bieżącego użytkownika można wysłać do zasobu `login` za pomocą metody GET HTTP , udostępniając podstawowe informacje uwierzytelniające w celu uwierzytelnienia żądania. To żądanie zwraca informacje na temat nazwy użytkownika i przypisanych mu ról. Więcej informacji na ten temat zawiera sekcja GET `/login`.

Procedura

1. Konkatenuj nazwę użytkownika z dwukropkiem i hasłem. Należy zauważyć, że w nazwie użytkownika rozróżniana jest wielkość liter.

   Na przykład nazwa użytkownika admin i hasło admin stają się następującym łańcuchem:

   ```
   admin:admin
   ```

2. Zakoduj tę nazwę użytkownika i hasło w kodowaniu base64 .
3. Dołącz tę zakodowaną nazwę użytkownika i hasło do nagłówka HTTP `Authorization: Basic` .

   Na przykład w przypadku zakodowanej nazwy użytkownika admin i hasła admin 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 `ibm-mq-rest-csrf-token` HTTP . Nagłówek `ibm-mq-rest-csrf-token` HTTP musi być obecny w żądaniu, ale jego wartość może być dowolna, w tym pusta.
5. Wyślij żądanie REST do IBM MQ z odpowiednimi nagłówkami.

Przykład

Poniższy przykład przedstawia sposób tworzenia nowej kolejki Q1w menedżerze kolejek QM1z podstawowym uwierzytelnianiem w systemach Windows . W przykładzie użyto komendy cURL:

- Należy użyć metody HTTP POST z zasobem kolejki, który jest uwierzytelniany przy użyciu uwierzytelniania podstawowego i zawiera nagłówek `ibm-mq-rest-csrf-token` HTTP o dowolnej wartości. Ta wartość może być dowolna, w tym 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\"}"
  ```

Korzystanie z uwierzytelniania opartego na znacznikach w interfejsie REST API

Użytkownicy serwera REST API mogą uwierzytelniać się, podając identyfikator użytkownika i hasło dla zasobu REST API `login` za pomocą metody HTTP POST. Generowany jest znacznik LTPA, który umożliwia użytkownikowi uwierzytelnianie przyszłych żądań. Ten znacznik LTPA ma przedrostek `LtpaToken2`. Użytkownik może wylogować się za pomocą metody HTTP DELETE i może wysłać zapytanie do informacji logowania bieżącego użytkownika za pomocą metody HTTP GET.

Zanim rozpoczniesz

- Skonfiguruj użytkowników, grupy i role, które mają być autoryzowane do używania REST API. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie użytkowników i ról” na stronie 561.
- Domyślnie nazwa informacji cookie zawierającej znacznik LTPA rozpoczyna się od łańcucha `LtpaToken2`i zawiera przyrostek, który może ulec zmianie po zrestartowaniu serwera mqweb. Ta losowa nazwa informacji cookie umożliwia uruchomienie więcej niż jednego serwera mqweb w tym samym systemie. Jeśli jednak nazwa informacji cookie ma pozostać spójna, można określić nazwę informacji 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. Czas utraty ważności informacji cookie znacznika LTPA można skonfigurować za pomocą komendy **setmqweb** . Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.

- Upewnij się, że podczas wysyłania żądań REST używane jest bezpieczne połączenie. W przypadku użycia metody HTTP POST dla zasobu `login` kombinacja nazwy użytkownika i hasła, która jest wysyłana z żądaniem, nie jest szyfrowana. Dlatego należy używać bezpiecznego połączenia (HTTPS), gdy w produkcie REST APIużywane jest uwierzytelnianie oparte na znacznikach. Domyślnie nie można używać protokołu HTTP z uwierzytelnianiem za pomocą znacznika LTPA. Można włączyć używanie znacznika LTPA przez niezabezpieczone połączenia HTTP , ustawiając wartość parametru **secureLTPA** na `False`. Więcej informacji na ten temat zawiera sekcja Konfigurowanie znacznika LTPA.
- Informacje autoryzacyjne bieżącego użytkownika można wysłać za pomocą metody GET HTTP dla zasobu `login` , udostępniając znacznik LTPA do uwierzytelnienia żądania. To żądanie zwraca informacje na temat nazwy użytkownika i przypisanych mu ról. Więcej informacji na ten temat zawiera sekcja GET /login.

Procedura

1. Zaloguj użytkownika:
   a) Użyj metody HTTP POST dla zasobu `login` :

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   Dołącz nazwę użytkownika i hasło do treści żądania JSON w następującym formacie:

   ```
   {
       "username" : name,
       "password" : password
   }
   ```

   b) Zapisz token LTPA 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 dla każdego żądania.

   W przypadku żądań, które używają metod PUT, PATCH lub DELETE protokołu HTTP , należy dołączyć nagłówek `ibm-mq-rest-csrf-token` . Wartość tego nagłówka może być dowolna, w tym pusta.
3. Wyloguj użytkownika:
   a) Użyj metody DELETE HTTP dla zasobu `login` :

   ```
   https://host:9443/ibmmq/rest/v1/login
   ```

   Należy podać znacznik LTPA jako informację cookie, aby uwierzytelnić żądanie, i dołączyć nagłówek `ibm-mq-rest-csrf-token` . Wartość tego nagłówka może być dowolna, w tym pusta

   b) Przetwórz instrukcję usunięcia znacznika LTPA z lokalnej składnicy informacji cookie.

   Uwaga: Jeśli instrukcja nie jest przetwarzana, a znacznik LTPA pozostaje w lokalnej składnicy informacji cookie, znacznik LTPA może być używany do uwierzytelniania przyszłych żądań REST. Oznacza to, że gdy użytkownik próbuje uwierzytelnić się przy użyciu tokenu LTPA po zakończeniu sesji, tworzona jest nowa sesja używająca istniejącego tokenu.

Przykład

Poniższy przykład komendy cURL przedstawia sposób tworzenia nowej kolejki Q1w menedżerze kolejek QM1z uwierzytelnianiem opartym na znacznikach 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 POST protokołu HTTP z zasobem kolejki, uwierzytelniając się przy użyciu znacznika LTPA. Znacznik LTPA z przedrostkiem `LtpaToken2` jest pobierany z pliku `cookiejar.txt` za pomocą opcji `-b` . Ochrona CSRF jest zapewniana przez obecność nagłówka `ibm-mq-rest-csrf-token` HTTP :

```
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` . Zabezpieczenie CSRF jest zapewniane przez obecność nagłówka `ibm-mq-rest-csrf-token` HTTP . Położenie pliku `cookiejar.txt` jest określane przez opcję `-c` , więc 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

Osadzanie IBM MQ Console w i-ramce

Elementu HTML < iframe> można użyć do osadzenia jednej strony WWW w innej za pomocą ramki wstawianej (IFrame). Ze względów bezpieczeństwa pliku IBM MQ Console nie można domyślnie osadzić w i-ramce. Można jednak włączyć i-ramkę, używając właściwości konfiguracyjnej **mqConsoleFrameAncestors** na serwerze mqweb.

O tym zadaniu

Serwer mqweb przechowuje listę dozwolonych źródeł stron WWW, które mogą osadzać IBM MQ Console przy użyciu i-ramki. Źródło jest kombinacją schematu URL , domeny i portu, na przykład `https://example.com:1234`.

Aby określić pozycje na liście, można użyć właściwości konfiguracyjnej **mqConsoleFrameAncestors** na serwerze mqweb.

Domyślnie pole **mqConsoleFrameAncestors** jest puste, co oznacza, że nie można osadzić pola IBM MQ Console w i-ramce.

Procedura

Podaj listę źródeł stron WWW, które mogą osadzać IBM MQ Console w i-ramce, wprowadzając następującą komendę:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

gdzie *allowedOrigins* jest listą źródeł oddzielonych przecinkami. Każde pochodzenie powinno składać się z:

- Nazwa hosta lub adres IP
- Opcjonalny schemat URL
- Opcjonalny numer portu

Należy zauważyć, że nazwa hosta może zaczynać się od znaku wieloznacznego (*), a numer portu może również używać znaku wieloznacznego (*).

Przykładowe źródła:

```
https://example.com:1234
```

która umożliwia dowolnej stronie WWW udostępnianej przez serwis `https://example.com:1234` osadzenie pliku IBM MQ Console w i-ramce.

```
https://*.example.com:*
```

która umożliwia dowolnej stronie WWW HTTPS z nazwą hosta kończącą się na `example.com`i z użyciem dowolnego portu osadzenie IBM MQ Console w i-ramce.

Przykład

Poniższy przykład umożliwia osadzenie pliku IBM MQ Console w ramce IFrame z poziomu stron WWW udostępnianych z serwisu `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
```

Konfigurowanie mechanizmu CORS dla serwera REST API

Domyślnie przeglądarka WWW nie zezwala skryptom, takim jak JavaScript, na wywoływanie skryptu REST API , gdy skrypt nie pochodzi z tego samego źródła co skrypt REST API. Oznacza to, że żądania z różnych źródeł nie są włączone. Istnieje możliwość skonfigurowania mechanizmu CORS (Cross Origin Resource Sharing), aby zezwolić na żądania z różnych źródeł pochodzące z określonych źródeł.

O tym zadaniu

Dostęp do pliku REST API można uzyskać za pomocą przeglądarki WWW, na przykład za pomocą skryptu. Ponieważ żądania te pochodzą z innego źródła niż serwer REST API, przeglądarka WWW odrzuca żądanie, ponieważ jest to żądanie z innego źródła. Pochodzenie jest inne, jeśli domena, port lub schemat nie są takie same.

Jeśli na przykład istnieje skrypt, który jest udostępniany w serwisie `http://localhost:1999/` , w przypadku wydania żądania HTTP GET w serwisie WWW, który jest udostępniany pod adresem `https://localhost:9443/`, zostanie wysłane żądanie międzyźródłowe. To żądanie jest żądaniem międzyźródłowym, ponieważ numery portów i schemat (HTTP) są różne.

Żądania z różnych źródeł można włączyć, konfigurując mechanizm CORS i określając źródła, które mają dostęp do serwera REST API.

Więcej informacji na temat mechanizmu CORS zawiera sekcja 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 źródła. Wpis `mqRestCorsMaxAgeInSeconds` określa czas (w sekundach), przez który przeglądarka WWW może buforować wyniki wszystkich sprawdzeń CORS przed lotem.
2. Określ źródła, które mają dostęp do REST API , wprowadzając następującą komendę:

   `setmqweb properties -k mqRestCorsAllowedOrigins -v` *`allowedOrigins`*

   gdzie *allowedOrigins* określa źródło, z którego mają być dozwolone żądania z różnych źródeł. Można użyć znaku gwiazdki ujętego w podwójny cudzysłów, "*", aby zezwolić na wszystkie żądania o różnych pochodzeniu. Można wprowadzić więcej niż jedno źródło w postaci listy rozdzielanej przecinkami, ujętej w znaki cudzysłowu. Aby nie zezwalać na żądania o różnych źródłach, należy wprowadzić puste cudzysłowy jako wartość parametru *allowedOrigins*.

3. Podaj czas (w sekundach), przez który przeglądarka WWW ma buforować wyniki wszystkich sprawdzeń CORS przed lotem, wprowadzając następującą komendę:

   ```
   setmqweb properties -k mqRestCorsMaxAgeInSeconds -v time
   ```

Przykład

Poniższy przykład przedstawia żądania z różnych źródeł włączone dla `http://localhost:9883`, `https://localhost:1999i` `https://localhost:9663`. Maksymalny wiek buforowanych wyników kontroli przed lotem CORS jest ustawiony na 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 IBM MQ Console i REST API

Serwer mqweb można skonfigurować w taki sposób, aby ograniczyć dostęp do produktów IBM MQ Console i REST API w taki sposób, aby przetwarzane były tylko żądania wysyłane z nagłówkiem hosta zgodnym z określoną listą zaakceptowanych. Jeśli używana jest wartość nagłówka hosta, która nie znajduje się na liście zaakceptowanych, zwracany jest błąd.

O tym zadaniu

Serwer mqweb używa hostów wirtualnych do zdefiniowania listy zaakceptowanych nagłówków hostów. Więcej informacji na temat hostów wirtualnych zawiera dokumentacja systemu WebSphere Liberty : https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html

Aby wykonać tę czynność, użytkownik musi mieć uprawnienia wystarczające do edytowania pliku `mqwebuser.xml` :

- z/OS W systemie z/OSwymagane jest uprawnienie do zapisu w pliku `mqwebuser.xml` .
- Multi W przypadku wszystkich innych systemów operacyjnych użytkownik musi być użytkownikiem uprzywilejowanym.
- V 9.3.5 Linux Jeśli serwer mqweb jest częścią autonomicznej instalacji produktu IBM MQ Web Server , użytkownik musi mieć dostęp do zapisu do pliku `mqwebuser.xml` w katalogu danych produktu IBM MQ Web Server .

Procedura

1. Otwórz plik `mqwebuser.xml`. Ten plik znajduje się w jednym z następujących miejsc:
   - W przypadku instalacji w systemie IBM MQ :
     - Linux AIX W systemie AIX lub Linux: `/var/mqm/web/installations/`*`installationName`*`/servers/mqweb`
     - Windows W systemie Windows: *MQ_DATA_PATH*`\web\installations\`*`installationName`*`\servers\mqweb`, gdzie *MQ_DATA_PATH* jest ścieżką danych IBM MQ . Ta ścieżka jest ścieżką danych wybraną podczas instalowania produktu IBM MQ. Domyślna ścieżka to `C:\ProgramData\IBM\MQ`.
     - z/OS W systemie z/OS: *`WLP_user_directory`*`/servers/mqweb`

       Gdzie *katalog_użytkownika_WLP* to katalog, który został określony podczas wykonywania komendy **crtmqweb** w celu utworzenia definicji serwera mqweb.

- V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb

  gdzie *MQ_OVERRIDE_DATA_PATH* jest katalogiem danych produktu IBM MQ Web Server , na który wskazuje zmienna środowiskowa **MQ_OVERRIDE_DATA_PATH** .

2. Dodaj lub usuń znak komentarza z następującego kodu w pliku mqwebuser.xml :

```
<virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
        <hostAlias>localhost:9080</hostAlias>
</virtualHost>
```

3. Zmodyfikuj pole **<hostAlias>** , wstawiając kombinację nazwy hosta i portu, która ma być dopuszczona.

   Ta kombinacja może być nazwą hosta i nazwą portu, które zostały użyte w konfiguracji serwera mqweb. Na przykład, jeśli używana jest domyślna konfiguracja localhost:9443, można użyć wartości localhost:9443 w polu **<hostAlias>** .

   W razie potrzeby można dodać wiele pól **<hostAlias>** w znacznikach **<virtualHost>** , aby umożliwić więcej kombinacji nazwy hosta i portu. Aby na przykład zezwolić na nagłówki hosta, które używają portu HTTP , oraz nagłówki hosta, które używają portu HTTPS .

Kontrola

Rekordy kontroli operacji, które są wykonywane w plikach IBM MQ Console i REST API , można utworzyć, włączając zdarzenia komend i konfiguracji menedżera kolejek, a w przypadku AIX, Linux, and Windows znaczące zmiany stanu są rejestrowane w plikach dziennika serwera mqweb.

Znaczące zmiany stanu

ALW

W systemie AIX, Linux, and Windowsprodukt IBM MQ Console rejestruje znaczące zmiany stanu jako komunikaty w dziennikach serwera mqweb. Każdy komunikat wskazuje uwierzytelnioną nazwę użytkownika, który zażądał wykonania operacji.

Istotne zmiany stanu, takie jak utworzenie, uruchomienie, zakończenie lub usunięcie menedżerów kolejek, są rejestrowane w plikach messages.log i console.log serwera mqweb na poziomie rejestrowania [AUDIT]. Każda pozycja dziennika wskazuje uwierzytelnioną nazwę użytkownika, który zażądał wykonania operacji.

Pliki messages.log i console.log można znaleźć w następującej lokalizacji:

- W przypadku instalacji w systemie IBM MQ :
  - Linux AIX W systemie AIX lub Linux: /var/mqm/web/installations/*installationName*/servers/mqweb/logs
  - Windows W systemie Windows: *MQ_DATA_PATH*\web\installations*installationName*\servers\mqweb\logs, gdzie *MQ_DATA_PATH* jest ścieżką danych IBM MQ . Ta ścieżka jest ścieżką danych wybraną podczas instalowania produktu IBM MQ. Domyślna ścieżka to C:\ProgramData\IBM\MQ.
- V 9.3.5 Linux W przypadku instalacji autonomicznej produktu IBM MQ Web Server : *MQ_OVERRIDE_DATA_PATH*/web/installations/MQWEBINST/servers/mqweb/logs

  gdzie *MQ_OVERRIDE_DATA_PATH* jest katalogiem danych produktu IBM MQ Web Server , na który wskazuje zmienna środowiskowa **MQ_OVERRIDE_DATA_PATH** .

Więcej informacji na temat konfigurowania poziomów rejestrowania serwera mqweb zawiera sekcja Konfigurowanie rejestrowania.

Zdarzenia komend i konfiguracji

Opcjonalnie można włączyć zdarzenia 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 powoduje generowanie zdarzeń komend i konfiguracji. Więcej informacji na temat włączania zdarzeń konfiguracji i komend zawiera sekcja Kontrolowanie zdarzeń konfiguracji, komend i programów rejestrujących.

W przypadku tych komunikatów zdarzeń komend i 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 mqweb, a nie nazwę użytkownika, który wydał komendę. Jeśli jednak użytkownik ma rolę MQWebUser , **MQCACF_EVENT_USER_ID** zgłasza nazwę użytkownika, który wydał komendę.

Pojęcia pokrewne

“Kontrola” na stronie 526
Za pomocą komunikatów o zdarzeniach można sprawdzić, czy nie wystąpiły włamania lub próby włamania. Bezpieczeństwo systemu można również sprawdzić za pomocą konsoli IBM MQ Explorer.

Zagadnienia dotyczące zabezpieczeń produktów IBM MQ Console i REST API w systemie z/OS

Systemy IBM MQ Console i REST API mają opcje zabezpieczające określające, czy użytkownik może wydawać, wyświetlać lub zmieniać komendy. Komendy są następnie przekazywane do menedżera kolejek, a zabezpieczenia menedżera kolejek są następnie używane do kontrolowania, czy użytkownik może wydać komendę do tego konkretnego menedżera kolejek.

Procedura

1. Upewnij się, że identyfikator użytkownika uruchomionego zadania serwera mqweb ma odpowiednie uprawnienia do wydawania określonych komend PCF i uzyskiwania dostępu do określonych kolejek. Więcej informacji na ten temat zawiera “Uprawnienia wymagane przez ID użytkownika uruchomionego zadania serwera mqweb” na stronie 588.
2. Upewnij się, że wszyscy użytkownicy, którym nadano rolę MQWebUser , mają odpowiednie uprawnienia.

   Użytkownicy produktów IBM MQ Console i REST API , którzy są przypisani do roli MQWebUser , działają w kontekście zabezpieczeń nazwy użytkownika. Te identyfikatory użytkowników mogą wykonywać tylko te operacje, którym nadano ID użytkownika do wykonania w menedżerze kolejek, i muszą mieć nadane prawa dostępu do tych samych kolejek systemowych, co przestrzeń adresowa serwera mqweb.

   ID użytkownika uruchomionego zadania serwera mqweb musi mieć nadany alternatywny dostęp do wszystkich użytkowników przypisanych do roli MQWebUser .

   Więcej informacji na temat nadawania odpowiednich uprawnień użytkownikom z rolą MQWebUser zawiera sekcja “Dostęp do zasobów IBM MQ wymaganych do korzystania z IBM MQ Console lub REST API” na stronie 589.
3. Opcjonalne: Skonfiguruj protokół TLS dla produktów 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 590.

z/OS Uprawnienia wymagane przez ID użytkownika uruchomionego zadania serwera mqweb

W systemie z/OSidentyfikator użytkownika uruchomionego zadania serwera mqweb wymaga pewnych uprawnień do wydawania komend PCF i uzyskiwania dostępu do zasobów systemowych.

Identyfikator użytkownika uruchomionego zadania serwera mqweb musi być następujący:

- Identyfikator użytkownika systemu z/OS UNIX, który może używać z/OS UNIX System Services.
- Dostęp do zestawów danych `hlq.SCSQAUTH` i `hlq.SCSQANL*` w instalacji IBM MQ .
- Prawo do odczytu plików instalacyjnych IBM MQ w katalogu z/OS UNIX System Services.
- Prawo do odczytu i zapisu w katalogu użytkowników Liberty utworzonym przez skrypt **crtmqweb** .
- Uprawnienie do nawiązywania połączenia z menedżerem kolejek. Nadaj identyfikatorowi użytkownika uruchomionego zadania serwera mqweb dostęp *READ* do profilu `hlq.BATCH` w klasie MQCONN.
- Uprawnienie do wydawania komend IBM MQ i uzyskiwania dostępu do określonych kolejek. Te szczegóły zostały opisane w sekcjach "IBM MQ Console -wymagane profile zabezpieczeń komend" na stronie 243, "Bezpieczeństwo kolejki systemowej" na stronie 218i "Profile zabezpieczeń kontekstu" na stronie 230.
- Uprawnienie do subskrybowania tematu SYSTEM.FTE , aby można było używać REST API for MFT. Nadaj użytkownikowi uruchomionego zadania serwera mqweb o identyfikatorze *ALTER* dostęp do profilu `hlq.SUBSCRIBE.SYSTEM.FTE` w klasie MXTOPIC.
- W przypadku konfigurowania rejestru SAF dostęp do różnych profili zabezpieczeń. Więcej informacji zawiera sekcja "Konfigurowanie rejestru SAF dla systemów IBM MQ Console i REST API" na stronie 570.

Uwierzytelnianie połączenia

Jeśli menedżer kolejek został skonfigurowany w taki sposób, aby wszystkie aplikacje wsadowe udostępniały poprawny identyfikator użytkownika i hasło, ustawiając parametr CHKLOCL (REQUIRED), należy nadać identyfikatorowi użytkownika *UPDATE* uruchomionego zadania serwera mqweb 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 wszystkie aplikacje wsadowe udostępniały poprawny identyfikator użytkownika i hasło, wystarczy nadać identyfikatorowi użytkownika, który uruchamia zadanie serwera mqweb, dostęp *READ* do profilu `hlq.BATCH` w klasie MQCONN.

Więcej informacji na temat komendy CHCKLOCL zawiera sekcja "Korzystanie z programu CHCKLOCL w aplikacjach powiązanych lokalnie" na stronie 208.

Dostęp do zasobów IBM MQ wymaganych do korzystania z IBM MQ Console lub REST API

Operacje wykonywane w programie IBM MQ Consolelub REST APIprzez użytkownika o roli `MQWebUser` są wykonywane w kontekście zabezpieczeń tego użytkownika.

O tym zadaniu

Więcej informacji na temat ról w systemach IBM MQ Console i REST APIzawiera sekcja "Role w systemach IBM MQ Console i REST API" na stronie 572 .

Poniższa procedura umożliwia nadanie użytkownikowi w roli `MQWebUser` dostępu do zasobów menedżera kolejek, które są wymagane do używania konsoli IBM MQ Console lub programu REST API.

Procedura

1. Nadaj ID użytkownika `mqweb server started task` alternatywny dostęp do każdego ID użytkownika w roli `MQWebUser` .

   Tę czynność należy wykonać dla każdego menedżera kolejek, którym użytkownicy będą administrować za pośrednictwem programu IBM MQ Console lub programu REST API.

   Można użyć następujących przykładowych komend RACF , aby nadać użytkownikowi w roli `MQWebUser` alternatywny dostęp do identyfikatora użytkownika `mqweb server started task` :

   ```
   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 przedrostkiem profilu, który może być nazwą menedżera kolejek lub nazwą grupy współużytkowania kolejki.

userId
Użytkownik pełniący rolę `MQWebUser` .

mqwebUserId
Jest identyfikatorem użytkownika `mqweb server started task`

Uwaga: Jeśli używane są zabezpieczenia z mieszaną wielkością liter, należy użyć klasy MXADMIN, a nie klasy MQADMIN.

2. Nadaj każdemu użytkownikowi w roli `MQWebUser` dostęp do kolejek systemowych, które są niezbędne do korzystania z programów IBM MQ Console i REST API.

   W tym celu należy wykonać obie czynności w systemie SYSTEM.ADMIN.COMMAND.QUEUE i SYSTEM.REST.REPLY.QUEUE, przyznaj każdemu użytkownikowi dostęp UPDATE do klas MQQUEUE lub MXQUEUE, w zależności od tego, czy używane są zabezpieczenia z wielkością liter.

   Należy to zrobić dla każdego menedżera kolejek, który będzie administrowany przez użytkownika za pomocą programu REST API, w tym dla zdalnych menedżerów kolejek administrowanych za pomocą programu Brama administrative REST API.
3. Aby umożliwić użytkownikowi o roli `MQWebUser` administrowanie zdalnymi menedżerami kolejek, należy nadać użytkownikowi dostęp UPDATE do profilu w klasie MQQUEUE lub MXQUEUE, zabezpieczając kolejkę transmisji używaną do wysyłania komend do zdalnego menedżera kolejek. Należy pamiętać, że należy nadać użytkownikowi dostęp UPDATE do menedżera kolejek bramy.

   W zdalnym menedżerze kolejek nadaj temu samemu użytkownikowi dostęp do kolejki transmisji używanej do wysyłania komunikatów odpowiedzi komend z powrotem do menedżera kolejek bramy.
4. Nadaj użytkownikom z rolą `MQWebUser` dostęp do wszystkich innych zasobów wymaganych do wykonania operacji obsługiwanych przez IBM MQ Console i REST API.

   Dostęp potrzebny do:

   - Wykonywanie operacji w REST APIjest opisane w sekcjach *Wymagania dotyczące bezpieczeństwa* poszczególnych Zasoby REST API
   - Komendy wydawane przez IBM MQ Console są opisane w sekcji “IBM MQ Console -wymagane profile zabezpieczeń komend” na stronie 243

z/OS Konfigurowanie protokołu TLS dla serwerów REST API i IBM MQ Console w systemie z/OS

W systemie z/OSmożna skonfigurować serwer mqweb w taki sposób, aby używał pliku kluczy RACF do przechowywania certyfikatów na potrzeby bezpiecznych połączeń z protokołem TLS i uwierzytelnianiem przy użyciu certyfikatów klienta.

Zanim rozpoczniesz

Aby wykonać tę procedurę, użytkownik musi mieć uprawnienia do zapisu w pliku `mqwebuser.xml` oraz uprawnienia do pracy z plikami kluczy SAF.

O tym zadaniu

Domyślna konfiguracja serwera mqweb używa magazynów kluczy Java dla serwera i zaufanych certyfikatów. W systemie z/OSmożna skonfigurować serwer mqweb do używania pliku kluczy RACF zamiast magazynów kluczy Java . Serwer można również skonfigurować w taki sposób, aby umożliwić użytkownikom uwierzytelnianie przy użyciu certyfikatu klienta.

Informacje na temat używania plików kluczy RACF w pliku Libertyzawiera sekcja Liberty: Keystores .

Wykonaj tę procedurę, aby skonfigurować serwer mqweb do używania pliku kluczy RACF i opcjonalnie skonfigurować uwierzytelnianie certyfikatu klienta. W tej procedurze opisano czynności niezbędne do utworzenia i używania certyfikatów podpisanych przy użyciu własnych certyfikatów ośrodka certyfikacji (CA). W środowisku produkcyjnym można użyć certyfikatów uzyskanych z zewnętrznego ośrodka certyfikacji.

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 przy użyciu certyfikatu ośrodka CA utworzonego 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* jest identyfikatorem użytkownika uruchomionego zadania serwera mqweb, a *hostname* jest nazwą hosta serwera mqweb.

3. Połącz certyfikat ośrodka CA i certyfikat serwera z bazą kluczy SAF, wprowadzając następujące komendy:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
```

   gdzie *mqwebUserId* jest identyfikatorem użytkownika uruchomionego zadania serwera mqweb, a *keyring* jest nazwą pliku kluczy, który ma być używany.

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 ośrodka CA za pomocą protokołu FTP w formacie binarnym do stacji roboczej i zaimportuj go do przeglądarki jako certyfikat ośrodka certyfikacji.
6. Opcjonalne: Aby skonfigurować uwierzytelnianie certyfikatu klienta, należy utworzyć i wyeksportować 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 ośrodka CA z bazą kluczy SAF, wprowadzając następującą komendę:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

gdzie *mqwebUserId* jest identyfikatorem użytkownika uruchomionego zadania serwera mqweb, a *keyring* jest nazwą pliku kluczy, który ma być używany.

c) Utwórz certyfikat klienta podpisany przy użyciu certyfikatu 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* to nazwa 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 porównywane z użytkownikiem w rejestrze.
- Jeśli używany jest rejestr SAF i certyfikat znajduje się w bazie danych RACF , podczas tworzenia certyfikatu używany jest właściciel certyfikatu określony za pomocą parametru **ID** .
- Jeśli używany jest rejestr LDAP, pełna nazwa wyróżniająca w certyfikacie jest dopasowywana do rejestru LDAP.

d) Wyeksportuj certyfikat klienta do pliku PKCS #12 , wprowadzając następującą komendę:

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) -
         PASSWORD('password') DSN('hlq.USER.CERT')
```

e) Prześlij wyeksportowany certyfikat do stacji roboczej za pomocą protokołu FTP w postaci binarnej. Aby używać certyfikatu klienta z programem IBM MQ Console, zaimportuj go do przeglądarki WWW używanej do uzyskania dostępu do programu IBM MQ Console jako certyfikat osobisty.

7. Zmodyfikuj plik *WLP_user_directory*/servers/mqweb/mqwebuser.xml, gdzie *katalog_użytkownika_WLP* to katalog, który został określony podczas wykonywania skryptu **crtmqweb** w celu utworzenia definicji serwera mqweb.

   Wprowadź następujące zmiany, aby skonfigurować serwer mqweb do używania pliku kluczy RACF :

   a) Usuń lub przekształć w komentarz 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:

   - *mqwebUserIdentyfikator* to identyfikator użytkownika uruchomionego zadania serwera mqweb.
   - *keyring* to nazwa pliku kluczy RACF .
   - *mqwebServerCertyfikat* jest etykietą certyfikatu serwera 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 używać certyfikatu klienta z IBM MQ Console, wprowadź URL dla IBM MQ Console w przeglądarce WWW, w której zainstalowano certyfikat klienta.

- Aby używać certyfikatu klienta z interfejsem API REST, należy udostępnić certyfikat klienta dla każdego żądania REST.

Uwagi:

a. Jeśli do uwierzytelniania w programie IBM MQ Consoleużywane są tylko certyfikaty, przeglądarka może wyświetlić listę certyfikatów do wyboru.

b. Aby użyć innego certyfikatu, może być konieczne zamknięcie i ponowne uruchomienie przeglądarki.

c. Jeśli używane są certyfikaty klienta, które nie znajdują się w bazie danych RACF , można użyć filtrowania nazwy certyfikatu RACF , aby odwzorować atrybuty certyfikatu na ID 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

Skonfigurowano interfejs TLS dla IBM MQ Console i REST API.

ALW Zarządzanie kluczami i certyfikatami w systemie AIX, Linux, and Windows

W systemie AIX, Linux, and Windowsdo zarządzania kluczami, certyfikatami i żądaniami certyfikatów należy używać komend **runmqckm** i **runmqakm** .

O tym zadaniu

Komenda **runmqckm** udostępnia funkcje podobne do tych, które są dostępne w systemach **iKeyman**i , a komenda **runmqakm** udostępnia funkcje podobne do tych, które są dostępne w systemach **gskitcapicmd**. Przed użyciem systemu **runmqckm** lub **runmqakm**upewnij się, że zmienne środowiskowe systemu są poprawnie skonfigurowane, uruchamiając komendę **setmqenv** .

Komenda **runmqckm** wymaga zainstalowania komponentu IBM MQ JRE. Jeśli ten komponent nie jest zainstalowany, można użyć komendy **runmqakm** .

Aby zarządzać certyfikatami TLS w sposób zgodny ze standardem FIPS, należy użyć komendy **runmqakm** zamiast komendy **runmqckm** . Jest to spowodowane tym, że komenda **runmqakm** obsługuje silniejsze szyfrowanie.

Procedura

- Użyj komend **runmqckm** i **runmqakm** , aby wykonać następujące czynności:
  - V 9.3.0 Utwórz typ plików bazy danych kluczy CMS lub PKCS#12 , które są wymagane przez IBM MQ
  - Tworzenie żądań certyfikatów
  - Importuj certyfikaty osobiste
  - Importowanie certyfikatów CA
  - Zarządzanie certyfikatami samopodpisanymi

Zadania pokrewne

“Korzystanie z interfejsu użytkownika strmqikm” na stronie 328
Certyfikat osobisty można utworzyć za pomocą programu **strmqikm** (iKeyman) Interfejs GUI.

Odsyłacze pokrewne

Wywoływanie graficznego interfejsu użytkownika narzędzia IBM **strmqikm** (iKeyman)

Informacje pokrewne
Narzędzie klucza

ALW Komendy runmqckm i runmqakm w systemie AIX, Linux, and Windows

W tej sekcji opisano komendy **runmqckm** i **runmqakm** zgodnie z ich obiektem.

Główne różnice między tymi dwiema komendami są następujące:

- **runmqckm**
  - Udostępnia funkcje podobne do funkcji programu **iKeycmd**
  - Obsługuje formaty plików repozytorium kluczy JKS i JCEKS
- **runmqakm**
  - Udostępnia funkcje podobne do funkcji programu **gskitcapicmd**
  - 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** .

Ostrzeżenie: 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 AIX, Linux, and Windows” na stronie 606 .

ALW Komendy dla baz danych kluczy CMS lub PKCS#12 w systemie AIX, Linux, and Windows

Komendy **runmqckm** i **runmqakm** służą do zarządzania kluczami i certyfikatami bazy danych kluczy CMS lub 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 .

Deprecated 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:

Za pomocą komendy **runmqckm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password -expire days
```

Za pomocą komendy **runmqakm** :

```
-keydb -changepw -db filename -pw password -new_pw new_password -expire days
-fips -strong
```

-keydb -convert
W przypadku komendy **runmqckm** należy przekształcić bazę danych kluczy z jednego formatu na inny:

```
-keydb -convert -db filename -pw password
-old_format cms | pkcs12 -new_format cms
```

Za pomocą komendy **runmqakm** przekształć starą wersję bazy danych kluczy CMS w nową wersję bazy danych kluczy CMS :

```
-keydb -convert -db filename -pw password
-new_db filename -new_pw password -strong -fips
```

-keydb -create
Utwórz bazę danych kluczy:

Za pomocą komendy **runmqckm** :

```
V 9.3.0 -keydb -create -db filename -pw password -type cms
| pkcs12
```

Za pomocą komendy **runmqakm** :

```
V 9.3.0 -keydb -create -db filename -pw password -type  cms
/ p12 -fips -strong
```

-keydb -delete
Usuwanie bazy danych kluczy:

Przy użyciu jednej z następujących komend:

```
-keydb -delete -db filename -pw password
```

-keydb -list
Wyświetl aktualnie obsługiwane typy bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-keydb -list
```

Za pomocą komendy **runmqakm** :

```
-keydb -list -fips
```

-cert -add
Dodaj certyfikat z pliku do bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-cert -add -db filename -pw password -label label -file filename
-format ascii | binary
```

Za pomocą komendy **runmqakm** :

```
-cert -add -db filename -pw password -label label -file filename
-format ascii | binary -fips
```

-cert -create

Utwórz certyfikat samopodpisany:

Za pomocą komendy **runmqckm** :

```
-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
```

Za pomocą komendy **runmqakm** :

```
-cert -create -db filename -pw password -label label
-dn distinguished_name -size 2048 | 1024 | 512 -x509version 3 | 1 | 2
-expire days -fips -sig_alg md5 |
MD5_WITH_RSA | 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 |
EC_ecdsa_with_SHA512
```

-cert -delete

Usuń certyfikat:

Za pomocą komendy **runmqckm** :

```
-cert -delete -db filename -pw password -label label
```

Za pomocą komendy **runmqakm** :

```
-cert -delete -db filename -pw password -label label -fips
```

-cert -details

Wyświetl szczegółowe informacje o konkretnym certyfikacie:

Za pomocą komendy **runmqckm** :

```
-cert -details -db filename -pw password -label label
```

Za pomocą komendy **runmqakm** :

```
-cert -details -db filename -pw password -label label -fips
```

-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:

Za pomocą komendy **runmqckm** :

```
-cert -export -db filename -pw password -label label -type cms | pkcs12
-target filename -target_pw password -target_type  cms | pkcs12
```

Za pomocą komendy **runmqakm** :

```
-cert -export -db filename -pw password -label label -type cms | pkcs12
-target filename -target_pw password -target_type  cms | pkcs12
-encryption strong | weak -fips
```

-cert -extract
Wyodrębnij certyfikat z bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-cert -extract -db filename -pw password -label label -target filename
-format ascii | binary
```

Za pomocą komendy **runmqakm** :

```
-cert -extract -db filename -pw password -label label -target filename
-format ascii | binary -fips
```

-cert -import
Zaimportuj certyfikat osobisty z bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label  label
```

Za pomocą komendy **runmqakm** :

```
-cert -import -file filename -pw password -type cms -target filename
-target_pw password -target_type cms -label  label -fips
```

Dla obu tych komend:

- Opcja `-label` jest wymagana i określa etykietę certyfikatu, który ma zostać zaimportowany z źródłowej bazy danych kluczy.
- Dodatkowo można użyć opcji `-new_label` . Dzięki temu importowanemu certyfikatowi zostanie nadana inna etykieta w docelowej bazie danych kluczy niż etykieta w źródłowej bazie danych.

-cert -list
Wyświetl listę wszystkich certyfikatów w bazie danych kluczy:

Za pomocą komendy **runmqckm** :

```
-cert -list all | personal | CA -db filename -pw password
```

Za pomocą komendy **runmqakm** :

```
-cert -list all | personal | CA -db filename -pw password -fips
```

-cert -receive
Pobierz certyfikat z pliku:

Za pomocą komendy **runmqckm** :

```
-cert -receive -file filename -db filename -pw password
-format ascii | binary -default_cert yes | no
```

Za pomocą komendy **runmqakm** :

```
-cert -receive -file filename -db filename -pw password
-format ascii | binary -default_cert yes | no -fips
```

-cert -sign

Podpisz certyfikat:

Za pomocą komendy **runmqckm** :

```
-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
```

Za pomocą komendy **runmqakm** :

```
-cert -sign -db filename -file filename -pw password
-label label -target filename -format ascii | binary -expire days -fips
-sig_alg md5 | MD5_WITH_RSA | 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 |
EC_ecdsa_with_SHA512
```

-certreq -create

Utwórz żądanie certyfikatu:

Za pomocą komendy **runmqckm** :

```
-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
```

Za pomocą komendy **runmqakm** :

```
-certreq -create -db filename -pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -file filename -fips
-sig_alg md5 | MD5_WITH_RSA | 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 |
EC_ecdsa_with_SHA512
```

-certreq -delete
Usuń żądanie certyfikatu:

Za pomocą komendy **runmqckm** :

```
-certreq -delete -db filename -pw password -label  label
```

Za pomocą komendy **runmqakm** :

```
-certreq -delete -db filename -pw password -label  label -fips
```

-certreq -szczegóły
Wyświetl szczegółowe informacje dotyczące konkretnego żądania certyfikatu:

Za pomocą komendy **runmqckm** :

```
-certreq -details -db filename -pw password -label  label
```

Za pomocą komendy **runmqakm** :

```
-certreq -details -db filename -pw password -label  label -fips
```

Wyświetl szczegółowe informacje o żądaniu certyfikatu i wyświetl pełne żądanie certyfikatu:

Za pomocą komendy **runmqckm** :

```
-certreq -details -showOID -db filename -pw password -label label
```

Za pomocą komendy **runmqakm** :

```
-certreq -details -showOID -db filename -pw password -label label -fips
```

-certreq -extract
Wyodrębnij żądanie certyfikatu z bazy danych żądań certyfikatów do pliku:

W przypadku komendy **runmqckm** :

```
-certreq -extract -db filename -pw password -label label -target filename
```

Za pomocą komendy **runmqakm** :

```
-certreq -extract -db filename -pw password -label label -target filename -fips
```

-certreq -list
Wyświetl wszystkie żądania certyfikatów w bazie danych żądań certyfikatów:

Za pomocą komendy **runmqckm** :

```
-certreq -list -db filename -pw password
```

Za pomocą komendy **runmqakm** :

```
-certreq -list -db filename -pw password -fips
```

-certreq -odtwórz
Ponownie utwórz żądanie certyfikatu:

Za pomocą komendy **runmqckm** :

```
-certreq -recreate -db filename -pw password -label label -target filename
```

Za pomocą komendy **runmqakm** :

```
-certreq -recreate -db filename -pw password -label label -target filename -fips
```

ALW Komendy dla operacji urządzenia szyfrującego w systemie AIX, Linux, and Windows

Do zarządzania kluczami i certyfikatami dla operacji urządzeń szyfrujących można użyć komend **runmqckm** (iKeycmd) i **runmqakm** .

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 .

Deprecated 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:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-keydb -changepw -db filename -crypto module_name -tokenlabel  token_label
-pw password -new_pw new_password -fips -strong
```

-keydb -list
Wyświetl aktualnie obsługiwane typy bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-keydb -list -fips
```

-cert -add
Dodaj certyfikat z pliku do urządzenia szyfrującego:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -add -crypto module_name -tokenlabel token_label -pw password
-label label -file filename -format ascii | binary -fips
```

-cert -create

Utwórz certyfikat samopodpisany na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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
```

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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -x509version 3 | 1 | 2
-default_cert no | yes -expire days
-fips -sig_alg md5 | MD5_WITH_RSA | 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 |
EC_ecdsa_with_SHA512
```

-cert -delete

Usuwanie certyfikatu z urządzenia szyfrującego:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -delete -crypto module_name -tokenlabel token_label -pw password -label label -fips
```

-cert -details

Wyświetl szczegółowe informacje o konkretnym certyfikacie urządzenia szyfrującego:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -details -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

Wyświetl szczegółowe informacje i wyświetl pełny certyfikat dla konkretnego certyfikatu na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label -fips
```

-cert -extract

Wyodrębnij certyfikat z bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -extract -crypto module_name -tokenlabel token_label -pw password
-label label -target filename -format ascii | binary -fips
```

-cert -import

Zaimportuj certyfikat do urządzenia szyfrującego z obsługą dodatkowej bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-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:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw  password
-secondaryDB filename -secondaryDBpw password -fips
```

-cert -list

Wyświetl listę wszystkich certyfikatów na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -list all | personal | CA -crypto module_name
-tokenlabel token_label -pw  password -fips
```

-cert -receive

Pobierz certyfikat z pliku do urządzenia szyfrującego z obsługą dodatkowej bazy danych kluczy:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-cert -receive -file filename -crypto module_name -tokenlabel  token_label
-pw password -default_cert yes | no -secondaryDB filename
-secondaryDBpw password -format  ascii | binary -fips
```

-certreq -create

Utwórz żądanie certyfikatu na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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
```

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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -create -crypto module_name -tokenlabel token_label
-pw password -label label -dn distinguished_name
-size 2048 | 1024 | 512 -file filename -fips
-sig_alg md5 | MD5_WITH_RSA | SHA_WITH_DSA |
SHA_WITH_RA | 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 |
EC_ecdsa_with_SHA512
```

-certreq -delete

Usuń żądanie certyfikatu z urządzenia szyfrującego:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -delete -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

-certreq -szczegóły

Wyświetl szczegółowe informacje dotyczące konkretnego żądania certyfikatu w urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -details -crypto module_name -tokenlabel token_label
-pw password -label label -fips
```

Wyświetl szczegółowe informacje o żądaniu certyfikatu i wyświetl pełne żądanie certyfikatu na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -details -showOID -crypto module_name -tokenlabel  token_label
-pw password -label label -fips
```

-certreq -extract
Wyodrębnij żądanie certyfikatu z bazy danych żądań certyfikatów na urządzeniu szyfrującym do pliku:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -extract -crypto module_name -tokenlabel token_label
-pw password -label label -target filename -fips
```

-certreq -list
Wyświetl wszystkie żądania certyfikatów w bazie danych żądań certyfikatów na urządzeniu szyfrującym:

Za pomocą komendy **runmqckm** :

```
-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, dlatego należy zainstalować 64-bitową bibliotekę PKCS#11 do administrowania sprzętem szyfrującym. 32-bitowe platformy Windows i Linux x86 są jedynymi wyjątkami, ponieważ na tych platformach programy **strmqikm** i **runmqckm** są 32-bitowe.

Za pomocą komendy **runmqakm** :

```
-certreq -list -crypto module_name -tokenlabel token_label
-pw password -fips
```

ALW Opcje runmqckm i runmqakm w systemie AIX, Linux, and Windows

Do zarządzania kluczami, certyfikatami i żądaniami certyfikatów można użyć opcji wiersza komend **runmqckm** i **runmqakm** . **runmqckm** udostępnia funkcje podobne do tych, które są dostępne w systemie **iKeycmd**, a **runmqakm** udostępnia funkcje podobne do tych, które są dostępne w systemie **gskitcapicmd**.

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 .

Deprecated 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 97. Opcje, których można używać z opcjami **runmqckm** i **runmqakm***

Parametr	Opis
`-create`	Opcja tworzenia bazy danych kluczy.

*Tabela 97. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**
`-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. Podanie 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. W trybie FIPS komponent IBM Crypto for C (ICC) używa algorytmów, których poprawność została sprawdzona w trybie FIPS 140-2. Jeśli komponent ICC nie zostanie zainicjowany w trybie FIPS, wykonanie komendy **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 “Etykiety certyfikatów cyfrowych, zrozumienie wymagań” na stronie 27.
-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 “Etykiety certyfikatów cyfrowych, zrozumienie wymagań” na stronie 27.
-new_pw	Nowe hasło bazy danych.

*Tabela 97. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**
-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 .
runmqakm **-secretKey** -add -create -extract	 Dodaj klucz tajny. Utwórz losowy klucz tajny Wyodrębnij klucz tajny z bazy danych kluczy
runmqckm **-secKey** -create -list -export	 Utwórz losowy klucz tajny. Lista kluczy tajnych Eksportuj klucze tajne
-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.

*Tabela 97. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**
-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. Domyślną wielkością klucza RSA jest 2048 bitów. • 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.
-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** .
-stashpw	Zapisz hasło bazy danych kluczy w pliku. Dotyczy tylko baz danych typu CMS i PKCS12.
-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.

*Tabela 97. Opcje, których można używać z opcjami **runmqckm** i **runmqakm** (kontynuacja)*	
Parametr	**Opis**

-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`

ALW Kody błędów komendy runmqakm w systemie AIX, Linux, and Windows

Tabela zawierająca liczbowe kody błędów wydane przez **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.

Kod błędu	Komunikat o błędzie
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).
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. (Protokół 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.

Kod błędu	Komunikat o błędzie
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.
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.

Kod błędu	Komunikat o błędzie
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.
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 .

Kod błędu	Komunikat o błędzie
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.
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.

Kod błędu	Komunikat o błędzie
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.
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. (Protokół LDAP nie jest obsługiwany przez ten program)
144	Użytkownik LDAP nie jest poprawnym użytkownikiem. (Protokół LDAP nie jest obsługiwany przez ten program)
145	Zapytanie LDAP nie powiodło się. (Protokół 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.

Kod błędu	Komunikat o błędzie
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.
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.

Kod błędu	Komunikat o błędzie
221	Napotkano nieobsługiwany algorytm podpisu. Na tym etapie obsługiwane są tylko algorytmy Deprecated MD5 i Deprecated 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.
226	Jeśli używany jest znacznik -strong, maksymalna długość hasła wynosi 300 znaków.
227	Algorytm MD5 nie jest obsługiwany w trybie FIPS.
228	Znacznik ośrodka 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 haseł w plikach konfiguracyjnych komponentu IBM MQ

Aby można było korzystać z niektórych funkcji produktu IBM MQ, konieczne może być podanie haseł bezpośrednio do pliku IBM MQ lub w plikach konfiguracyjnych odczytywanych przez ten składnik. Od wersji IBM MQ 9.2.0zaimplementowano system ochrony haseł, który chroni hasła w tych plikach konfiguracyjnych.

Hasła w plikach konfiguracyjnych muszą być zaszyfrowane. Poniższa lista zawiera wyjaśnienie wspólnej terminologii, która jest używana dla każdego komponentu:

Klucz początkowy

Klucz szyfrowania używany do ochrony hasła.

Dla każdego wymienionego komponentu podaj unikalny klucz początkowy, który jest używany do ochrony haseł przechowywanych w konfiguracji tego komponentu. Ten sam klucz początkowy musi być również dostępny dla komponentu, aby hasło mogło zostać zdeszyfrowane.

Większość komponentów wymaga, aby klucz początkowy był podany w pliku. Początkowy plik kluczy musi:

- **Zawiera jeden wiersz zawierający co najmniej jeden znak.**
- Są odpowiednio chronione za pomocą uprawnień systemu operacyjnego.

Nie ma żadnych wymagań dotyczących długości klucza początkowego lub znaków, które można określić. Jednak w celu zapewnienia odpowiedniej ochrony należy podać klucz początkowy o długości co najmniej 16 znaków. Na przykład początkowy plik kluczy może zawierać:

```
Th1sIs@n3Ncypt|onK$y
```

Domyślny klucz początkowy
Domyślny klucz szyfrowania używany, jeśli podczas szyfrowania danych nie zostanie użyty klucz początkowy. **Nie** należy jednak używać domyślnego klucza początkowego, ponieważ nie chroni on zaszyfrowanych danych.

Zwykły łańcuch tekstowy
Łańcuch, który jest zaszyfrowany, zwykle jest to hasło.

Zaszyfrowany łańcuch hasła
Łańcuch zawierający zaszyfrowane hasło w formacie zrozumiałym dla produktu IBM MQ .

Ważne: Zaszyfrowanych łańcuchów haseł wygenerowanych w celu użycia z jednym komponentem nie można skopiować do pliku konfiguracyjnego innego komponentu w celu użycia. Każde hasło dla każdego komponentu musi być chronione za pomocą programu narzędziowego specyficznego dla komponentu.

Szczegółowe informacje na temat zabezpieczania haseł dla każdego komponentu produktu IBM MQ , który obsługuje ochronę haseł, znajdują się w następujących sekcjach:

- Advanced Message Security
- “Managed File Transfer” na stronie 619
- “IBM MQ Internet Pass-Thru” na stronie 620
- Deprecated “IBM MQ Bridge to blockchain” na stronie 621
- Deprecated “IBM MQ Bridge to Salesforce” na stronie 621
- V 9.3.0 “IBM MQ clients , które używają sprzętu szyfrującego” na stronie 622
- “IBM MQ menedżer kolejek” na stronie 623
- V 9.3.0 “Aplikacje klienckie IBM MQ C” na stronie 623
- V 9.3.2 “Rodzime konfiguracje wysokiej dostępności” na stronie 624
- V 9.3.4 “Menedżer kolejek IBM MQ (sekcjaAuthToken w pliku qm.ini)” na stronie 624

Advanced Message Security

Klienty Advanced Message Security (AMS) Java wymagają dostępu do magazynu kluczy zawierającego klucze prywatne w celu zabezpieczenia komunikatu.

V 9.3.0 Advanced Message Security (AMS) Klienty MQI lub menedżery kolejek skonfigurowane na potrzeby przechwytywania MCA mogą wymagać dostępu do sprzętu szyfrującego PKCS#11 lub plików PEM zawierających klucze prywatne w celu zabezpieczenia komunikatów.

Aby uzyskać dostęp do tych plików, należy podać hasło w pliku konfiguracyjnym AMS o nazwie `keystore.conf`. Komenda **runamscred** służy do ochrony poufnych informacji zawartych w pliku `keystore.conf` . Na przykład składnia

```
runamscred -f <keystore configuration file>
```

Komenda **runamscred** chroni poufne parametry w podanym pliku, używając opcji **-f** .

V 9.3.0 Do instalacji produktu IBM MQ dodano dwa programy **runamscred** :

- Program MQI **runamscred** znajdujący się w katalogu `<IBM MQ installation root>/bin`

- Program Java **runamscred** znajdujący się w katalogu <IBM MQ installation root>/java/bin

Ostrzeżenie: W celu zapewnienia zgodności

1. V 9.3.0 Program Java **runamscred** służy do zabezpieczania plików konfiguracyjnych, które mają być używane z klientami produktu Java AMS , oraz program MQI **runamscred** do zabezpieczania plików konfiguracyjnych, które mają być używane z klientami MQI AMS .
2. Po uruchomieniu komendy **runamscred**należy sprawdzić, czy wszystkie niezbędne informacje poufne są chronione.
3. Zabezpieczony plik należy udostępnić w normalny sposób aplikacjom z obsługą produktu AMS .

Aby nadpisać lub udostępnić początkowy plik kluczy, który ma być używany w czasie wykonywania aplikacji AMS , lub gdy plik konfiguracyjny magazynu kluczy jest chroniony za pomocą funkcji **runamscred**, należy użyć jednego z następujących czterech mechanizmów (w kolejności priorytetów):

1. Parametr **-sf** (tylko**runamscred**)
2. **MQS_AMSCRED_KEYFILE** , zmienna środowiskowa
3. Parametr **amscred.keyfile** w pliku konfiguracyjnym keystore.conf
4. Domyślny początkowy plik kluczy, jeśli nie określono żadnej z poprzednich opcji.

Ostrzeżenie: V 9.3.0 Nie należy używać domyślnego klucza początkowego.

W systemach wcześniejszych niż IBM MQ 9.2do ochrony haseł w plikach konfiguracyjnych produktu AMS Java był używany inny system ochrony haseł.

Domyślnie program **runamscred** chroni hasła, używając nowego systemu. Oznacza to, że nowe pliki konfiguracyjne nie są kompatybilne ze starszymi wersjami produktu AMS Java. Aby chronić pliki konfiguracyjne za pomocą starego systemu ochrony haseł, należy użyć opcji **-sp** *0* .

Managed File Transfer

Klasa Managed File Transfer (MFT) przechowuje referencje wymagane do uzyskania dostępu do menedżerów kolejek lub innych zasobów w kilku plikach właściwości XML:

- MQMFTCredentials.xml -dane uwierzytelniające na potrzeby nawiązywania połączenia z menedżerami kolejek agenta, koordynacji i komend oraz hasła na potrzeby nawiązywania połączenia z magazynami kluczy na potrzeby bezpiecznej komunikacji.
- ProtocolBridgeCredentials.xml -referencje na potrzeby nawiązywania połączeń z serwerami protokołu, takimi jak FTP/SFTP/FTPS.
- ConnectDirectCredentials.xml -informacje autoryzacyjne dla agenta Connect:Direct do połączenia z węzłem Connect:Direct .

Więcej informacji na ten temat zawiera “Szyfrowanie zapisanych referencji w produkcie MFT” na stronie 627.

Aby chronić informacje poufne przechowywane w tych plikach, należy użyć komendy fteObfuscate z pliku, który został określony, używając opcji **-f** , na przykład:

```
fteObfuscate -f <File to protect>
```

Aby udostępnić początkowy plik kluczy, który ma być używany podczas ochrony konfiguracji MFT , należy użyć opcji **-sf** :

```
fteObfuscate -f <File to protect> -sf <initial key file>
```

Jeśli nie podano klucza początkowego, do ochrony poufnych informacji używany jest klucz domyślny, ale nie należy używać tej opcji.

Ostrzeżenie:

1. Po uruchomieniu komendy **fteObfuscate**należy sprawdzić, czy wszystkie niezbędne informacje poufne są chronione.
2. Normalnie należy podać chroniony plik w pliku MFT.

W czasie wykonywania należy udostępnić początkowy plik kluczy, który ma być używany za pośrednictwem następujących trzech mechanizmów (w kolejności priorytetów):

1. Za pomocą właściwości systemowej Java .
   - V 9.3.0.10 V 9.3.1 Przed produktami IBM MQ 9.3.1 i IBM MQ 9.3.0 Fix Pack 10nazwa tej właściwości systemowej Java była błędnie zapisana w kodzie produktu w postaci `com.ibm.wqmfte.cred.keyfile`. W systemach IBM MQ 9.3.1 i IBM MQ 9.3.0 Fix Pack 10pisownia nazwy właściwości jest poprawiana na `com.ibm.wmqfte.cred.keyfile`. Produkt Managed File Transfer używa obu wersji właściwości systemowej Java podczas sprawdzania, czy użytkownik określił plik zawierający klucz początkowy, który ma być używany do szyfrowania i deszyfrowania referencji. Pozwala to na użycie poprawnej pisowni nazwy właściwości przy zachowaniu zgodności z wcześniejszą wersją ze starą nazwą z błędem pisowni. Należy zauważyć, że jeśli są ustawione obie właściwości systemowe Java , używana jest wartość poprawnie napisanej właściwości `com.ibm.wmqfte.cred.keyfile` .
   - W przypadku wersji wcześniejszych niż IBM MQ 9.3.1 i IBM MQ 9.3.0 Fix Pack 10należy użyć właściwości `com.ibm.wqmfte.cred.keyfile`.
2. W plikach właściwości agenta, programu rejestrującego, komend i koordynacji.
3. W pliku `installation.properties` .

Przed produktem IBM MQ 9.2do ochrony informacji autoryzacyjnych w plikach konfiguracyjnych MFT był używany inny system ochrony informacji autoryzacyjnych.

Domyślnie program **fteObfuscate** chroni referencje za pomocą nowego systemu. Oznacza to, że pliki konfiguracyjne nie są kompatybilne ze starszymi wersjami programu MFT.

Aby chronić pliki konfiguracyjne za pomocą starego systemu ochrony referencji, należy użyć parametru **-sp** *0* .

IBM MQ Internet Pass-Thru

Plik konfiguracyjny IBM MQ Internet Pass-Thru (MQIPT) może zawierać hasła dostępu do różnych zasobów oraz hasło administratora MQIPT .

Hasła te można chronić za pomocą komendy **mqiptPW** , która jest dostarczana z systemem MQIPT.

```
mqiptPW
```

Aby zabezpieczyć hasło za pomocą konkretnego klucza początkowego, należy podać opcję **-sf** :

```
mqiptPW -sf <intial key file>
```

Więcej informacji na ten temat zawiera sekcja Określanie klucza szyfrowania hasła.

Jeśli nie podano klucza początkowego, do ochrony poufnych informacji używany jest klucz domyślny, ale nie należy używać tej opcji.

Program **mqiptPW** wyświetla zachętę do bezpiecznego wprowadzenia hasła, które ma być chronione, i zwraca łańcuch, który musi zostać skopiowany do pliku konfiguracyjnego MQIPT .

W czasie wykonywania należy udostępnić początkowy plik kluczy, który będzie używany przez następujące cztery mechanizmy. W kolejności priorytetów są to:

1. Za pomocą parametru **-sf** , gdy uruchamiany jest program MQIPT .
2. W zmiennej środowiskowej MQS_MQIPTCRED_KEYFILE.
3. We właściwości **com.ibm.mq.ipt.cred.keyfile** Java .

4. W pliku o nazwie `mqipt_cred.key` w katalogu głównym MQIPT jest to katalog zawierający pliki konfiguracyjne i pliki dziennika produktu MQIPT itp.

Przed produktem IBM MQ 9.2do ochrony informacji autoryzacyjnych w plikach konfiguracyjnych MQIPT był używany inny system ochrony informacji autoryzacyjnych.

Domyślnie program **mqiptPW** chroni referencje, które korzystają z nowego systemu; oznacza to, że pliki konfiguracyjne nie są kompatybilne ze starszymi wersjami programu MQIPT.

Aby chronić hasła magazynu kluczy, które korzystają ze starego systemu ochrony referencji, należy użyć składni komendy **mqiptPW** , która jest obsługiwana w wersjach wcześniejszych niż IBM MQ 9.2.

IBM MQ Bridge to blockchain

Deprecated

Konfiguracje produktu Bridge to blockchain są przechowywane w plikach, które można wygenerować za pomocą komendy **runmqbcb** . Po uruchomieniu tej komendy zostanie wyświetlona prośba o bezpieczne podanie haseł i położenia początkowego pliku kluczy, który ma być używany.

Aby nadpisać początkowy plik kluczy, który ma być używany w czasie wykonywania lub w trybie konfiguracji, należy użyć opcji **-sf** . Na przykład wygeneruj konfigurację z konkretnym początkowym plikiem kluczy:

```
runmqbcb -o <output file> -sf <initial key file>
```

Aby użyć konkretnego początkowego pliku kluczy w czasie wykonywania:

```
runmqbcb -f <config file> -sf <initial key file>
```

Przed produktem IBM MQ 9.2do ochrony informacji autoryzacyjnych w plikach konfiguracyjnych Bridge to blockchain był używany inny system ochrony informacji autoryzacyjnych.

Domyślnie program **runmqbcb** chroni referencje za pomocą nowego systemu, co oznacza, że pliki konfiguracyjne nie są kompatybilne ze starszymi wersjami programu Bridge to blockchain.

Aby chronić pliki konfiguracyjne za pomocą starego systemu ochrony referencji, należy użyć opcji **-sp** *0* .

Ważne:

- Deprecated Produkt IBM MQ Bridge to blockchain jest nieaktualny we wszystkich wersjach od 22 listopada 2022 r. (patrz US Announcement letter 222-341). Blockchain można nawiązać połączenie z produktem IBM App Connect lub za pośrednictwem funkcji App Connect dostępnych w produkcie IBM Cloud Pak for Integration.
- W systemie Continuous Deliveryplik IBM MQ Bridge to blockchain został usunięty z produktu pod adresem IBM MQ 9.3.2.

IBM MQ Bridge to Salesforce

Deprecated

Konfiguracje produktu Bridge to Salesforce są przechowywane w plikach, które można wygenerować za pomocą komendy **runmqsfb** . Podczas uruchamiania tej komendy użytkownik jest proszony o bezpieczne podanie haseł i położenia początkowego pliku kluczy, który ma być używany.

Aby nadpisać początkowy plik kluczy, który ma być używany w czasie wykonywania lub w trybie konfiguracji, należy użyć opcji **-sf** . Na przykład, aby wygenerować konfigurację z określonym początkowym plikiem kluczy:

```
runmqsfb -o <output file> -sf <initial key file>
```

Aby użyć konkretnego początkowego pliku kluczy w czasie wykonywania:

```
runmqsfb -f <config file> -sf <initial key file>
```

Przed produktem IBM MQ 9.2do ochrony informacji autoryzacyjnych w plikach konfiguracyjnych Bridge to Salesforce był używany inny system ochrony informacji autoryzacyjnych.

Domyślnie program **runmqfsb** chroni referencje za pomocą nowego systemu, co oznacza, że pliki konfiguracyjne nie są kompatybilne ze starszymi wersjami programu Bridge to Salesforce.

Aby chronić pliki konfiguracyjne za pomocą starego systemu ochrony referencji, należy użyć opcji **-sp** *0* .

Ważne: Produkt IBM MQ Bridge to Salesforce jest nieaktualny we wszystkich wersjach od 22 listopada 2022 r. (patrz US Announcement letter 222-341).

IBM MQ clients , które używają sprzętu szyfrującego

V 9.3.0

Klienty IBM MQ można skonfigurować tak, aby używały sprzętu szyfrującego PKCS #11 do przechowywania kluczy prywatnych i certyfikatów używanych w komunikacji TLS. Aby uzyskać dostęp do urządzeń PKCS #11 , należy podać hasło jako część łańcucha konfiguracji, który jest dostarczany do IBM MQ client.

Ważne: Hasła podane za pomocą pola **CryptoHardware** w strukturze MQCSO lub atrybutu **SSLCRYP** menedżera kolejek nie mogą być chronione przy użyciu tego mechanizmu.

Hasło to można zabezpieczyć za pomocą komendy **runp11cred** , która znajduje się w folderze `bin` w katalogu instalacyjnym IBM MQ .

Komenda **runp11cred** pyta o hasło, które ma zostać zaszyfrowane, i zwraca zaszyfrowane hasło. Zaszyfrowane hasło musi zostać skopiowane do łańcucha konfiguracji sprzętu szyfrującego.

Na przykład, jeśli łańcuch konfiguracji sprzętu szyfrującego jest następujący:

```
GSK_PKCS11=/usr/lib/pkcs11/PKCS11_API.so;tokenlabel;Passw0rd;SYMMETRIC_CIPHER_ON
```

Gdy komenda **runp11cred** wyświetli zachętę do wprowadzenia hasła, wpisz `Passw0rd`. Komenda zwraca łańcuch podobny do następującego:

```
<P11>!2!0TyDxrRaS6JUsjON9zfK6S4wEHmSNF0/ZsOdCaTD2dc=!MdpCoxGnFqPtZ1dTLQ58kg==
```

Zastąp hasło w łańcuchu konfiguracji sprzętu szyfrującego łańcuchem zwróconym przez komendę **runp11cred** , aby podać następujący łańcuch, który zawiera zaszyfrowane hasło:

```
GSK_PKCS11=/usr/lib/pkcs11/PKCS11_API.so;tokenlabel;<P11>!2!0TyDxrRaS6JUsjON9zfK6S4wEHm SNF0/
ZsOdCaTD2dc=!MdpCoxGnFqPtZ1dTLQ58kg==;SYMMETRIC_CIPHER_ON
```

Zapisz łańcuch konfiguracji sprzętu szyfrującego, który zawiera zaszyfrowane hasło, w atrybucie **SSLCryptoHardware** w sekcji SSL pliku konfiguracyjnego klienta lub w zmiennej środowiskowej **MQSSLCRYP** .

Domyślnie komenda **runp11cred** szyfruje hasło przy użyciu domyślnego klucza początkowego. Aby zabezpieczyć hasło za pomocą własnego klucza początkowego, należy określić nazwę pliku, który zawiera klucz początkowy, używając jednego z następujących mechanizmów w kolejności priorytetów:

1. Parametr **-sf** komendy **runp11cred** .
2. Zmienna środowiskowa **MQS_SSLCRYP_KEYFILE** .

UWAGA: Nie należy używać domyślnego klucza początkowego do szyfrowania haseł, ponieważ nie chroni on haseł w sposób bezpieczny.

Jeśli początkowy plik kluczy jest określony podczas szyfrowania hasła, należy również podać nazwę pliku, który zawiera początkowy klucz, gdy uruchamiany jest program IBM MQ client . Podaj początkową nazwę pliku kluczy, używając jednego z następujących mechanizmów, w kolejności priorytetów:

1. Zmienna środowiskowa **MQS_SSLCRYP_KEYFILE** .
2. Atrybut **SSLCryptoHardwareKeyFile** w sekcji **SSL** pliku konfiguracyjnego klienta.

IBM MQ menedżer kolejek

Menedżer kolejek systemu IBM MQ przechowuje hasła wewnętrznie w różnych atrybutach, na przykład w polu **KEYRPWD** menedżera kolejek. Program IBM MQ automatycznie szyfruje hasło przed zapisaniem go w plikach na dysku.

Hasło magazynu kluczy może być chronione za pomocą systemu zabezpieczenia hasłem IBM MQ lub pliku ukrytych haseł. Więcej informacji na temat tych dwóch metod zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316.

Gdy menedżer kolejek szyfruje hasło, używany jest domyślny klucz początkowy, chyba że określono alternatywny klucz za pomocą atrybutu **INITKEY** w obiekcie menedżera kolejek. Przed podaniem haseł, które mają być szyfrowane, należy ustawić unikalny, silny klucz.

Ostrzeżenie: Zmodyfikowanie klucza początkowego po podaniu frazy hasła repozytorium kluczy nie powoduje, że hasło repozytorium kluczy jest szyfrowane przy użyciu nowego klucza początkowego. W związku z tym zmiana klucza początkowego bez ponownego dostarczenia frazy hasła repozytorium kluczy powoduje, że program IBM MQ nie może zdeszyfrować frazy hasła repozytorium kluczy i dlatego nie może uzyskać dostępu do repozytorium kluczy.

Więcej informacji na ten temat zawiera sekcja INITKEY.

Aplikacje klienckie IBM MQ C

V 9.3.0

Biblioteki klienta C IBM MQ wymagają haseł w celu uzyskania dostępu do pewnych zabezpieczonych zasobów, na przykład magazynu kluczy TLS dla aplikacji, które łączą się z menedżerem kolejek przy użyciu protokołu TLS.

Hasło magazynu kluczy może być chronione za pomocą systemu zabezpieczenia hasłem IBM MQ lub pliku ukrytych haseł. Więcej informacji na temat tych dwóch metod zawiera sekcja “Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows” na stronie 316.

Aby zabezpieczyć hasła za pomocą systemu IBM MQ , należy użyć komendy **runmqicred** . Komenda znajduje się w katalogu *MQ_INSTALLATION_PATH*/bin .

Komenda **runmqicred** pyta o hasło, które ma być zaszyfrowane, i zwraca zaszyfrowane hasło, którego można użyć zamiast hasła w postaci jawnej.

Na przykład, jeśli zostanie podane hasło magazynu kluczy TLS za pomocą zmiennej środowiskowej *MQKEYRPWD* , a hasłem magazynu kluczy TLS jest Passw0rd. Po uruchomieniu programu **runmqicred**po wyświetleniu zachęty wpisz Passw0rd . Komenda zwraca łańcuch podobny do następującego:

```
<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w==
```

Ustaw ten łańcuch jako wartość zmiennej środowiskowej *MQKEYRPWD* :

```
export MQKEYRPWD="<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w=="
set MQKEYRPWD="<MQI>!2!G4lRxBuiNfJ3uOeYTD3lG1hrL5NvVZLAlgZCX3Tn6d8=!pUDOErDfDi9+JFVa0usS7w=="
```

Domyślnie komenda **runmqicred** szyfruje hasło przy użyciu domyślnego klucza początkowego. Aby zabezpieczyć hasło za pomocą własnego klucza początkowego, należy użyć jednego z następujących mechanizmów, aby określić nazwę pliku, który zawiera klucz, w kolejności priorytetów:

1. Parametr **-sf** komendy **runmqicred** .
2. Zmienna środowiskowa **MQS_MQI_KEYFILE** .

UWAGA: Nie należy używać domyślnego klucza początkowego do szyfrowania haseł, ponieważ nie chroni on haseł w sposób bezpieczny.

Więcej informacji na ten temat zawiera “Podawanie hasła repozytorium kluczy dla IBM MQ MQI client w systemie AIX, Linux, and Windows” na stronie 323.

Rodzime konfiguracje wysokiej dostępności

V 9.3.2

Rodzimy ruch replikacji dziennika wysokiej dostępności między instancjami może być szyfrowany przy użyciu protokołu TLS. Certyfikaty używane do zabezpieczania ruchu replikacji dziennika są przechowywane w magazynie kluczy, który jest określony w sekcji **NativeHALocalInstance** pliku `qm.ini` .

Hasło magazynu kluczy może być chronione za pomocą systemu zabezpieczenia hasłem IBM MQ lub pliku ukrytych haseł. Więcej informacji na temat tych dwóch metod zawiera sekcja "Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows" na stronie 316.

Aby zabezpieczyć hasło do magazynu kluczy o rodzimej wysokiej dostępności za pomocą systemu zabezpieczenia hasłem IBM MQ , należy użyć komendy **runmqicred** .

Komenda **runmqicred** pyta o hasło, które ma być zaszyfrowane, i zwraca zaszyfrowane hasło, które powinno być użyte zamiast hasła w postaci jawnej. Ustaw wartość atrybutu **KeyRepositoryPassword** w sekcji **NativeHALocalInstance** pliku `qm.ini` na zaszyfrowane hasło zwracane przez komendę.

Domyślnie komenda **runmqicred** szyfruje hasło przy użyciu domyślnego klucza początkowego. Aby zabezpieczyć hasło za pomocą własnego klucza początkowego, należy użyć jednego z następujących mechanizmów, aby określić nazwę pliku, który zawiera klucz, w kolejności priorytetów:

1. Parametr **-sf** komendy **runmqicred** .
2. Zmienna środowiskowa *MQS_MQI_KEYFILE* .

UWAGA: Nie należy używać domyślnego klucza początkowego do szyfrowania haseł, ponieważ nie chroni on haseł w sposób bezpieczny.

Jeśli hasło magazynu kluczy jest szyfrowane przy użyciu własnego klucza początkowego, należy również podać ten sam początkowy plik kluczy za pomocą atrybutu **InitialKeyFile** w sekcji **NativeHALocalInstance** pliku `qm.ini` .

Więcej informacji na ten temat zawiera sekcja instancji NativeHALocalw pliku qm.ini.

Menedżer kolejek IBM MQ (sekcjaAuthToken w pliku `qm.ini`)

V 9.3.4 Linux AIX

Począwszy od programu IBM MQ 9.3.4, program IBM MQ MQI clients , który łączy się z menedżerami kolejek systemu IBM MQ uruchomionymi w systemach AIX lub Linux , może używać znaczników uwierzytelniania do uwierzytelniania w menedżerze kolejek. Menedżer kolejek musi być skonfigurowany tak, aby akceptował znaczniki uwierzytelniania i mógł uzyskać dostęp do certyfikatu klucza publicznego wystawcy znacznika lub klucza tajnego używanego do podpisywania znacznika. Magazyn kluczy, który zawiera certyfikaty klucza publicznego lub klucze tajne zaufanego wystawcy, jest zabezpieczony hasłem.

Hasło magazynu kluczy może być chronione za pomocą systemu zabezpieczenia hasłem IBM MQ lub pliku ukrytych haseł. Więcej informacji na temat tych dwóch metod zawiera sekcja "Szyfrowanie haseł repozytorium kluczy w systemie AIX, Linux, and Windows" na stronie 316.

Aby zabezpieczyć hasło magazynu kluczy tokenu uwierzytelniania za pomocą systemu zabezpieczenia hasłem IBM MQ , należy użyć komendy **runqmcred** w celu zaszyfrowania hasła.

Aby zaszyfrować hasło przy użyciu konkretnego klucza początkowego, należy użyć parametru **-sf** w celu określenia ścieżki do pliku, który zawiera klucz początkowy. Jeśli nie podasz klucza początkowego, zostanie użyty domyślny klucz początkowy.

UWAGA: Nie należy używać domyślnego klucza początkowego do szyfrowania haseł, ponieważ nie chroni on haseł w sposób bezpieczny.

Ważne: Jeśli zostanie podany początkowy plik kluczy, który zawiera klucz szyfrowania, ten sam klucz początkowy musi być określony w atrybucie **INITKEY** menedżera kolejek, aby menedżer kolejek mógł deszyfrować hasło. Jeśli atrybut **INITKEY** menedżera kolejek jest już ustawiony, należy użyć tego samego

klucza początkowego podczas uruchamiania komendy **runqmcred** . Więcej informacji na temat atrybutu **INITKEY** menedżera kolejek zawiera sekcja INITKEY.

Na przykład, aby zaszyfrować hasła magazynu kluczy tokenu uwierzytelniania za pomocą klucza początkowego w pliku /home/initial.key, należy wydać następującą komendę:

```
runqmcred -sf /home/initial.key
```

Po wyświetleniu zapytania wprowadź hasło, które ma być szyfrowane.

```
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
Enter password:
*************
<QM>!2!UnH/9hRXEGA0cenLVSGCW9a0s5A2vHDkTiA7vRv8ogc=!yhlsHFw7MIh48SvaYeTwRQ==
```

Zaszyfrowane hasło jest wyświetlane w ostatnim wierszu. Skopiuj zaszyfrowane hasło do pliku i dołącz ścieżkę do pliku w atrybucie **KeyStorePwdFile** w sekcji **AuthToken** pliku qm.ini .

Więcej informacji na ten temat zawiera “Konfigurowanie menedżera kolejek w celu akceptowania znaczników uwierzytelniania” na stronie 376.

Ograniczenia ochrony przez szyfrowanie haseł

IBM MQ obsługuje szyfrowanie AES-128 dla haseł przechowywanych w różnych plikach konfiguracyjnych. Jeśli do ochrony haseł w konfiguracji IBM MQ używane jest szyfrowanie AES (Advanced Encryption Standard), należy rozumieć ograniczenia zapewnianej przez nie ochrony.

Szyfrowanie hasła w plikach konfiguracyjnych IBM MQ nie oznacza, że hasło jest bezpieczne lub chronione. Zapobiega to tylko łatwemu odzyskiwaniu hasła przez osobę, która może uzyskać dostęp do zaszyfrowanego hasła, ale nie zna klucza szyfrowania. Procesy IBM MQ wymagają dostępu zarówno do zaszyfrowanego hasła, jak i do klucza deszyfrowania w celu uzyskania hasła w postaci jawnego tekstu. Oba te elementy danych muszą być zapisane w systemie plików w miejscu dostępnym dla systemu IBM MQ. Każdy, kto szyfruje hasło umieszczone w pliku konfiguracyjnym, wymaga również dostępu do klucza szyfrowania. Jeśli atakujący ma dostęp do tego samego zestawu plików co IBM MQ, zastosowanie szyfrowania AES do hasła zapewnia minimalny poziom ochrony.

Niemniej jednak szyfrowanie haseł w spoczynku jest ważne, ponieważ zapobiega przypadkowemu ujawnieniu haseł i umożliwia współużytkowanie plików konfiguracyjnych, jeśli klucz deszyfrowania nie jest również współużytkowany.

Oprócz zapewnienia, że plik zawierający klucz deszyfrujący nie jest współużytkowany, należy zadbać o to, aby plik był chroniony przed innymi użytkownikami w systemie. Chociaż pliki konfiguracyjne IBM MQ mogą być dostępne dla wszystkich użytkowników, należy ograniczyć uprawnienia do pliku, który zawiera klucz deszyfrujący, do niezbędnego minimum. ID użytkowników, dla których działają procesy IBM MQ , muszą mieć nadany dostęp do odczytu pliku zawierającego klucz deszyfrowania. Nie jest jednak konieczne nadawanie dostępu do odczytu pliku grupie lub wszystkim użytkownikom w systemie.

Ochrona szczegółów uwierzytelniania w bazie danych

Jeśli do nawiązywania połączenia z menedżerem bazy danych używane jest uwierzytelnianie za pomocą nazwy użytkownika i hasła, można je zapisać w składnicy referencji XA produktu MQ , aby uniknąć zapisywania hasła w postaci jawnego tekstu w pliku qm.ini .

Zaktualizuj łańcuch XAOpenString dla menedżera zasobów

Aby użyć składnicy referencji, należy zmodyfikować łańcuch XAOpenString w pliku qm.ini . Łańcuch jest używany do nawiązywania połączenia z menedżerem bazy danych. Należy podać zastępowalne pola, aby określić miejsce podstawienia nazwy użytkownika i hasła w łańcuchu XAOpenString .

- Pole +USER+ jest zastępowane wartością nazwy użytkownika zapisaną w magazynie XACrezalogowanego użytkownika.

- Pole +PASSWORD+ jest zastępowane wartością hasła przechowywaną w składnicy XACredentials.

W poniższych przykładach przedstawiono sposób modyfikowania pliku XAOpenString w celu użycia pliku referencji do nawiązania połączenia z bazą danych.

Nawiązywanie połączenia z bazą danych Db2

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
  XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t
  ThreadOfControl=THREAD
```

Nawiązywanie połączenia 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 bazy danych w składnicy referencji interfejsu XA produktu MQ

Po zaktualizowaniu pliku qm.ini przy użyciu zastępowanych łańcuchów referencji należy dodać nazwę użytkownika i hasło do składnicy referencji produktu MQ za pomocą komendy **setmqxacred** . Można również użyć programu **setmqxacred** do modyfikowania istniejących referencji, usuwania referencji lub wyświetlania referencji. W poniższych przykładach przedstawiono kilka typowych przypadków użycia:

Dodawanie referencji

Poniższa komenda bezpiecznie zapisuje nazwę użytkownika i hasło dla menedżera kolejek QM1 dla zasobu mqdb2.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

Aktualizowanie referencji

Aby zaktualizować nazwę użytkownika i hasło używane do nawiązywania połączenia z bazą danych, należy ponownie wydać 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 referencje:

```
setmqxacred -m QM1 -x mydb2 -d
```

Wyświetlanie informacji autoryzacyjnych

Następująca 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 testowania lub próbnego używania w środowisku chronionym. Jednak w środowisku produkcyjnym należy rozważyć odpowiednie kontrolowanie, kto może rozpocząć operacje przesyłania plików, kto może odczytywać i zapisywać przesyłane pliki oraz jak chronić integralność plików.

Zadania pokrewne

Ograniczanie uprawnień grupowych dla zasobów specyficznych dla systemu MFT

Zarządzanie uprawnieniami do zasobów specyficznych dla systemu MFT

“Używanie produktu Advanced Message Security z produktem Managed File Transfer” na stronie 695
W tym scenariuszu wyjaśniono, w jaki sposób skonfigurować produkt Advanced Message Security w taki sposób, aby zapewnił prywatność komunikatów dla danych wysyłanych za pośrednictwem Managed File Transfer.

Odsyłacze pokrewne

Uprawnienia MFT do dostępu do systemów plików

Właściwość commandPath MFT

Uprawnienia do publikowania dziennika agentów MFT i komunikatów o statusie

Szyfrowanie zapisanych referencji w produkcie MFT

Produkt Managed File Transfer (MFT) wymaga kilku identyfikatorów użytkowników i referencji, które są przechowywane w dwóch plikach XML. Można je zaciemnić za pomocą komendy **fteObfuscate** . W produkcie IBM MQ 9.2.0ta komenda zapewnia rozszerzoną ochronę zapisanych referencji.

Pliki referencji

MQMFTCredentials.xml
Ten plik zawiera identyfikator użytkownika i referencje na potrzeby nawiązywania połączenia z agentami oraz menedżerów kolejek koordynacji i komend. Referencje umożliwiające dostęp do magazynów kluczy na potrzeby bezpiecznych połączeń z menedżerami kolejek są również przechowywane w tym samym pliku.

Szczegółowe informacje na temat wartości właściwości definiujących położenie pliku `MQMFTCredentials.xml` zawiera sekcja “Uwierzytelnianie w systemach MFT i IBM MQ” na stronie 630 .

ProtocolBridgeCredentials.xml
Ten plik zawiera identyfikator użytkownika i referencje na potrzeby nawiązywania połączenia z serwerami protokołu.

Szyfrowanie referencji za pomocą komendy fteObfuscate

W pliku IBM MQ 9.2.0komenda **fteObfuscate** akceptuje następujące parametry:

- **-f** *nazwa_pliku_referencji* (wymagane)

  Uwaga: Deprecated Ten parametr zastępuje parametr **-credentialsFile** , który jest nieaktualny od wersji IBM MQ 9.2.0.
- **-sp** *tryb_ochrony*
- **-sf** *plik_kluczy_informacji_autoryzacyjnych*
- **-o** *nazwa_pliku_wyjściowego*

Szczegółowe informacje na temat parametrów zawiera sekcja **fteObfuscate** .

Jeśli nie zostanie określony tryb ochrony lub plik kluczy referencji, komenda użyje domyślnego trybu ochrony i najnowszego algorytmu, ale ze stałym kluczem do zaszyfrowania referencji.

Jeśli tryb ochrony zostanie określony jako `0i` nie zostanie podany plik kluczy referencji, komenda będzie działać tak jak w poprzednich wersjach produktu. Na konsoli wyświetlany jest komunikat ostrzegawczy informujący o użyciu nieaktualnej ochrony.

Jeśli tryb ochrony zostanie określony jako `0i` zostanie określony plik kluczy referencji, na konsoli zostaną wyświetlone dane wyjściowe błędu wskazujące, że nie można określić pliku kluczy podczas korzystania z trybu ochrony `0`.

Jeśli zostanie określony tryb ochrony 1i nie zostanie podany plik klucza referencji, komenda użyje najnowszego algorytmu, ale z kluczem stałym do zaszyfrowania referencji.

Jeśli zostanie określony tryb ochrony 1i plik kluczy referencji, komenda zaszyfruje referencje przy użyciu najnowszego algorytmu.

Jeśli zostanie określony tryb zabezpieczeń 1lub nie zostanie określony tryb zabezpieczeń i zostanie podany plik klucza referencji, który nie istnieje, na konsoli zostanie wyświetlony błąd wskazujący, że plik nie istnieje.

Jeśli zostanie podany tryb zabezpieczeń 1lub nie zostanie podany tryb zabezpieczeń i zostanie podany plik klucza referencji, który nie jest dostępny do odczytu, na konsoli zostanie wyświetlony błąd wskazujący, że plik nie jest dostępny do odczytu.

V 9.3.0 Jeśli zostanie określony tryb ochrony 2i nie zostanie podany plik kluczy referencji, komenda będzie używać trybu ochrony 2 do szyfrowania referencji przy użyciu najnowszego algorytmu i stałego klucza do szyfrowania.

V 9.3.0 Jeśli zostanie określony tryb ochrony 2i plik kluczy referencji, komenda użyje trybu ochrony 2 do zaszyfrowania referencji przy użyciu najnowszego algorytmu oraz klucza określonego przez użytkownika do zaszyfrowania.

V 9.3.0 Jeśli zostanie określony tryb zabezpieczeń 2lub nie zostanie określony tryb zabezpieczeń i zostanie podany plik klucza referencji, który nie istnieje, na konsoli zostanie wyświetlony błąd wskazujący, że plik nie istnieje.

V 9.3.0 Jeśli zostanie podany tryb zabezpieczeń 2lub nie zostanie podany tryb zabezpieczeń i zostanie podany plik klucza referencji, który nie jest dostępny do odczytu, na konsoli zostanie wyświetlony błąd wskazujący, że plik nie jest dostępny do odczytu.

Deszyfrowanie referencji

Ścieżkę do początkowego pliku kluczy można określić w różnych miejscach. Aby zdeszyfrować referencje, które zostały zaszyfrowane przy użyciu klucza początkowego innego niż domyślny, nazwa pliku zawierającego klucz początkowy musi zostać dostarczona do MFT w jeden z następujących sposobów (w tej kolejności):

1. Za pomocą właściwości systemowej Java , na przykład:

   ```
   -Dcom.ibm.wmqfte.cred.keyfile=/usr/hime/credkeyfile.key
   ```

   Uwaga:

   - V 9.3.1 Przed IBM MQ 9.3.1nazwa tej właściwości systemowej Java została błędnie zapisana w kodzie produktu jako `com.ibm.wqmfte.cred.keyfile`. W pliku IBM MQ 9.3.1pisownia nazwy właściwości jest poprawiana na `com.ibm.wmqfte.cred.keyfile`. Produkt Managed File Transfer używa obu wersji właściwości systemowej Java podczas sprawdzania, czy użytkownik określił plik zawierający klucz początkowy, który powinien być używany do szyfrowania i deszyfrowania referencji. Pozwala to na użycie poprawnej pisowni nazwy właściwości przy zachowaniu wstecznej zgodności ze starą nazwą z błędem pisowni. Należy zauważyć, że jeśli są ustawione obie właściwości systemowe Java , używana jest wartość poprawnie napisanej właściwości `com.ibm.wmqfte.cred.keyfile` .

- W przypadku wartości wcześniejszych niż IBM MQ 9.3.1należy użyć właściwości `com.ibm.wqmfte.cred.keyfile`.

.

2. Przez ustawienie właściwości w pliku właściwości agenta, komendy, koordynacji lub programu rejestrującego. Nazwa pliku właściwości i właściwość, którą należy w nim ustawić, są przedstawione w poniższej tabeli:

Plik właściwości	**Nazwa właściwości**
agent.properties	agentCredentialsKeyFile
command.properties	commandCredentialsKeyFile
coordination.properties	coordinationCredentialsKeyFile
logger.properties	loggerCredentialsKeyFile

3. W pliku installation.properties .

   Zamiast dodawać właściwości w pojedynczych plikach właściwości, można dodać właściwość **commonCredentialsKeyFile** do istniejącego wspólnego pliku `installation.properties` , aby agent, program rejestrujący i komendy mogły używać tej samej właściwości.

Jeśli zdefiniowano różne właściwości **CredentialsKeyFile** w wielu położeniach:

- Ścieżka pliku kluczy informacji autoryzacyjnych używanego dla agenta i programu rejestrującego jest rejestrowana w pliku `output0.log` dla tego agenta lub programu rejestrującego.
- Ścieżka do pliku kluczy referencji używanego dla komend jest wyświetlana na konsoli.

Java Właściwość systemowa **com.ibm.wmqfte.cred.keyfile** nadpisuje wszystkie pozostałe. Jeśli właściwość systemowa nie jest ustawiona, agent szuka początkowego pliku kluczy w pliku `agent.properties` , po którym następuje plik `installation.properties` .

Jeśli początkowy plik kluczy nadal nie zostanie znaleziony, a tryb ochrony został ustawiony w komendzie **fteObfuscate** na 1, agent zarejestruje komunikat o błędzie w pliku `output0.log` .

Jeśli tryb ochrony został ustawiony na wartość `0` w komendzie **fteObfuscate** , rejestrowany jest komunikat ostrzegawczy wskazujący, że jest on nieaktualny.

Program rejestrujący i komendy wykonają te same kroki w celu znalezienia początkowego pliku kluczy.

Most protokołu i most Connect:Direct

Most protokołu używa pliku właściwości `ProtocolBridgeProperties.xml`na potrzeby nawiązywania połączeń z serwerami FTP, SFTP i FTPS. Ten plik właściwości zawiera atrybuty połączenia wymagane do nawiązania połączenia z tymi serwerami.

Restart agenta mostu jest wymagany, jeśli wartość atrybutów **credentialsFile** lub **credentialsKeyFile** została zmodyfikowana w pliku `ProtocolBridgeProperties.xml` .

Jednym z atrybutów jest **credentialsFile**, a wartość zawiera ścieżkę do pliku XML zawierającego identyfikator UID, PWD lub klucz wymagany do nawiązania połączenia z tymi serwerami. Wartością domyślną tego atrybutu jest *ProtocolBridgeCredentials.xml* , a plik znajduje się w katalogu osobistym, podobnie jak plik `MQMFTCredentials.xml` .

```
<tns:credentialsFile path="$HOME/ProtocolBridgeCredentials.xml" />
```

Podobnie jak plik *MQMFTCredentails.xml*, można zaszyfrować plik *ProtocolBridgeCredentials.xml* za pomocą komendy **fteObfuscate** . W celu deszyfrowania można określić wymaganą ścieżkę do pliku kluczy referencji za pomocą dodatkowego elementu **credentialsKeyFile** , jak pokazano w poniższym tekście. Ścieżka może zawierać zmienne środowiskowe.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key"/>
```

Uwaga: Określenie wartości dla właściwości agenta **agentCredentialsKeyFile** , właściwości **commonCredentialsKeyFile** w pliku `installation.propertieslub` za pośrednictwem właściwości systemowej **com.ibm.wqmfte.cred.keyfile**nie ma wpływu na wartość określoną dla atrybutu **credentialsKeyFile** .

Podobnie program Connect:Direct Bridge używa pliku *ConnectDirectNodeProperties.xml* do nawiązania połączenia z serwerem Connect:Direct . Plik XML zawiera wymagane informacje o połączeniu wraz z atrybutem, który definiuje ścieżkę do pliku XML referencji. Ten plik XML referencji zawiera identyfikator UID lub PWD oraz dodatkowe informacje wymagane do nawiązania połączenia z serwerem Connect:Direct .

```
<tns:credentialsFile path="$HOME/ ConnectDirectCredentials.xml" />
```

Podobnie jak plik *ProtocolBridgeCredentials.xml* , można szyfrować plik *ConnectDirectCredentials.xml* za pomocą komendy **fteObfuscate** . W celu deszyfrowania można określić wymaganą ścieżkę do pliku kluczy referencji za pomocą dodatkowego elementu **credentialsKeyFile** , jak pokazano w poniższym tekście. Ścieżka może zawierać zmienne środowiskowe.

```
<tns:credentialsKeyFile path="$HOME/CredKey.key"/>
```

Uwaga: Określenie wartości dla właściwości agenta **agentCredentialsKeyFile** , właściwości **commonCredentialsKeyFile** w pliku `installation.propertieslub` za pośrednictwem właściwości systemowej **com.ibm.wqmfte.cred.keyfile** nie ma wpływu na wartość określoną dla atrybutu **credentialsKeyFile** .

Można określić element **credentialsKeyFile** bez określania elementu **credentialsFile** w pliku *ProtocolBridgeProperties.xml* .

Jeśli element **credentialsFile** nie zostanie określony, agent mostu protokołu użyje domyślnego pliku referencji *ProtocolBridgeCredentials.xml* , a wartość pliku kluczy określona w atrybucie **credentialsKeyFile** zostanie użyta do deszyfrowania pliku referencji.

Podobnie można określić element **credentialsKeyFile** bez określania elementu **credentialsFile** w pliku *ConnectDirectNodeProperties.xml* .

Jeśli element **credentialsFile** nie zostanie określony, domyślny plik referencji *ConnectDirectCredentials.xml* jest używany przez most Connect:Direct , a wartość pliku kluczy określona w atrybucie **credentialsKeyFile** jest używana do deszyfrowania pliku referencji.

Używanie klucza z zestawu danych w systemie z/OS

z/OS

W systemie z/OSmożna podać wartość **MQMFTCredentials** i podać plik kluczy referencji za pomocą zestawu PDSE. Patrz “Konfigurowanie produktu MQMFTCredentials.xml w systemie z/OS” na stronie 633.

Odsyłacze pokrewne

Która komenda MFT łączy się z którym menedżerem kolejek

Format pliku referencji zarządzanego przesyłania plików

fteObfuscate (szyfrowanie danych wrażliwych)

Uwierzytelnianie w systemach MFT i IBM MQ

Uwierzytelnianie połączenia umożliwia skonfigurowanie menedżera kolejek na potrzeby uwierzytelniania aplikacji przy użyciu podanego identyfikatora użytkownika i hasła. Jeśli powiązany menedżer kolejek ma włączone zabezpieczenia i wymaga szczegółów referencji (ID użytkownika i hasło), przed nawiązaniem pomyślnego połączenia z menedżerem kolejek należy włączyć opcję uwierzytelniania połączenia. Uwierzytelnianie połączenia można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Metody dostarczania szczegółów referencji

Wiele komend Managed File Transfer obsługuje następujące metody dostarczania szczegółów referencji:

Szczegóły podawane w argumentach wiersza komend.
Szczegóły informacji autoryzacyjnych można określić przy użyciu parametrów **-mquserid** i **-mqpassword** . Jeśli parametr **-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 referencji można wstępnie zdefiniować w pliku `MQMFTCredentials.xml` jako tekst jawny lub zaciemniony.

Informacje na temat konfigurowania pliku MQMFTCredentials.xml w systemie IBM MQ for Multiplatforms zawiera sekcja “Konfigurowanie pliku MQMFTCredentials.xml na platformie Multiplatforms” na stronie 631.

Informacje 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 633.

Pierwszeństwo

Kolejność określania szczegółów informacji autoryzacyjnych jest następująca:

1. Argument wiersza komend.
2. Indeks `MQMFTCredentials.xml` według powiązanego menedżera kolejek i użytkownika uruchamiającego komendę.
3. Indeks `MQMFTCredentials.xml` według powiązanego menedżera kolejek.
4. Domyślny tryb kompatybilności wstecznej, w którym nie podano szczegółów informacji autoryzacyjnych w celu zapewnienia zgodności 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 można podać tylko w pliku `MQMFTCredentials.xml` .
- z/OS

  W systemie z/OShasło musi być zapisane wielkimi literami, nawet jeśli hasło użytkownika zawiera małe litery. Jeśli na przykład hasło użytkownika to "password", należy je wprowadzić jako "PASSWORD".

Odsyłacze pokrewne
Która komenda MFT łączy się z którym menedżerem kolejek
Format pliku referencji zarządzanego przesyłania plików

Konfigurowanie pliku MQMFTCredentials.xml na platformie Multiplatforms

Jeśli w produkcie Managed File Transfer (MFT) włączono zabezpieczenia, 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 mogą być wymagane programy rejestrujące MFT do określenia identyfikatora użytkownika i hasła. Te informacje autoryzacyjne mogą być zapisane w pliku referencji MFT .

O tym zadaniu

Elementy w pliku `MQMFTCredentials.xml` muszą być zgodne ze schematem `MQMFTCredentials.xsd` . Informacje na temat formatu `MQMFTCredentials.xml`zawiera sekcja Format pliku referencji MFT.

Przykładowy plik referencji można znaleźć w katalogu `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Może istnieć jeden plik referencji MFT dla menedżera kolejek koordynacji, jeden dla menedżera kolejek komend, jeden dla każdego agenta i jeden dla każdego programu rejestrującego. Alternatywnie może istnieć jeden plik, który jest używany przez wszystkie elementy topologii.

Domyślne położenie pliku referencji MFT jest następujące:

AIX and Linux

$HOME

Windows

%USERPROFILE% lub %HOMEDRIVE%%HOMEPATH%

Jeśli plik referencji jest przechowywany w innym położeniu, można użyć następujących właściwości, aby określić miejsce, w którym komendy powinny go szukać:

Tabela 98. : 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 99. : 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.

Zamiast dodawać właściwości w pojedynczych plikach właściwości, można dodać właściwość **commonCredentialsKeyFile** do istniejącego wspólnego pliku `installation.properties` , aby agent, program rejestrujący i komendy mogły używać tej samej właściwości.

Ponieważ plik referencji zawiera informacje o identyfikatorze użytkownika i haśle, wymaga specjalnych uprawnień, aby uniemożliwić dostęp do niego bez uprawnień:

AIX 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, które uruchamiają agenta lub program rejestrujący, który będzie używał pliku referencji.

Szczegóły referencji używane do nawiązywania połączenia z menedżerem kolejek koordynacji MFT we wtyczce IBM MQ Explorer Managed File Transfer zależą od typu konfiguracji:

Globalne (konfiguracja na dysku lokalnym)

Konfiguracja globalna używa pliku referencji określonego we właściwościach koordynacji i komendy.

Lokalne (zdefiniowane w pliku IBM MQ Explorer):

Konfiguracja lokalna używa właściwości szczegółów połączenia powiązanego menedżera kolejek w programie IBM MQ Explorer.

Zadania pokrewne

“Włączanie uwierzytelniania połączenia dla produktu MFT” na stronie 635

Uwierzytelnianie połączenia wtyczki produktu IBM MQ Explorer MFT łączącej się z menedżerem kolejek koordynacji lub menedżerem kolejek komend oraz uwierzytelnianie połączenia dla agenta produktu Managed File Transfer łączącego się z menedżerem kolejek koordynacji lub menedżerem kolejek komend można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Tworzenie struktury przesyłania plików w systemie IBM MQ

Odsyłacze pokrewne

Format pliku referencji zarządzanego przesyłania plików

Szyfrowanie zapisanych referencji w produkcie MFT

fteObfuscate: szyfrowanie danych wrażliwych

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 100. : 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 101. : 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 pliku MQMFTCredentials.xml na platformie Multiplatforms” na stronie 631
Jeśli w produkcie Managed File Transfer (MFT) włączono zabezpieczenia, 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 mogą być wymagane programy rejestrujące MFT do określenia identyfikatora użytkownika i hasła. Te informacje autoryzacyjne mogą być zapisane w pliku referencji MFT .

Włączanie uwierzytelniania połączenia dla produktu MFT

Uwierzytelnianie połączenia wtyczki produktu IBM MQ Explorer MFT łączącej się z menedżerem kolejek koordynacji lub menedżerem kolejek komend oraz uwierzytelnianie połączenia dla agenta produktu 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

W systemach wcześniejszych niż IBM MQ 9.2.0tryb zgodności jest domyślnym ustawieniem uwierzytelniania połączenia. Można jednak wyłączyć domyślny tryb zgodności i włączyć tryb uwierzytelniania MQCSP.

W produkcie IBM MQ 9.2.0domyślnym trybem uwierzytelniania jest MQCSP.

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 podczas autoryzowania w trybie zgodności zostanie podane hasło dłuższe niż 12 znaków, wystąpi błąd i agent nie zostanie uwierzytelniony w menedżerze kolejek. Patrz 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 i z menu podręcznego wybierz opcję **Szczegóły połączenia-> Właściwości** .
  c) Kliknij kartę **ID użytkownika**.
  d) Upewnij się, że pole wyboru trybu uwierzytelniania połączenia, który ma być używany, jest zaznaczone:
     – W produkcie IBM MQ 9.1.0domyślnie pole wyboru **Tryb zgodności identyfikacji użytkownika** nie jest zaznaczone. Oznacza to, że jeśli pole wyboru **Włącz identyfikator użytkownika** jest zaznaczone, produkt IBM MQ Explorer użyje 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, upewnij się, że zaznaczone jest zarówno pole wyboru **Włącz identyfikację użytkownika** , jak i pole wyboru **Tryb zgodności identyfikacji użytkownika** .

  - Przed wersją IBM MQ 9.1.0domyślnie zaznaczone jest pole wyboru **Tryb zgodności identyfikacji użytkownika** . Oznacza to, że jeśli pole wyboru **Włącz identyfikator użytkownika** jest zaznaczone, program IBM MQ Explorer będzie używać trybu zgodności podczas nawiązywania połączenia z menedżerem kolejek. Jeśli produkt IBM MQ Explorer ma nawiązać połączenie z menedżerem kolejek przy użyciu uwierzytelniania MQCSP, upewnij 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:

  Prawda
  Tryb uwierzytelniania MQCSP jest używany do uwierzytelniania użytkownika w menedżerze kolejek.

  Od wersji IBM MQ 9.2.0wartością domyślną jest `true` . Jeśli parametr **useMQCSPAuthentication** nie jest określony, jest on domyślnie ustawiony na wartość `true` (prawda), a do uwierzytelniania użytkownika w menedżerze kolejek używany jest tryb uwierzytelniania MQCSP.

  Fałsz
  Tryb zgodności jest używany do uwierzytelniania użytkownika w menedżerze kolejek.

  W produkcie IBM MQ 9.2.0, jeśli parametr **useMQCSPAuthentication** nie jest określony, jest on domyślnie ustawiony na wartość `false` i 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

“Zabezpieczenie hasłem MQCSP” na stronie 32
Referencje uwierzytelniające, które są określone w strukturze MQCSP, mogą być chronione przy użyciu funkcji ochrony hasła MQCSP IBM MQ lub szyfrowane przy użyciu szyfrowania TLS.

Odsyłacze pokrewne

“Uwierzytelnianie w systemach MFT i IBM MQ” na stronie 630
Uwierzytelnianie połączenia umożliwia skonfigurowanie menedżera kolejek na potrzeby uwierzytelniania aplikacji przy użyciu podanego identyfikatora użytkownika i hasła. Jeśli powiązany menedżer kolejek ma włączone zabezpieczenia i wymaga szczegółów referencji (ID użytkownika i hasło), przed nawiązaniem pomyślnego połączenia z menedżerem kolejek należy włączyć opcję uwierzytelniania połączenia. Uwierzytelnianie połączenia można uruchomić w trybie zgodności lub w trybie uwierzytelniania MQCSP.

Format pliku referencji zarządzanego przesyłania plików

MFT przestrzenie prywatne

Można ograniczyć obszar systemu plików, do którego agent może uzyskać dostęp w ramach operacji przesyłania. Obszar, do którego agent jest ograniczony, jest nazywany przestrzenią prywatną. Ograniczenia można zastosować do agenta lub użytkownika, który żąda przesłania.

Środowiska testowe nie są obsługiwane, jeśli agent jest agentem mostu protokołu lub agentem mostu Connect:Direct . Nie można używać środowiska testowego agenta dla agentów, które mają być przesyłane do lub z kolejek systemu IBM MQ .

Odsyłacze pokrewne

“Praca z przestrzeniami prywatnymi agentów MFT” na stronie 637
Aby dodać dodatkowy poziom zabezpieczeń do programu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent ma dostęp.

“Praca z przestrzeniami prywatnymi użytkowników MFT” na stronie 638
Można ograniczyć obszar systemu plików, z którego pliki mogą być przesyłane do i z systemu plików, na podstawie nazwy użytkownika MQMD, który żąda przesłania.

Praca z przestrzeniami prywatnymi agentów MFT

Aby dodać dodatkowy poziom zabezpieczeń do programu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent ma dostęp.

Nie można używać środowiska testowego agenta dla agentów, które są przesyłane do lub z kolejek systemu IBM MQ . Ograniczanie dostępu do kolejek IBM MQ z użyciem przestrzeni prywatnej można zaimplementować zamiast tego, korzystając z przestrzeni prywatnych użytkownika, co jest zalecanym rozwiązaniem w przypadku wszystkich wymagań dotyczących przestrzeni prywatnej. Więcej informacji na temat środowiska testowego użytkownika zawiera sekcja “Praca z przestrzeniami prywatnymi użytkowników MFT” na stronie 638

Aby włączyć środowisko testowe agenta, dodaj następującą właściwość do pliku `agent.properties` dla agenta, którego chcesz ograniczyć:

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

gdzie:

- *`restricted_directory_name`* jest ścieżką do katalogu, która ma być dozwolona lub zabroniona.
- `!` jest opcjonalna i określa, że następująca wartość dla *`restricted_directory_name`* jest odrzucona (wykluczona). Jeśli parametr `!` nie jest określony, *`restricted_directory_name`* jest dozwoloną (dołączoną) ścieżką.
- *`separator`* jest separatorem specyficznym dla platformy.

Na przykład, aby ograniczyć dostęp agenta AGENT1 tylko do katalogu `/tmp` , ale nie zezwalać na dostęp do podkatalogu `private` , należy ustawić następującą właściwość w pliku `agent.properties` należącym do AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

Właściwość sandboxRoot jest opisana w sekcji Zaawansowane właściwości agenta.

Zarówno agent, jak i środowisko testowe użytkownika nie są obsługiwane w agentach mostu protokołu ani w agentach mostu Connect:Direct .

Praca w środowisku testowym na platformach AIX, Linux, and Windows

ALW Na platformach AIX, Linux, and Windows przestrzeń prywatna ogranicza katalogi, do których Managed File Transfer Agent może odczytywać i zapisywać dane. Po aktywowaniu środowiska testowego program Managed File Transfer Agent może odczytywać i zapisywać katalogi określone jako dozwolone, a także wszystkie podkatalogi, które zawierają określone katalogi, chyba że podkatalogi te zostały określone jako zabronione w katalogu sandboxRoot. Środowisko testowe Managed File Transfer nie ma pierwszeństwa przed bezpieczeństwem systemu operacyjnego. Użytkownik, który uruchomił program Managed File Transfer Agent , musi mieć dostęp na odpowiednim poziomie systemu operacyjnego do dowolnego katalogu, aby mieć możliwość odczytu z tego katalogu lub zapisu w tym katalogu. Dowiązanie symboliczne do katalogu nie jest stosowane, jeśli katalog, do którego tworzone jest dowiązanie, znajduje się poza określonymi katalogami sandboxRoot (i podkatalogami).

Praca w środowisku testowym w systemie z/OS

z/OS W systemie z/OSprzestrzeń prywatna ogranicza kwalifikatory nazw zestawów danych, które mogą być odczytywane i zapisywane przez Managed File Transfer Agent . Użytkownik, który uruchomił program Managed File Transfer Agent , musi mieć odpowiednie uprawnienia systemu operacyjnego do wszystkich zestawów danych. Jeśli wartość kwalifikatora nazwy zestawu danych sandboxRoot zostanie ujęta w cudzysłów, będzie ona zgodna z normalną konwencją języka z/OS i będzie traktowana jako pełna nazwa. Jeśli znaki cudzysłowu zostaną pominięte, katalog sandboxRoot będzie poprzedzony bieżącym identyfikatorem użytkownika. Na przykład, jeśli właściwość sandboxRoot zostanie ustawiona na następującą wartość: `sandboxRoot=//test`, agent może uzyskać 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 wartością sandboxRoot, żądanie przesłania zostanie odrzucone.

Praca w środowisku testowym w systemach IBM i

IBM i W przypadku plików w zintegrowanym systemie plików w systemach IBM i przestrzeń prywatna ogranicza katalogi, do których Managed File Transfer Agent może odczytywać i zapisywać dane. Po aktywowaniu środowiska testowego program Managed File Transfer Agent może odczytywać i zapisywać katalogi określone jako dozwolone, a także wszystkie podkatalogi, które zawierają określone katalogi, chyba że podkatalogi te zostały określone jako zabronione w katalogu sandboxRoot. Środowisko testowe Managed File Transfer nie ma pierwszeństwa przed bezpieczeństwem systemu operacyjnego. Użytkownik, który uruchomił program Managed File Transfer Agent , musi mieć dostęp na odpowiednim poziomie systemu operacyjnego do dowolnego katalogu, aby mieć możliwość odczytu z tego katalogu lub zapisu w tym katalogu. Dowiązanie symboliczne do katalogu nie jest stosowane, jeśli katalog, do którego tworzone jest dowiązanie, znajduje się poza określonymi katalogami sandboxRoot (i podkatalogami).

Odsyłacze pokrewne

“Dodatkowe sprawdzenia dla przesyłania znaków wieloznacznych” na stronie 641
Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia miejsc, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia dla przesyłania z użyciem znaków wieloznacznych dla tego agenta.

“Praca z przestrzeniami prywatnymi agentów MFT” na stronie 637
Aby dodać dodatkowy poziom zabezpieczeń do programu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent ma dostęp.

Plik MFT `agent.properties`

Praca z przestrzeniami prywatnymi użytkowników MFT

Można ograniczyć obszar systemu plików, z którego pliki mogą być przesyłane do i z systemu plików, na podstawie nazwy użytkownika MQMD, który żąda przesłania.

Środowiska testowe użytkownika nie są obsługiwane, jeśli agent jest agentem mostu protokołu lub agentem mostu Connect:Direct .

Aby włączyć tworzenie przestrzeni prywatnych użytkowników, dodaj następującą właściwość do pliku `agent.properties` dla agenta, którego chcesz ograniczyć:

```
userSandboxes=true
```

Jeśli ta właściwość jest obecna i ma wartość true, agent używa informacji w pliku *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/agents/`*agent_name*`/UserSandboxes.xml` do określenia, do których części systemu plików może uzyskać dostęp użytkownik żądający operacji przesyłania.

Kod XML `UserSandboxes.xml` składa się z elementu `<agent>` , który zawiera zero lub więcej elementów `<sandbox>` . Te elementy opisują, które reguły są stosowane do poszczególnych użytkowników. Atrybut `user` elementu `<sandbox>` jest wzorcem używanym w celu dopasowania do użytkownika MQMD żądania.

Plik UserSandboxes.xml jest okresowo przeładowywany przez agenta i wszystkie poprawne zmiany w pliku będą miały wpływ na zachowanie agenta. Domyślny odstęp czasu przeładowywania wynosi 30 sekund. Ten odstęp czasu można zmienić, określając właściwość agenta xmlConfigReloadInterval w pliku agent.properties .

Jeśli zostanie podany atrybut userPattern="regex" lub wartość, atrybut user jest interpretowany jako wyrażenie regularne Java . Więcej informacji na ten temat zawiera sekcja Wyrażenia regularne używane przez produkt MFT.

Jeśli nie zostanie podany atrybut userPattern="regex" lub wartość, atrybut user będzie interpretowany jako wzorzec z następującymi znakami wieloznacznymi:

- 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. Używane jest tylko pierwsze dopasowanie, wszystkie następujące potencjalne dopasowania w pliku są ignorowane. Jeśli żaden z elementów <sandbox> podanych w pliku nie jest zgodny z użytkownikiem MQMD powiązanym z komunikatem żądania przesyłania, operacja przesyłania nie może uzyskać dostępu do systemu plików. Po znalezieniu dopasowania między nazwą użytkownika MQMD i atrybutem user , dopasowanie identyfikuje zestaw reguł wewnątrz elementu <sandbox> , które są stosowane do przesyłania. Ten zestaw reguł służy do określania, które plikilub zestawy danych mogą być odczytywane lub zapisywane w ramach przesyłania.

Każdy zestaw reguł może określać element <read> , który identyfikuje, które pliki mogą być odczytywane, oraz element <write> , który identyfikuje, które pliki mogą być zapisywane. Jeśli elementy <read> lub <write> zostaną pominięte w zestawie reguł, zakłada się, że użytkownik powiązany z tym zestawem reguł nie może wykonywać żadnych odczytów ani zapisów.

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, które są używane do określenia, czy plik znajduje się w środowisku testowym i czy można go przesłać. Te wzorce należy określić przy użyciu elementów <include> i <exclude> . Atrybut name elementu <include> lub <exclude> określa wzorzec do dopasowania. Opcjonalny atrybut type określa, czy wartość nazwy jest wzorcem pliku czy kolejki. Jeśli atrybut type nie jest określony, agent traktuje 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>
```

Wzorce <include> i <exclude> name są używane przez agenta do określenia, czy pliki, zestawy danych, lub kolejki mogą być odczytywane lub zapisywane. Operacja jest dozwolona, jeśli kanoniczna ścieżka pliku, zestaw danych lub nazwa kolejki jest zgodna z co najmniej jednym z dołączonych wzorców i dokładnie zerem wykluczonych wzorców. Wzorce określone za pomocą atrybutu name elementów <include> i <exclude> używają separatorów ścieżek i konwencji odpowiednich dla platformy, na której działa agent. Jeśli zostaną podane względne ścieżki do plików, zostaną one rozstrzygnięte względem właściwości transferRoot agenta.

Podczas określania ograniczeń kolejki obsługiwana jest składnia QUEUE@QUEUEMANAGER z następującymi regułami:

- Jeśli w pozycji brakuje znaku @, wzorzec jest traktowany jako nazwa kolejki, do której można uzyskać dostęp w dowolnym menedżerze kolejek. Jeśli na przykład wzorzec ma postać name , jest on traktowany tak samo jak wzorzec name@**.
- Jeśli znak at (@) jest pierwszym znakiem w pozycji, wzorzec jest traktowany jako nazwa menedżera kolejek i można uzyskać dostęp do wszystkich kolejek w menedżerze kolejek. Jeśli na przykład wzorzec ma postać @name , jest on traktowany tak samo jak wzorzec **@name.

Następujące znaki wieloznaczne mają specjalne znaczenie, gdy są określane jako część atrybutu name elementów <include> i <exclude> :

*****
Pojedyncza gwiazdka oznacza zero lub więcej znaków w nazwie katalogu, kwalifikatorze nazwy zestawu danych lub nazwy kolejki .

?
Znak zapytania odpowiada dokładnie jednemu znakowi w nazwie katalogu, kwalifikatorowi nazwy zestawu danych lub nazwy kolejki .

******
Dwie gwiazdki zastępujące zero lub więcej nazw katalogów lub zero lub więcej kwalifikatorów w nazwie zestawu danych lub kolejki. Ponadto ścieżki, które kończą się separatorem ścieżki, mają niejawny znak "**" dodany na końcu ścieżki. Zatem wartość /home/user/ jest taka sama jak wartość /home/user/**.

Na przykład:

- /**/test/** jest zgodny z dowolnym plikiem, w którym ścieżce znajduje się katalog test
- /test/file? oznacza dowolny plik w katalogu /test , który rozpoczyna się od łańcucha file , po którym następuje dowolny pojedynczy znak
- c:\test*.txt oznacza dowolny plik w katalogu c:\test z rozszerzeniem .txt
- Wzorzec c:\test***.txt jest zgodny z dowolnym plikiem w katalogu 'c:\test lub z jednym z jego podkatalogów, który ma rozszerzenie .txt .
- z/OS Wzorzec //'TEST.*.DATA' jest zgodny z zestawem danych, który ma pierwszy kwalifikator TEST, drugi kwalifikator oraz trzeci kwalifikator DATA.
- *@QM1 jest zgodna z dowolną kolejką w menedżerze kolejek QM1 , która ma pojedynczy kwalifikator.
- Wzorzec TEST.*.QUEUE@QM1 jest zgodny z dowolną kolejką w menedżerze kolejek QM1 , która ma pierwszy kwalifikator TEST, ma dowolny drugi kwalifikator i trzeci kwalifikator QUEUE.
- **@QM1 zgodne z dowolną kolejką w menedżerze kolejek QM1.

Dowiązania symboliczne

Należy w pełni rozstrzygnąć wszystkie dowiązania symboliczne, które są używane w ścieżkach plików w pliku UserSandboxes.xml , przez określenie dowiązań stałych w elementach <include> i <exclude> . Jeśli na przykład istnieje dowiązanie symboliczne, w którym /var jest odwzorowane na /SYSTEM/var, należy określić tę ścieżkę jako <tns:include name="/SYSTEM/var"/>. W przeciwnym razie operacja przesyłania nie powiedzie się i zostanie zgłoszony błąd zabezpieczeń środowiska testowego użytkownika.

Przykład

W tym przykładzie przedstawiono sposób zezwolenia użytkownikowi o nazwie użytkownika MQMD guest na przesłanie dowolnego pliku z katalogu /home/user/public lub 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 przedstawiono sposób zezwolenia każdemu użytkownikowi o nazwie MQMD `account` , po której następuje pojedyncza cyfra, na przykład `account4`, na wykonanie następujących działań:

- Prześlij dowolny plik z katalogu `/home/account` lub 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 jego podkatalogów w systemie, w którym działa agent AGENT_SATURN
- Odczytywanie komunikatów z kolejek w lokalnym menedżerze kolejek, zaczynając od przedrostka `ACCOUNT.` , chyba że rozpoczyna się od łańcucha `ACCOUNT.PRIVATE.` (na drugim poziomie znajduje się łańcuch `PRIVATE`).
- Prześlij dane do kolejek zaczynających się od przedrostka `ACCOUNT.OUTPUT.` w dowolnym menedżerze kolejek.

Aby umożliwić użytkownikowi o nazwie MQMD `account` wykonanie tych działań, należy dodać następujący element <sandbox> do pliku `UserSandboxes.xml`w katalogu konfiguracyjnym agenta 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 dla przesyłania znaków wieloznacznych” na stronie 641
Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia miejsc, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia dla przesyłania z użyciem znaków wieloznacznych dla tego agenta.

Plik MFT `agent.properties`

Dodatkowe sprawdzenia dla przesyłania znaków wieloznacznych

Jeśli agent został skonfigurowany z użyciem środowiska testowego użytkownika lub agenta w celu ograniczenia miejsc, do których agent może przesyłać pliki, można określić, że mają być wykonywane dodatkowe sprawdzenia dla przesyłania z użyciem znaków wieloznacznych dla tego agenta.

Właściwość additionalWildcardSandboxChecking

Aby włączyć dodatkowe sprawdzanie dla przesyłania z użyciem znaków wieloznacznych, dodaj następującą właściwość do pliku `agent.properties` dla agenta, który ma być sprawdzany.

```
additionalWildcardSandboxChecking=true
```

Jeśli ta właściwość ma wartość true, a agent wysyła żądanie przesłania, które próbuje odczytać położenie spoza zdefiniowanego środowiska testowego w celu dopasowania pliku do znaku wieloznacznego, operacja przesyłania kończy się niepowodzeniem. Jeśli w jednym żądaniu przesyłania występuje wiele operacji przesyłania, a jedno z tych żądań nie powiedzie się z powodu próby odczytania położenia poza środowiskiem testowym, cała operacja przesyłania nie powiedzie się. Jeśli sprawdzanie nie powiedzie się, przyczyna niepowodzenia jest podana w komunikacie o błędzie.

Jeśli właściwość additionalWildcardSandboxChecking zostanie pominięta w pliku `agent.properties` agenta lub zostanie ustawiona na wartość false (fałsz), dla tego agenta nie będą wykonywane żadne dodatkowe sprawdzenia dotyczące przesyłania z użyciem znaków wieloznacznych.

Komunikaty o błędach dotyczące sprawdzania znaków wieloznacznych

Komunikaty, które są zgłaszane po przesłaniu żądania przesłania znaku wieloznacznego do położenia poza skonfigurowanym położeniem środowiska testowego, są następujące.

Następujący komunikat pojawia się, gdy ścieżka do pliku zastępczego w żądaniu przesyłania znajduje się poza ograniczonym środowiskiem testowym:

```
BFGSS0077E: Próba odczytania ścieżki do pliku ścieżka została odrzucona.
Ścieżka do pliku znajduje się poza ograniczonym środowiskiem testowym
przesyłania.
```

Następujący komunikat pojawia się, gdy przesyłanie w ramach wielu żądań przesyłania zawiera żądanie przesyłania ze znakiem wieloznacznym, w którym ścieżka znajduje się poza ograniczonym środowiskiem testowym:

```
BFGSS0078E: Próba odczytania ścieżki do pliku ścieżka została zignorowana jako kolejna operacja
przesyłania.
Element w zarządzanym przesyłaniu podjął próbę odczytu poza ograniczonym środowiskiem testowym
przesyłania.
```

Następujący komunikat pojawia się, gdy plik znajduje się poza ograniczonym środowiskiem testowym:

```
BFGSS0079E: Próba odczytania pliku ścieżka została odrzucona.
Plik znajduje się poza wyznaczonym środowiskiem
testowym przesyłania.
```

Następujący komunikat pojawia się w wielu żądaniach przesyłania, w których inne żądanie przesyłania z użyciem znaku wieloznacznego spowodowało zignorowanie tego żądania:

```
BFGSS0080E: Próba odczytania pliku ścieżka została zignorowana podczas innego przesyłania.
Element w zarządzanym przesyłaniu podjął próbę odczytu poza ograniczonym środowiskiem testowym
przesyłania.
```

W przypadku pojedynczych operacji przesyłania plików, które nie zawierają znaków wieloznacznych, komunikat zgłaszany, gdy operacja przesyłania obejmuje plik, który znajduje się poza środowiskiem testowym, pozostaje niezmieniony w stosunku do wcześniejszych wersji:

```
Niepowodzenie z błędem BFGIO0056E: Odmowa próby odczytu pliku "PLIK".
Plik znajduje się poza wyznaczonym środowiskiem
testowym przesyłania.
```

Odsyłacze pokrewne

“Praca z przestrzeniami prywatnymi użytkowników MFT” na stronie 638
Można ograniczyć obszar systemu plików, z którego pliki mogą być przesyłane do i z systemu plików, na podstawie nazwy użytkownika MQMD, który żąda przesłania.

“Praca z przestrzeniami prywatnymi agentów MFT” na stronie 637
Aby dodać dodatkowy poziom zabezpieczeń do programu Managed File Transfer, można ograniczyć obszar systemu plików, do którego agent ma dostęp.

Plik MFT `agent.properties`

Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT

Do zabezpieczenia komunikacji między agentami i ich menedżerami kolejek agentów, komendami i menedżerami kolejek, z którymi nawiązywane jest połączenie, oraz między różnymi menedżerami kolejek w topologii można użyć protokołu SSL lub TLS w połączeniu z produktem IBM MQ Managed File Transfer .

Zanim rozpoczniesz

Do szyfrowania komunikatów przepływających przez topologię produktu IBM MQ Managed File Transfer można użyć szyfrowania SSL lub TLS. takie jak:

- Komunikaty przekazywane między agentem i jego menedżerem kolejek agenta.
- Komunikaty dla komend i menedżerów kolejek, z którymi nawiązywane jest połączenie.
- Wewnętrzne komunikaty, które przepływają 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 293. W terminologii IBM MQ Managed File Transfer jest standardową aplikacją kliencką systemu Java .

Aby używać protokołu SSL z produktem Managed File Transfer, wykonaj następujące kroki:

Procedura

1. Utwórz plik zaufanych certyfikatów i opcjonalnie plik kluczy (te pliki mogą być tym samym plikiem). Jeśli uwierzytelnianie klienta (czyli SSLCAUTH=OPTIONAL w kanałach) nie jest potrzebne, nie trzeba udostępniać magazynu kluczy. Do uwierzytelnienia certyfikatu menedżera kolejek wymagany jest tylko magazyn zaufanych certyfikatów.

   Algorytm klucza używany do tworzenia certyfikatów dla magazynu zaufanych certyfikatów i magazynów kluczy musi być algorytmem RSA, aby pracować z produktem IBM MQ.
2. Skonfiguruj menedżer kolejek systemu IBM MQ do korzystania z protokołu SSL.

   Informacje na temat konfigurowania menedżera kolejek do korzystania z protokołu SSL na przykład za pomocą programu IBM MQ Explorer zawiera sekcja Konfigurowanie protokołu SSL w menedżerach kolejek.
3. Zapisz plik zaufanych certyfikatów i plik kluczy (jeśli istnieją) w odpowiednim miejscu. Sugerowane położenie to katalog *config_directory*/*coordination_qmgr*/agents/*agent_name* .
4. Ustaw właściwości SSL zgodnie z wymaganiami dla każdego menedżera kolejek z włączonym SSL w odpowiednim pliku właściwości Managed File Transfer . Każdy zestaw właściwości odwołuje się do osobnego menedżera kolejek (agenta, koordynacji i komendy), chociaż jeden menedżer kolejek może pełnić dwie lub więcej z tych ról.

   Wymagana jest jedna z właściwości **CipherSpec** lub **CipherSuite** . W przeciwnym razie klient podejmie próbę nawiązania połączenia bez użycia protokołu SSL. Obie właściwości **CipherSpec** lub **CipherSuite** są udostępniane z powodu różnic terminologicznych między produktami IBM MQ i Java. Produkt Managed File Transfer akceptuje dowolną z tych właściwości i wykonuje niezbędną konwersję, dlatego nie trzeba ustawiać obu tych właściwości. Jeśli zostaną podane obie właściwości (**CipherSpec** lub **CipherSuite**), pierwszeństwo ma właściwość **CipherSpec** .

   Właściwość **PeerName** jest opcjonalna. Właściwość można ustawić na nazwę wyróżniającą menedżera kolejek, z którym ma zostać nawiązane połączenie. Produkt Managed File Transfer odrzuca połączenia z niepoprawnym serwerem SSL o niezgodnej nazwie wyróżniającej.

   Ustaw właściwości **SslTrustStore** i **SslKeyStore** na nazwy plików, które wskazują na pliki magazynu zaufanych certyfikatów i magazynu kluczy. Jeśli te właściwości są ustawione dla agenta, który jest już uruchomiony, zatrzymaj i zrestartuj agenta, aby ponownie nawiązać połączenie w trybie SSL.

   Pliki właściwości zawierają hasła w postaci jawnego tekstu, dlatego należy rozważyć ustawienie odpowiednich uprawnień w systemie plików.

   Więcej informacji na temat właściwości SSL zawiera sekcja “Właściwości SSL/TLS dla MFT” na stronie 644.

5. Jeśli menedżer kolejek agenta używa protokołu SSL, nie można podać niezbędnych szczegółów podczas tworzenia agenta. Wykonaj następujące czynności, aby utworzyć agenta:
   a) Utwórz agenta za pomocą komendy **fteCreateAgent** . Zostanie wyświetlone ostrzeżenie o tym, że nie można opublikować istnienia agenta w menedżerze kolejek koordynacji.
   b) Zmodyfikuj plik `agent.properties` , który został utworzony w poprzednim kroku, dodając informacje o protokole SSL. Po pomyślnym uruchomieniu agenta zostanie podjęta ponowna próba publikowania.
6. Jeśli agenty lub instancje programu IBM MQ Explorer są uruchomione podczas zmiany właściwości SSL w pliku `agent.properties` lub pliku `coordination.properties` , należy zrestartować agenta lub IBM MQ Explorer.

Odsyłacze pokrewne
Plik MFT `agent.properties`

Właściwości SSL/TLS dla MFT

Niektóre pliki właściwości MFT zawierają właściwości SSL i TLS. Za pomocą protokołu SSL lub TLS z produktami IBM MQ i Managed File Transfer można zapobiegać nieautoryzowanym połączeniom między agentami i menedżerami kolejek oraz szyfrować ruch komunikatów między agentami i menedżerami kolejek.

Następujące pliki właściwości MFT zawierają właściwości SSL:

- Właściwości SSL/TLS dla pliku MFT `agent.properties`
- Właściwości SSL/TLS dla pliku MFT `coordination.properties`
- Właściwości SSL/TLS dla pliku MFT `command.properties`
- Właściwości SSL/TLS dla pliku MFT `logger.properties`

Informacje na temat używania protokołu SSL lub TLS z produktem Managed File Transferzawiera sekcja “Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT” na stronie 642.

W produkcie IBM WebSphere MQ 7.5można używać zmiennych środowiskowych w niektórych właściwościach produktu Managed File Transfer , które reprezentują położenia plików lub katalogów. Dzięki temu położenia plików lub katalogów używanych podczas uruchamiania części produktu mogą być różne w zależności od zmian w środowisku, na przykład od tego, który użytkownik uruchamia proces. Więcej informacji na ten temat zawiera sekcja Używanie zmiennych środowiskowych we właściwościach produktu MFT.

Pojęcia pokrewne
Opcje konfiguracyjne produktu MFT w wersji wieloplatformowej
Odsyłacze pokrewne
Użycie zmiennych środowiskowych we właściwościach MFT

Nawiązywanie połączenia z menedżerem kolejek w trybie klienta z uwierzytelnianiem kanału

Produkt IBM MQ używa rekordów uwierzytelniania kanału do precyzyjniejszego sterowania dostępem na poziomie kanału. Oznacza to, że domyślnie nowo utworzone menedżery kolejek odrzucają połączenia klientów z komponentu Managed File Transfer .

Więcej informacji na temat uwierzytelniania kanału zawiera sekcja “Rekordy uwierzytelniania kanału” na stronie 53.

Jeśli konfiguracja uwierzytelniania kanału dla SVRCONN używanego przez produkt Managed File Transfer określa nieuprzywilejowany identyfikator MCAUSER bez uprawnień, należy nadać rekordy uprawnień szczegółowych dla menedżera kolejek, kolejek i tematów, aby umożliwić poprawne działanie komendy Managed File Transfer Agent i komend. Użyj komendy MQSC SET CHLAUTH lub komendy PCF Set Channel Authentication Record (Ustaw rekord uwierzytelniania kanału), aby utworzyć, zmodyfikować lub usunąć rekordy uwierzytelniania kanału. Dla wszystkich agentów systemu Managed File Transfer , które mają być

połączone z menedżerem kolejek systemu IBM MQ , można skonfigurować identyfikator MCAUSER, który będzie 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 agenta, czyli nazw kolejek kończących się na *nazwa_agenta* na poniższej liście, należy utworzyć te rekordy uprawnień kolejki dla każdego agenta, który ma zostać połączony z menedżerem kolejek produktu IBM MQ za pomocą połączenia klienta.
  - 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 (systemSYSTEM.FTE.STATE.*nazwa_agenta*)
  - put, get, browse (systemSYSTEM.FTE.EVENT.*nazwa_agenta*)
  - put, get (SYSTEM.FTE).
- Rekordy uprawnień wymagane dla tematów:
  - sub, pub (SYSTEM.FTE).
- Rekordy uprawnień wymagane do przesyłania plików.

  Jeśli dla agenta źródłowego i docelowego istnieją osobne identyfikatory MCAUSER, należy utworzyć rekordy uprawnień w kolejkach agentów zarówno w miejscu źródłowym, jak i w miejscu docelowym.

  Na przykład, jeśli identyfikator MCAUSER agenta źródłowego to **user1** , a identyfikator MCAUSER agenta docelowego to **user2**, ustaw następujące uprawnienia dla użytkowników agenta:

Użytkownik AGENT	**Kolejka**	**Wymagane uprawnienia**
user1	SYSTEM SYSTEM.FTE.DATA.*nazwa_agenta_docelowego*	put
user1	SYSTEM SYSTEM.FTE.COMMAND.*nazwa_agenta_docelowego*	put
user2	SYSTEM SYSTEM.FTE.REPLY.*nazwa_agenta_źródłowego*	put
user2	SYSTEM SYSTEM.FTE.COMMAND.*nazwa_źródłowego_agenta*	put

Konfigurowanie protokołu SSL lub TLS między agentem mostu Connect:Direct i węzłem Connect:Direct

Skonfiguruj agent mostu Connect:Direct i węzeł Connect:Direct , aby łączyły się ze sobą za pośrednictwem protokołu SSL, tworząc magazyn kluczy i magazyn zaufanych certyfikatów oraz 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 jest używany ośrodek certyfikacji, można wygenerować certyfikat samopodpisany. Więcej informacji na temat generowania certyfikatu samopodpisanego zawiera sekcja “Praca z protokołem SSL/TLS w systemie AIX, Linux, and Windows” na stronie 312.

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, których używa do bezpiecznego nawiązywania połączeń z menedżerami kolejek systemu IBM MQ , można użyć istniejącego magazynu kluczy i magazynu zaufanych certyfikatów podczas bezpiecznego nawiązywania połączeń z węzłem Connect:Direct . Aby uzyskać więcej informacji, zapoznaj się z sekcją: "Konfigurowanie szyfrowania SSL lub TLS dla produktu MFT" na stronie 642.

Procedura

Dla 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 z produktem IBM MQ. Więcej informacji na ten tematzawiera sekcja "Praca z protokołem SSL/TLS" na stronie 293.
2. Wyślij żądanie do ośrodka certyfikacji w celu podpisania klucza. Otrzymasz certyfikat w zamian.
3. Utwórz plik tekstowy, na przykład `/test/ssl/certs/CAcert`, który zawiera klucz publiczny ośrodka certyfikacji.
4. Zainstaluj opcję Secure + Option na węźle Connect:Direct .

   Jeśli węzeł już istnieje, można zainstalować opcję Secure + Option, uruchamiając ponownie instalator, określając położenie istniejącej instalacji i wybierając instalację tylko opcji Secure + Option.
5. Utwórz nowy plik tekstowy, na przykład `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt`.
6. Skopiuj certyfikat otrzymany od ośrodka certyfikacji i klucz prywatny, który znajduje się w katalogu `/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 Secure + Admin Tool.
   - W systemach AIX and Linux uruchom komendę **spadmin.sh**.

- W systemach Windows kliknij opcję **Start** > **Programy** > **Sterling Commerce Connect:Direct** > **CD Secure + Admin Tool** .

Zostanie uruchomione narzędzie CD Secure + Admin Tool.

8. W narzędziu CD Secure + Admin Tool kliknij dwukrotnie plik **.Lokalna linia** do edycji głównych ustawień SSL lub TLS.
   a) W zależności od używanego protokołu wybierz opcję **Włącz protokół SSL** lub **Włącz protokół TLS**.
   b) Wybierz opcję **Wyłącz nadpisanie**.
   c) Wybierz co najmniej jeden zestaw algorytmów szyfrowania.
   d) Jeśli wymagane jest uwierzytelnianie dwukierunkowe, zmień wartość opcji **Włącz uwierzytelnianie klienta** na `Yes`.
   e) W polu **Zaufany certyfikat główny** wpisz ścieżkę do pliku certyfikatu publicznego ośrodka certyfikacji `/test/ssl/certs/CAcert`.
   f) W polu **Key Certificate File** (Plik certyfikatu klucza) wpisz ścieżkę do utworzonego pliku `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt`.
9. Kliknij dwukrotnie plik **.Wiersz** klienta do edycji głównych ustawień protokołu SSL lub TLS.
   a) W zależności od używanego protokołu wybierz opcję **Włącz protokół SSL** lub **Włącz protokół TLS**.
   b) Wybierz opcję **Wyłącz nadpisanie**.

Dla agenta mostu Connect:Direct wykonaj następujące kroki:

10. Utwórz magazyn zaufanych certyfikatów. Można to zrobić, tworząc klucz fikcyjny, a następnie usuwając ten klucz.

    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. Zmodyfikuj 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 używanym protokołem (SSL lub TLS), a *hasło* jest hasłem podanym podczas tworzenia magazynu zaufanych certyfikatów.

13. Jeśli wymagane jest uwierzytelnianie 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) Zmodyfikuj plik właściwości agenta mostu Connect:Direct .

Uwzględnij następujące wiersze w dowolnym miejscu pliku:

```
cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
cdNodeKeystorePassword=password
```

W przykładzie w tym kroku *hasło* jest hasłem podanym podczas tworzenia magazynu kluczy.

Zadania pokrewne

Konfigurowanie mostu Connect:Direct

ALW Zabezpieczanie klientów AMQP

Do zabezpieczania połączeń z klientami AMQP i zapewnienia odpowiedniej ochrony danych w sieci używany jest szereg mechanizmów zabezpieczeń. Zabezpieczenia można wbudować w aplikacje MQ Light . Można również używać istniejących opcji zabezpieczających produktu IBM MQ z klientami AMQP w taki sam sposób, w jaki są one używane dla innych aplikacji.

Reguły uwierzytelniania kanału (CHLAUTH)

Za pomocą reguł uwierzytelniania kanału można ograniczyć połączenia TCP do menedżera kolejek. Kanały AMQP obsługują użycie reguł uwierzytelniania kanału skonfigurowanych dla menedżera kolejek. Jeśli reguły uwierzytelniania kanału są zdefiniowane z profilem, który jest zgodny z dowolnym kanałem 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 zakończyć co najmniej niektóre czynności konfiguracyjne.

Więcej informacji na temat konfigurowania reguł uwierzytelniania kanału w celu umożliwienia połączeń AMQP z menedżerem kolejek zawiera sekcja Tworzenie i używanie kanałów AMQP.

Uwierzytelnianie połączenia (CONNAUTH)

Za pomocą uwierzytelniania połączenia można uwierzytelniać połączenia z menedżerem kolejek. Kanały AMQP obsługują użycie uwierzytelniania połączenia w celu kontrolowania dostępu do menedżera kolejek z aplikacji AMQP.

Protokół AMQP używa środowiska SASL (Simple Authentication and Security Layer) do określenia sposobu uwierzytelniania połączenia. Istnieją różne mechanizmy SASL i program IBM MQ obsługuje dwa mechanizmy SASL: ANONYMOUS i PLAIN.

W przypadku wartości ANONYMOUS referencje nie są przekazywane z klienta do menedżera kolejek w celu uwierzytelnienia. Jeśli obiekt AUTHINFO produktu MQ określony w atrybucie CONNAUTH ma wartość CHCKCLNT równą REQUIRED lub REQDADM (jeśli połączenie jest nawiązywane jako użytkownik administracyjny), połączenie jest odrzucane. Jeśli wartością parametru CHCKCLNT jest NONE lub OPTIONAL, połączenie jest akceptowane.

W przypadku PLAIN nazwa użytkownika i hasło są przekazywane z klienta do menedżera kolejek w celu uwierzytelnienia. Jeśli obiekt AUTHINFO produktu MQ określony w atrybucie CONNAUTH ma wartość CHCKCLNT równą NONE, połączenie jest odrzucane. Jeśli wartością parametru CHCKCLNT jest OPTIONAL, REQUIRED lub REQDADM (w przypadku nawiązywania połączenia jako użytkownik administracyjny), nazwa użytkownika i hasło są sprawdzane przez menedżer kolejek. Menedżer kolejek sprawdza system operacyjny (jeśli obiekt AUTHINFO jest typu IDPWOS) lub repozytorium LDAP (jeśli obiekt AUTHINFO jest typu IDPWLDAP).

Poniższa tabela zawiera podsumowanie tego zachowania uwierzytelniania:

Tabela 102. Podsumowanie mechanizmów SASL i uwierzytelniania połączenia

Mechanizm SASL	**Czy referencje zostały przekazane z klienta do menedżera kolejek?**	**CHKCLNT, wartość**
Anonimowe	Nie	REQUIRED lub REQDADM-odmowa połączenia NONE lub OPTIONAL-połączenie zaakceptowane
PLAIN	Tak, nazwa użytkownika i hasło	REQUIRED, REQDADM lub OPTIONAL-nazwa użytkownika i hasło sprawdzane przez menedżer kolejek BRAK-odmowa połączenia

Jeśli używany jest klient MQ Light , można podać referencje, dołączając je do adresu AMQP, z którym jest nawiązywane połączenie, na przykład:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

Ustawienie MCAUSER w kanale

Kanały AMQP mają atrybut MCAUSER, którego można użyć do ustawienia identyfikatora użytkownika produktu IBM MQ , dla którego autoryzowane są wszystkie połączenia z tym kanałem. Wszystkie połączenia klientów AMQP z tym kanałem przyjmują skonfigurowany identyfikator MCAUSER. Ten ID użytkownika jest używany do autoryzacji przesyłania komunikatów w różnych tematach.

Zalecane jest użycie uwierzytelniania kanału (CHLAUTH) w celu zabezpieczenia połączeń z menedżerami kolejek. Jeśli używane jest uwierzytelnianie kanału, zaleca się skonfigurowanie wartości MCAUSER dla użytkownika nieuprzywilejowanego. Dzięki temu, jeśli połączenie z kanałem nie jest zgodne z regułą CHLAUTH, połączenie nie jest autoryzowane do przesyłania komunikatów w menedżerze kolejek.

Uwaga: Windows W systemie Windows, przed IBM MQ 9.2, ustawienie identyfikatora użytkownika MCAUSER jest obsługiwane tylko dla identyfikatorów użytkowników o długości do 12 znaków. Od wersji IBM MQ 9.2Long Term Support ten limit 12 znaków został usunięty.

Obsługa 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 produktu MQ . Można określić specyfikację szyfru oraz określić, czy menedżer kolejek wymaga certyfikatów z połączeń klienckich AMQP.

Za pomocą atrybutów FIPS menedżera kolejek można sterować zestawami algorytmów szyfrowania SSL/TLS, których można używać do zabezpieczania połączeń z klientami AMQP.

Informacje na temat konfigurowania repozytorium kluczy dla menedżera kolejek zawiera sekcja "Praca z protokołem SSL/TLS w systemie AIX, Linux, and Windows" na stronie 312.

Informacje na temat konfigurowania obsługi protokołu SSL/TLS dla połączenia klienta AMQP zawiera sekcja Tworzenie i używanie kanałów AMQP.

Usługa Java Authentication and Authorization Service (JAAS)

Opcjonalnie można skonfigurować kanały AMQP z modułem logowania JAAS , który może sprawdzić nazwę użytkownika i hasło udostępnione przez klient AMQP. Patrz sekcja "Konfigurowanie usługi JAAS dla kanałów AMQP" na stronie 651.

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie i używanie kanałów AMQP

ALW Ograniczanie przejęcia klienta AMQP

Po nawiązaniu połączenia klienta AMQP, które ma ten sam identyfikator klienta, co istniejące połączenie klienta AMQP, istniejące połączenie klienta jest domyślnie rozłączane. Można jednak skonfigurować menedżer kolejek w taki sposób, aby ograniczyć zachowanie klienta podczas przejmowania, tak aby przejęcie było możliwe tylko wtedy, gdy spełnione są określone kryteria.

Na przykład rozłączenie istniejącego połączenia klienta może nie być odpowiednie, jeśli istnieją aplikacje AMQP tworzone przez różne zespoły i używają one tego samego identyfikatora klienta. Aby rozwiązać ten problem, można ograniczyć przejęcie klienta na podstawie nazwy używanego kanału AMQP, adresu IP klienta i identyfikatora użytkownika klienta (jeśli włączone jest uwierzytelnianie SASL).

Użyj ustawień atrybutów menedżera kolejek **AdoptNewMCA** i **AdoptNewMCACheck** , aby określić wymagany poziom ograniczenia przejęcia klienta, zgodnie z opisem w poniższej tabeli:

*Tabela 103. Ustawienia **AdoptNewMCA** i **AdoptNewMCACheck** ograniczające przejęcie klienta*

AdoptNewMCA	**AdoptNewMCACheck**	**Kryteria sprawdzane przed zezwoleniem na przejęcie klienta**
NO lub niezdefiniowany	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 niezdefiniowany	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 (przy włączonej opcji SASL) Nazwa kanału
ALL (lub wartość inna niż NO)	ADDRESS	ID użytkownika (przy włączonej opcji SASL) Adres IP

*Tabela 103. Ustawienia **AdoptNewMCA** i **AdoptNewMCACheck** ograniczające przejęcie klienta (kontynuacja)*		
AdoptNewMCA	**AdoptNewMCACheck**	**Kryteria sprawdzane przed zezwoleniem na przejęcie klienta**
ALL (lub wartość inna niż NO)	ALL	ID użytkownika (przy włączonej opcji SASL) Nazwa kanału Adres IP

Atrybuty menedżera kolejek **AdoptNewMCA** i **AdoptNewMCACheck** są częścią konfiguracji menedżera kolejek, która jest zdefiniowana w sekcji CHANNELS. W systemach IBM MQ for Windows i IBM MQ for Linux x86-64 zmodyfikuj informacje konfiguracyjne za pomocą pliku IBM MQ Explorer. W innych systemach zmodyfikuj informacje, edytując plik konfiguracyjny `qm.ini` . Informacje na temat modyfikowania informacji o kanałach menedżera kolejek zawiera sekcja Atrybuty kanałów.

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie i używanie kanałów AMQP

ALW

Konfigurowanie usługi JAAS dla kanałów AMQP

Moduły niestandardowe usługi Java Authentication and Authorization Service (JAAS) mogą być używane do uwierzytelniania referencji nazwy użytkownika i hasła przekazywanych do kanału AMQP przez klient AMQP podczas nawiązywania połączenia.

O tym zadaniu

Niestandardowy moduł JAAS może być używany, jeśli moduły JAAS są już używane do uwierzytelniania w innych systemach Javaoraz jeśli te moduły mają być ponownie wykorzystywane do 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.

Konfigurowanie modułów JAAS dla kanałów AMQP jest wykonywane na poziomie menedżera kolejek. Oznacza to, że jeśli moduł JAAS zostanie skonfigurowany na potrzeby uwierzytelniania połączeń AMQP z menedżerem kolejek, moduł zostanie zastosowany do wszystkich kanałów AMQP. Nazwa kanału, który wywołał moduł JAAS , jest przekazywana do modułu, co umożliwia zakodowanie różnych zachowań logowania JAAS dla różnych kanałów.

Inne informacje są również przekazywane do modułu JAAS :

- Identyfikator klienta AMQP, który próbuje się uwierzytelnić.
- 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 więcej sekcji konfiguracji modułu JAAS . W sekcji musi być podana pełna nazwa klasy Java implementującej interfejs JAAS `javax.security.auth.spi.LoginModule` .
   - Domyślny plik `jaas.config` jest dostarczany z produktem i 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.
   - Linux AIX 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, aby uwzględnić 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 MQ service.env . Zmodyfikuj plik service.env w katalogu konfiguracji produktu MQ (*MQ_config_directory*) 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 z produktem w katalogu *mq_installation_directory*/amqp/samples . Przykładowy moduł logowania JAAS uwierzytelnia wszystkie połączenia klienckie, niezależnie od nazwy użytkownika i hasła, z którymi łączy się klient.

Można zmodyfikować kod źródłowy przykładu i ponownie go skompilować, aby uwierzytelnić tylko konkretnych użytkowników z określonym hasłem. Aby skonfigurować kanał AMQP w systemie UNIX do używania przykładowego modułu logowania JAAS dostarczanego z produktem:

1. Zmodyfikuj plik /var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties i ustaw właściwość com.ibm.mq.MQXR.JAASConfig=MQXRConfig.
2. Zmodyfikuj 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 wypróbowaniem przykładowego modułu nie są wymagane żadne zmiany w pliku jaas.config .

Zadania pokrewne

Tworzenie aplikacji klienckich AMQP

Tworzenie i używanie kanałów AMQP

Advanced Message Security

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

Przegląd produktu Advanced Message Security

Aplikacje IBM MQ mogą używać programu Advanced Message Security do wysyłania poufnych danych, takich jak transakcje finansowe o dużej wartości i dane osobowe, z różnymi poziomami ochrony, za pomocą modelu kryptograficznego z kluczem publicznym.

Pojęcia pokrewne

“Przechwytywanie agenta kanału komunikatów (MCA) i AMS” na stronie 706

Przechwytywanie MCA umożliwia menedżerowi kolejek działającemu w ramach produktu IBM MQ selektywne włączanie strategii stosowanych dla kanałów połączeń serwera.

Odsyłacze pokrewne

Kody powrotu IBM Global Security Kit (GSKit) używane w komunikatach AMS

Funkcje i cechy produktu Advanced Message Security

Produkt Advanced Message Security rozszerza usługi zabezpieczeń systemu IBM MQ , aby zapewnić podpisywanie i szyfrowanie danych na poziomie komunikatu. Rozwinięte usługi gwarantują, że dane komunikatu nie zostały zmodyfikowane między początkowym umieszczaniem w kolejce a pobraniem. Ponadto produkt AMS sprawdza, czy nadawca danych komunikatu ma uprawnienia do umieszczania podpisanych komunikatów w kolejce docelowej.

Program AMS udostępnia następujące funkcje:

- Zabezpiecza wrażliwe lub wartościowe transakcje przetwarzane przez IBM MQ.
- Wykrywa i usuwa obce lub nieautoryzowane komunikaty przed ich przetworzeniem przez aplikację odbierającą.
- Sprawdza, czy komunikaty nie zostały zmodyfikowane podczas przesyłania z kolejki do kolejki.
- Chroni dane nie tylko podczas ich przepływu przez sieć, ale także podczas umieszczania w kolejce.
- Zabezpiecza istniejące aplikacje zastrzeżone i napisane przez klienta dla IBM MQ.
- z/OS W produkcie IBM MQ 9.1.3produkt IBM MQ for z/OS umożliwia opcjonalne usuwanie i dodawanie zabezpieczeń AMS odpowiednio w przypadku komunikatów przepływającego przez sieć lub do komunikatów, które przepływają przez sieć. Jest to określane jako *Server to Server Message Channel Agent (MCA) Interception*.
- ALW W systemach IBM MQ 9.1.4 i IBM MQ 9.1.0 Fix Pack 4do kodu biblioteki IBM MQ , który jest uruchamiany w aplikacji klienta, dodawane jest sprawdzenie. Sprawdzanie jest uruchamiane na wczesnym etapie inicjowania w celu odczytania wartości zmiennej środowiskowej *AMQ_AMS_FIPS_OFF* . Jeśli ta wartość jest ustawiona, kod IBM Global Security Kit (GSKit) jest uruchamiany w trybie innym niż FIPS w tej aplikacji.

Jakość ochrony dostępna w produkcie AMS

Istnieją trzy rodzaje ochrony: Advanced Message Security, `Integrity`, `Privacy`i `Confidentiality`.

Ochrona systemu `Integrity` jest zapewniana przez podpisywanie cyfrowe, które zapewnia, kto utworzył komunikat oraz że komunikat nie został zmieniony ani zmodyfikowany.

Ochrona `Privacy` jest zapewniana przez połączenie cyfrowego podpisywania i szyfrowania. Szyfrowanie zapewnia, że dane komunikatu są widoczne tylko dla adresata lub adresatów. Nawet jeśli nieautoryzowani odbiorcy uzyskają kopię zaszyfrowanych danych komunikatu, nie będą w stanie samodzielnie wyświetlić rzeczywistych danych komunikatu.

Ochrona `Confidentiality` jest zapewniana przez szyfrowanie tylko z opcjonalnym ponownym wykorzystaniem klucza.

Wpływ na wydajność

AMS wykorzystuje kombinację symetrycznych i asymetrycznych procedur szyfrujących w celu zapewnienia cyfrowego podpisywania i szyfrowania. Ponieważ operacje klucza symetrycznego są bardzo szybkie w porównaniu z operacjami klucza asymetrycznego, które intensywnie wykorzystują procesor, może to z kolei mieć znaczący wpływ na koszty związane z ochroną dużej liczby komunikatów za pomocą programu AMS.

Asymetryczne procedury szyfrujące

Na przykład podczas umieszczania podpisanego komunikatu krzyżyk komunikatu jest podpisywany przy użyciu operacji klucza asymetrycznego.

Podczas pobierania podpisanego komunikatu do zweryfikowania podpisanej wartości mieszającej używana jest dalsza operacja klucza asymetrycznego.

Dlatego do podpisania i zweryfikowania danych komunikatu wymagane są co najmniej dwie operacje klucza asymetrycznego na komunikat.

Asymetryczne i symetryczne procedury kryptograficzne

Podczas umieszczania zaszyfrowanego komunikatu generowany jest klucz symetryczny, a następnie jest on szyfrowany przy użyciu operacji klucza asymetrycznego dla każdego zamierzonego odbiorcy komunikatu.

Dane komunikatu są następnie szyfrowane za pomocą klucza symetrycznego. Podczas pobierania zaszyfrowanego komunikatu zamierzony odbiorca musi użyć operacji klucza asymetrycznego w celu wykrycia klucza symetrycznego używanego dla komunikatu.

Wszystkie trzy rodzaje ochrony zawierają zatem różne elementy asymetrycznych operacji kluczowych intensywnie wykorzystujących procesor, co będzie miało znaczący wpływ na maksymalną osiągalną szybkość przesyłania komunikatów dla aplikacji umieszczających i pobierających komunikaty.

Strategie `Confidentiality` umożliwiają jednak ponowne wykorzystanie klucza symetrycznego w sekwencji komunikatów. Za pomocą strategii `Confidentiality` można uzyskać znaczne oszczędności na kosztach procesora dzięki możliwości ponownego wykorzystania klucza symetrycznego. Ten tryb działania nadal używa formatu PKCS#7 do współużytkowania symetrycznego klucza szyfrowania. Nie ma jednak podpisu cyfrowego, który eliminuje niektóre operacje na kluczu asymetrycznym komunikatu. Klucz symetryczny nadal musi być zaszyfrowany za pomocą operacji klucza asymetrycznego dla każdego odbiorcy, ale klucz symetryczny może być opcjonalnie ponownie wykorzystany w wielu komunikatach, które są przeznaczone dla tych samych odbiorców. Jeśli strategia zezwala na ponowne wykorzystanie klucza, tylko pierwszy komunikat wymaga operacji klucza asymetrycznego. Kolejne komunikaty muszą używać tylko operacji klucza symetrycznego.

Ponowne wykorzystanie klucza

W przypadku strategii `Confidentiality` można użyć metody ponownego wykorzystania klucza symetrycznego, aby znacząco zmniejszyć koszty związane z szyfrowaniem pewnej liczby komunikatów umieszczanych w tej samej kolejce i przeznaczonych dla tego samego odbiorcy lub odbiorców.

Na przykład podczas umieszczania 10 zaszyfrowanych komunikatów w tym samym zestawie odbiorców generowany jest klucz symetryczny, a następnie zaszyfrowany dla pierwszego komunikatu przy użyciu operacji klucza asymetrycznego dla każdego zamierzonego odbiorcy komunikatu.

Na podstawie limitów sterowanych przez strategię zaszyfrowany klucz symetryczny może być ponownie wykorzystywany przez kolejne komunikaty przeznaczone dla tych samych odbiorców. Aby umożliwić ponowne wykorzystanie klucza symetrycznego przez kolejne komunikaty, aplikacja musi zachować otwartą kolejkę po umieszczeniu komunikatu w kolejce. Klucz symetryczny nie może być ponownie wykorzystywany przez operacje MQPUT1 . Aplikacja, która otrzymuje zaszyfrowane komunikaty, może zastosować tę samą optymalizację, ponieważ aplikacja może wykryć, czy klucz symetryczny nie uległ zmianie, i uniknąć konieczności pobierania klucza symetrycznego.

W tym przykładzie 90% operacji klucza asymetrycznego można uniknąć zarówno przez umieszczanie, jak i pobieranie aplikacji przez ponowne wykorzystanie tego samego klucza.

Więcej informacji na temat ponownego wykorzystania klucza zawiera sekcja:

- Komenda MQSC SET POLICY
- Komenda sterująca setmqspl
- IBM i IBM i komenda SETMQMSPL

Kluczowe pojęcia w produkcie AMS

Zapoznaj się z kluczowymi pojęciami, które można znaleźć w sekcji Advanced Message Security , aby zrozumieć, w jaki sposób narzędzie działa i jak skutecznie nim zarządzać.

Infrastruktura klucza publicznego i Advanced Message Security

Infrastruktura klucza publicznego (public key infrastructure-PKI) jest systemem infrastruktury, strategii i usług, które obsługują szyfrowanie klucza publicznego w celu uzyskania bezpiecznej komunikacji.

Nie istnieje jeden standard definiujący komponenty infrastruktury klucza publicznego, ale infrastruktura PKI zazwyczaj obejmuje korzystanie z certyfikatów klucza publicznego i składa się z ośrodków certyfikacji (CA) i innych ośrodków rejestracji (RA), które świadczą 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 przechowywany jest certyfikat i powiązany klucz prywatny. Każdy certyfikat jest reprezentowany przez etykietę w magazynie kluczy.

Pojęcia pokrewne

“Używanie magazynów kluczy i certyfikatów z programem AMS” na stronie 699
Aby zapewnić aplikacjom IBM MQ przezroczystą ochronę kryptograficzną, program Advanced Message Security używa 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 programie AMS

Advanced Message Security wiąże użytkowników i aplikacje ze standardowymi certyfikatami cyfrowymi X.509 . Certyfikaty X.509 są zazwyczaj podpisywane przez zaufany ośrodek certyfikacji (CA) i obejmują klucze prywatne i publiczne używane do szyfrowania i deszyfrowania.

Certyfikaty cyfrowe zapewniają ochronę przed imitowaniem przez powiązanie klucza publicznego z właścicielem, niezależnie od tego, czy jest to osoba fizyczna, menedżer kolejek, czy inna jednostka. Certyfikaty cyfrowe są również nazywane certyfikatami klucza publicznego, ponieważ dają pewność co do prawa własności klucza publicznego, gdy używany jest schemat klucza asymetrycznego. Ten schemat wymaga wygenerowania klucza publicznego i klucza prywatnego dla aplikacji. Dane zaszyfrowane przy użyciu klucza publicznego mogą być deszyfrowane tylko przy użyciu odpowiedniego klucza prywatnego, a dane zaszyfrowane przy użyciu klucza prywatnego mogą być deszyfrowane tylko przy użyciu 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 wiadomości, które są szyfrowane przy użyciu odpowiedniego klucza publicznego.

Jeśli klucze publiczne są wysyłane bezpośrednio przez właściciela do innej jednostki, istnieje ryzyko przechwycenia komunikatu, a klucz publiczny jest zastępowany przez inny. Nazywa się to atakiem typu "człowiek w środku". Rozwiązaniem jest wymiana kluczy publicznych za pośrednictwem zaufanej osoby trzeciej, dając użytkownikowi silne zapewnienie, że klucz publiczny należy do jednostki, z którą się komunikujesz. Zamiast wysyłać klucz publiczny bezpośrednio, należy poprosić zaufaną osobę trzecią o włączenie go do certyfikatu cyfrowego. Zaufana osoba trzecia, która wydaje certyfikaty cyfrowe, jest nazywana ośrodkiem certyfikacji (CA).

Więcej informacji na temat certyfikatów cyfrowych zawiera sekcja Co to jest certyfikat cyfrowy.

Certyfikat cyfrowy zawiera klucz publiczny dla jednostki i określa, że klucz publiczny należy do tej jednostki:

- gdy certyfikat jest przeznaczony dla pojedynczej jednostki, jest nazywany *certyfikatem osobistym* lub *certyfikatem użytkownika*.
- gdy certyfikat jest przeznaczony dla ośrodka certyfikacji, jest on nazywany *certyfikatem ośrodka CA* lub *certyfikatem osoby podpisującej*.

Uwaga: Produkt Advanced Message Security obsługuje certyfikaty samopodpisane zarówno w aplikacji Java , jak i w aplikacjach rodzimych.

Pojęcia pokrewne

"Kryptografia" na stronie 11
Kryptografia jest procesem przekształcania tekstu możliwego do odczytania, nazywanego *tekstem jawnym*, i postaci nieczytelnej, nazywanej *tekstem zaszyfrowanym*.

Multi *Object authority manager (menedżer uprawnień do obiektów) i AMS*

W przypadku wielu platform menedżer uprawnień do obiektów (Object Authority Manager-OAM) jest komponentem usługi autoryzacji dostarczanym z produktami IBM MQ .

Dostęp do obiektów Advanced Message Security jest kontrolowany przez grupy 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 wykonywać zarówno operacje PUT, jak i GET dla konkretnej kolejki, podczas gdy inna grupa może tylko przeglądać tę kolejkę. Podobnie niektóre grupy mogą mieć uprawnienia GET i PUT do kolejki, ale nie mogą zmieniać ani usuwać kolejki.

Za pomocą OAM można kontrolować:

- Dostęp do obiektów Advanced Message Security za pośrednictwem interfejsu kolejki komunikatów (Message Queue Interface-MQI). Gdy aplikacja próbuje uzyskać dostęp do obiektów, funkcja OAM sprawdza, czy profil użytkownika wysyłający żądanie ma uprawnienia do żądanej operacji. Oznacza to, że kolejki i komunikaty w kolejkach mogą być chronione przed dostępem bez uprawnień.
- Uprawnienie do używania komend PCF i MQSC.

Pojęcia pokrewne

Menedżer uprawnień do obiektów

Przegląd interfejsu kolejki komunikatów

Technologia obsługiwana przez Advanced Message Security

Produkt Advanced Message Security udostępnia infrastrukturę zabezpieczeń w zależności od kilku komponentów technologicznych.

Produkt Advanced Message Security obsługuje następujące aplikacyjne interfejsy programistyczne (API) języka IBM MQ :

- Message Queue Interface (MQI)
- IBM MQ Java Message Service (JMS) 1.0.2 i 1.1.
- IBM MQ Klasy bazowe dla Java
- Klasy IBM MQ dla środowiska. Net w trybie niezarządzanym

Uwaga: Advanced Message Security obsługuje ośrodki certyfikacji zgodne ze standardem X.509 .

Znane ograniczenia produktu AMS

Istnieje pewna liczba opcji IBM MQ , które nie są obsługiwane lub mają ograniczenia dotyczące produktu Advanced Message Security.

- Następujące opcje IBM MQ nie są obsługiwane lub mają ograniczenia:

  Publikowanie / subskrypcja

  Jedną z głównych zalet modelu przesyłania komunikatów w trybie publikowania/subskrypcji w porównaniu do modelu typu punkt z punktem jest to, że aplikacje wysyłające i odbierające nie muszą wiedzieć nic o sobie, aby dane były wysyłane i odbierane. Korzyści te są zanegowane przez użycie strategii Advanced Message Security , które muszą definiować zamierzonych odbiorców lub autoryzowanych osób podpisujących. Aplikacja może publikować w temacie za pośrednictwem definicji kolejki aliasowej, która jest chroniona przez strategię. Aplikacja subskrybująca może również otrzymywać komunikaty z kolejki zabezpieczonej przez strategię. Nie jest możliwe

przypisanie strategii bezpośrednio do łańcucha tematu. Strategie mogą być przypisane tylko do definicji kolejek.

Konwersja danych kanału
Zabezpieczony ładunek zabezpieczonego komunikatu Advanced Message Security jest przesyłany w formacie binarnym, dzięki czemu konwersja danych w kanale między aplikacjami nie powoduje unieważnienia streszczenia komunikatu. Aplikacje pobierają komunikaty z kolejki zabezpieczonej przez strategię powinny zażądać konwersji danych. Po pomyślnym zweryfikowaniu i niezabezpieczeniu komunikatów zostanie podjęta próba konwersji zabezpieczonego ładunku.

Lista dystrybucyjna
Strategii Advanced Message Security można używać podczas zabezpieczania aplikacji umieszczanych na listach dystrybucyjnych, pod warunkiem, że każda kolejka docelowa na liście ma zdefiniowaną identyczną strategię. Jeśli podczas otwierania listy dystrybucyjnej przez aplikację zostaną zidentyfikowane niespójne strategie, operacja otwierania nie powiedzie się i do aplikacji zostanie zwrócony błąd zabezpieczeń.

Segmentacja komunikatów aplikacji
Wielkość komunikatów chronionych przez strategię zostanie zwiększona i nie jest możliwe dokładne określenie przez aplikacje granic segmentu komunikatu.

Aplikacje używające programu IBM MQ classes for .NET w trybie zarządzanym (połączenia klienckie)
Aplikacje używające programu IBM MQ classes for .NET w trybie zarządzanym (połączenia klienckie) nie są obsługiwane.

Uwaga: Przechwycenia MCA można użyć 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: Przechwycenia MCA można użyć, aby umożliwić nieobsługiwanym klientom korzystanie z opcji AMS.

Kolejki produktu IBM MQ przetwarzane przez most IMS
Kolejki produktu IBM MQ przetwarzane przez most IMS nie są obsługiwane.

Uwaga: Produkt AMS jest obsługiwany w kolejkach mostu CICS . W kolejkach mostu CICS należy używać tego samego identyfikatora użytkownika dla MQPUT (szyfrowanie) i MQGET (deszyfrowanie).

Umieść w oczekującej metodzie pobierającej
Metoda put to waiting getter nie jest obsługiwana dla aplikacji pobierających w odniesieniu do kolejek, dla których zdefiniowano strategie AMS .

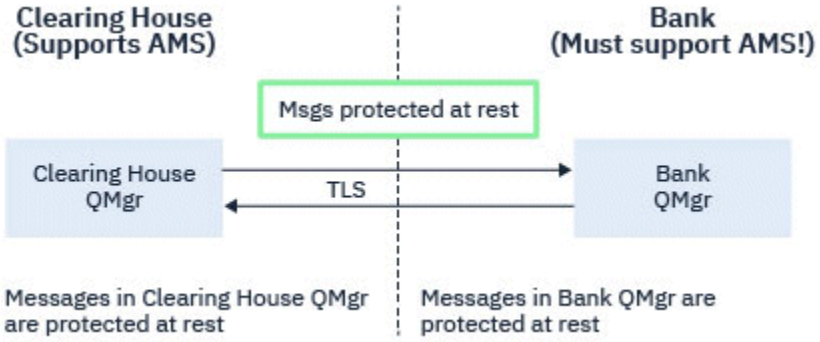
Przechwytywanie MCA od serwera do serwera
W produkcie IBM MQ for z/OS 9.1.3przechwytywanie MCA między serwerami jest obsługiwane tylko w przypadku typów kanałów nadawcy, serwera, odbiorcy i requestera.

- 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.
- Parametr 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 Przechwytywanie Advanced Message Security w kanałach komunikatów

W systemie z/OSprzechwytywanie Advanced Message Security (AMS) udostępnia dodatkową opcję ochrony strategii bezpieczeństwa (SPLPROT) dla kanałów nadawczych, serwerowych, odbiorczych i requestera, umożliwiając obsługę systemu AMS i komunikację z partnerami biznesowymi, którzy nie obsługują systemu AMS.

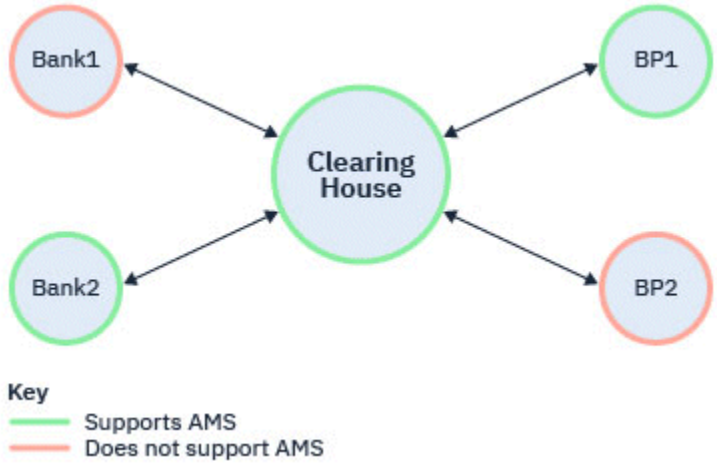
Rysunek 1 pokazuje, że bez AMS przechwytywania, obie strony systemu muszą obsługiwać AMS.



Rysunek 32. Użycie opcji AMS bez przechwycenia AMS

Główną zaletą opcji przechwytywania AMS jest to, że jeśli w przedsiębiorstwie skonfigurowano AMS , a nie wszyscy partnerzy handlowi obsługują AMS, można usunąć ochronę przed komunikatami wychodzącymi i chronić komunikaty przychodzące w kanałach do i od tych partnerów biznesowych, którzy nie obsługują AMS.

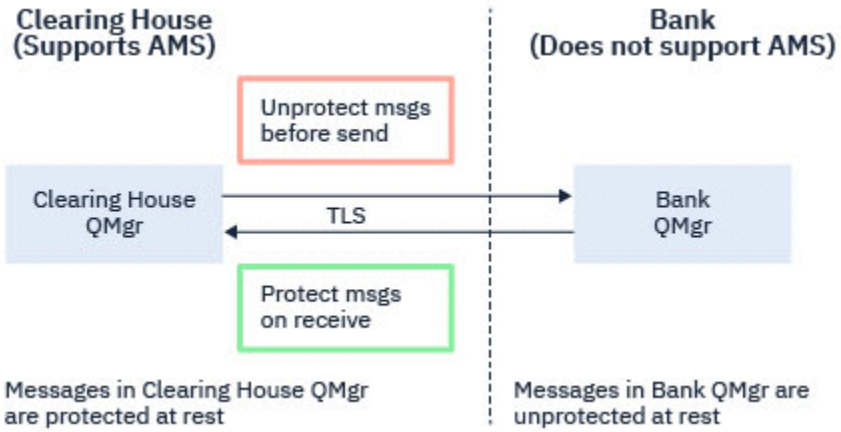
Na podstawie przykładu izby rozliczeniowej i banków scenariusz ten jest przedstawiony na Rysunku 2, w którym występuje przepływ komunikatów między izbę rozliczeniową, bankami i partnerami handlowymi, w których niektóre instytucje mają AMS, a inne nie.



Rysunek 33. Niektórzy partnerzy wspierają AMS, a inni nie

Zazwyczaj kanały obsługują protokół TLS.

Może jednak wystąpić sytuacja, w której niektóre banki i partnerzy handlowi nie obsługują produktu AMSi istnieje wymaganie, aby możliwa była wymiana komunikatów między wszystkimi bankami i partnerami handlowymi. Ten scenariusz jest przedstawiony na Rysunku 3



Rysunek 34. Przepływ komunikatów między partnerami biznesowymi

Zadania pokrewne

Przykładowe konfiguracje przechwytywania kanału komunikatów typu serwer-serwer

z/OS *Przechwytywanie AMS w kanałach komunikatów serwer-serwer*

Przechwytywanie kanału komunikatów typu serwer-serwer umożliwia określenie, czy do komunikatów mają być stosowane odpowiednie strategie produktu Advanced Message Security (AMS), gdy agenty kanału komunikatów typu nadawczego pobierają komunikaty z kolejek transmisji, a agenty kanału komunikatów typu odbiorczego umieszczają komunikaty w kolejkach docelowych.

Umożliwia to włączenie ochrony produktu AMS w menedżerze kolejek podczas komunikacji przy użyciu kanałów komunikatów typu serwer-serwer (nadawca, serwer, odbiorca i requester) z menedżerem kolejek bez włączonej opcji AMS .

Oznacza to, że komunikaty zabezpieczone AMS w menedżerach kolejek z włączoną opcją AMS mogą być niezabezpieczone przed wysłaniem do menedżerów kolejek z włączoną opcją inną niżAMS , a niechronione komunikaty odebrane z menedżerów kolejek z włączoną opcją inną niżAMS mogą być chronione za pomocą odpowiednich strategii systemu AMS w menedżerach kolejek z włączoną opcją AMS .

Konfigurowanie przechwytywania kanału komunikatów serwer-serwer

Przechwytywanie kanału komunikatów serwer-serwer jest konfigurowane za pomocą atrybutu SPLPROT kanałów, których typem kanału jest nadawca, serwer, odbiorca lub requester. Dostępne opcje konfigurowania zachowania zależą od określonego 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 na potrzeby przechwytywania kanału komunikatów

Wymagania dotyczące identyfikatorów użytkowników używanych z przechwytywaniem kanału komunikatów serwer-serwer są takie same, jak w przypadku istniejących aplikacji z włączoną obsługą języka AMS . W przypadku działającego kanału agent kanału komunikatów wysyłający pobiera komunikaty z kolejki transmisji, a agent kanału komunikatów odbierający umieszcza komunikaty w kolejkach docelowych. Pole ID użytkownika agenta kanału komunikatów (MCAUSER), ustawione na serwerze dla kanałów serwera, definiuje ID użytkownika, pod którym agenty kanału komunikatów wykonują żądania umieszczania i pobierania.

W przypadku przechwytywania kanału komunikatów serwer-serwer funkcje AMS są wykonywane podczas żądań pobierania i umieszczania (get), podobnie jak w przypadku innych aplikacji z obsługą AMS . Dlatego identyfikatory użytkowników agenta kanału komunikatów mają takie same wymagania, jak identyfikatory użytkowników aplikacji AMS .

Atrybut MCAUSER używany do wykonywania operacji put i get jest konfigurowalny i zależy od tego, czy jest to kanał wychodzący, czy przychodzący. Więcej informacji na temat wykonywania działań na agencie kanału komunikatów zawiera sekcja MCAUSER . Oznacza to, że identyfikator użytkownika używany przez inicjator kanału jest identyfikatorem użytkownika, który ma być używany dla funkcji AMS wykonywanych podczas przechwytywania kanału komunikatów między serwerami. Dlatego te identyfikatory użytkowników mają takie same wymagania, jak identyfikatory użytkowników aplikacji AMS .

Uwierzytelnianie jest wykonywane przy użyciu istniejących reguł dla kanału szczegółowego dla kanałów z konfiguracją PUTAUT. Więcej informacji na ten temat zawiera sekcja Identyfikatory użytkowników używane przez inicjator kanału .

Uwaga: Przechwytywanie kanału komunikatów serwer-serwer nie uwzględnia wartości atrybutu kanału PUTAUT.

Wielkość komunikatu i MAXMSGL

Ze względu na ochronę systemu AMS wielkość chronionych komunikatów będzie większa niż oryginalna wielkość komunikatu.

Komunikaty chronione są większe niż komunikaty niechronione. Dlatego wartość atrybutu **MAXMSGL** , zarówno w kolejkach, jak i w kanałach, może wymagać zmiany w celu uwzględnienia wielkości chronionych komunikatów.

Odsyłacze pokrewne
Przykładowe konfiguracje przechwytywania kanału komunikatów typu serwer-serwer

Obsługa błędów dla AMS

Produkt IBM MQ Advanced Message Security definiuje kolejkę obsługi błędów w celu zarządzania komunikatami zawierającymi błędy lub komunikatami, które nie mogą być niechronione.

Wadliwe komunikaty są traktowane jako wyjątkowe przypadki. Jeśli odebrany komunikat nie spełnia wymagań bezpieczeństwa dla kolejki, w której się znajduje, na przykład jeśli komunikat jest podpisany, a powinien być zaszyfrowany, lub jeśli deszyfrowanie lub weryfikacja podpisu nie powiedzie się, komunikat zostanie wysłany do kolejki obsługi błędów. Komunikat może zostać wysłany do kolejki obsługi błędów z następujących powodów:

- Niezgodność jakości ochrony-występuje niezgodność jakości ochrony (QOP) między odebranym komunikatem a definicją QOP w strategii bezpieczeństwa.
- Błąd deszyfrowania-nie można zdeszyfrować komunikatu.
- Błąd nagłówka PDMQ-nie można uzyskać dostępu do nagłówka komunikatu Advanced Message Security (AMS).
- Niezgodność wielkości-długość komunikatu po deszyfrowaniu jest inna niż oczekiwana.
- Niezgodność mocy algorytmu szyfrowania-algorytm szyfrowania komunikatów jest słabszy niż wymagany.
- Nieznany błąd-wystąpił nieoczekiwany błąd.

AMS korzysta z systemu SYSTEM.PROTECTION.ERROR.QUEUE jako kolejka obsługi błędów. Wszystkie komunikaty wysłane przez produkt IBM MQ AMS do systemu SYSTEM.PROTECTION.ERROR.QUEUE są poprzedzone nagłówkiem MQDLH.

Administrator IBM MQ może również zdefiniować system SYSTEM.PROTECTION.ERROR.QUEUE jako kolejka aliasowa wskazująca inną kolejkę.

z/OS Od wersji IBM MQ 9.1.3w systemie IBM MQ for z/OS, jeśli przechwytywanie agenta kanału komunikatów (MCA) od serwera jest używane:

- Jeśli z jednej z wcześniej wymienionych przyczyn produkt IBM MQ AMS przeniesie komunikaty z kolejki transmisji do kolejki obsługi błędów, agent MCA nadawcy kontynuuje przetwarzanie następnego dostępnego komunikatu w kolejce transmisji.
- Ogólnie rzecz biorąc, istniejące reguły kanału mają zastosowanie do:
  - Umieszczanie komunikatów w kolejce niedostarczonych komunikatów
  - Działania podejmowane w przypadku umieszczenia w kolejce niedostarczonych komunikatów powinny zakończyć się niepowodzeniem.

Więcej informacji na temat konkretnych scenariuszy zawiera sekcja "Niedostarczone komunikaty dla AMS w systemie z/OS" na stronie 661 .

z/OS *Niedostarczone komunikaty dla AMS w systemie z/OS*

Konkretne scenariusze dotyczące przechwytywania agenta kanału komunikatów od serwera do serwera w systemie IBM MQ for z/OS.

Od wersji IBM MQ 9.1.3w systemie IBM MQ for z/OS, jeśli przechwytywanie agenta kanału komunikatów (MCA) od serwera jest używane:

- Jeśli po otrzymaniu i usunięciu zabezpieczeń komunikatu agent MCA nadawcy nie dostarczy komunikatu z jakiegoś powodu, na przykład z powodu zbyt dużego komunikatu dla kanału, jeśli atrybut kanału nadawczego USEDLQ ma wartość YES, agent MCA nadawcy przenosi komunikat do lokalnej kolejki niedostarczonych komunikatów (DLQ).

  W przypadku systemu SYSTEM.DEAD.LETTER.QUEUE jest używana jako lokalna kolejka DLQ, komunikat jest umieszczany bez ochrony.

  Uwaga: Produkt IBM MQ AMS nie obsługuje ochrony komunikatów umieszczanych w kolejkach systemowych.

  Jeśli jako lokalna kolejka DLQ jest używana nazwana kolejka DLQ, komunikat zostanie umieszczony jako chroniony, jeśli zdefiniowano strategię IBM MQ AMS o takiej samej nazwie jak podana kolejka DLQ, a niezabezpieczony, jeśli nie zdefiniowano odpowiedniej strategii.
- Jeśli z jakiegoś powodu nie można umieścić komunikatu w lokalnej kolejce DLQ, to jeśli parametr NPMSPEED kanału jest ustawiony na wartość NORMAL lub komunikat jest komunikatem trwałym, bieżąca partia komunikatów jest wycofywana, a kanał jest umieszczany w stanie RETRY. W przeciwnym razie komunikat jest usuwany, a agent MCA nadawcy kontynuuje przetwarzanie następnego komunikatu w kolejce transmisji.

- Strategie bezpieczeństwa nie mają wpływu na system SYSTEM.DEAD.LETTER.QUEUElub inne kolejki systemowe wymienione w sekcji “Ochrona kolejki systemowej w programie AMS” na stronie 738, jeśli używany jest system SYSTEM.DEAD.LETTER.QUEUE są używane, komunikaty umieszczane w tej kolejce przez MCA są umieszczane w stanie, w jakim się znajdują ("as is"). Oznacza to, że jeśli wiadomości były wcześniej chronione, są one chronione; w przeciwnym razie są one niechronione.

  Jeśli atrybut DEADQ menedżera kolejek został ustawiony na nazwę alternatywnej (nie systemowej) kolejki niedostarczonych komunikatów, a strategia AMS o takiej samej nazwie nie istnieje, komunikaty umieszczane w tej kolejce przez adaptery MCA są umieszczane w takiej postaci, w jakiej są. Oznacza to, że jeśli wiadomości były wcześniej chronione, są one chronione; w przeciwnym razie są one niechronione.

  Jeśli atrybut DEADQ menedżera kolejek został ustawiony na nazwę alternatywnej (nie systemowej) kolejki niedostarczonych komunikatów i istnieje strategia AMS o takiej samej nazwie jak DLQ, strategia ta jest używana do zabezpieczania komunikatów umieszczanych w tej kolejce przez konsole HMC. Jeśli komunikat był już wcześniej chroniony, nie jest ponownie chroniony; ma to na celu uniknięcie podwójnej ochrony. Jeśli strategia AMS o takiej samej nazwie nie istnieje, komunikaty są umieszczane w takim samym miejscu.
- Jeśli istnieje strategia dla kolejki DLQ z opcją tolerancji w komendzie setmqspl ustawioną na wartość off, to znaczy '**-t** O', operacja umieszczania w kolejce DLQ nie powiedzie się, jeśli komunikat nie jest chroniony przez AMS i dlatego nie ma nagłówka PDMQ. Ma to miejsce, gdy komunikat dociera do odbiornika bez nagłówka PDMQ. Oznacza to, że oryginalny putter komunikatu nie miał strategii dla miejsca docelowego, a odbiorca nie ma ustawionego parametru SPLPROT (ASPOLICY).
- Agent MCA może nie umieścić komunikatu w kolejce DLQ, jeśli strategia AMS zdefiniowana dla tej kolejki DLQ nie zezwala na ID użytkownika, w ramach którego działa inicjator kanału, w celu zabezpieczenia komunikatu.
- Kanały odbiorcze zwykle umieszczają niedostarczone komunikaty w lokalnej kolejce DLQ, podczas gdy kanały nadawcze zwykle umieszczają komunikaty, których nie można przetworzyć z jakiegoś powodu, na przykład komunikat zbyt duży dla kolejki lub błędny nagłówek MQXQH, itd. do lokalnej kolejki DLQ.
- Procedury obsługi DLQ zwykle patrzą tylko na nagłówek DLQ (DLH), a nie na sam ładunek komunikatu. Dlatego fakt, że ładunek komunikatu może być zabezpieczony, nie uniemożliwia procedurowi określenia przyczyny umieszczenia komunikatu w kolejce DLQ.
- Jeśli kolejka DLQ nie jest zdefiniowana, kanał:
  - Kończy działanie nieprawidłowo (i przechodzi w stan ponawiania), jeśli nie można dostarczyć trwałego komunikatu.
  - Usuwa nietrwały niedostarczony komunikat i kontynuuje działanie.

Pojęcia pokrewne

“Obsługa błędów dla AMS” na stronie 660
Produkt IBM MQ Advanced Message Security definiuje kolejkę obsługi błędów w celu zarządzania komunikatami zawierającymi błędy lub komunikatami, które nie mogą być niechronione.

Scenariusze użytkownika dla produktu AMS

Zapoznaj się z możliwymi scenariuszami, aby zrozumieć, jakie cele biznesowe można osiągnąć w produkcie Advanced Message Security.

Windows *Publikacja Szybki start dla systemu AMS na platformach Windows*

Ten podręcznik umożliwia szybkie skonfigurowanie produktu Advanced Message Security (AMS) w celu zapewnienia bezpieczeństwa komunikatów na platformach Windows . Przed jego wykonaniem zostanie utworzona baza danych kluczy w celu zweryfikowania tożsamości użytkowników i zdefiniowania strategii podpisywania/szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

W systemie powinny być zainstalowane co najmniej następujące opcje:

- Serwer
- Development Toolkit (dla programów przykładowych)
- Advanced Message Security (AMS)

Szczegółowe informacje można znaleźć w sekcji IBM MQ dla systemów Windows .

Informacje na temat inicjowania bieżącego środowiska za pomocą komendy **setmqenv** w celu zlokalizowania i wykonania odpowiednich komend IBM MQ przez system operacyjny zawiera sekcja setmqenv (set IBM MQ environment).

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach do przekazywania komunikatów między aplikacjami używana jest kolejka o nazwie TEST.Q . Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są one wprowadzane do infrastruktury IBM MQ za pośrednictwem standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM MQ i jest konfigurowana w następujących krokach.

Produkt IBM MQ Explorer umożliwia utworzenie menedżera kolejek QM_VERIFY_AMS i jego kolejki lokalnej o nazwie TEST.Q przy użyciu wszystkich domyślnych ustawień kreatora lub przy użyciu komend znajdujących się w pliku `C:\Program Files\IBM\MQ\bin`. Należy pamiętać, że użytkownik musi należeć do grupy użytkowników `mqm` , aby mógł uruchamiać następujące komendy administracyjne.

Procedura

1. Tworzenie menedżera kolejek

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Uruchom menedżer 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 na temat programu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym przykładzie są wyświetlani dwaj użytkownicy: `alice`, nadawca i bob, odbiorca. Aby korzystać z kolejki aplikacji, użytkownicy ci muszą mieć nadane uprawnienia do jej używania. Ponadto, aby pomyślnie korzystać ze strategii ochrony, które zostaną zdefiniowane dla tych użytkowników, należy nadać im dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** zawiera sekcja **setmqaut**.

Procedura

1. Utwórz dwóch użytkowników i upewnij się, że HOMEPATH i HOMEDRIVE są ustawione dla obu tych użytkowników.
2. Autoryzowanie użytkowników do nawiązywania połączenia z menedżerem kolejek i 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: Produkt IBM MQ optymalizuje wydajność, buforując strategie, dzięki czemu nie ma potrzeby przeglądania rekordów w poszukiwaniu szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Program IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Oznacza to, że jeśli dla menedżera kolejek zdefiniowano małą liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Należy jednak nadać uprawnienie do przeglądania tej kolejki w przypadku, gdy zdefiniowano dużą liczbę strategii lub gdy używane są stare klienty. SYSTEM SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach generowanych przez kod AMS. Uprawnienie do umieszczania dla tej kolejki jest sprawdzane tylko podczas próby umieszczenia komunikatu o błędzie w kolejce. Uprawnienia do umieszczania w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki zabezpieczonej AMS.

Wyniki

Użytkownicy są teraz tworzeni i nadawane im są 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 667.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Przechwytywacz wymaga klucza publicznego wysyłających użytkowników w celu zaszyfrowania komunikatu. Dlatego należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W rzeczywistym systemie, w którym użytkownicy i aplikacje są rozproszone na kilku komputerach, każdy użytkownik miałby własny prywatny magazyn kluczy. Podobnie w tym podręczniku tworzone są bazy danych kluczy dla produktów `alice` i bob oraz współużytkowane między nimi certyfikaty użytkowników.

Uwaga: W tym podręczniku używane są przykładowe aplikacje napisane w języku C i łączące się przy użyciu powiązań lokalnych. Jeśli planowane jest użycie aplikacji Java przy użyciu powiązań klienta, należy

utworzyć magazyn kluczy JKS i certyfikaty przy użyciu komendy **keytool** , która jest częścią środowiska JRE (więcej informacji na ten temat zawiera sekcja “Szybki start produktu AMS z klientami Java” na stronie 686). W przypadku wszystkich innych języków oraz w przypadku aplikacji Java korzystających z powiązań lokalnych kroki w tym podręczniku są poprawne.

Procedura

1. Użyj interfejsu GUI 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:

   - Do zabezpieczenia bazy danych zaleca się użycie silnego hasła.
   - Upewnij się, że pole wyboru **Skryj hasło do pliku** jest zaznaczone.
2. Zmień widok zawartości bazy danych kluczy na **Certyfikaty osobiste**.
3. Wybierz opcję **New Self Signed** (Nowy samopodpisany). W tym scenariuszu używane są certyfikaty samopodpisane.
4. Utwórz certyfikat identyfikujący użytkownika `alice` do użycia w szyfrowaniu, używając następujących pól:

   ```
   Key label: Alice_Cert
   Common Name: alice
   Organisation: IBM
   Country: GB
   ```

   Uwaga:

   - Na potrzeby niniejszego podręcznika używany jest certyfikat samopodpisany, który można utworzyć bez użycia ośrodka certyfikacji. W systemach produkcyjnych zaleca się, aby nie używać certyfikatów samopodpisanych, ale polegać na certyfikatach podpisanych przez ośrodek certyfikacji.
   - Parametr **Key label** określa nazwę certyfikatu, który przechwytywacze będą szukać w celu uzyskania niezbędnych informacji.
   - Parametr **Common Name** i parametry opcjonalne określają szczegóły nazwy **Nazwa wyróżniająca** (DN), która musi być unikalna dla każdego użytkownika.
5. Powtórz kroki 1-4 dla użytkownika bob

Wyniki

Każdy z tych dwóch użytkowników `alice` i bob ma teraz certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Należy wskazać przechwytywaczem Advanced Message Security katalog, w którym znajdują się bazy danych kluczy i certyfikaty. Jest to wykonywane za pośrednictwem pliku `keystore.conf` , który zawiera te informacje w postaci zwykłego tekstu. Każdy użytkownik musi mieć osobny plik `keystore.conf` w folderze `.mqs` . Ten krok należy wykonać zarówno dla systemu `alice` , jak i dla systemu bob.

Treść pliku `keystore.conf` musi mieć następującą 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" (ze spacją na końcu) na przykład, są rozpoznawane jako etykiety dwóch różnych certyfikatów. Jednak aby uniknąć pomyłek, 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 700.
- *%HOMEDRIVE%\%HOMEPATH%*`\.mqs\keystore.conf` (np. C:\Documents and Settings\alice\.mqs\keystore.conf) jest domyślnym położeniem, w którym produkt Advanced Message Security wyszukuje plik `keystore.conf` . Informacje na temat używania położenia innego niż domyślne dla `keystore.conf`zawiera sekcja “Używanie magazynów kluczy i certyfikatów z programem AMS” na stronie 699.
- Aby utworzyć katalog `.mqs` , należy użyć wiersza komend.

5. Współużytkowanie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwiema bazami danych kluczy, aby każdy użytkownik mógł pomyślnie zidentyfikować drugą bazę danych. W tym celu należy wyodrębnić certyfikat publiczny każdego użytkownika do pliku, który jest następnie dodawany do bazy danych kluczy innego użytkownika.

Uwaga: Należy zachować ostrożność, używając opcji *extract* , a nie opcji *export* . Opcja *Wyodrębnij* pobiera klucz publiczny użytkownika, natomiast opcja *Eksportuj* pobiera zarówno klucz publiczny, jak i prywatny. Użycie *eksportu* przez pomyłkę może całkowicie naruszyć ochronę aplikacji, przekazując jej klucz prywatny.

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 pliku 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 mogą teraz pomyślnie identyfikować się wzajemnie po utworzeniu i utworzeniu współużytkowanych certyfikatów samopodpisanych.

Co dalej

Sprawdź, czy 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

Po utworzeniu menedżera kolejek i przygotowaniu przechwytywaczy do przechwytywania komunikatów i kluczy szyfrowania dostępu można rozpocząć definiowanie strategii ochrony w systemie `QM_VERIFY_AMS` za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy zawiera sekcja setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Jest to przykład strategii zdefiniowanej dla kolejki `TEST.Q` . W tym przykładzie komunikaty są podpisywane przy użyciu algorytmu Deprecated SHA1 i szyfrowane przy użyciu 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 dokładnie zgodne z podanymi w odpowiednim certyfikacie użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wykonaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend `setmqspl` , należy użyć opcji `-export` . Pozwala to na przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testowanie konfiguracji

O tym zadaniu

Uruchamiając różne programy dla różnych użytkowników, można sprawdzić, czy aplikacja została poprawnie skonfigurowana.

Procedura

1. Przełącz użytkownika, aby uruchomić jako użytkownik `alice`

Kliknij prawym przyciskiem myszy plik `cmd.exe` i wybierz opcję **Uruchom jako ...**. Po wyświetleniu zachęty zaloguj się jako użytkownik `alice`.

2. Gdy użytkownik `alice` umieścił komunikat przy użyciu przykładowej aplikacji:

```
amqsput TEST.Q QM_VERIFY_AMS
```

3. Wpisz tekst komunikatu i naciśnij klawisz Enter.
4. Przełącz użytkownika, aby uruchomić jako użytkownik bob

   Otwórz inne okno, klikając prawym przyciskiem myszy plik `cmd.exe` i wybierając opcję **Uruchom jako ...**. Po wyświetleniu zachęty 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, po uruchomieniu aplikacji pobierającej przez program bob zostanie wyświetlony komunikat użytkownika `alice` .

8. Testowanie szyfrowania

O tym zadaniu

Aby sprawdzić, czy szyfrowanie działa zgodnie z oczekiwaniami, należy utworzyć kolejkę aliasową, która odwołuje się do oryginalnej kolejki TEST.Q. Ta kolejka aliasowa nie będzie miała strategii bezpieczeństwa i dlatego żaden użytkownik nie będzie miał informacji potrzebnych do deszyfrowania komunikatu i dlatego zostaną wyświetlone zaszyfrowane dane.

Procedura

1. Za pomocą komendy **runmqsc** dla menedżera kolejek QM_VERIFY_AMS utwórz kolejkę aliasową.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Nadaj uprawnienie dostępu bob do przeglądania z kolejki aliasowej

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako użytkownik `alice`, umieść kolejny komunikat przy użyciu przykładowej aplikacji, tak jak wcześniej:

```
amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako użytkownik bobprzejrzyj komunikat za pomocą przykładowej aplikacji, używając kolejki aliasowej:

```
amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako użytkownik bobpobierz komunikat z kolejki lokalnej przy użyciu przykładowej aplikacji:

```
amqsget TEST.Q QM_VERIFY_AMS
```

Wyniki

Dane wyjściowe z aplikacji `amqsbcg` zawierają zaszyfrowane dane znajdujące się w kolejce, co potwierdza, że komunikat został zaszyfrowany.

Linux AIX *Publikacja Szybki start dla produktu AMS w systemie AIX and Linux*

Ten podręcznik umożliwia szybkie skonfigurowanie produktu Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów w systemie AIX and Linux. Przed jego wykonaniem zostanie utworzona baza danych kluczy w celu zweryfikowania tożsamości użytkowników i zdefiniowania strategii podpisywania/szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

W systemie powinny być zainstalowane co najmniej następujące komponenty:

- Środowisko wykonawcze
- Serwer
- programy przykładowe
- IBM Global Security Kit (GSKit)
- Advanced Message Security

Nazwy komponentów na poszczególnych platformach można znaleźć w następujących tematach:

- Linux Komponenty IBM MQ dla systemów Linux
- AIX Komponenty IBM MQ dla systemów AIX

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach do przekazywania komunikatów między aplikacjami używana jest kolejka o nazwie TEST.Q . Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są one wprowadzane do infrastruktury IBM MQ za pośrednictwem standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM MQ i jest konfigurowana w następujących krokach.

Do utworzenia menedżera kolejek QM_VERIFY_AMS i jego kolejki lokalnej o nazwie TEST.Q można użyć programu IBM MQ Explorer, używając wszystkich domyślnych ustawień kreatora lub komend znajdujących się w katalogu *MQ_INSTALLATION_PATH*/bin. Należy pamiętać, że użytkownik musi należeć do grupy użytkowników mqm , aby mógł uruchamiać następujące komendy administracyjne.

Procedura

1. Tworzenie menedżera kolejek

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Uruchom menedżer 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 na temat programu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym przykładzie są wyświetlani dwaj użytkownicy: `alice`, nadawca i bob, odbiorca. Aby korzystać z kolejki aplikacji, użytkownicy ci muszą mieć nadane uprawnienia do jej używania. Ponadto, aby pomyślnie korzystać ze strategii ochrony, które zostaną zdefiniowane dla tych użytkowników, należy nadać im dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** zawiera sekcja **setmqaut**.

Procedura

1. Utwórz dwóch użytkowników

   ```
   useradd alice
   ```

   ```
   useradd bob
   ```

2. Autoryzowanie użytkowników do nawiązywania połączenia z menedżerem kolejek i 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: Produkt IBM MQ optymalizuje wydajność, buforując strategie, dzięki czemu nie ma potrzeby przeglądania rekordów w poszukiwaniu szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

   Program IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Oznacza to, że jeśli dla menedżera kolejek zdefiniowano małą liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

   Należy jednak nadać uprawnienie do przeglądania tej kolejki w przypadku, gdy zdefiniowano dużą liczbę strategii lub gdy używane są stare klienty. SYSTEM SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach generowanych przez kod AMS. Uprawnienie do umieszczania dla tej kolejki jest sprawdzane tylko podczas próby umieszczenia komunikatu o błędzie w kolejce. Uprawnienie do

umieszczania w kolejce nie jest sprawdzane podczas próby umieszczenia lub pobrania komunikatu z kolejki zabezpieczonej AMS.

Wyniki

Grupy użytkowników są teraz tworzone i nadawane im wymagane uprawnienia. W ten sposób użytkownicy przypisani do tych grup będą również mieli uprawnienia do nawiązywania połączeń 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 675.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Aby zaszyfrować komunikat, przechwytywacz wymaga klucza prywatnego wysyłającego użytkownika i klucza publicznego odbiorcy. Dlatego należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W rzeczywistym systemie, w którym użytkownicy i aplikacje są rozproszone na kilku komputerach, każdy użytkownik miałby własny prywatny magazyn kluczy. Podobnie w tym podręczniku tworzone są bazy danych kluczy dla produktów `alice` i bob oraz współużytkowane między nimi certyfikaty użytkowników.

Uwaga: W tym podręczniku używane są przykładowe aplikacje napisane w języku C i łączące się przy użyciu powiązań lokalnych. Jeśli planowane jest użycie aplikacji Java przy użyciu powiązań klienta, należy utworzyć magazyn kluczy JKS i certyfikaty przy użyciu komendy **keytool** , która jest częścią środowiska JRE (więcej informacji na ten temat zawiera sekcja “Szybki start produktu AMS z klientami Java” na stronie 686). W przypadku wszystkich innych języków oraz w przypadku aplikacji Java korzystających z powiązań lokalnych kroki 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:

   - Do zabezpieczenia bazy danych zaleca się użycie silnego hasła.
   - Parametr **stash** zapisuje hasło w pliku `key.sth` , który może być używany przez przechwytywacze do otwierania bazy danych.
2. Upewnij się, że baza danych kluczy jest dostępna do odczytu

   ```
   chmod +r /home/alice/.mqs/alicekey.kdb
   ```
3. Utwórz certyfikat identyfikujący użytkownika `alice` do 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:

   - Na potrzeby niniejszego podręcznika używany jest certyfikat samopodpisany, który można utworzyć bez użycia ośrodka certyfikacji. W systemach produkcyjnych zaleca się, aby nie używać certyfikatów samopodpisanych, ale polegać na certyfikatach podpisanych przez ośrodek certyfikacji.

- Parametr **label** określa nazwę certyfikatu, który przechwytywacze będą szukać w celu uzyskania niezbędnych informacji.
- Parametr **DN** określa szczegóły nazwy **Nazwa wyróżniająca** (DN), która musi być unikalna dla każdego użytkownika.

4. Teraz utworzyliśmy bazę danych kluczy, powinniśmy ustawić jej właściciela i upewnić się, 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 kroki 1-4 dla użytkownika bob

Wyniki

Każdy z tych dwóch użytkowników `alice` i bob ma teraz certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Należy wskazać przechwytywaczy Advanced Message Security katalog, w którym znajdują się bazy danych kluczy i certyfikaty. Odbywa się to za pośrednictwem pliku `keystore.conf` , który przechowuje te informacje w postaci zwykłego tekstu. Każdy użytkownik musi mieć osobny plik `keystore.conf` w folderze `.mqs` . Ten krok należy wykonać zarówno dla systemu `alice` , jak i dla systemu bob.

Treść pliku `keystore.conf` musi mieć następującą 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 700.
- HOME/`.mqs/keystore.conf` jest domyślnym położeniem, w którym program Advanced Message Security wyszukuje plik `keystore.conf` . Informacje na temat używania położenia innego niż domyślne dla `keystore.conf`zawiera sekcja “Używanie magazynów kluczy i certyfikatów z programem AMS” na stronie 699.

5. Udostępnianie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwiema bazami danych kluczy, aby każdy użytkownik mógł pomyślnie zidentyfikować drugą bazę danych. W tym celu należy wyodrębnić certyfikat publiczny każdego użytkownika do pliku, który jest następnie dodawany do bazy danych kluczy innego użytkownika.

Uwaga: Należy zachować ostrożność, używając opcji *extract* , a nie opcji *export* . Opcja *Wyodrębnij* pobiera klucz publiczny użytkownika, natomiast opcja *Eksportuj* pobiera zarówno klucz publiczny, jak i prywatny. Użycie *eksportu* przez pomyłkę mogłoby całkowicie naruszyć ochronę aplikacji, przekazując jej klucz prywatny.

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 pliku bob:

```
runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
bob_public.arm
```

4. Dodaj certyfikat dla bob do magazynu kluczy `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 mogą teraz pomyślnie identyfikować się nawzajem po utworzeniu i utworzeniu współużytkowanych certyfikatów samopodpisanych.

Co dalej

Sprawdź, czy certyfikat znajduje się w magazynie kluczy, uruchamiając następujące komendy, które wyświetlają 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

Po utworzeniu menedżera kolejek i przygotowaniu przechwytywaczy do przechwytywania komunikatów i kluczy szyfrowania dostępu można rozpocząć definiowanie strategii ochrony w systemie `QM_VERIFY_AMS` za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy zawiera sekcja setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Jest to przykład strategii zdefiniowanej dla kolejki `TEST.Q` . W tym przykładzie komunikaty są podpisywane przez użytkownika `alice` przy użyciu algorytmu Deprecated SHA1 i szyfrowane przy

użyciu 256-bitowego algorytmu 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 dokładnie zgodne z podanymi w odpowiednim certyfikacie użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wykonaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend `setmqspl` , należy użyć opcji `-export` . Pozwala to na przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testowanie konfiguracji

O tym zadaniu

Uruchamiając różne programy dla różnych użytkowników, 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 być inne miejsce.

   ```
   cd /opt/mqm/samp/bin
   ```

2. Przełącz użytkownika do uruchamiania 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 i naciśnij klawisz Enter.
5. Zatrzymaj działanie jako użytkownik `alice`

   ```
   exit
   ```

6. Przełącz użytkownika do uruchamiania jako użytkownik bob

   ```
   su bob
   ```

7. Jako użytkownik bob, uzyskaj komunikat przy użyciu przykładowej aplikacji:

   ```
   ./amqsget TEST.Q QM_VERIFY_AMS
   ```

Wyniki

Jeśli aplikacja została poprawnie skonfigurowana dla obu użytkowników, po uruchomieniu aplikacji pobierającej przez program bob zostanie wyświetlony komunikat użytkownika `alice` .

8. Testowanie szyfrowania

O tym zadaniu

Aby sprawdzić, czy szyfrowanie działa zgodnie z oczekiwaniami, należy utworzyć kolejkę aliasową, która odwołuje się do oryginalnej kolejki TEST.Q. Ta kolejka aliasowa nie będzie miała strategii bezpieczeństwa i dlatego żaden użytkownik nie będzie miał informacji potrzebnych do deszyfrowania komunikatu i dlatego zostaną wyświetlone zaszyfrowane dane.

Procedura

1. Za pomocą komendy **runmqsc** dla menedżera kolejek QM_VERIFY_AMS utwórz kolejkę aliasową.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Nadanie uprawnień bob do przeglądania z kolejki aliasowej

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Jako użytkownik `alice`umieść kolejny komunikat przy użyciu przykładowej aplikacji, tak jak wcześniej:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Jako użytkownik bobprzejrzyj komunikat za pomocą przykładowej aplikacji, używając kolejki aliasowej:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Jako użytkownik bobpobierz komunikat z kolejki lokalnej przy użyciu przykładowej aplikacji:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Wyniki

Dane wyjściowe z aplikacji `amqsbcg` będą zawierać zaszyfrowane dane, które znajdują się w kolejce, potwierdzając, że komunikat został zaszyfrowany.

z/OS *Przykładowe konfiguracje produktu AMS w systemie z/OS*

Ta sekcja zawiera przykładowe konfiguracje strategii i certyfikatów dla scenariuszy kolejkowania 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 obejmują wymagane strategie Advanced Message Security oraz certyfikaty cyfrowe, które muszą istnieć względem użytkowników i kluczy. W przykładach założono, że użytkownicy biorący udział w scenariuszach zostali skonfigurowani zgodnie z instrukcjami podanymi w sekcji Nadawanie użytkownikom uprawnień do zasobów dla produktu Advanced Message Security.

Dodatkowo, począwszy od wersji IBM MQ 9.1.3 , należy zapoznać się z przykładami przechwytywania kanału komunikatów między serwerami.

z/OS *Lokalne kolejkowanie komunikatów chronionych przez integralność dla produktu AMS w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje o strategiach i certyfikatach systemu Advanced Message Security , które są potrzebne do wysyłania i pobierania komunikatów chronionych integralnością do i z kolejki (lokalnie do aplikacji umieszczanych i pobieranych).

Przykładowy menedżer kolejek i kolejka to:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Używani są następujący użytkownicy:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Utwórz certyfikaty użytkowników

W tym przykładzie potrzebny jest tylko jeden certyfikat użytkownika. Jest to certyfikat użytkownika wysyłającego, który jest wymagany do podpisywania komunikatów chronionych przez integralność. Użytkownik wysyłający to 'TELLER5'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA). Certyfikat ośrodka CA jest certyfikatem ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, 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 RACDCERT systemu RACF . Ten certyfikat jest używany do wystawiania certyfikatów użytkowników. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, którego można następnie użyć do wystawienia certyfikatu 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 będzie zawierać procedury wyboru lub tworzenia certyfikatu ośrodka CA, a także procedury wydawania certyfikatów i dystrybuowania ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów program Advanced Message Security wymaga:

- Certyfikat ośrodka 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 komenda RACDCERT ADD może być używana do importowania certyfikatów z zestawu danych. Więcej informacji na temat tych i innych komend RACDCERT zawiera podręcznik *z/OS: Security Server RACF Command Language Reference*.

W tym przypadku certyfikaty są wymagane w systemie z/OS , w którym działa menedżer kolejek BNK6.

Po zaimportowaniu certyfikatów do systemu z/OS , na którym działa BNK6, 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 żaden certyfikat.

Połącz certyfikaty z odpowiednimi pliku kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane i zostały ustawione jako zaufane, muszą być połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS , na którym działa BNK6. Aby utworzyć pliki 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 WMQBNK6i pliku kluczy dla użytkownika wysyłającego 'TELLER5'. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie rozróżniana jest wielkość liter.

Po utworzeniu pliku kluczy można połączyć odpowiednie certyfikaty:

```
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))
```

Wysyłający certyfikat użytkownika musi być połączony jako DEFAULT. Jeśli użytkownik wysyłający ma więcej niż jeden certyfikat w pliku drq.ams.keyring, do podpisywania używany jest certyfikat domyślny.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez program Advanced Message Security do momentu zatrzymania i zrestartowania menedżera kolejek lub użycia komendy z/OS **MODIFY** do odświeżenia konfiguracji certyfikatu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH KEYRING
```

Tworzenie strategii Advanced Message Security

W tym przykładzie komunikaty chronione przez integralność są umieszczane w kolejce FIN.XFER.Q7 przez aplikację działającą jako użytkownik 'TELLER5' i pobraną z tej samej kolejki przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagana jest tylko jedna strategia Advanced Message Security .

Strategie Advanced Message Security są tworzone za pomocą programu narzędziowego CSQ0UTIL , który jest opisany 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 z nią 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 zrestartuj menedżer kolejek BNK6 lub użyj komendy z/OS **MODIFY** , aby odświeżyć konfigurację strategii Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Lokalne kolejkowanie komunikatów chronionych ochroną prywatności dla produktu AMS w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje o strategiach i certyfikatach systemu Advanced Message Security , które są potrzebne do wysyłania i pobierania komunikatów chronionych prywatności

do i z kolejki (lokalnie do aplikacji umieszczanych i pobieranych). Wiadomości chronione prywatnością są zarówno podpisane, jak i zaszyfrowane.

Poniżej przedstawiono przykładowy menedżer kolejek i kolejkę lokalną:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Używani są następujący użytkownicy:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Aby skonfigurować ten scenariusz, wykonaj następujące kroki:

Utwórz certyfikaty użytkowników

W tym przykładzie wymagane są dwa certyfikaty użytkownika. Są to certyfikat użytkownika wysyłającego, który jest potrzebny do podpisywania komunikatów, oraz certyfikat użytkownika odbierającego, który jest potrzebny do szyfrowania i deszyfrowania danych komunikatu. Użytkownik wysyłający to 'TELLER5', a użytkownik odbiorcy to 'FINADM2'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA jest certyfikatem ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, 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 RACDCERT systemu RACF . Ten certyfikat jest używany do wystawiania certyfikatów użytkowników. 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 użytkowników 'TELLER5' i 'FINADM2'. 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 będzie zawierać procedury wyboru lub tworzenia certyfikatu ośrodka CA, a także procedury wydawania certyfikatów i dystrybuowania ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów program Advanced Message Security wymaga:

- Certyfikat ośrodka 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 komenda RACDCERT ADD może być używana do importowania certyfikatów z zestawu danych. Więcej informacji na temat tych i innych komend RACDCERT zawiera sekcja RACDCERT (Zarządzanie certyfikatami cyfrowymi RACF) w publikacji *z/OS: Security Server RACF Command Language Reference*.

W tym przypadku certyfikaty są wymagane w systemie z/OS , w którym działa menedżer kolejek BNK6.

Po zaimportowaniu certyfikatów do systemu z/OS , na którym działa BNK6, 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 pliku kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane i zostały ustawione jako zaufane, muszą być połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS , na którym działa BNK6. Aby utworzyć pliki 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 i pliku kluczy dla użytkowników wysyłającego i odbierający. Należy pamiętać, że nazwa pliku kluczy `drq.ams.keyring` jest obowiązkowa, a w nazwie rozróżniana jest wielkość liter.

Po utworzeniu pliku kluczy można połączyć odpowiednie certyfikaty.

```
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 odbierjącego muszą być połączone jako domyślne. Jeśli użytkownik ma więcej niż jeden certyfikat w pliku drq.ams.keyring, do podpisywania i deszyfrowania używany jest certyfikat domyślny.

Certyfikat użytkownika odbiorcy musi być również połączony z pierścieniem kluczy użytkownika zadania Advanced Message Security za pomocą komendy USAGE (SITE). Dzieje się tak, ponieważ zadanie zaawansowanych zabezpieczeń komunikatów wymaga klucza publicznego odbiorcy podczas szyfrowania danych komunikatu. Komenda USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez program Advanced Message Security do momentu zatrzymania i zrestartowania menedżera kolejek lub użycia komendy z/OS **MODIFY** do odświeżenia konfiguracji certyfikatu Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH KEYRING
```

Tworzenie strategii Advanced Message Security

W tym przykładzie komunikaty chronione przez ochronę prywatności są umieszczane w kolejce FIN.XFER.Q8 przez aplikację działającą jako użytkownik 'TELLER5' i pobraną z tej samej kolejki przez aplikację działającą jako użytkownik 'FINADM2', dlatego wymagana jest tylko jedna strategia Advanced Message Security .

Strategie Advanced Message Security są tworzone za pomocą programu narzędziowego CSQ0UTIL , który jest opisany 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 z nią kolejka to FIN.XFER.Q8. Algorytm używany do generowania podpisu nadawcy to Deprecated SHA1, a nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US', a użytkownik odbierający to 'CN=FinAdm2,O=BCO,C=US'. Algorytmem używanym do szyfrowania danych komunikatu jest Deprecated 3DES.

Po zdefiniowaniu strategii zrestartuj menedżer kolejek BNK6 lub użyj komendy z/OS **MODIFY** , aby odświeżyć konfigurację strategii Advanced Message Security . Na przykład:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Zdalne kolejkowanie komunikatów chronionych przez integralność dla produktu AMS w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje o strategiach i certyfikatach produktu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów chronionych integralnością do i z 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 być uruchomiony w systemie rozproszonym z systemem 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 działającymi w różnych systemach z/OS .

Używani są następujący użytkownicy:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMStask user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Aby skonfigurować ten scenariusz, wykonaj następujące kroki:

Utwórz certyfikaty użytkowników

W tym przykładzie potrzebny jest tylko jeden certyfikat użytkownika. Jest to certyfikat użytkownika wysyłającego, który jest potrzebny do podpisania komunikatu zabezpieczonego przed integralnością. Użytkownik wysyłający to 'TELLER5'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA jest certyfikatem ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, 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 RACDCERT systemu RACF . Ten certyfikat jest używany do wystawiania certyfikatów użytkowników. Na przykład:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Ta komenda RACDCERT tworzy certyfikat ośrodka CA, którego można następnie użyć do wystawienia 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 będzie zawierać procedury wyboru lub tworzenia certyfikatu ośrodka CA, a także procedury wydawania certyfikatów i dystrybuowania ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów program Advanced Message Security wymaga:

- Certyfikat ośrodka 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 komenda RACDCERT ADD może być używana do importowania certyfikatów z zestawu danych. Więcej informacji na temat tych i innych komend RACDCERT zawiera sekcja RACDCERT (Zarządzanie certyfikatami cyfrowymi RACF) w publikacji *z/OS: Security Server RACF Command Language Reference*.

W tym przypadku certyfikaty są wymagane w systemie z/OS , w którym działa menedżer kolejek BNK6 i BNK7.

W tym przykładzie certyfikat wysyłający musi być zaimportowany do systemu z/OS , na którym działa BNK6, a certyfikat ośrodka CA musi być zaimportowany do systemu z/OS , na którym działa BNK7. Po zaimportowaniu certyfikatów 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 pliku kluczy

Po utworzeniu lub zaimportowaniu wymaganych certyfikatów i ustawieniu ich jako zaufanych muszą one być połączone z odpowiednimi pierścieniami kluczy użytkownika w systemie z/OS z uruchomionymi BNK6 i BNK7.

Aby utworzyć pliki kluczy, użyj komendy RACDCERT ADDRING w systemie BNK6:

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika wysyłającego w systemie BNK6. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie rozróżniana jest wielkość liter.

W systemie BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Spowoduje to utworzenie pliku kluczy dla użytkownika zadania Advanced Message Security w BNK7. Nie jest wymagany plik kluczy użytkownika dla 'TELLER5' w BNK7.

Po utworzeniu pliku kluczy można połączyć odpowiednie certyfikaty.

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))
```

Wysyłający certyfikat użytkownika musi być połączony jako DEFAULT. Jeśli użytkownik wysyłający ma więcej niż jeden certyfikat w pliku drq.ams.keyring, do podpisywania używany jest certyfikat domyślny.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez program Advanced Message Security do momentu zatrzymania i zrestartowania menedżera kolejek lub użycia komendy z/OS **MODIFY** do odświeżenia konfiguracji certyfikatu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Tworzenie strategii Advanced Message Security

W tym przykładzie komunikaty chronione przez integralność są umieszczane w kolejce zdalnej FIN.XFER.Q7 dla BNK6 przez aplikację uruchomioną jako użytkownik 'TELLER5' i pobraną z kolejki lokalnej FIN.RCPT.Q7 dla BNK7 przez aplikację uruchomioną jako użytkownik 'FINADM2', dlatego wymagane są dwie strategie Advanced Message Security .

Strategie Advanced Message Security są tworzone za pomocą programu narzędziowego CSQ0UTIL , który jest opisany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę w celu zdefiniowania strategii integralności dla kolejki zdalnej w 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 z nią 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 , aby uruchomić następującą komendę w celu zdefiniowania strategii integralności dla kolejki lokalnej w 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 z nią kolejka to FIN.RCPT.Q7. Oczekiwanym algorytmem podpisu nadawcy jest MD5, a nazwą wyróżniającą (DN) wysyłającego użytkownika jest '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 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 ochroną prywatności dla produktu AMS w systemie z/OS*

W tym przykładzie przedstawiono szczegółowe informacje o strategiach i certyfikatach systemu Advanced Message Security wymaganych do wysyłania i pobierania komunikatów chronionych prywatności do i z 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 być uruchomiony w systemie rozproszonym z systemem 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 działającymi w różnych systemach z/OS o tej samej nazwie.

Używani są następujący użytkownicy:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMS task user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

Aby skonfigurować ten scenariusz, wykonaj następujące kroki:

Utwórz certyfikaty użytkowników

W tym przykładzie wymagane są dwa certyfikaty użytkownika. Są to certyfikat użytkownika wysyłającego, który jest potrzebny do podpisywania komunikatów, oraz certyfikat użytkownika odbierającego, który jest potrzebny do szyfrowania i deszyfrowania danych komunikatu. Użytkownik wysyłający to 'TELLER5', a użytkownik odbiorcy to 'FINADM2'.

Wymagany jest również certyfikat ośrodka certyfikacji (CA).Certyfikat ośrodka CA jest certyfikatem ośrodka, który wystawił certyfikat użytkownika. Może to być łańcuch certyfikatów. Jeśli tak, 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 RACDCERT systemu RACF . Ten certyfikat jest używany do wystawiania certyfikatów użytkowników. 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 użytkowników 'TELLER5' i 'FINADM2'. 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 będzie zawierać procedury wyboru lub tworzenia certyfikatu ośrodka CA, a także procedury wydawania certyfikatów i dystrybuowania ich do odpowiednich systemów.

Podczas eksportowania i importowania tych certyfikatów program Advanced Message Security wymaga:

- Certyfikat ośrodka 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 komenda RACDCERT ADD może być używana do importowania certyfikatów z zestawu danych.

Więcej informacji na temat tych i innych komend RACDCERT zawiera sekcja RACDCERT (Zarządzanie certyfikatami cyfrowymi RACF) w publikacji *z/OS: Security Server RACF Command Language Reference*.

W tym przypadku certyfikaty są wymagane w systemie z/OS , w którym działa menedżer kolejek BNK6 i BNK7.

W tym przykładzie certyfikaty wysyłającego i odbierającego muszą zostać zaimportowane w systemie z/OS , w którym działa BNK6, a certyfikaty ośrodka CA i odbiorcy muszą zostać zaimportowane w systemie z/OS , w którym działa BNK7. Po zaimportowaniu certyfikatów 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 pliku kluczy

Jeśli wymagane certyfikaty zostały utworzone lub zaimportowane i ustawione jako zaufane, muszą być połączone z odpowiednimi pierścieniami kluczy użytkownika w systemach z/OS , na których działa BNK6 i BNK7.

Aby utworzyć pliki 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 i pliku kluczy dla użytkownika wysyłającego w BNK6. Należy zauważyć, że nazwa pliku kluczy drq.ams.keyring jest obowiązkowa, a w nazwie rozróżniana jest 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 i pliku kluczy dla użytkownika odbiorcy w BNK7.

Po utworzeniu pliku kluczy można połączyć odpowiednie certyfikaty.

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 odbierającego muszą być połączone jako domyślne. Jeśli użytkownik ma więcej niż jeden certyfikat w pliku drq.ams.keyring, do podpisywania i szyfrowania/deszyfrowania używany jest certyfikat domyślny.

W systemie BNK6certyfikat użytkownika odbiorcy musi być również połączony z pierścieniem kluczy użytkownika zadania Advanced Message Security za pomocą komendy USAGE (SITE). Dzieje się tak, ponieważ zadanie zaawansowanych zabezpieczeń komunikatów wymaga klucza publicznego odbiorcy podczas szyfrowania danych komunikatu. Komenda USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy.

Tworzenie i modyfikowanie certyfikatów nie jest rozpoznawane przez program Advanced Message Security do momentu zatrzymania i zrestartowania menedżera kolejek lub użycia komendy z/OS **MODIFY** do odświeżenia konfiguracji certyfikatu Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Tworzenie strategii Advanced Message Security

W tym przykładzie komunikaty chronione przez ochronę prywatności są umieszczane w kolejce zdalnej FIN.XFER.Q7 dla BNK6 przez aplikację uruchomioną jako użytkownik 'TELLER5' i pobraną z kolejki lokalnej FIN.RCPT.Q7 dla BNK7 przez aplikację uruchomioną jako użytkownik 'FINADM2', dlatego wymagane są dwie strategie Advanced Message Security .

Strategie Advanced Message Security są tworzone za pomocą programu narzędziowego CSQ0UTIL , który jest opisany w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

Użyj programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę w celu zdefiniowania strategii prywatności dla kolejki zdalnej w 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 z nią kolejka to FIN.XFER.Q7. Algorytm używany do generowania podpisu nadawcy to Deprecated SHA1, nazwa wyróżniająca (DN) użytkownika wysyłającego to 'CN=Teller5,O=BCO,C=US', a użytkownik odbierający to 'CN=FinAdm2,O=BCO,C=US'. Algorytmem używanym do szyfrowania danych komunikatu jest Deprecated 3DES.

Należy również użyć programu narzędziowego CSQ0UTIL , aby uruchomić następującą komendę w celu zdefiniowania strategii 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 z nią kolejka to FIN.RCPT.Q7. Oczekiwanym algorytmem podpisu nadawcy jest Deprecated SHA1, nazwą wyróżniającą (DN) wysyłającego użytkownika jest 'CN=Teller5,O=BCO,C=US', a odbiorcą jest

'CN=FinAdm2,O=BCO,C=US'. Algorytm używany do deszyfrowania danych komunikatu to Deprecated 3DES.

Po zdefiniowaniu dwóch strategii zrestartuj menedżery kolejek BNK6 i BNK7 lub użyj komendy z/OS **MODIFY** , aby odświeżyć konfigurację strategii Advanced Message Security . Na przykład:

W systemie BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

W systemie BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Szybki start produktu AMS z klientami Java

Ten podręcznik umożliwia szybkie skonfigurowanie produktu Advanced Message Security w celu zapewnienia bezpieczeństwa komunikatów dla aplikacji Java łączących się przy użyciu powiązań klienta. Przed jego wykonaniem zostanie utworzony magazyn kluczy służący do weryfikowania tożsamości użytkowników oraz zdefiniowane strategie podpisywania/szyfrowania dla menedżera kolejek.

Zanim rozpoczniesz

Upewnij się, że zostały zainstalowane odpowiednie komponenty zgodnie z opisem w publikacji **Szybki start** (Windows lub AIX and Linux).

1. Tworzenie menedżera kolejek i kolejki

O tym zadaniu

We wszystkich poniższych przykładach do przekazywania komunikatów między aplikacjami używana jest kolejka o nazwie TEST.Q . Produkt Advanced Message Security używa przechwytywaczy do podpisywania i szyfrowania komunikatów w punkcie, w którym są one wprowadzane do infrastruktury IBM MQ za pośrednictwem standardowego interfejsu IBM MQ . Podstawowa konfiguracja jest wykonywana w produkcie IBM MQ i jest konfigurowana w następujących krokach.

Procedura

1. Tworzenie menedżera kolejek

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Uruchom menedżer 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 aplikacji, za pośrednictwem którego będzie nawiązywane 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 programu TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Tworzenie i autoryzowanie użytkowników

O tym zadaniu

W tym scenariuszu występują dwaj użytkownicy: alice, nadawca i bob, odbiorca. Aby korzystać z kolejki aplikacji, użytkownicy ci muszą mieć nadane uprawnienia do jej używania. Ponadto, aby pomyślnie korzystać ze strategii ochrony zdefiniowanych w tym scenariuszu, użytkownicy ci muszą mieć dostęp do niektórych kolejek systemowych. Więcej informacji na temat komendy **setmqaut** zawiera sekcja **setmqaut**.

Procedura

1. Utwórz dwóch użytkowników zgodnie z opisem w publikacji **Szybki start** (Windows lub AIX and Linux) dla danej platformy.
2. Autoryzowanie użytkowników do nawiązywania połączenia z menedżerem kolejek i 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: Produkt IBM MQ optymalizuje wydajność, buforując strategie, dzięki czemu nie ma potrzeby przeglądania rekordów w poszukiwaniu szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Program IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Oznacza to, że jeśli dla menedżera kolejek zdefiniowano małą liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Należy jednak nadać uprawnienie do przeglądania tej kolejki w przypadku, gdy zdefiniowano dużą liczbę strategii lub gdy używane są stare klienty. SYSTEM SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach generowanych przez kod AMS. Uprawnienie do umieszczania dla tej kolejki jest sprawdzane tylko podczas próby umieszczenia komunikatu o błędzie w kolejce. Uprawnienia do

umieszczania w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki zabezpieczonej AMS.

Wyniki

Użytkownicy są teraz tworzeni i nadawane im są 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 691.

3. Tworzenie bazy danych kluczy i certyfikatów

O tym zadaniu

Aby zaszyfrować komunikat do przechwytywacza, wymagany jest klucz publiczny wysyłających użytkowników. Dlatego należy utworzyć bazę danych kluczy tożsamości użytkowników odwzorowanych na klucze publiczne i prywatne. W rzeczywistym systemie, w którym użytkownicy i aplikacje są rozproszone na kilku komputerach, każdy użytkownik miałby własny prywatny magazyn kluczy. Podobnie w tym podręczniku tworzone są bazy danych kluczy dla produktów `alice` i bob oraz współużytkowane między nimi certyfikaty użytkowników.

Uwaga: W tym podręczniku używane są aplikacje przykładowe napisane w języku Java i łączące się przy użyciu powiązań klienta. Jeśli planowane jest użycie aplikacji Java korzystających z powiązań lokalnych lub aplikacji C, należy utworzyć magazyn kluczy i certyfikaty CMS za pomocą komendy **runmqakm** . Zostało to przedstawione w publikacji **Szybki start** (Windows lub AIX and Linux).

Procedura

1. Utwórz katalog, w którym ma zostać utworzony magazyn kluczy, na przykład `/home/alice/.mqs`. Można go utworzyć w tym samym katalogu, który jest używany w publikacji **Szybki start** (Windows lub AIX and Linux) dla używanej platformy.

   Uwaga: W poniższych krokach ten katalog jest określany jako *katalog_magazynu_kluczy* .
2. Utwórz nowy magazyn kluczy i certyfikat identyfikujący 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 *katalog_magazynu_kluczy* zawiera spacje, należy ująć pełną nazwę magazynu kluczy w cudzysłów.
   - Zaleca się użycie silnego hasła do zabezpieczenia magazynu kluczy.
   - Na potrzeby niniejszego podręcznika używany jest certyfikat samopodpisany, który można utworzyć bez użycia ośrodka certyfikacji. W systemach produkcyjnych zaleca się, aby nie używać certyfikatów samopodpisanych, ale polegać na certyfikatach podpisanych przez ośrodek certyfikacji.
   - Parametr **alias** określa nazwę certyfikatu, który przechwytywacze będą szukać w celu uzyskania niezbędnych informacji.
   - Parametr **dname** określa szczegóły nazwy **Nazwa wyróżniająca** (DN), która musi być unikalna dla każdego użytkownika.
3. W systemie AIX and Linuxupewnij się, że magazyn kluczy jest dostępny do odczytu

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Powtórz step1-4 dla użytkownika bob

Wyniki

Każdy z tych dwóch użytkowników `alice` i bob ma teraz certyfikat samopodpisany.

4. Tworzenie pliku keystore.conf

O tym zadaniu

Należy wskazać przechwytywaczem Advanced Message Security katalog, w którym znajdują się bazy danych kluczy i certyfikaty. Jest to wykonywane za pośrednictwem pliku `keystore.conf` , który zawiera te informacje w postaci zwykłego tekstu. Każdy użytkownik musi mieć osobny plik `keystore.conf` . Ten krok należy wykonać zarówno dla systemu `alice` , jak i dla systemu 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 dostępny, ponieważ wykonano instrukcje zamieszczone w publikacji Szybki start (Windows lub AIX and Linux), można zmodyfikować istniejący plik, dodając odpowiednie wiersze.
- Więcej informacji na ten temat zawiera “Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf) dla systemu AMS” na stronie 700.

5. Współużytkowanie certyfikatów

O tym zadaniu

Współużytkuj certyfikaty między dwoma magazynami kluczy, aby każdy użytkownik mógł pomyślnie zidentyfikować drugi magazyn kluczy. Odbywa się to przez wyodrębnienie certyfikatu każdego użytkownika i zaimportowanie go do magazynu kluczy drugiego użytkownika.

Uwaga: Terminy *extract* i *export* są używane inaczej przez różne narzędzia certyfikatów. Na przykład narzędzie komendy IBM Global Security Kit (GSKit) **strmqikm** (ikeyman) rozróżnia *wyodrębnianie* certyfikatów (kluczy publicznych) i *eksportowanie* kluczy prywatnych. To rozróżnienie jest niezwykle ważne dla narzędzi, które oferują obie opcje, ponieważ użycie *eksportu* przez pomyłkę spowoduje całkowite naruszenie ochrony aplikacji przez przekazanie jej klucza prywatnego. Ponieważ rozróżnienie jest tak ważne, dokumentacja IBM MQ dąży do spójnego używania tych terminów. Jednak program Java keytool udostępnia opcję wiersza komend o nazwie *exportcert* , która wyodrębnia tylko klucz publiczny. Z tych powodów poniższa procedura odnosi się do *wyodrębniania* certyfikatów za pomocą 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 plik `alice` do magazynu kluczy, który będzie używany przez program bob . Po wyświetleniu monitu wskaż, 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 pliku bob .

Wyniki

Dwaj użytkownicy `alice` i bob mogą teraz pomyślnie identyfikować się wzajemnie po utworzeniu i utworzeniu współużytkowanych certyfikatów samopodpisanych.

Co dalej

Sprawdź, czy certyfikat znajduje się w magazynie kluczy, uruchamiając następujące komendy, które wyświetlają 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

Po utworzeniu menedżera kolejek i przygotowaniu przechwytywaczy do przechwytywania komunikatów i kluczy szyfrowania dostępu można rozpocząć definiowanie strategii ochrony w systemie `QM_VERIFY_AMS` za pomocą komendy `setmqspl` . Więcej informacji na temat tej komendy zawiera sekcja setmqspl . Każda nazwa strategii musi być taka sama, jak nazwa kolejki, do której ma zostać zastosowana.

Przykład

Poniżej przedstawiono przykład strategii zdefiniowanej w kolejce `TEST.Q` podpisanej przez użytkownika `alice` przy użyciu algorytmu Deprecated SHA1 i zaszyfrowanej przy użyciu 256-bitowego algorytmu 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 dokładnie zgodne z podanymi w odpowiednim certyfikacie użytkownika z bazy danych kluczy.

Co dalej

Aby sprawdzić zdefiniowaną strategię, wykonaj następującą komendę:

```
dspmqspl -m QM_VERIFY_AMS
```

Aby wydrukować szczegóły strategii jako zestaw komend `setmqspl` , należy użyć opcji `-export` . Pozwala to na przechowywanie już zdefiniowanych strategii:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

Zanim rozpoczniesz

Upewnij się, że w używanej wersji systemu Java są zainstalowane pliki nieograniczonej strategii JCE.

Uwaga: Wersja Java podana w instalacji IBM MQ zawiera już te pliki strategii. Można go znaleźć w katalogu *MQ_INSTALLATION_PATH*/java/bin.

O tym zadaniu

Uruchamiając różne programy dla różnych użytkowników, można sprawdzić, czy aplikacja została poprawnie skonfigurowana. Szczegółowe informacje na temat uruchamiania programów przez różnych użytkowników zawiera publikacja **Szybki start** (Windows lub AIX) dla danej platformy.

Procedura

1. Aby uruchomić te przykładowe aplikacje JMS , należy użyć ustawienia CLASSPATH dla używanej platformy, jak to pokazano w sekcji Zmienne środowiskowe używane przez produkt IBM MQ classes for JMS , aby upewnić się, że katalog przykładów został dołączony.
2. Jako użytkownik `alice`umieść komunikat przy użyciu przykładowej aplikacji, nawiązując połączenie jako klient:

   ```
   java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
   ```

3. Jako użytkownik bob, uzyskaj 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, po uruchomieniu aplikacji pobierającej przez program bob zostanie wyświetlony komunikat użytkownika `alice` .

Zabezpieczanie kolejek zdalnych w systemie AMS

Aby w pełni chronić kolejki zdalne, należy ustawić strategie w kolejce zdalnej i kolejce lokalnej, do której są przesyłane komunikaty.

Gdy komunikat jest umieszczany w kolejce zdalnej, produkt Advanced Message Security przechwytuje operację i przetwarza komunikat zgodnie z zestawem strategii dla kolejki zdalnej. Na przykład w przypadku strategii szyfrowania komunikat jest szyfrowany przed przekazaniem go do serwera IBM MQ w celu jego obsługi. Po przetworzeniu przez program Advanced Message Security komunikatu umieszczonego w kolejce zdalnej program IBM MQ umieszcza go w powiązanej kolejce transmisji i przekazuje do docelowego menedżera kolejek i kolejki docelowej.

Gdy operacja GET jest wykonywana na kolejce lokalnej, program Advanced Message Security próbuje zdekodować komunikat zgodnie ze strategią ustawioną w kolejce lokalnej. Aby operacja zakończyła się pomyślnie, strategia używana do deszyfrowania komunikatu musi być taka sama, jak strategia używana do szyfrowania komunikatu. Każda rozbieżność spowoduje odrzucenie komunikatu.

Jeśli z jakiegokolwiek powodu obie strategie nie mogą być ustawione w tym samym czasie, zapewniana jest obsługa etapowego propagacji. Strategię można ustawić w kolejce lokalnej z flagą tolerancji, która wskazuje, że strategia powiązana z kolejką może być ignorowana, gdy próba pobrania komunikatu z kolejki obejmuje komunikat, który nie ma ustawionej strategii bezpieczeństwa. W takim przypadku komenda GET spróbuje zdeszyfrować komunikat, ale zezwoli na dostarczenie niezaszyfrowanych komunikatów. W ten sposób strategie w kolejkach zdalnych mogą być ustawiane po zabezpieczeniu (i przetestowaniu) kolejek lokalnych.

Zapamiętaj: Usuń flagę tolerancji po zakończeniu propagacji Advanced Message Security .

Odsyłacze pokrewne
setmqspl (ustawienie strategii bezpieczeństwa)

Kierowanie chronionych komunikatów za pomocą programu AMS przy użyciu programu IBM Integration Bus

Produkt Advanced Message Security może chronić komunikaty w infrastrukturze, w której jest zainstalowany produkt IBM Integration Buslub WebSphere Message Broker 8.0.0.1 (lub nowszy). Przed zastosowaniem zabezpieczeń w środowisku IBM Integration Bus należy zapoznać się z istotą obu produktów.

O tym zadaniu

Produkt Advanced Message Security zapewnia kompleksową ochronę ładunku komunikatu. Oznacza to, że tylko podmioty określone jako poprawni nadawcy i odbiorcy wiadomości mogą je produkować lub odbierać. Oznacza to, że w celu zabezpieczenia komunikatów przepływających przez produkt IBM Integration Busmożna zezwolić produktowi IBM Integration Bus na przetwarzanie komunikatów bez znajomości ich treści (Scenariusz 1). lub sprawić, że autoryzowany użytkownik będzie mógł odbierać i wysyłać komunikaty (Scenariusz 2).

Scenariusz 1-produkt Integration Bus nie widzi treści komunikatu

Zanim rozpoczniesz

Program IBM Integration Bus powinien być połączony z istniejącym menedżerem kolejek. Zastąp symbol *QMgrName* nazwą istniejącego menedżera kolejek w kolejnych komendach.

O tym zadaniu

W tym scenariuszu Alicja umieszcza zabezpieczony komunikat w kolejce wejściowej `QIN`. Na podstawie właściwości komunikatu `routeTo`komunikat jest kierowany do obiektu *bob's* (`QBOB`),[1](`QCECIL`) lub domyślna kolejka (`QDEF`). Routing jest możliwy, ponieważ produkt Advanced Message Security chroni tylko ładunek komunikatu, a nie jego nagłówki i właściwości, które pozostają niechronione i mogą być odczytywane przez produkt IBM Integration Bus. Advanced Message Security jest używana tylko przez *alice*, *bob* i *cecil*. Nie jest konieczne instalowanie ani konfigurowanie go dla IBM Integration Bus.

Produkt IBM Integration Bus odbiera zabezpieczony komunikat z niezabezpieczonej kolejki aliasowej, aby uniknąć próby deszyfrowania komunikatu. Jeśli bezpośrednio korzystałaby z kolejki chronionej, komunikat zostałby umieszczony w kolejce DEAD LETTER jako niemożliwy do odszyfrowania. Komunikat jest kierowany przez IBM Integration Bus i dociera do kolejki docelowej bez zmian. Oznacza to, że jest on nadal podpisany przez oryginalnego autora (zarówno *bob* , jak i *cecil* akceptują tylko wiadomości wysłane przez *alice*) i chronione jak poprzednio (tylko *bob* i *cecil* mogą je odczytać). IBM Integration Bus umieszcza kierowany komunikat w niezabezpieczonym aliasie. Odbiorcy pobierają komunikat z zabezpieczonej kolejki wyjściowej, w której program AMS w sposób przezroczysty deszyfruje komunikat.

Procedura

1. Skonfiguruj *alice*, *bob* i *cecil* do używania Advanced Message Security zgodnie z opisem w publikacji **Szybki start** (Windows lub AIX).

   Upewnij się, że zostały wykonane następujące kroki:

   - Tworzenie i autoryzowanie użytkowników
   - Tworzenie bazy danych kluczy i certyfikatów
   - Tworzenie pliku keystore.conf
2. Należy udostępnić certyfikat *alice* produktowi *bob* i *cecyl*, aby produkt *alice* mógł być przez nie identyfikowany podczas sprawdzania podpisów cyfrowych komunikatów.

[1] cecil

W tym celu należy wyodrębnić certyfikat identyfikujący *alice* do pliku zewnętrznego, a następnie dodać wyodrębniony certyfikat do magazynów kluczy *bob* i *cecil* . Ważne jest, aby użyć metody opisanej w sekcji **Czynność 5. Udostępnianie certyfikatów** w publikacji **Szybki start** (Windows lub AIX).

3. Udostępnij certyfikaty *bob* i *cecil* dla *alice*, aby *alice* mogła wysyłać komunikaty 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 `QIN` w konfiguracji kwalifikującej się. Należy użyć identycznej 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 przyjęto strategię bezpieczeństwa, w której *alice* jest jedynym autoryzowanym nadawcą, a *bob* i *cecil* są odbiorcami.

6. Zdefiniuj kolejki aliasowe `AIN`, `ABOB` i `ACECIL` odwołujące się do kolejek lokalnych `QIN`, `QBOB` i `QCECIL` .

   ```
   DEFINE QALIAS(AIN) TARGET(QIN)
   ```

7. Sprawdź, czy konfiguracja zabezpieczeń dla aliasów podanych w poprzednim kroku jest nieobecna. W przeciwnym razie ustaw strategię na wartość NONE.

   ```
   dspmqspl -m QMgrName -p AIN
   ```

8. W produkcie IBM Integration Bus utwórz przepływ komunikatów, aby kierować komunikaty przychodzące do kolejki aliasowej `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 nazwę kolejki.
   b) Utwórz węzły `MQOutput` o nazwach `BOB`, `CECIL` i `DEF`oraz przypisz kolejki aliasowe `ABOB`, `ACECIL` i `ADEF` jako odpowiednie nazwy kolejek.
   c) Utwórz węzeł trasy i nazwij go `TEST`.
   d) Połącz węzeł `IN` z wejściowym punktem końcowym węzła `TEST` .
   e) Utwórz terminale wyjściowe bobi `cecil` dla węzła `TEST` .
   f) Połącz wyjściowy punkt końcowy `bob` z węzłem `BOB` .
   g) Połącz wyjściowy punkt końcowy `cecil` z węzłem `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 IBM Integration Bus .
10. Uruchomiony jako użytkownik `Alice` umieścił komunikat, który zawiera również właściwość komunikatu o nazwie `routeTo` z wartością `bob` lub `cecil`. Uruchomienie przykładowej aplikacji **amqsstm** pozwoli na wykonanie tej czynności.

```
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. Uruchom jako użytkownik *bob* , aby pobrać komunikat z kolejki QBOB przy użyciu przykładowej aplikacji **amqsget**.

Wyniki

Gdy użytkownik *alice* umieszcza komunikat w kolejce QIN , komunikat jest chroniony. Jest on pobierany w formie chronionej przez IBM Integration Bus z kolejki aliasowej AIN . IBM Integration Bus decyduje o tym, gdzie skierować komunikat, odczytując właściwość routeTo , która nie jest zaszyfrowana jako wszystkie właściwości. Program IBM Integration Bus umieszcza komunikat w odpowiednim niezabezpieczonym aliasie, unikając jego dalszej ochrony. Po odebraniu komunikatu *bob* lub *cecil* z kolejki jest on deszyfrowany i weryfikowany jest podpis cyfrowy.

Scenariusz 2-produkt Integration Bus może wyświetlać treść komunikatu

O tym zadaniu

W tym scenariuszu grupa osób może wysyłać komunikaty do IBM Integration Bus. Inna grupa jest uprawniona do odbierania komunikatów, które są tworzone przez program IBM Integration Bus. Transmisji między stronami i IBM Integration Bus nie można podsłuchiwać.

Należy pamiętać, że program IBM Integration Bus odczytuje strategie ochrony i certyfikaty tylko wtedy, gdy otwarta jest kolejka, dlatego należy przeładować grupę wykonawczą po wprowadzeniu zmian w strategiach ochrony, aby zmiany odniosły skutek.

```
mqsireload execution-group-name
```

Jeśli produkt IBM Integration Bus jest uznawany za autoryzowany podmiot uprawniony do odczytu lub podpisywania ładunku komunikatu, należy skonfigurować plik Advanced Message Security dla użytkownika uruchamiającego usługę IBM Integration Bus . Należy pamiętać, że nie musi to być ten sam użytkownik, który umieszcza/pobiera komunikaty w kolejkach, ani użytkownik tworzący i wdrażający aplikacje IBM Integration Bus .

Procedura

1. Skonfiguruj *alice*, *bob*, *cecil* i *dave* oraz użytkownika usługi IBM Integration Bus , aby użyć pliku Advanced Message Security zgodnie z opisem w **publikacji Szybki start** (Windows lub AIX).

   Upewnij się, że zostały wykonane następujące kroki:

   - Tworzenie i autoryzowanie użytkowników
   - Tworzenie bazy danych kluczy i certyfikatów
   - Tworzenie pliku keystore.conf
2. Udostępnij certyfikaty *alice*, *bob*, *cecil* i *dave* użytkownikowi usługi IBM Integration Bus .

   W tym celu wyodrębnij wszystkie certyfikaty identyfikujące *alice*, *bob*, *cecil* i *dave* do plików zewnętrznych, a następnie dodaj wyodrębnione certyfikaty do magazynu kluczy IBM Integration Bus . Ważne jest, aby użyć metody opisanej w sekcji **Czynność 5. Udostępnianie certyfikatów** w publikacji **Szybki start** (Windows lub AIX).
3. Udostępnij certyfikat użytkownika usługi IBM Integration Bus dla *alice*, *bob*, *cecil* i *dave*.

W tym celu należy użyć metody określonej w poprzednim kroku.

Uwaga: Użytkownicy *Alice* i *bob* muszą mieć certyfikat użytkownika usługi IBM Integration Bus , aby poprawnie szyfrować komunikaty. Użytkownik usługi IBM Integration Bus musi mieć certyfikaty *alice* i *bob* , aby można było zweryfikować autorów komunikatów. Użytkownik usługi IBM Integration Bus potrzebuje certyfikatów *cecil* i *dave* , aby zaszyfrować dla nich komunikaty. Komendy *cecil* i *dave* wymagają certyfikatu użytkownika usługi IBM Integration Bus , aby sprawdzić, czy komunikat pochodzi z pliku IBM Integration Bus.

4. Zdefiniuj kolejkę lokalną o nazwie IN i zdefiniuj strategię bezpieczeństwa z *alice* i *bob* jako autorami, 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 lokalną kolejkę o nazwie OUTi zdefiniuj strategię bezpieczeństwa z użytkownikiem usługi dla IBM Integration Bus określonego jako autor oraz *cecil* i *dave* określonego jako adresaci:

```
setmqspl -m QMgrName -p OUT -s MD5 -a "CN=broker,O=IBM,C=GB" -e AES256
-r "CN=cecil,O=IBM,C=GB" -r "CN=dave,O=IBM,C=GB"
```

6. W produkcie IBM Integration Bus utwórz przepływ komunikatów z węzłem MQInput i MQOutput . Skonfiguruj węzeł MQInput do korzystania z kolejki IN i węzeł MQOutput do korzystania z kolejki OUT .
7. Wdróż przepływ komunikatów w komponencie środowiska wykonawczego IBM Integration Bus .
8. Użytkownik *alice* lub *bob* umieścił komunikat w kolejce IN przy użyciu przykładowej aplikacji **amqsput**.
9. Uruchom jako użytkownik *cecil* lub *dave* pobierz komunikat z kolejki OUT przy użyciu przykładowej aplikacji **amqsget**.

Wyniki

Komunikaty wysyłane przez *alice* lub *bob* do kolejki wejściowej IN są szyfrowane i tylko IBM Integration Bus może je odczytać. IBM Integration Bus akceptuje tylko komunikaty z *alice* i *bob* , a następnie odrzuca wszystkie inne komunikaty. Zaakceptowane komunikaty są odpowiednio przetwarzane, a następnie podpisywane i szyfrowane za pomocą kluczy *cecil* i *Dave'a* przed umieszczeniem ich w kolejce wyjściowej OUT. Tylko komendy *cecil* i *dave* mogą je odczytywać, komunikaty niepodpisane przez IBM Integration Bus są odrzucane.

Używanie produktu Advanced Message Security z produktem Managed File Transfer

W tym scenariuszu wyjaśniono, w jaki sposób skonfigurować produkt Advanced Message Security w taki sposób, aby zapewnił prywatność komunikatów dla danych wysyłanych za pośrednictwem Managed File Transfer.

Zanim rozpoczniesz

Upewnij się, że komponent Advanced Message Security jest zainstalowany w instalacji IBM MQ udostępniającej kolejki używane przez produkt Managed File Transfer , które mają być chronione.

Jeśli agenty Managed File Transfer łączą się w trybie powiązań, upewnij się, że komponent IBM Global Security Kit (GSKit) jest zainstalowany w ich instalacji lokalnej.

O tym zadaniu

Jeśli przesyłanie danych między dwoma agentami Managed File Transfer zostanie przerwane, dane poufne mogą pozostać niezabezpieczone w bazowych kolejkach IBM MQ używanych do zarządzania przesyłaniem. W tym scenariuszu wyjaśniono sposób konfigurowania i używania produktu Advanced Message Security do ochrony takich danych w kolejkach Managed File Transfer .

W tym scenariuszu rozważamy prostą topologię składającą się z jednego komputera z dwiema kolejkami Managed File Transfer i dwoma agentami, AGENT1 i AGENT2, współużytkującymi pojedynczy menedżer kolejek, zgodnie z opisem w scenariuszu Scenariusz Managed File Transfer. Oba agenty łączą się w ten sam sposób, w trybie powiązań lub 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 Managed File Transfer Agent . Jeśli używane są własne nazwy użytkowników i grup, należy odpowiednio zmienić komendy.

O tym zadaniu

Produkt Advanced Message Security używa szyfrowania z kluczem publicznym do podpisywania i/lub szyfrowania komunikatów w chronionych kolejkach.

Uwaga:

- Jeśli agenty Managed File Transfer są uruchomione w trybie powiązań, komendy używane do utworzenia magazynu kluczy CMS (Cryptographic Message Syntax) są opisane w publikacji **Szybki start** (Windows lub AIX) dla danej platformy.
- Jeśli agenty Managed File Transfer działają w trybie klienta, komendy wymagane do utworzenia pliku JKS (Java Keystore) są opisane w sekcji “Szybki start produktu AMS z klientami Java” na stronie 686.

Procedura

1. Utwórz certyfikat samopodpisany, aby zidentyfikować użytkownika `ftagent` zgodnie z opisem w odpowiedniej publikacji 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 określić położenie magazynu kluczy i certyfikatu w nim zawartego, zgodnie z opisem w odpowiednim podręczniku Szybki start.

2. Konfigurowanie ochrony komunikatów

O tym zadaniu

Za pomocą komendy **setmqspl** należy zdefiniować strategię bezpieczeństwa dla kolejki danych używanej przez produkt AGENT2. W tym scenariuszu do uruchomienia obu agentów używany jest ten sam użytkownik, dlatego nazwa wyróżniająca osoby podpisującej i odbiorcy jest taka sama i zgodna z wygenerowanym certyfikatem.

Procedura

1. Zamknij agenty Managed File Transfer w ramach przygotowania do ochrony za pomocą komendy **fteStopAgent** .
2. Utwórz strategię bezpieczeństwa w celu ochrony kolejki 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 systemowej 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. Sprawdź, czy agenty zostały pomyślnie zrestartowane, używając komendy **fteListAgents** i sprawdzając, czy mają status READY .

Wyniki

Teraz można przesyłać przesyłanie z systemu AGENT1 do systemu AGENT2, a zawartość plików będzie bezpiecznie przesyłana między dwoma agentami.

Advanced Message Security instalacja, przegląd

Zainstaluj komponent Advanced Message Security na różnych platformach.

Procedura

- Zainstaluj produkt Advanced Message Security na wielu platformach.
- Zainstaluj produkt IBM MQ Advanced for z/OS.
- Zainstaluj produkt IBM MQ Advanced for z/OS Value Unit Edition.

Zadania pokrewne

Deinstalacja produktuAdvanced Message Security

z/OS Kontrola dla AMS w systemie z/OS

Advanced Message Security (AMS) for z/OS umożliwia opcjonalną kontrolę operacji wykonywanych przez aplikacje w kolejkach chronionych przez strategię. Jeśli ta opcja jest włączona, rekordy kontroli SMF (IBM System Management Facility) są generowane dla powodzenia i niepowodzenia tych operacji w kolejkach chronionych przez strategię. Do kontrolowanych operacji należą: MQPUT, MQPUT1i MQGET.

Kontrola jest domyślnie wyłączona, ale można ją aktywować, konfigurując opcje _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 określenia typu rekordu SMF i jest liczbą z zakresu od 128 do 255. Rekord SMF typu 180 jest zwykle typu 180, ale nie jest obowiązkowy. Kontrola jest wyłączana przez podanie wartości 0. Zmienna _AMS_SMF_AUDIT określa, czy rekordy kontroli są tworzone dla operacji, które się powiodły, operacji, które się nie powiodły, czy dla obu tych operacji. Opcje kontroli mogą być również dynamicznie zmieniane, gdy program AMS jest aktywny za pomocą komend operatora. Więcej informacji na ten temat zawiera sekcja Środowisko operacyjne Advanced Message Security.

Rekord SMF jest definiowany przy użyciu podtypów, a podtyp 1 jest ogólnym zdarzeniem kontroli. Rekord SMF zawiera wszystkie dane związane z przetwarzanym żądaniem.

Rekord SMF jest odwzorowywany przez makro CSQ0KSMF (zero w nazwie makra), które jest udostępniane w bibliotece docelowej SCSQMACS. W przypadku pisania programów redukcji danych dla danych SMF można dołączyć to makro odwzorowania, aby ułatwić programowanie i dostosowywanie procedur przetwarzania końcowego SMF.

W rekordach SMF generowanych 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 rekordu SMF jest zawsze obecna w rekordach generowanych przez produkt Advanced Message Security for z/OS. Sekcja danych różni się w zależności od podtypu. Obecnie zdefiniowany jest jeden podtyp i dlatego używana jest pojedyncza sekcja danych.

SMF został opisany w podręczniku z/OS System Management Facilities (SA22-7630). Poprawne typy rekordów są opisane w podzbiorze SMFPRMxx zestawu danych PARMLIB systemu. Więcej informacji na ten temat zawiera dokumentacja SMF.

Generator raportów kontroli Advanced Message Security (CSQ0USMF)

Produkt Advanced Message Security for z/OS udostępnia narzędzie generatora raportów kontroli o nazwie CSQ0USMF , które jest dostępne w bibliotece SCSQAUTH instalacji. Przykładowy kod JCL do uruchomienia programu narzędziowego CSQ0USMF o nazwie CSQ40RSM jest dostępny w bibliotece instalacyjnej SCSQPROC.

Przed uruchomieniem programu narzędziowego CSQ0USMF rekordy SMF typu 180 muszą zostać zrzucone 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 sprawdzić rzeczywiste nazwy zestawów danych SMF używane przez instalację. Docelowy zestaw danych dla zrzuconych rekordów musi mieć format rekordu VBS i długość rekordu 32760.

Uwaga: Jeśli używane są strumienie dziennika SMF, należy użyć programu IFASMFDL , aby zrzucić strumień dziennika do sekwencyjnego zestawu danych. Przykład użytego 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 wygenerowania raportu kontroli 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 parametry opcjonalne, które są wymienione w sekcji Tabela 104 na stronie 698:

Tabela 104. Opcjonalne parametry CSQ0USMF

Parametr	Wartość	Opis
TYP SMF	nnn	Typ rekordu SMF, który ma zastosowanie do raportu kontroli. Program CSQ0USMF używa tylko rekordów SMF zgodnych z wartością SMFTYPE podczas generowania raportu. Jeśli parametr SMFTYPE nie zostanie podany, zostanie użyta wartość domyślna 180.

Tabela 104. Opcjonalne parametry CSQ0USMF (kontynuacja)		
Parametr	**Wartość**	**Opis**
M	QMGR	Nazwa menedżera kolejek produktu IBM MQ , która 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.

Używanie magazynów kluczy i certyfikatów z programem AMS

Aby zapewnić aplikacjom IBM MQ przezroczystą ochronę kryptograficzną, program Advanced Message Security używa pliku kluczy, w którym przechowywane są certyfikaty klucza publicznego i klucz prywatny. W systemie z/OSzamiast pliku kluczy używany jest plik kluczy SAF.

W systemie 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 **nazwy wyróżniającej (DN)** podmiotu w certyfikacie, który jest powiązany z podpisanymi i zaszyfrowanymi komunikatami. Aby użytkownik lub aplikacja mogła szyfrować swoje komunikaty, musi mieć dostęp do pliku kluczy, w którym przechowywane są certyfikaty i powiązane z nimi klucze prywatne i publiczne.

W systemie AIX, Linux, and Windowspołożenie magazynu kluczy jest podane w pliku konfiguracyjnym magazynu kluczy, który domyślnie ma nazwę `keystore.conf` . Każdy użytkownik Advanced Message Security musi mieć plik konfiguracyjny magazynu kluczy, który wskazuje plik kluczy. Advanced Message Security akceptuje następujący format plików kluczy: `.kdb`, `.jceks`, `.jks`.

Domyślne położenie pliku `keystore.conf` to:

- Linux IBM i AIX W systemie IBM i: AIX and Linux: `$HOME/.mqs/keystore.conf`
- Windows W systemie Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Jeśli używana jest określona nazwa pliku kluczy i położenie, należy podać tę wartość w zmiennej środowiskowej **MQS_KEYSTORE_CONF** , jak pokazano w poniższych przykładowych komendach:

- W systemie Java: `java -D`*`MQS_KEYSTORE_CONF=path/filename app_name`*
- W przypadku klienta i serwera w języku C:
  - W systemie AIX and Linux: `export MQS_KEYSTORE_CONF=`*`path/filename`*
  - W systemie Windows: `set MQS_KEYSTORE_CONF=`*`path\filename`*

    Uwaga: Ścieżka w systemie Windows może i powinna określać literę napędu, jeśli dostępna jest więcej niż jedna litera napędu.

Ochrona poufnych informacji w pliku `keystore.conf`

Aby uzyskać dostęp do poufnych informacji pliku kluczy, takich jak hasła, należy podać znaczniki, aby serwer IBM MQ Advanced Message Security (AMS) mógł uzyskać dostęp do magazynu kluczy oraz podpisywać i szyfrować komunikaty.

Poufne informacje znajdujące się w pliku konfiguracyjnym magazynu kluczy należy chronić za pomocą komendy **runamscred** dostarczanej z produktem AMS. Szczegółowe informacje na temat zabezpieczania plików konfiguracyjnych zawiera sekcja “Konfigurowanie zabezpieczenia hasłem systemu AMS dla systemu pliki konfiguracyjne” na stronie 719 .

Podczas zabezpieczania haseł należy używać niestandardowego, silnego klucza szyfrowania. Aby uzyskać dostęp do haseł w czasie wykonywania, ten klucz szyfrowania należy podać w pliku AMS.

Istnieją dwie metody dostarczania położenia pliku klucza szyfrowania, które są dostępne za pośrednictwem:

- Właściwość konfiguracyjna **amscred.keyfile** w pliku `keystore.conf`
- **MQS_AMSCRED_KEYFILE** , zmienna środowiskowa

Kolejność wykonywania operacji jest następująca: **MQS_AMSCRED_KEYFILE**, po którym następuje łańcuch **amscred.keyfile**, a następnie klucz domyślny.

Pojęcia pokrewne

"Nazwy wyróżniające nadawców w produkcie AMS" na stronie 729
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 AMS" na stronie 731
Nazwy wyróżniające odbiorców identyfikują użytkowników, którzy mają uprawnienia 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:

AMSCRED
Parametry związane z systemem zabezpieczania hasłem.

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 MQ Adv. VUE **JCERACFKS,**
Java Cryptographic Encryption RACF keyring KeyStore, 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 z produktem AMS" na stronie 705.

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
V 9.3.0 pkcs11.encrypted = no
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
V 9.3.0 pem.encrypted = no
```

Java JKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
```

Java JCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
```

Java JCERACFKS,

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

Java PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
pkcs11.secondary_keystore_pass = password
pkcs11.encrypted = no
```

Tabela 105. Podsumowanie parametrów wymaganych dla każdego typu pliku konfiguracyjnego

Parametry	Wymagany	Typ pliku konfiguracyjnego				
		Java (PKCS#11, JKS, JCEKS i JCERACFKS)	**IBM i PEM**	**PKCS#11**	**CMS**	**AMSCRED**
keystore	✓	✓			✓	
IBM i private	✓		IBM i ✓			

Tabela 105. Podsumowanie parametrów wymaganych dla każdego typu pliku konfiguracyjnego (kontynuacja)

Parametry	Wymagany	Typ pliku konfiguracyjnego				
		Java (PKCS#11, JKS, JCEKS i JCERACFKS)	**IBM i PEM**	**PKCS#11**	**CMS**	**AMSCRED**
IBM i `public`	✓		IBM i ✓			
IBM i `password`	✓		IBM i ✓			
`library`	✓	✓		✓		
`certificate`	✓	✓		✓	✓	
`token`	✓	✓		✓		
`token_pin`	✓	✓		✓		
`secondary_keystore`	✓	✓		✓		
`secondary_keystore_password`	✓	✓				
`encrypted`		✓	V 9.3.0 IBM i ✓	V 9.3.0 ✓		
`keystore_pass`	✓	✓				
`key_pass`		✓				
`provider`		✓				
`keyfile`						✓ Użytkownik

Komentarze można dodawać za pomocą symbolu # .

Parametry pliku konfiguracyjnego są zdefiniowane w następujący sposób:

`keystore`
Tylko konfiguracja systemów CMS i Java .

Ścieżka do pliku kluczy dla konfiguracji CMS, JKS i JCEKS.

z/OS MQ Adv. VUE Identyfikator URI pliku kluczy RACF dla konfiguracji JCERACFKS.

Ważne:

- Ścieżka do pliku kluczy nie może zawierać rozszerzenia nazwy pliku.

- z/OS 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.

V 9.3.0 Pole to należy chronić za pomocą rodzimego narzędzia do zabezpieczania haseł systemu AMS ; patrz “Ochrona haseł” na stronie 704

library
Tylko PKCS#11 .

Nazwa ścieżki biblioteki PKCS#11 .

certificate
Tylko w konfiguracji CMS, PKCS#11 i Java .

Etykieta certyfikatu.

token
Tylko PKCS#11 .

Etykieta tokenu.

token_pin
Tylko PKCS#11 .

Numer PIN, aby odblokować token.

Tylko dla operacji Java ; należy chronić to pole za pomocą narzędzia do zabezpieczania haseł Java AMS ; patrz “Ochrona haseł” na stronie 704.

V 9.3.0 Tylko w przypadku operacji rodzimych; należy chronić to pole za pomocą rodzimego narzędzia do zabezpieczania haseł systemu AMS ; patrz sekcja “Ochrona haseł” na stronie 704.

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. Do tego magazynu kluczy CMS musi być dołączony plik ukrytych haseł, który musi znajdować się w tym samym katalogu, co dodatkowy magazyn kluczy.

W środowiskach Java wymagany jest magazyn kluczy JKS i należy podać parametr **secondary_keystore_password**.

secondary_keystore_password
Tylko Java PKCS#11 .

Hasło do magazynu kluczy JKS podanego we właściwości `secondary_keystore` . Pole to należy chronić za pomocą narzędzia do zabezpieczania hasłem systemu Java AMS ; patrz sekcja “Ochrona haseł” na stronie 704.

encrypted

Java V 9.3.0 oraz, począwszy od IBM MQ 9.3.0, tylko PKCS#11 i IBM i PEM .

Status hasła.

keystore_pass

Tylko konfiguracja Java .

Hasło do pliku kluczy.

Tylko dla operacji Java . Pole to należy chronić za pomocą narzędzia do zabezpieczania hasłem systemu Java AMS ; patrz sekcja “Ochrona haseł” na stronie 704.

key_pass

Tylko konfiguracja Java .

Hasło dla klucza prywatnego użytkownika.

Tylko dla operacji Java ; należy chronić to pole za pomocą narzędzia do zabezpieczania haseł Java AMS ; patrz “Ochrona haseł” na stronie 704.

keyfile

Określa położenie klucza początkowego, który ma być używany podczas zabezpieczania lub deszyfrowania haseł zawartych w tym pliku konfiguracyjnym. Informacje na ten temat zawiera sekcja “Ochrona haseł” na stronie 704

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.

Ochrona haseł

Należy chronić hasła i inne poufne informacje zawarte w pliku `keystore.conf` . Więcej informacji na ten temat zawiera sekcja **runamscred**.

Przykład pliku `keystore.conf` :

```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configuration
jceks.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

“Konfigurowanie zabezpieczenia hasłem systemu AMS dla systemu pliki konfiguracyjne” na stronie 719
Przechowywanie haseł do plików kluczy i kluczy prywatnych w postaci jawnego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego produkt Advanced Message Security udostępnia narzędzie umożliwiające zaszyfrowanie tych haseł przy użyciu klucza użytkownika.

Obsługa środowisk JRE innych niżIBM z produktem AMS

Systemy IBM MQ classes for Java i IBM MQ classes for JMS obsługują Advanced Message Security działanie w przypadku uruchamiania ze środowiskami JRE innymi niżIBM .

Advanced Message Security (AMS) implementuje Cryptographic Message Syntax (CMS). Składnia CMS jest używana do cyfrowego podpisywania, tworzenia skrótu, uwierzytelniania lub szyfrowania dowolnej treści komunikatu.

W serwisie IBM MQ 9.0dział wsparcia Advanced Message Security w systemach IBM MQ classes for Java i IBM MQ classes for JMS używa pakietów Open Source Bouncy Castle do obsługi systemu CMS. Oznacza to, że te klasy mogą obsługiwać operację Advanced Message Security podczas działania ze środowiskami JRE innymi niżIBM .

W systemach wcześniejszych niż IBM MQ 9.0środowisko Advanced Message Security nie było obsługiwane w przypadku środowisk JRE innych niżIBM w klientach Java . Obsługa języka Advanced Message Security w systemach IBM MQ classes for Java i IBM MQ classes for JMS zależy od obsługi CMS udostępnianej specjalnie przez implementację IBM rozszerzenia Java Cryptography Extensions (JCE). Ze względu na to ograniczenie funkcjonalność była dostępna tylko w przypadku korzystania ze środowiska Java runtime environment (JRE), które obejmowało dostawcę Java JCE.

Położenie i numeracja wersji plików JAR Bouncy Castle

Pliki JAR Bouncy Castle, które są potrzebne do obsługi środowisk JRE innych niżIBM , są dołączane jako część pakietu instalacyjnego produktów IBM MQ classes for Java i IBM MQ classes for JMS .

Używane są następujące pliki JAR Bouncy Castle:

Plik JAR dostawcy, który ma podstawowe znaczenie dla operacji Bouncy Castle.

V 9.3.5 W przypadku pliku Continuous Delivery z katalogu IBM MQ 9.3.5ten plik JAR ma nazwę `bcprov-jdk18on.jar`.

LTS W systemach Long Term Support i Continuous Delivery przed IBM MQ 9.3.5ten plik JAR ma nazwę `bcprov-jdk15to18.jar`.

Plik JAR "PKIX", który zawiera obsługę operacji CMS używanych przez system Advanced Message Security.

V 9.3.5 W przypadku pliku Continuous Delivery z katalogu IBM MQ 9.3.5ten plik JAR ma nazwę `bcpkix-jdk18on.jar`.

LTS W systemach Long Term Support i Continuous Delivery przed IBM MQ 9.3.5ten plik JAR ma nazwę `bcpkix-jdk15to18.jar`.

Plik JAR programu narzędziowego "util", który zawiera klasy używane przez inne pliki JAR programu Bouncy Castle.

V 9.3.5 W przypadku pliku Continuous Delivery z katalogu IBM MQ 9.3.5ten plik JAR ma nazwę `bcutil-jdk18on.jar`.

LTS W systemach Long Term Support i Continuous Delivery przed IBM MQ 9.3.5ten plik JAR ma nazwę `bcutil-jdk15to18.jar`.

Zależności

Klasy IBM MQ 9.1 i nowsze zostały przetestowane ze środowiskami JRE firmy IBM i Oracle . Prawdopodobnie również działają poprawnie w dowolnym środowisku J2SE-compliant . Należy jednak zwrócić uwagę na następujące zależności:

- Brak zmian w konfiguracji Advanced Message Security .
- Klasy Bouncy Castle 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 podpisu, korzystają z funkcji udostępnianych 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 *nieograniczonej* strategii dla implementacji JCE środowiska JRE.

  Więcej informacji na ten temat zawiera dokumentacja środowiska JRE.

- Jeśli włączono zabezpieczenia Java :
  - Dodaj do aplikacji parametr `java.security.SecurityPermissioninsertProvider.BC` , aby klasy Bouncy Castle mogły być używane jako dostawca zabezpieczeń.
  - Nadaj uprawnienie `java.security.AllPermission` do plików JAR Bouncy Castle.

    V 9.3.5 W przypadku systemu Continuous Delivery z produktu IBM MQ 9.3.5są to następujące pliki:

    mq_install_dir`/java/lib/bcutil-jdk18on.jar`
    mq_install_dir`/java/lib/bcpkix-jdk18on.jar`
    mq_install_dir`/java/lib/bcprov-jdk18on.jar`

    LTS W systemach Long Term Support i Continuous Delivery przed IBM MQ 9.3.5

    mq_install_dir`/java/lib/bcutil-jdk15to18.jar`
    mq_install_dir`/java/lib/bcpkix-jdk15to18.jar`
    mq_install_dir`/java/lib/bcprov-jdk15to18.jar`

Pojęcia pokrewne

Co jest zainstalowane dla klas produktu IBM MQ dla usługi JMS
Co jest zainstalowane dla klas IBM MQ classes for Java

Multi Przechwytywanie agenta kanału komunikatów (MCA) i AMS

Przechwytywanie MCA umożliwia menedżerowi kolejek działającemu w ramach produktu IBM MQ selektywne włączanie strategii stosowanych dla kanałów połączeń serwera.

Przechwytywanie MCA umożliwia zaszyfrowanie i zdeszyfrowanie klientów pozostających poza produktem AMS nadal połączonych z menedżerem kolejek i ich komunikatów.

Przechwytywanie MCA ma na celu udostępnienie AMS możliwości, gdy produktu AMS nie można włączyć na kliencie. Należy zauważyć, że użycie przechwytywania MCA i klienta z włączoną obsługą AMSprowadzi do podwójnej ochrony komunikatów, która może być problematyczna w przypadku odbierania aplikacji. Więcej informacji na ten temat zawiera sekcja “Wyłączanie Advanced Message Security na kliencie” na stronie 709.

Uwaga: Przechwytywacze MCA nie są obsługiwane dla kanałów AMQP lub MQTT.

Plik konfiguracyjny magazynu kluczy

Domyślnie plik konfiguracyjny magazynu kluczy dla przechwytywania MCA ma nazwę `keystore.conf` i znajduje się w katalogu `.mqs` w ścieżce do katalogu HOME użytkownika, który uruchomił menedżer kolejek lub program nasłuchujący. Magazyn kluczy można również skonfigurować przy użyciu zmiennej środowiskowej MQS_KEYSTORE_CONF. Więcej informacji na temat konfigurowania magazynu kluczy AMS zawiera sekcja “Używanie magazynów kluczy i certyfikatów z programem AMS” na stronie 699.

Aby włączyć przechwytywanie MCA, należy podać nazwę kanału, który ma być używany w pliku konfiguracyjnym magazynu kluczy. W przypadku przechwytywania MCA można używać tylko magazynu kluczy typu cms.

Przykład konfigurowania przechwytywania MCA zawiera sekcja “Przykład przechwytywania MCA dla produktu AMS” na stronie 707 .

Ostrzeżenie: Należy przeprowadzić uwierzytelnianie i szyfrowanie klienta w wybranych kanałach, na przykład za pomocą SSL i SSLPEER lub CHLAUTH TYPE (SSLPEERMAP), aby zapewnić, że tylko autoryzowani klienci będą mogli łączyć się i korzystać z tej możliwości.

IBM i

Jeśli w przedsiębiorstwie używany jest program IBM i, a do podpisania certyfikatu wybrano komercyjny ośrodek certyfikacji (CA), program Digital Certificate Manager utworzy żądanie certyfikatu w formacie PEM (Privacy-Enhanced Mail). Należy przekazać żądanie do wybranego ośrodka CA.

W tym celu należy użyć następującej komendy, aby wybrać poprawny certyfikat dla kanału określonego w parametrze `channelname`:

```
pem.certificate.channel.channelname
```

Przykład przechwytywania MCA dla produktu AMS

Przykładowe zadanie dotyczące sposobu konfigurowania przechwytywania MCA produktu AMS .

Zanim rozpoczniesz

Ostrzeżenie: Należy przeprowadzić uwierzytelnianie i szyfrowanie klienta w wybranych kanałach, na przykład za pomocą SSL i SSLPEER lub CHLAUTH TYPE (SSLPEERMAP), aby zapewnić, że tylko autoryzowani klienci będą mogli łączyć się i korzystać z tej możliwości.

Jeśli w przedsiębiorstwie używany jest program IBM i, a do podpisania certyfikatu wybrano komercyjny ośrodek certyfikacji (CA), program Digital 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 w celu użycia przechwytywania MCA, a następnie weryfikowania konfiguracji.

Uwaga: Plik IBM MQzawiera przechwytywacze AMS i umożliwia ich dynamiczne włączanie w środowiskach wykonawczych klienta i serwera produktu MQ .

Ostrzeżenie:

- Zastąp symbol `userID` w kodzie identyfikatorem użytkownika.
- Poniższa procedura nie działa zgodnie z oczekiwaniami w produkcie IBM MQ , chyba że przechwytywanie AMS zostało zdezaktywowane na kliencie.

Procedura

1. Utwórz bazę danych kluczy i certyfikaty, używając następujących komend do utworzenia skryptu powłoki.

   Zmień również wartości **INSTLOC** i **KEYSTORELOC** lub uruchom wymagane komendy. Należy zauważyć, że może nie być konieczne tworzenie certyfikatu dla bob.

```
INSTLOC=/opt/mqm
KEYSTORELOC=/home/userID/var/mqm
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

runmqakm -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
runmqakm -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
runmqakm -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd \
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
```

```
runmqakm -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 dwiema bazami danych kluczy, aby każdy użytkownik mógł pomyślnie zidentyfikować drugą bazę danych.

   Ważne jest, aby użyć metody opisanej do współużytkowania certyfikatów w publikacji *Szybki start*dla platformy używanej w przedsiębiorstwie:

   Windows
   Czynność 5 Współużytkowanie certyfikatów

   AIX and Linux
   Czynność 5 Współużytkowanie certyfikatów

   Java klienty
   Czynność 5 Współużytkowanie certyfikatów

3. Utwórz plik `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
```

   Ostrzeżenie:

   a. Magazyn kluczy musi znajdować się w systemie, w którym znajduje się menedżer kolejek.
   b. Należy określić konkretny kanał dla produktu `cms.certificate` , aby włączyć interwencję agenta MCA, a następnie menedżer kolejek wykonuje operacje AMS w aplikacjach łączących się za pośrednictwem tego kanału z kolejkami z ustawionymi strategiami.

4. Tworzenie i uruchamianie menedżera kolejek `AMSQMGR1`
5. Zdefiniuj program nasłuchujący TCP, używając dostępnego numeru portu pod kontrolą menedżera kolejek (QMGR).

   Na przykład:

   ```
   DEFINE LISTENER(MY.LISTENER) TRPTYPE(TCP) PORT(14567) CONTROL(QMGR)
   ```

6. Uruchom program nasłuchujący i sprawdź, czy został uruchomiony poprawnie.

   Na przykład:

   ```
   START  LISTENER(MY.LISTENER)
   DISPLAY LSSTATUS(MY.LISTENER) PORT
   ```

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, aby zmienna środowiskowa MQS_KEYSTORE_CONF była dostępna dla menedżera kolejek.
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 można znaleźć w sekcji setmqspl i dspmqspl .

11. Ustaw zmienną środowiskową *MQSERVER* :

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Usuń strategię bezpieczeństwa i sprawdź wynik:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

13. Przejrzyj kolejkę z instalacji produktu IBM MQ 9.3 :

```
/opt/mq93/samp/bin/amqsbcg TESTQ AMSQMGR1
```

    Dane wyjściowe przeglądania zawierają komunikaty w formacie zaszyfrowanym.

14. 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
```

15. Uruchom program **amqsgetc** z poziomu instalacji produktu IBM MQ 9.3 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Pojęcia pokrewne

“Struktura pliku konfiguracyjnego magazynu kluczy (keystore.conf) dla systemu AMS” na stronie 700
Plik konfiguracyjny magazynu kluczy (`keystore.conf`) wskazuje Advanced Message Security położenie odpowiedniego magazynu kluczy.

Odsyłacze pokrewne

“Znane ograniczenia produktu AMS” na stronie 656
Istnieje pewna liczba opcji IBM MQ , które nie są obsługiwane lub mają ograniczenia dotyczące produktu Advanced Message Security.

Wyłączanie Advanced Message Security na kliencie

Należy wyłączyć IBM MQ Advanced Message Security (AMS), jeśli do nawiązania połączenia z menedżerem kolejek z wcześniejszej wersji produktu używany jest klient IBM MQ i zgłaszany jest błąd `2085 (MQRC_UNKNOWN_OBJECT_NAME)`.

O tym zadaniu

Funkcja IBM MQ Advanced Message Security (AMS) jest automatycznie włączana w kliencie IBM MQ i dlatego domyślnie klient próbuje sprawdzić strategie bezpieczeństwa dla obiektów w menedżerze kolejek.

Jeśli ten błąd jest zgłaszany podczas próby nawiązania połączenia z menedżerem kolejek z wcześniejszej wersji produktu, można wyłączyć program AMS w następujący sposób:

- W przypadku klientów systemu Java można to wykonać w jeden z następujących sposobów:
  - Przez ustawienie zmiennej środowiskowej **AMQ_DISABLE_CLIENT_AMS**.
  - Przez ustawienie właściwości systemowej Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - Używając właściwości **DisableClientAMS** w sekcji Security w pliku `mqclient.ini` .
- W przypadku klientów w języku C-przez ustawienie zmiennej środowiskowej **MQS_DISABLE_ALL_INTERCEPT**.

Uwaga: Zmiennej środowiskowej **AMQ_DISABLE_CLIENT_AMS** nie można używać dla klientów w języku C. Zamiast niej należy użyć zmiennej środowiskowej **MQS_DISABLE_ALL_INTERCEPT** .

Procedura

- Aby wyłączyć funkcję AMS na kliencie, należy użyć jednej z następujących opcji:

  AMQ_DISABLE_CLIENT_AMS, zmienna środowiskowa
  Tę zmienną należy ustawić w następujących przypadkach:

- Jeśli używane jest środowisko Java runtime environment (JRE) inne niż IBM Java runtime environment (JRE)
- Jeśli używany jest klient IBM MQ 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 działa aplikacja. Na przykład:

```
export AMQ_DISABLE_CLIENT_AMS=TRUE
```

Java właściwość systemowa com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS

W przypadku klientów systemów 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` po wywołaniu komendy Java :

V 9.3.0 JM 3.0 V 9.3.0
```
java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE
-cp <MQ_INSTALLATION_PATH>/java/lib/com.ibm.mq.jakarta.client.jar
my.java.applicationClass
```

JMS 2.0
```
java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/
java/lib/com.ibm.mq.allclient.jar  my.java.applicationClass
```

Alternatywnie można określić właściwość systemową Java w pliku konfiguracyjnym JMS (`jms.config`), jeśli aplikacja używa tego pliku.

MQS_DISABLE_ALL_INTERCEPT, zmienna środowiskowa

Tę zmienną środowiskową należy ustawić, jeśli produkt IBM MQ jest używany z rodzimymi klientami i konieczne jest wyłączenie funkcji 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 w języku C. W przypadku klientów systemu Java należy użyć zmiennej środowiskowej **AMQ_DISABLE_CLIENT_AMS** .

Właściwość `DisableClientAMS` w pliku `mqclient.ini`

Tej opcji można użyć dla klientów w systemach IBM MQ classes for JMS i IBM MQ classes for Java oraz dla klientów w języku C.

Dodaj nazwę właściwości `DisableClientAMS` w sekcji **`Security`** w pliku `mqclient.ini` , jak pokazano w poniższym przykładzie:

```
Security:
DisableClientAMS=Yes
```

Można również włączyć opcję AMS , jak pokazano 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 używania produktu AMS z produktem JMS.

Pojęcia pokrewne

“Przechwytywanie agenta kanału komunikatów (MCA) i AMS” na stronie 706

Przechwytywanie MCA umożliwia menedżerowi kolejek działającemu w ramach produktu IBM MQ selektywne włączanie strategii stosowanych dla kanałów połączeń serwera.

Zadania pokrewne

IBM MQ MQI client plik konfiguracyjny, `mqclient.ini`

Odsyłacze pokrewne

Plik konfiguracyjny IBM MQ classes for JMS

Wymagania dotyczące certyfikatów dla systemu AMS

Aby można było używać certyfikatów z produktem Advanced Message Security, muszą one mieć klucz publiczny RSA.

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 48.

Rozszerzenia użycia klucza

Rozszerzenia użycia klucza nakładają dodatkowe ograniczenia na sposób używania certyfikatu.

W systemie Advanced Message Securityużycie klucza certyfikatów X.509 v3 musi być ustawione zgodnie ze specyfikacją RFC 5280.

W celu zapewnienia integralności jakości ochrony, jeśli ustawiono rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać co najmniej jedną z dwóch następujących wartości:

- **`nonRepudiation`**
- **`digitalSignature`**

W celu zapewnienia jakości ochrony prywatności, jeśli ustawiono rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać:

- **`keyEncipherment`**

W celu zapewnienia jakości ochrony poufności, jeśli ustawiono rozszerzenia użycia klucza certyfikatu, zestaw ten musi zawierać:

- **`dataEncipherment`**

Rozszerzone użycie klucza dodatkowo precyzuje rozszerzenia użycia klucza. W przypadku wszystkich cech ochrony, jeśli ustawiono rozszerzone użycie klucza certyfikatu, zestaw musi zawierać:

- **`emailProtection`**

Pojęcia pokrewne

“Jakość ochrony w AMS” na stronie 732
Strategie ochrony danych Advanced Message Security implikują jakość ochrony (QOP).

Metody sprawdzania poprawności certyfikatów w programie AMS

Za pomocą programu Advanced Message Security można wykrywać i odrzucać odwołane certyfikaty, aby komunikaty w kolejkach nie były chronione przy użyciu certyfikatów, które nie spełniają standardów bezpieczeństwa.

Produkt AMS umożliwia sprawdzenie poprawności certyfikatu przy użyciu protokołu Online Certificate Status Protocol (OCSP) lub listy odwołań certyfikatów (CRL).

Produkt AMS można skonfigurować na potrzeby sprawdzania protokołu OCSP i/lub CRL. Jeśli obie metody są włączone, ze względu na wydajność produkt AMS najpierw używa protokołu OCSP do określania statusu odwołania. Jeśli status odwołania certyfikatu jest nieokreślony po sprawdzeniu OCSP, produkt AMS używa sprawdzania CRL.

Należy zauważyć, że sprawdzanie OCSP i CRL jest domyślnie włączone.

Pojęcia pokrewne

"Protokół OCSP (Online Certificate Status Protocol) w produkcie AMS" na stronie 712
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 domyślnie włączony.

"Listy odwołań certyfikatów (Certificate Revocation List-CRL) w programie AMS" na stronie 714
Listy CRL zawierają listę certyfikatów, które zostały oznaczone przez ośrodek certyfikacji (CA) jako niezaufane z różnych powodów, na przykład z powodu utraty lub naruszenia ochrony klucza prywatnego.

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 domyślnie włączony.

Protokół OCSP nie jest obsługiwany w systemach IBM i .

Włączanie sprawdzania OCSP w rodzimych przechwytywaczach produktu Advanced Message Security
Sprawdzanie protokołu OCSP (Online Certificate Status Protocol) w produkcie Advanced Message Security jest domyślnie włączone na podstawie informacji w używanych certyfikatach.

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego magazynu kluczy:

Uwaga: Wszystkie sekcje OCSP są opcjonalne i mogą być określane niezależnie.

Opcja	Opis
`ocsp.enable=off`	Włącz sprawdzanie OCSP, jeśli sprawdzany certyfikat ma rozszerzenie AIA (Authority Info Access) z metodą dostępu PKIX_AD_OCSP zawierającą identyfikator URI miejsca, w którym znajduje się program odpowiadający OCSP. Możliwe wartości: on lub `off`.
`ocsp.url=`*`responder_URL`*	Adres URL modułu odpowiadającego OCSP. Jeśli ta opcja zostanie pominięta, sprawdzanie OCSP bez AIA jest wyłączone.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	Adres URL serwera proxy OCSP. Jeśli ta opcja zostanie pominięta, serwer proxy nie będzie używany do sprawdzania certyfikatów w trybie z połączeniem bez obsługi AIA.
`ocsp.http.proxy.port=`*`port_number`*	Numer portu serwera proxy OCSP. Jeśli ta opcja zostanie pominięta, zostanie użyty domyślny port 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 jest nieosiągalny w okresie limitu czasu. Możliwe wartości: • `ACCEPT` Zezwala na certyfikat • `WARN` Umożliwia zarejestrowanie certyfikatu i ostrzeżenia. • `REJECT` Uniemożliwia używanie certyfikatu i rejestruje błąd.

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 OCSP w produkcie Advanced Message Security:

Korzystanie z interfejsu java.security
Sprawdź, czy certyfikat zawiera rozszerzenie certyfikatu AIA (Authority Information Access).

Procedura

1. Jeśli aplikacja AIA nie jest skonfigurowana lub certyfikat ma zostać nadpisany, zmodyfikuj plik `$JAVA_HOME/lib/security/java.security` , wprowadzając następujące właściwości:

   ```
   ocsp.responderURL=http://url.to.responder:port
   ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
   ```

   i włącz sprawdzanie OCSP, edytując plik `$JAVA_HOME/lib/security/java.security` w następującym wierszu:

   ```
   ocsp.enable=true
   ```

2. Jeśli skonfigurowano funkcję AIA, włącz sprawdzanie OCSP, edytując plik `$JAVA_HOME/lib/security/java.security` w następującym wierszu:

   ```
   ocsp.enable=true
   ```

Co dalej

Jeśli używany jest program Java Security Manager, należy dodać następujące uprawnienie Java do pliku `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 konfigurację, należy dodać następujące uprawnienia Java do pliku `lib/security/java.policy`:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Listy odwołań certyfikatów (Certificate Revocation List-CRL) w programie AMS

Listy CRL zawierają listę certyfikatów, które zostały oznaczone przez ośrodek certyfikacji (CA) jako niezaufane z różnych powodów, na przykład z powodu utraty lub naruszenia ochrony klucza prywatnego.

Aby sprawdzić poprawność certyfikatów, program Advanced Message Security tworzy łańcuch certyfikatów składający się z certyfikatu osoby podpisującej i łańcucha certyfikatów ośrodka certyfikacji (CA) aż do bazy zaufania. Baza zaufania to zaufany plik magazynu kluczy, który zawiera zaufany certyfikat lub zaufany certyfikat główny używany do potwierdzania zaufania certyfikatu. Program AMS weryfikuje ścieżkę certyfikatu przy użyciu algorytmu sprawdzania poprawności PKIX. Gdy łańcuch jest tworzony i weryfikowany, program AMS kończy sprawdzanie poprawności certyfikatu, które obejmuje sprawdzanie poprawności wydania i daty ważności każdego certyfikatu w łańcuchu w odniesieniu do bieżącej daty, sprawdzając, czy rozszerzenie użycia klucza jest obecne w certyfikacie jednostki końcowej. Jeśli rozszerzenie jest dołączone do certyfikatu, AMS sprawdza, czy ustawiono również **digitalSignature** lub **nonRepudiation** . Jeśli nie są, raportowana i rejestrowana jest wartość `MQRC_SECURITY_ERROR` . Następnie program AMS pobiera listy CRL z plików lub z katalogu LDAP w zależności od wartości podanych w pliku konfiguracyjnym. AMSobsługuje tylko te listy CRL, które są zakodowane w formacie DER. Jeśli w pliku konfiguracyjnym magazynu kluczy nie znaleziono konfiguracji związanej z listą CRL, program AMS nie wykonuje sprawdzenia poprawności listy CRL. Dla każdego certyfikatu ośrodka CA program AMS wysyła do LDAP zapytanie o listy CRL przy użyciu nazw wyróżniających ośrodka CA. Zapytanie LDAP zawiera następujące atrybuty:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Uwaga: Opcja `deltaRevocationList` jest obsługiwana tylko wtedy, gdy jest określona jako punkty rozkładu.

Włączanie obsługi sprawdzania poprawności certyfikatów i listy odwołań certyfikatów w przechwytywaczach rodzimych
Należy zmodyfikować plik konfiguracyjny magazynu kluczy, aby program Advanced Message Security mógł pobierać pliki CLR z serwera LDAP (Lightweight Directory Access Protocol).

O tym zadaniu

IBM i Włączanie obsługi sprawdzania poprawności certyfikatów i listy odwołań certyfikatów w przechwytywaczach rodzimych nie jest obsługiwane w systemie Advanced Message Security na platformie IBM i.

Procedura

Dodaj następujące opcje do pliku konfiguracyjnego:

Uwaga: Wszystkie sekcje CRL są opcjonalne i można je określić 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 do zapewnienia przezroczystego przełączania awaryjnego w przypadku awarii połączenia LDAP. Oczekuje się, że wszystkie serwery LDAP są replikami i zawierają te same dane. Jeśli przechwytywacz produktu AMS Java pomyślnie nawiąże połączenie z serwerem LDAP, nie będzie próbował pobrać list CRL z pozostałych udostępnionych serwerów.
`crl.cdp=off`	Użyj tej opcji, aby sprawdzić lub użyć 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 dostępne do odczytu dla całego świata.
`crl.ldap.pass=`*`password`*	Hasło dla serwera LDAP.
V 9.3.0 `crl.ldap.encrypted=`*`no/yes`*	Określa, czy plik `clr.ldap.pass` jest zaszyfrowany. Więcej informacji na ten temat zawiera sekcja Ochrona haseł w plikach konfiguracyjnych AMS .
`crl.ldap.cache_lifetime=0`	Czas ważności pamięci podręcznej LDAP w sekundach. Możliwe wartości: 0-86400.
`crl.ldap.cache_size=50`	Wielkość pamięci podręcznej LDAP. Tę opcję można podać tylko wtedy, gdy wartość parametru `crl.ldap.cache_lifetime` jest większa niż `0`.
`crl.http.proxy.host=some.host.com`	Port serwera proxy HTTP dla pobierania listy CRL CDP.
`crl.http.proxy.port=8080`	Numer portu serwera proxy HTTP.

Opcja	Opis
`crl.http.max_response_size=204800`	Maksymalna wielkość listy CRL (w bajtach), która może zostać pobrana z serwera HTTP akceptowanego przez program IBM Global Security Kit (GSKit).
`crl.http.timeout=30`	Czas oczekiwania na odpowiedź serwera (w sekundach), po którym upłynie limit czasu oczekiwania AMS .
`crl.http.cache_size=0`	Wielkość pamięci podręcznej HTTP w bajtach.
`crl.unknown=ACCEPT`	Definiuje zachowanie, gdy serwer CRL jest nieosiągalny w określonym limicie czasu. Możliwe wartości: • `ACCEPT` Zezwala na certyfikat • `WARN` Umożliwia zarejestrowanie certyfikatu i ostrzeżenia. • `REJECT` Uniemożliwia używanie certyfikatu i rejestruje błąd.

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 do zapewnienia przezroczystego przełączania awaryjnego w przypadku awarii połączenia LDAP. Oczekuje się, że wszystkie serwery LDAP są replikami i zawierają te same dane. Jeśli przechwytywacz produktu AMS Java pomyślnie nawiąże połączenie z serwerem LDAP, nie będzie próbował pobrać list CRL z pozostałych udostępnionych serwerów. 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 katalogu LDAP muszą być dostępne do odczytu dla całego świata.
`crl.cdp=on/off`	Użyj tej opcji, aby sprawdzić lub użyć rozszerzeń CRLDistributionPoints w certyfikatach.

2. Zmodyfikuj plik `JRE/lib/security/java.security` , wprowadzając następujące właściwości:

Nazwa właściwości	Opis
com.ibm.security.enableCRLDP	Ta właściwość przyjmuje następujące wartości: true, false. Jeśli ma wartość true, podczas sprawdzania odwołań certyfikatów listy CRL są lokalizowane przy użyciu URL z rozszerzenia punktów dystrybucji CRL certyfikatu. Jeśli ma wartość false lub nie jest ustawiona, sprawdzanie CRL przy użyciu 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 na wartość wyrażoną w sekundach. Wartość 0 wyłącza pamięć podręczną; -1 oznacza nieograniczony czas życia. Jeśli nie jest ustawiony, domyślny czas życia wynosi 30 sekund.
com.ibm.security.enableAIAEXT	Ta właściwość przyjmuje następujące wartości: true, false. Jeśli ma wartość true, wszystkie rozszerzenia Authority Information Access, 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 i dodawany do kolekcji CertStores , która jest używana do znajdowania innych certyfikatów wymaganych do zbudowania ścieżki certyfikatu. Jeśli ma wartość false lub nie jest ustawiona, dodatkowe obiekty LDAPCertStore nie są tworzone.

z/OS *Włączanie list odwołań certyfikatów (CRL) w systemie z/OS*

Advanced Message Security obsługuje sprawdzanie listy odwołań certyfikatów (CRL) certyfikatów cyfrowych używanych do ochrony komunikatów danych.

O tym zadaniu

Jeśli ta opcja jest włączona, program Advanced Message Security będzie sprawdzać poprawność certyfikatów odbiorców, gdy komunikaty są umieszczane w kolejce chronionej przez ochronę prywatności, oraz sprawdzać poprawność certyfikatów nadawców, gdy komunikaty są pobierane z kolejki chronionej (integralność lub prywatność). Sprawdzenie poprawności w tym przypadku obejmuje sprawdzenie, czy odpowiednie certyfikaty nie są zarejestrowane w odpowiednim CRL.

Produkt Advanced Message Security używa usług IBM System SSL do sprawdzania poprawności certyfikatów nadawcy i odbiorcy. Szczegółową dokumentację dotyczącą sprawdzania poprawności certyfikatów SSL systemu można znaleźć w podręczniku z/OS Cryptographic Services System Secure Sockets Layer Programming .

Aby włączyć sprawdzanie listy CRL, należy określić położenie pliku konfiguracyjnego listy CRL za pomocą definicji danych CRLFILE DD w uruchomionym zadaniu JCL dla przestrzeni adresowej AMS. Przykładowy plik konfiguracyjny CRL, który można dostosować, znajduje się w pliku *thlqual*.SCSQPROC (CSQ40CRL). Ustawienia dozwolone w tym pliku są następujące:

Tabela 106. Advanced Message Security zmienne konfiguracyjne CRL		
Zmienna	**Poprawne wartości**	**Opis**
crl.ldap.host[.n]	*nazwa_hosta -or-hostname: port*	Adres IP/nazwa hosta serwera LDAP, który obsługuje 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 crl.ldap.user.

Można podać 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 do 10 nazw hostów. Jeśli nie zostanie podany numer portu dla serwerów LDAP, zostanie użyty numer portu określony przez parametr crl.ldap.port . Każdy serwer LDAP musi używać tej samej kombinacji crl.ldap.user/password w celu uzyskania dostępu.

Jeśli określono instrukcję CRLFILE DD, konfiguracja jest ładowana podczas inicjowania przestrzeni adresowej Advanced Message Security i włączone jest sprawdzanie CRL. Jeśli nie określono definicji danych CRLFILE, plik konfiguracyjny CRL jest niedostępny lub niepoprawny, sprawdzanie CRL jest wyłączone.

AMS wykonuje sprawdzanie listy CRL przy użyciu usług sprawdzania poprawności certyfikatów SSL systemu IBM w następujący sposób:

Tabela 107. Advanced Message Security sprawdzanie listy CRL		
Operacja	**Jakość ochrony**	**Sprawdzone certyfikaty**
PUT	Ochrona prywatności	Odbiorca/-y
GET	Integralność/prywatność	Nadawca

Jeśli operacja na komunikacie nie powiedzie się, sprawdzenie listy CRL Advanced Message Security wykonuje następujące działania:

Tabela 108. Advanced Message Security Działanie niepowodzenia sprawdzania listy CRL	
Operacja	**Sprawdzenie listy CRL nie powiodło się**
PUT	Komunikat nie jest umieszczany w kolejce docelowej. Do aplikacji zwracany jest kod zakończenia MQCC_FAILED i kod przyczyny MQRC_SECURITY_ERROR.

Tabela 108. Advanced Message Security Działanie niepowodzenia sprawdzania listy CRL (kontynuacja)	
Operacja	**Sprawdzenie listy CRL nie powiodło się**
GET	Komunikat jest usuwany z kolejki docelowej i przenoszony do kolejki błędów ochrony systemu. Do aplikacji zwracany jest kod zakończenia MQCC_FAILED i kod przyczyny MQRC_SECURITY_ERROR.

Produkt AMS for z/OS używa usług SSL systemu IBM do sprawdzania poprawności certyfikatów, w tym listy CRL i sprawdzania zaufania.

Program IBM MQ używa ustawień zabezpieczeń, w przypadku których sprawdzanie poprawności certyfikatu wymaga, aby można było skontaktować się z serwerem LDAP, ale nie wymaga zdefiniowania listy CRL.

Uwaga: Obowiązkiem administratorów jest zapewnienie dostępności odpowiednich usług LDAP i utrzymywanie wpisów CRL dla odpowiednich ośrodków certyfikacji.

Konfigurowanie zabezpieczenia hasłem systemu AMS dla systemu pliki konfiguracyjne

Przechowywanie haseł do plików kluczy i kluczy prywatnych w postaci jawnego tekstu stanowi zagrożenie dla bezpieczeństwa, dlatego produkt Advanced Message Security udostępnia narzędzie umożliwiające zaszyfrowanie tych haseł przy użyciu klucza użytkownika.

Zanim rozpoczniesz

Właściciel pliku `keystore.conf` musi upewnić się, że tylko właściciel pliku jest uprawniony do odczytu i zapisu pliku. Ochrona haseł opisana w tym temacie jest tylko dodatkową miarą ochrony. Ponadto należy wykonać tę procedurę w systemie chronionym.

V 9.3.0 Upewnij się, że dla typu klienta AMS , który będzie odczytywany plik konfiguracyjny, używany jest poprawny wariant **runamscred** . Jeśli klient AMS jest:

- Java klienta, należy użyć komendy Java **runamscred** , która znajduje się w katalogu `<IBM MQ installation root>/java/bin`
- Klient MQI, należy użyć komendy MQI **runmqascred** , która znajduje się w katalogu `<IBM MQ installation root>/bin`

Procedura

1. Zmodyfikuj pliki `keystore.conf` , aby zawierały wszystkie wymagane informacje, w tym hasła wymagające ochrony.

```
jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

2. Umieść klucz szyfrowania, aby zaszyfrować hasła w pliku dostępnym dla użytkownika chroniącego plik `keystore.conf` .

   V 9.3.0 Ten klucz musi być taki sam, jak ten, który będzie później używany przez klienta AMS :

```
ThisIsAnExampleEncryptionKey
```

3. Uruchom komendę **runamscred** , aby zabezpieczyć plik `keystore.conf` , podając plik klucza szyfrowania.

```
runamscred -f <location of keystore.conf> -sf <location of encryption keyfile>
```

4. Sprawdź, czy plik `keystore.conf` jest zabezpieczony i zawiera zaszyfrowane hasła.

Przykład

Poniższy przykład przedstawia, jak wygląda chroniony plik `keystore.conf` :

```
jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = yes
jceks.keystore_pass =
<AMS>1!62K/a4RinT+bks4RjFWx4A==!Vhi/RjIN2FH5qStUJ/0hsgKyn2IdMuhanemRRDrJq
HM=
jceks.key_pass =
<AMS>1!qmnxY++rsOUtZfDSgwcR1g==!VmWVREdVkNp1xYJstvuW64ph5vxxf7SPoqtsXxYh2
Tk=
jceks.provider = IBMJCE
```

Informacje pokrewne

runamscred: chroń słowa kluczowe AMS

z/OS Korzystanie z certyfikatów w systemie AMS na platformie z/OS

O tym zadaniu

Advanced Message Security implementuje trzy poziomy ochrony: integralność, poufność i prywatność.

W przypadku strategii integralności komunikaty są podpisywane przy użyciu klucza prywatnego nadawcy (aplikacji wykonującej komendę MQPUT). Integralność umożliwia wykrywanie modyfikacji komunikatu, ale sam tekst komunikatu nie jest szyfrowany.

W przypadku strategii poufności komunikat jest szyfrowany po umieszczeniu go w kolejce. Komunikat jest szyfrowany przy użyciu klucza symetrycznego i algorytmu określonego w odpowiedniej strategii Advanced Message Security . Sam klucz symetryczny jest szyfrowany przy użyciu klucza publicznego każdego odbiorcy (aplikacja wykonująca operację MQGET). Klucze publiczne są powiązane z certyfikatami przechowywanymi w plikach kluczy.

W przypadku strategii ochrony prywatności komunikaty są zarówno podpisane, jak i zaszyfrowane.

Jeśli aplikacja odbierająca wykonująca operację MQGET wykolejkuje komunikat chroniony prywatnością, komunikat ten musi zostać zdeszyfrowany. Ponieważ został zaszyfrowany przy użyciu klucza publicznego odbiorcy, musi zostać zdeszyfrowany przy użyciu klucza prywatnego odbiorcy znalezionego w pliku kluczy.

z/OS *Używanie plików kluczy SAF z systemem AMS w systemie z/OS*

Advanced Message Security (AMS) używa usług pliku kluczy SAF systemu z/OS do definiowania i zarządzania certyfikatami potrzebnymi do podpisywania i szyfrowania. Produkty zabezpieczające, które funkcjonalnie są równoważne produktom RACF , mogą być używane zamiast produktów RACF , jeśli zapewniają ten sam poziom obsługi.

Efektywne wykorzystanie pliku kluczy może zmniejszyć liczbę zadań administracyjnych wymaganych do zarządzania certyfikatami.

Po wygenerowaniu (lub zaimportowaniu) certyfikatu musi on być połączony z siecią kluczy, aby stał się dostępny. Ten sam certyfikat może być podłączony do więcej niż jednego pliku kluczy.

Program Advanced Message Security używa dwóch zestawów kluczy. Jeden zestaw zawiera pliki kluczy należące do poszczególnych identyfikatorów użytkowników, które są źródłem lub odbierają komunikaty. Każdy plik kluczy zawiera klucz prywatny powiązany z certyfikatem ID użytkownika będącego właścicielem. Klucz prywatny każdego certyfikatu jest używany do podpisywania komunikatów dla kolejek chronionych integralnością lub ochroną prywatności. Jest on również używany do deszyfrowania komunikatów z kolejek chronionych ochroną prywatności lub ochroną poufności podczas odbierania komunikatów.

Drugi zestaw to pojedynczy plik kluczy, którego właścicielem jest użytkownik przestrzeni adresowej AMS . Zawiera on łańcuch podpisujących certyfikatów CA niezbędnych do sprawdzenia poprawności certyfikatów nadawcy i odbiorców komunikatu.

Jeśli używana jest ochrona prywatności lub poufność, plik kluczy, którego właścicielem jest użytkownik przestrzeni adresowej AMS , zawiera również certyfikaty odbiorców komunikatów. Klucze publiczne w tych certyfikatach są używane do szyfrowania klucza symetrycznego, który był używany do szyfrowania danych komunikatu podczas umieszczania komunikatu w zabezpieczonej kolejce. Podczas pobierania 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 program Advanced Message Security używa nazwy pliku kluczy **drq.ams.keyring** . Dotyczy to zarówno pliku kluczy użytkownika, jak i pliku kluczy przestrzeni adresowej AMS .

Więcej informacji na temat certyfikatów i pliku kluczy oraz ich roli w ochronie danych zawiera sekcja Podsumowanie operacji związanych z certyfikatami.

Klucz prywatny używany do podpisywania może mieć dowolną etykietę, ale musi być połączony jako certyfikat domyślny. Przed raportem APAR PH44820klucz prywatny używany do deszyfrowania może mieć dowolną etykietę, ale musi być połączony jako certyfikat domyślny. Po zastosowaniu poprawki APAR PH44820 klucz prywatny lub klucze używane do deszyfrowania mogą mieć dowolną etykietę i muszą być połączone z pierścieniem kluczy, ale nie muszą być już połączone jako certyfikat domyślny.

Certyfikaty cyfrowe i pliki kluczy są zarządzane w produkcie RACF przede wszystkim za pomocą komendy RACDCERT.

Więcej informacji na temat certyfikatów, etykiet i komendy RACDCERT zawiera podręcznik *z/OS: Security Server RACF Command Language Reference* oraz podręcznik *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Zastępowanie certyfikatów*

Gdy certyfikat jest odnawiany lub zastępowany (na przykład, gdy istniejący certyfikat zbliża się do daty utraty ważności), nie zawsze jest możliwe usunięcie ochrony z istniejących komunikatów, które są już w kolejkach chronionych przez zasady poufności lub prywatności.

Taka sytuacja może wystąpić, gdy certyfikat:

- Odnowiono przy użyciu tego samego klucza prywatnego, a ponownie wystawiony certyfikat zastąpił oryginalny certyfikat
- Ponownie utworzono klucz prywatny z nowym kluczem prywatnym, a komenda RACDCERT ROLLOVER usunęła oryginalny klucz prywatny

W przypadku raportu APAR PH44820, gdy nowy certyfikat jest połączony z plikiem kluczy użytkownika jako certyfikat domyślny, nie jest już możliwe deszyfrowanie komunikatów zaszyfrowanych przy użyciu starego certyfikatu. Po zastosowaniu raportu APAR PH44820 komunikaty zostaną zdeszyfrowane, pod warunkiem, że niezbędny certyfikat jest połączony z plikiem kluczy użytkownika. Nie jest już wymagane połączenie domyślne. Umożliwia to pomyślne zdeszyfrowanie komunikatów znajdujących się już w kolejce po nawiązaniu połączenia z nowym certyfikatem.

W poniższym przykładzie przedstawiono sposób generowania nowego certyfikatu na podstawie istniejącego certyfikatu po zastosowaniu raportu APAR PH44820 :

- Nowy certyfikat jest tworzony na podstawie istniejącego certyfikatu z nową parą kluczy publiczny/prywatny.
- Nowy certyfikat jest podpisany przez organ wydający.
- Klucz publiczny starego certyfikatu jest usuwany z pliku kluczy przestrzeni adresowej AMS i dodawany jest klucz publiczny nowego certyfikatu.

- Oprócz starego certyfikatu do pliku kluczy użytkownika zostanie dodany nowy certyfikat i klucz prywatny.

```
RACDCERT ID(user1) REKEY(LABEL('user1'))          -
         WITHLABEL('user1new')

RACDCERT GENREQ(LABEL('user1new')) ID(user1)      -
         DSN(output_data_set_name)

RACDCERT GENCERT(output_data_set_name) ID(user1)  -
         SIGNWITH(CERTAUTH LABEL('AMSCA'))

RACDCERT ID(user1) ALTER (LABEL('user1new'))      -
         TRUST

RACDCERT ID(WMQAMSD) REMOVE(ID(user1)             -
         LABEL('user1')                           -
         RING(drq.ams.keyring)  )

RACDCERT ID(WMQAMSD) CONNECT(ID(user1)            -
         LABEL('user1new') USAGE(SITE)            -
         RING(drq.ams.keyring)  )

RACDCERT ID(user1) CONNECT(ID(user1)              -
         LABEL('user1new') USAGE(PERSONAL)        -
         RING(drq.ams.keyring) DEFAULT )
```

Więcej informacji na temat certyfikatów, etykiet i komendy RACDCERT zawiera podręcznik *z/OS: Security Server RACF Command Language Reference* oraz podręcznik *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Autoryzowanie dostępu do komendy RACDCERT dla systemu AMS na platformie z/OS*

Autoryzacja do używania komendy RACDCERT jest zadaniem poinstalacyjnym, które powinno zostać wykonane przez programistę systemu z/OS . To zadanie obejmuje nadanie odpowiednich uprawnień administratorowi zabezpieczeń systemu Advanced Message Security .

Podsumowując, aby umożliwić dostęp do komendy RACDCERT systemu RACF , należy wykonać następujące komendy:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

W tym przykładzie *admin* określa identyfikator administratora zabezpieczeń lub dowolnego użytkownika, który ma użyć komendy RACDCERT.

z/OS *Tworzenie certyfikatów i pliku kluczy dla użytkowników AMS w systemie z/OS*

W tej sekcji opisano kroki, które należy wykonać, aby utworzyć certyfikaty i pliki kluczy niezbędne dla użytkowników programu z/OS w systemie Advanced Message Security (AMS) przy użyciu ośrodka certyfikacji (CA) firmy RACF .

Rozwiązywanie problemów z certyfikatami podczas używania programu Advanced Message Security w systemie z/OS

Jeśli występują problemy z certyfikatami i brakującymi pozycjami w magazynach kluczy, można włączyć śledzenie GSKIT.

W pliku, do którego odwołuje się ENVARS DD 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 w pliku śledzenia określonym w parametrze GSK_TRACE_FILE.

Aby sformatować plik śledzenia, użyj komendy:

```
gsktrace inputtrace file > output_file
```

Scenariusz

Do wyjaśnienia wymaganych kroków używany jest scenariusz aplikacji wysyłającej i aplikacji odbierającej.

W poniższych przykładach user1 jest nadawcą komunikatu, a user2 jest odbiorcą. ID użytkownika przestrzeni adresowej Advanced Message Security to WMQAMSD.

Wszystkie komendy w przykładach przedstawionych w tym miejscu są wywoływane z opcji 6 narzędzia ISPF przez identyfikator administratora admin.

z/OS *Definiowanie lokalnego certyfikatu ośrodka certyfikacji dla systemu AMS w systemie z/OS*

Jeśli jako ośrodek CA używany jest program RACF , należy utworzyć certyfikat ośrodka certyfikacji (jeśli nie został jeszcze utworzony). Przedstawiona tutaj komenda tworzy certyfikat ośrodka certyfikacji (lub osoby podpisującej). W tym przykładzie tworzony jest certyfikat o nazwie AMSCA, który ma być używany podczas tworzenia kolejnych certyfikatów odzwierciedlających tożsamość użytkowników i aplikacji Advanced Message Security .

Ta komenda może zostać zmodyfikowana, w szczególności w pliku SUBJECTSDN, w celu odzwierciedlenia struktury i konwencji nazewnictwa używanych w danej 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 wystawcę CN=AMSCA, O=ibm, C=us na liście w komendzie RACDCERT LIST.

z/OS *Tworzenie certyfikatu cyfrowego z kluczem prywatnym dla AMS w systemie z/OS*

Dla każdego użytkownika Advanced Message Security musi zostać wygenerowany certyfikat cyfrowy z kluczem prywatnym. W przedstawionym przykładzie komendy RACDCERT są używane do generowania certyfikatów dla użytkowników user1 i user2podpisanych przy użyciu certyfikatu lokalnego ośrodka CA identyfikowanego 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 wymagana jest komenda RACDCERT ALTER. Gdy certyfikat jest tworzony po raz pierwszy za pomocą tej procedury, ma on inny zakres dat niż certyfikat podpisywania. W rezultacie program RACF oznacza go jako NOTRUST, co oznacza, że certyfikat nie ma być używany. Użyj komendy RACDCERT ALTER, aby ustawić atrybut TRUST.

Atrybuty KEYUSAGE HANDSHAKE, DATAENCRYPT i DOCSIGN muszą być określone dla certyfikatów używanych przez Advanced Message Security.

Tabela 109. Wartości i indykatory RACDCERT KEYUSAGE

Wartość KEYUSAGE	**Zestaw wskaźników**
uzgadnianie	digitalSignature i keyEncipherment
SZYFROWANIE danych	dataEncipherment
DOCSIGN	nonRepudiation
CERTOWANIE	keyCertPodpisz i cRLSign

z/OS *Tworzenie pliku kluczy RACF dla systemu AMS na platformie z/OS*

Przedstawione komendy tworzą plik kluczy dla zdefiniowanych przez RACFidentyfikatorów użytkowników user1, user2i użytkownika zadania przestrzeni adresowej Advanced Message Security WMQAMSD. Nazwa pliku kluczy jest ustalona przez 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 *Podłączanie certyfikatów do pliku kluczy dla systemu AMS w systemie z/OS*

Połącz certyfikaty użytkownika i ośrodka CA z pliku kluczy:

```
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))
```

Przed raportem APAR PH44820certyfikat zawierający klucz prywatny używany do deszyfrowania musi być połączony z certyfikatem domyślnym pliku kluczy użytkownika. Po zastosowaniu poprawki APAR PH44820 wszystkie certyfikaty zawierające klucz prywatny lub klucze używane do deszyfrowania muszą być połączone z pierścieniem kluczy użytkownika, ale nie muszą być już połączone jako certyfikat domyślny.

Atrybut RACDCERT USAGE (SITE) uniemożliwia dostęp do klucza prywatnego w pliku kluczy, natomiast atrybut RACDCERT USAGE (PERSONAL) umożliwia użycie klucza prywatnego, jeśli istnieje. Certyfikat użytkownika User2musi być podłączony do pliku kluczy przestrzeni adresowej Advanced Message Security , ponieważ jego klucz publiczny jest wymagany do szyfrowania komunikatów podczas ich umieszczania w kolejce. UŻYCIE (SITE) ogranicza narażenie na działanie klucza prywatnego użytkownika user2.

Certyfikat CERTAUTH z etykietą AMSCA musi być połączony z archiwum kluczy przestrzeni adresowej Advanced Message Security , ponieważ został użyty do podpisania certyfikatu użytkownika user1, który jest nadawcą komunikatu. Jest on używany do sprawdzania poprawności certyfikatu podpisującego użytkownika user1.

z/OS *Weryfikacja pliku kluczy dla AMS w systemie z/OS*

Po wprowadzeniu wszystkich komend plik kluczy powinien zostać wyświetlony w następujący sposób:

```
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
```

Lista poszczególnych certyfikatów zawiera również powiązanie pierścienia.

```
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 powiązanego z przestrzenią adresową AMS jest buforowana przez cały czas życia przestrzeni adresowej. Zmiany w tym pliku kluczy nie są automatycznie wprowadzane. Administrator może odświeżyć pamięć podręczną, korzystając z jednej z następujących możliwości:

- Zatrzymywanie i restartowanie menedżera kolejek.
- Za pomocą komendy z/OS MODIFY:

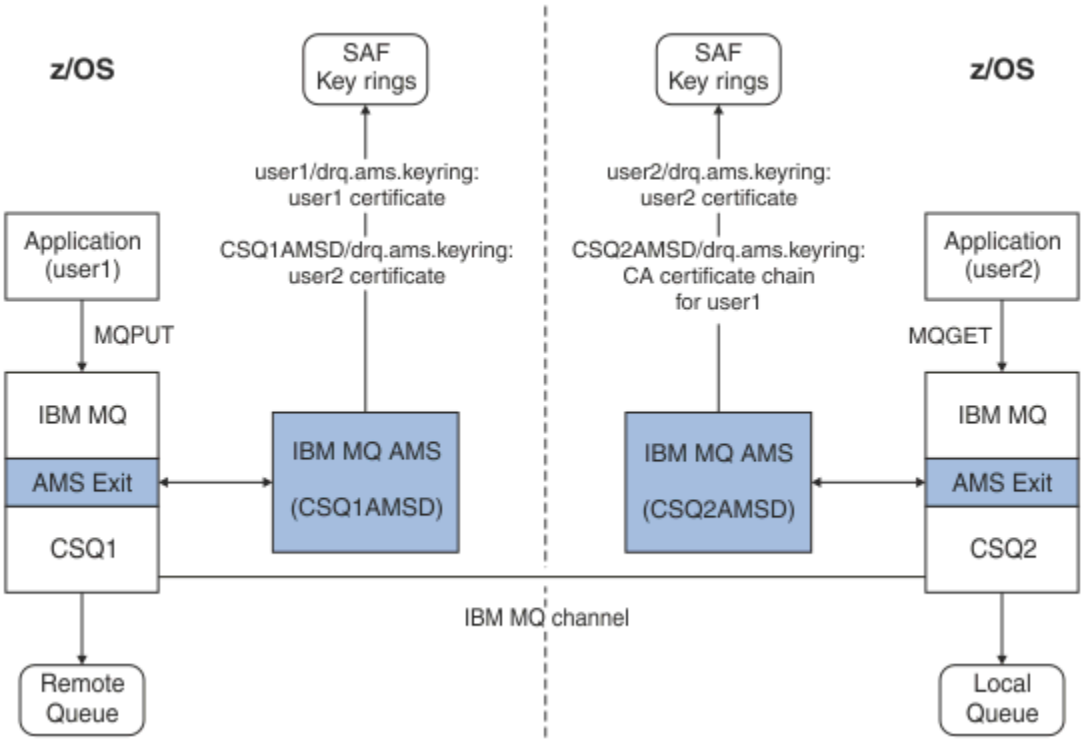
```
F qmgrAMSM,REFRESH KEYRING
```

Zadania pokrewne

System operacyjny Advanced Message Security

z/OS *Podsumowanie operacji związanych z certyfikatami dla AMS w systemie z/OS*

Na ilustracji Rysunek 35 na stronie 726 przedstawiono relacje między aplikacjami wysyłającymi i odbierającymi oraz odpowiednimi certyfikatami. Przedstawiony scenariusz obejmuje zdalne kolejkowanie między dwoma menedżerami kolejek systemu z/OS przy użyciu strategii ochrony danych o prywatności. W produkcie Rysunek 35 na stronie 726wartość "AMS" oznacza " Advanced Message Security".



Rysunek 35. Relacje aplikacji i certyfikatów

Na tym diagramie aplikacja działająca jako użytkownikuser1umieszcza komunikat w kolejce zdalnej zarządzanej przez menedżer kolejek CSQ1, która ma zostać pobrana przez aplikację działającą jako użytkownikuser2z kolejki lokalnej zarządzanej przez menedżer kolejek CSQ2. Na diagramie przyjęto strategię prywatności Advanced Message Security , która oznacza, że komunikat jest zarówno podpisany, jak i zaszyfrowany.

Advanced Message Security przechwytuje komunikat, gdy wystąpi operacja put i używa certyfikatu użytkownika user2(zapisanego w pliku kluczy użytkownika przestrzeni adresowej AMS) do zaszyfrowania klucza symetrycznego używanego do zaszyfrowania danych komunikatu.

Należy zauważyć, że certyfikat użytkownika user2jest połączony z siecią kluczy użytkownika przestrzeni adresowej AMS za pomocą opcji USAGE (SITE). Oznacza to, że użytkownik przestrzeni adresowej AMS może uzyskać dostęp do certyfikatu i klucza publicznego, ale nie do klucza prywatnego.

Na odbierającym końcu program Advanced Message Security przechwytuje komendę get wystawioną przez użytkownika user2i używa certyfikatu użytkownika user2do deszyfrowania klucza symetrycznego, aby mógł on deszyfrować dane komunikatu. Następnie sprawdza poprawność podpisu użytkownika user1za pomocą łańcucha certyfikatów CA certyfikatu użytkownika user1zapisanego w pliku kluczy użytkownika przestrzeni adresowej AMS.

W tym scenariuszu, ale ze strategią ochrony danych dotyczącą integralności, certyfikaty dla użytkownika user2 nie będą wymagane.

Aby można było używać produktu Advanced Message Security do wpisywania do kolejki komunikatów w kolejkach chronionych przez system IBM MQ, które mają strategię ochrony komunikatów o prywatności lub integralności, produkt Advanced Message Security musi mieć dostęp do następujących elementów danych:

- Certyfikat X.509 V2 lub V3 i klucz prywatny dla użytkownika umieszczającego komunikat w kolejce.
- Łańcuch certyfikatów używany do podpisywania certyfikatów cyfrowych wszystkich osób podpisujących komunikaty.
- Jeśli strategią ochrony danych jest ochrona prywatności, certyfikat X.509 V2 lub V3 adresatów. Zamierzeni odbiorcy są wyświetlani w strategii Advanced Message Security powiązanej z kolejką.

W przypadku procesów i aplikacji działających w systemie z/OSprogram Advanced Message Security musi mieć certyfikaty w dwóch miejscach:

- W pliku kluczy zarządzanym przez SAF powiązanym z tożsamością RACF aplikacji wysyłającej (aplikacji, która umieszcza w kolejce zabezpieczony komunikat) lub aplikacji odbierającej (jeśli używana jest ochrona prywatności).

  Certyfikat, który jest lokalizowany przez program Advanced Message Security , jest certyfikatem domyślnym i musi zawierać klucz prywatny. Advanced Message Security zakłada tożsamość użytkownika z/OS aplikacji wysyłającej. Oznacza to, że działa jako odpowiednik, więc może uzyskać dostęp do klucza prywatnego użytkownika.
- W pliku kluczy zarządzanym przez SAF powiązanym z użytkownikiem przestrzeni adresowej AMS.

  Podczas wysyłania wiadomości chronionych prywatnością ten plik kluczy zawiera certyfikaty kluczy publicznych odbiorców wiadomości. Podczas odbierania komunikatów zawiera on łańcuch certyfikatów ośrodka certyfikacji potrzebnych do sprawdzenia poprawności podpisu nadawcy komunikatu.

We wcześniejszych przykładach użyto RACF jako lokalnego ośrodka CA. Podczas instalacji można jednak użyć innego dostawcy infrastruktury PKI (ośrodka certyfikacji). Jeśli ma być używany inny produkt PKI, należy pamiętać, że klucz prywatny i certyfikat muszą zostać zaimportowane do pliku kluczy powiązanego z identyfikatorami użytkowników z/OS RACF , które pochodzą z komunikatów IBM MQ chronionych przez Advanced Message Security.

Komendy RACDCERT systemu RACF można użyć jako mechanizmu generowania żądań certyfikatów, które można wyeksportować i wysłać do wybranego dostawcy infrastruktury PKI w celu wystawienia.

Poniżej przedstawiono podsumowanie kroków związanych z certyfikatem:

1. Zażądaj utworzenia certyfikatu ośrodka CA, w którym RACF jest lokalnym ośrodkiem CA. Pomiń ten krok, jeśli używany jest inny dostawca infrastruktury PKI.
2. Wygeneruj certyfikaty użytkowników podpisane przez ośrodek CA.
3. Utwórz pliki kluczy dla użytkowników i identyfikator przestrzeni adresowej AMS Advanced Message Security .
4. Połącz certyfikat użytkownika z bazą kluczy użytkownika przy użyciu atrybutu domyślnego.
5. Połącz certyfikaty odbiorców z bazą danych Advanced Message Security kluczy użytkowników przestrzeni adresowej AMS za pomocą atrybutu usage (site) (Ten krok jest wymagany tylko dla certyfikatów użytkowników, które będą ostatecznie odbiorcami wiadomości chronionych prywatności).
6. Połącz łańcuchy certyfikatów CA dla nadawców komunikatów z bazą kluczy użytkowników przestrzeni adresowej AMS Advanced Message Security . (Ten krok jest wymagany tylko w przypadku zadań AMS, które będą weryfikować podpisy nadawcy).

z/OS *Konfigurowanie infrastruktury PKI rezydentnej innej niżz/OS dla systemu AMS*

Produkt Advanced Message Security dla systemu z/OSużywa certyfikatów cyfrowych X.509 V3 do zabezpieczania-przetwarzania komunikatów umieszczanych w kolejkach lub odbieranych z kolejek systemu IBM MQ . Sam produkt Advanced Message Security nie tworzy cyklu życia tych certyfikatów ani nie zarządza nim. Funkcja ta jest udostępniana przez infrastrukturę klucza publicznego (PKI). Przykłady w tej publikacji ilustrujące użycie certyfikatów używają serwera z/OS Security Server RACF do wypełniania żądań certyfikatów.

Niezależnie od tego, czy używana jest infrastruktura PKI rezydentna w systemie z/OS lub innym niżz/OS , produkt AMS for z/OS używa tylko tych pierścieni kluczy, które są zarządzane przez produkt RACF lub jego odpowiednik. Te pliki kluczy są oparte na narzędziu SAF (Security Authorization Facility) i są repozytorium używanym przez produkt AMS for z/OS do pobierania certyfikatów dla nadawców i odbiorców komunikatów umieszczonych w kolejkach systemu IBM MQ lub odebranych z tych kolejek.

W przypadku komunikatów pochodzących z produktu z/OS, które są chronione przez strategię integralności lub szyfrowania, certyfikat i klucz prywatny ID użytkownika inicjującego muszą być

przechowywane w pliku kluczy zarządzanym przez SAF, który jest powiązany z identyfikatorem użytkownika z/OS nadawcy komunikatu.

RACF umożliwia importowanie certyfikatów i kluczy prywatnych do plików kluczy zarządzanych przez RACF. Szczegółowe informacje i przykłady ładowania certyfikatów do zarządzanych przez RACF pliku kluczy znajdują się w publikacjach z/OS Security Server RACF .

Jeśli instalacja korzysta z jednego z obsługiwanych produktów PKI, należy zapoznać się z publikacjami dołączanymi do produktu, aby uzyskać informacje na temat jego wdrażania.

Administrowanie strategiami bezpieczeństwa Advanced Message Security

Program Advanced Message Security używa strategii bezpieczeństwa do określenia algorytmów szyfrowania i podpisywania na potrzeby szyfrowania i uwierzytelniania komunikatów przepływających przez kolejki.

Przegląd strategii bezpieczeństwa dla produktu AMS

Strategie bezpieczeństwa systemu Advanced Message Security są obiektami koncepcyjnymi opisującymi sposób szyfrowania i podpisywania komunikatu.

Szczegółowe informacje na temat atrybutów strategii bezpieczeństwa znajdują się w następujących podtematach:

Pojęcia pokrewne

“Jakość ochrony w AMS” na stronie 732
Strategie ochrony danych Advanced Message Security implikują jakość ochrony (QOP).

“Atrybuty strategii bezpieczeństwa w programie AMS” na stronie 732
Aby wybrać konkretny algorytm lub metodę ochrony danych, można użyć programu Advanced Message Security .

Nazwy strategii w produkcie AMS

Nazwa strategii jest unikalną nazwą identyfikującą konkretną strategię Advanced Message Security i kolejkę, do której ma ona zastosowanie.

Nazwa strategii musi być taka sama jak nazwa kolejki, do której ma zastosowanie. Istnieje odwzorowanie jeden do jednego między Advanced Message Security (AMS) Strategia i kolejka.

Utworzenie strategii o takiej samej nazwie jak nazwa kolejki powoduje aktywowanie strategii 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. Zdalne menedżery kolejek muszą mieć własne lokalnie zdefiniowane strategie dla kolejek, którymi zarządzają.

Algorytm podpisu w programie AMS

Algorytm podpisu wskazuje algorytm, który powinien być używany podczas podpisywania 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 ze strategią nie są podpisywane.

Uwaga: Jakość ochrony używana dla funkcji umieszczania i pobierania komunikatów musi być zgodna. Jeśli występuje niezgodność jakości ochrony strategii między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno do kolejek lokalnych, jak i zdalnych.

Algorytm szyfrowania w programie AMS

Algorytm szyfrowania wskazuje algorytm, który powinien być używany podczas szyfrowania komunikatów danych umieszczonych w kolejce powiązanej ze strategią.

Poprawne wartości to:

- Deprecated RC2
- Deprecated DES
- Deprecated 3DES
- AES128
- AES256

Strategia, która nie określa algorytmu szyfrowania lub określa algorytm NONE , oznacza, że komunikaty umieszczone w kolejce powiązanej ze strategią nie są szyfrowane.

Należy zauważyć, że strategia, która określa algorytm szyfrowania inny niż NONE , musi również określać co najmniej jedną nazwę wyróżniającą odbiorcy i algorytm podpisu, ponieważ zaszyfrowane komunikaty produktu Advanced Message Security również są podpisane.

Ważne: Jakość ochrony używana dla funkcji umieszczania i pobierania komunikatów musi być zgodna. Jeśli występuje niezgodność jakości ochrony strategii między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno do kolejek lokalnych, jak i zdalnych.

Tolerancja w programie AMS

Atrybut tolerancji wskazuje, czy program Advanced Message Security może akceptować komunikaty bez określonej strategii bezpieczeństwa.

Podczas pobierania komunikatu z kolejki ze strategią w celu zaszyfrowania 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 ma wartość 0, oznacza, że komunikaty umieszczone w kolejce powiązanej ze strategią muszą być zgodne z regułami strategii.

Tolerancja jest opcjonalna i istnieje w celu ułatwienia wdrażania konfiguracji, w której strategie zostały zastosowane do kolejek, ale te kolejki już zawierają 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 komponentów DN 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 AIX and Linux z włączonym kodowaniem UTF-8 lub przy użyciu interfejsu GUI systemu **strmqikm** . Następnie należy utworzyć strategię na platformie Linux lub AIX z włączonym kodowaniem UTF-8 lub użyć wtyczki AMS do programu 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 cudzysłów.

Pojęcia pokrewne

“Nazwy wyróżniające odbiorców w AMS” na stronie 731

Nazwy wyróżniające odbiorców identyfikują użytkowników, którzy mają uprawnienia do pobierania komunikatów z kolejki.

Nazwy wyróżniające odbiorców w AMS

Nazwy wyróżniające odbiorców identyfikują użytkowników, którzy mają uprawnienia 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 komponentów DN 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 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.
- Advanced Message Security 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, która jest tworzona w kodowaniu UTF-8 przy użyciu systemu AIX lub Linux z włączonym kodowaniem UTF-8 lub przy użyciu interfejsu GUI systemu **strmqikm** . Następnie należy utworzyć strategię na platformie Linux lub AIX z włączonym kodowaniem UTF-8 lub użyć wtyczki Advanced Message Security dla IBM MQ.

Pojęcia pokrewne

“Nazwy wyróżniające nadawców w produkcie AMS” na stronie 729

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 programie AMS

Aby wybrać konkretny algorytm lub metodę ochrony danych, można użyć programu Advanced Message Security .

Strategia bezpieczeństwa to obiekt koncepcyjny opisujący sposób szyfrowania i podpisywania komunikatu.

Tabela 110. Atrybuty strategii bezpieczeństwa w programie 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 odbiorców komunikatu.
Lista kontrolna nazwy wyróżniającej podpisu	Lista nazw wyróżniających sygnatur, których poprawność ma zostać sprawdzona 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 przy użyciu algorytmu RSA, klucze o efektywnej długości do 2048 bitów. Rzeczywiste szyfrowanie klucza asymetrycznego zależy od długości klucza certyfikatu.

Obsługiwane algorytmy klucza symetrycznego są następujące:

- Deprecated RC2
- Deprecated DES
- Deprecated 3DES
- AES128
- AES256

Advanced Message Security obsługuje również następujące kryptograficzne funkcje mieszające:

- Deprecated MD5
- Deprecated 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 umieszczania i pobierania komunikatów musi być zgodna. Jeśli występuje niezgodność jakości ochrony strategii między kolejką a komunikatem w kolejce, komunikat nie jest akceptowany i jest wysyłany do kolejki obsługi błędów. Ta reguła ma zastosowanie zarówno do kolejek lokalnych, jak i zdalnych.

Jakość ochrony w AMS

Strategie ochrony danych Advanced Message Security implikują jakość ochrony (QOP).

Trzy poziomy jakości zabezpieczeń w produkcie Advanced Message Security są uzupełnione o czwarty poziom w produkcie IBM MQ 9.0 i nowszych, a wszystkie zależą od algorytmów szyfrowania, które są używane do podpisywania i szyfrowania komunikatu:

- Ochrona prywatności-komunikaty umieszczane w kolejce muszą być podpisane i zaszyfrowane.
- Integralność-komunikaty umieszczane w kolejce muszą być podpisane przez nadawcę.
- Poufność-komunikaty umieszczane w kolejce muszą być zaszyfrowane. Więcej informacji na ten temat zawiera sekcja “Jakość ochrony dostępna w produkcie AMS” na stronie 653
- Brak-ochrona danych nie ma zastosowania.

Strategia, która określa, że komunikaty muszą być podpisane, gdy są umieszczane w kolejce, ma QOP o wartości INTEGRITY. QOP o wartości INTEGRITY oznacza, że strategia określa algorytm podpisu, ale nie określa algorytmu szyfrowania. Komunikaty chronione przez integralność są również nazywane "SIGNED".

Strategia, która określa, że komunikaty muszą być podpisywane i szyfrowane, gdy są umieszczane w kolejce, ma QOP o wartości PRIVACY. Wartość QOP PRIVACY oznacza, że gdy strategia określa algorytm podpisu i algorytm szyfrowania. Wiadomości chronione prywatnością są również określane jako "SEALED" (zapieczętowane).

Strategia, która określa, że komunikaty muszą być szyfrowane, gdy są umieszczane w kolejce z klauzulą poufności (QOP). Wartość QOP POUFNOŚCI oznacza, że strategia określa algorytm szyfrowania.

Strategia, która nie określa algorytmu podpisu lub algorytmu szyfrowania, ma QOP o wartości NONE. Produkt Advanced Message Security nie zapewnia ochrony danych dla kolejek, które mają strategię z wartością NONE parametru QOP.

Zarządzanie strategiami bezpieczeństwa w programie AMS

Strategia bezpieczeństwa to obiekt koncepcyjny opisujący sposób szyfrowania i podpisywania komunikatu.

Miejsce, z którego uruchamiane są wszystkie zadania administracyjne związane ze strategiami bezpieczeństwa, zależy od używanej platformy.

- ALW W systemie AIX, Linux, and Windowsdo zarządzania strategiami bezpieczeństwa używane są komendy DELETE POLICY, DISPLAY POLICYi SET POLICY (lub równoważne komendy PCF).
  - Linux AIX W systemie AIX and Linuxzadania administracyjne można uruchamiać z poziomu programu *MQ_INSTALLATION_PATH*/bin.
  - Windows Na platformach Windows zadania administracyjne można uruchamiać z dowolnego miejsca, ponieważ 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 podczas instalowania systemu IBM MQ .

  Dodatkowe wersje języków narodowych są instalowane w bibliotekach QSYS29xx zgodnie z ładowaniem opcji językowych. Na przykład komputer z językiem angielskim (Stany Zjednoczone) jako językiem podstawowym i językiem koreańskim jako językiem dodatkowym ma zainstalowane komendy języka angielskiego (Stany Zjednoczone) w bibliotece QSYS, a ładowanie języka koreańskiego w języku dodatkowym (QSYS2962) w języku koreańskim (2962) jest ładowaniem języka koreańskiego.
- z/OS W systemie z/OSkomendy administracyjne są uruchamiane za pomocą programu narzędziowego strategii bezpieczeństwa komunikatów (CSQ0UTIL). Podczas tworzenia, modyfikowania lub usuwania strategii w systemie z/OSzmiany nie są rozpoznawane przez program Advanced Message Security do momentu zatrzymania i zrestartowania menedżera kolejek lub użycia komendy z/OS MODIFY w celu odświeżenia konfiguracji strategii Advanced Message Security . Na przykład:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

Zadania pokrewne

“Tworzenie strategii bezpieczeństwa w programie AMS” na stronie 734
Strategie bezpieczeństwa definiują sposób, w jaki komunikat jest chroniony, gdy jest umieszczany, lub sposób, w jaki komunikat musi być chroniony, gdy jest odbierany.

“Zmiana strategii bezpieczeństwa w programie AMS” na stronie 735
Aby zmienić szczegóły strategii bezpieczeństwa, które zostały już zdefiniowane, można użyć programu Advanced Message Security .

“Wyświetlanie i zrzucanie strategii bezpieczeństwa w programie AMS” na stronie 736
Komenda **dspmqspl** umożliwia wyświetlenie listy wszystkich strategii bezpieczeństwa lub szczegółów nazwanej strategii w zależności od podanych parametrów wiersza komend.

“Usuwanie strategii bezpieczeństwa w programie AMS” na stronie 737
Aby usunąć strategie bezpieczeństwa w programie Advanced Message Security, należy użyć komendy `setmqspl` .

System operacyjny Advanced Message Security

Odsyłacze pokrewne

Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL)

Tworzenie strategii bezpieczeństwa w programie AMS

Strategie bezpieczeństwa definiują sposób, w jaki komunikat jest chroniony, gdy jest umieszczany, lub sposób, w jaki komunikat musi być chroniony, gdy jest odbierany.

Zanim rozpoczniesz

Podczas tworzenia strategii bezpieczeństwa muszą być spełnione pewne warunki wejściowe:

- 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, należy mieć odpowiednie uprawnienia:
  - z/OS W systemie z/OSnależy nadać uprawnienia opisane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na 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 139.
- z/OS W systemie z/OSupewnij się, że wymagane obiekty systemowe zostały zdefiniowane zgodnie z definicjami w CSQ4INSM.

Przykład

Poniżej przedstawiono przykład tworzenia strategii w menedżerze kolejek QMGR. Strategia określa, że komunikaty mają być podpisywane przy użyciu algorytmu SHA256 i szyfrowane przy użyciu algorytmu AES256 dla certyfikatów o nazwie DN: CN=joe, O=IBM, C=US i DN: CN=jane, O=IBM, C = US. Ta strategia jest przyłączona do `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 będą szyfrowane przy użyciu algorytmu 3DES dla certyfikatów o nazwach wyróżniających:

CN=john, O=IBM, C=US i CN=jeff, O=IBM, C=US i podpisane 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 operacji umieszczania i pobierania komunikatu musi być zgodna. Jeśli jakość ochrony strategii zdefiniowana dla komunikatu jest słabsza niż zdefiniowana 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 programie AMS

Aby zmienić szczegóły strategii bezpieczeństwa, które zostały już zdefiniowane, można użyć programu Advanced Message Security .

Zanim rozpoczniesz

- Menedżer kolejek, na którym ma być wykonywana operacja, musi być uruchomiony.
- Aby nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, należy mieć odpowiednie uprawnienia.
  - z/OS W systemie z/OSnależy nadać uprawnienia opisane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na 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 139.

O tym zadaniu

Aby zmienić strategie bezpieczeństwa, należy zastosować komendę `setmqspl` do już istniejącej strategii udostępniającej 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 z nazwą wyróżniającą CN=alice, O=IBM, C=US i podpisane przy użyciu algorytmu SHA256 dla odbiorców (**-r**) posiadających certyfikaty z nazwą wyróżniającą 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 wprowadzić komendę `setmqspl` ze wszystkimi atrybutami z przykładu, zmieniając tylko wartości, które mają zostać zmodyfikowane. W tym przykładzie poprzednio utworzona strategia jest przyłączona do nowej kolejki, a jej algorytm szyfrowania został zmieniony 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 programie AMS

Komenda **dspmqspl** umożliwia wyświetlenie 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, należy mieć odpowiednie uprawnienia.
  - z/OS W systemie z/OSnależy nadać uprawnienia opisane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).
  - Multi Na 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 139.

O tym zadaniu

Poniżej znajduje się lista opcji komendy **dspmqspl** :

*Tabela 111. Opcje komendy **dspmqspl** .*

Flaga komendy	Objaśnienie
-m	Nazwa menedżera kolejek (obowiązkowa).
-p	Nazwa strategii.
-export	Dodanie tej flagi powoduje wygenerowanie danych wyjściowych, które można łatwo zastosować do innego menedżera kolejek.

Przykład

Poniższy przykład przedstawia sposób tworzenia dwóch strategii bezpieczeństwa dla systemu `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, która wyświetla szczegóły wszystkich strategii zdefiniowanych dla `venus.queue.manager` oraz dane wyjściowe:

```
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, która wyświetla szczegóły wybranej strategii bezpieczeństwa zdefiniowanej dla `venus.queue.manager` oraz dane wyjściowe:

```
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 zostanie utworzona strategia bezpieczeństwa, a następnie strategia zostanie wyeksportowana przy użyciu 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/OSeksportowane informacje o strategii są zapisywane przez CSQ0UTIL w eksportowanej definicji danych.

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:

- Linux AIX W systemie AIX and Linux:
  1. Zaloguj się jako użytkownik należący do grupy administracyjnej produktu `mqm` IBM MQ .
  2. Wydaj komendę `. policies.sh`.
- Windows W systemie Windowsuruchom plik `policies.bat`.
- z/OS W systemie z/OS należy użyć programu narzędziowego CSQ0UTIL , określając dla parametru SYSIN zestaw danych zawierający wyeksportowane informacje o strategii.

Odsyłacze pokrewne

Pełna lista atrybutów komendy dspmqspl

Usuwanie strategii bezpieczeństwa w programie AMS

Aby usunąć strategie bezpieczeństwa w programie Advanced Message Security, należy użyć komendy `setmqspl` .

Zanim rozpoczniesz

Istnieją pewne warunki wejściowe, które muszą być spełnione podczas zarządzania strategiami bezpieczeństwa:

- Menedżer kolejek musi być uruchomiony.
- Aby nawiązać połączenie z menedżerem kolejek i utworzyć strategię bezpieczeństwa, należy mieć odpowiednie uprawnienia.
  - z/OS W systemie z/OSnależy nadać uprawnienia opisane w sekcji Program narzędziowy strategii bezpieczeństwa komunikatów (CSQ0UTIL).

– Multi Na 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 139.

O tym zadaniu

Komendy **setmqspl** należy używać 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 produktem IBM MQ i jego aplikacjami pomocniczymi. Za każdym razem, gdy tworzony jest menedżer kolejek, tworzona jest również kolejka systemowa, w której zapisywane są wewnętrzne komunikaty i dane programu IBM MQ . Kolejki systemowe można chronić za pomocą programu Advanced Message Security , aby tylko autoryzowani użytkownicy mieli do nich dostęp lub mogli je deszyfrować.

Ochrona kolejki systemowej jest zgodna z tym samym wzorcem, co ochrona zwykłych kolejek. Patrz “Tworzenie strategii bezpieczeństwa w programie AMS” na stronie 734.

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 plików `keystore` i `keystore.conf`, które zawierają klucze i konfigurację, aby serwer komend mógł uzyskać dostęp do kluczy i certyfikatów. Wszystkie zmiany wprowadzone w strategii bezpieczeństwa produktu `SYSTEM.ADMIN.COMMAND.QUEUE` wymagają zrestartowania serwera komend.

Wszystkie komunikaty wysyłane i odbierane z kolejki komend są podpisywane lub podpisywane i szyfrowane w zależności od ustawień strategii. Jeśli administrator definiuje autoryzowane osoby podpisujące, komunikaty komend, które nie przeszły sprawdzenia nazwy wyróżniającej osoby podpisującej, nie są wykonywane przez serwer komend i nie są kierowane do kolejki obsługi błędów systemu 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 systemowe:

- 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

V 9.3.0 Multi Kolejki strumieniowe i AMS

Możliwe jest strumieniowanie zduplikowanych chronionych komunikatów Advanced Message Security (AMS).

Jeśli kolejka ma zdefiniowaną strategię AMS , która powoduje, że komunikaty umieszczane w tej kolejce są podpisywane i/lub szyfrowane, można również skonfigurować atrybut **STREAMQ** kolejki w taki sposób, aby umieszczał kopię każdego zabezpieczonego komunikatu w drugiej kolejce. Zduplikowany komunikat przesyłany strumieniowo jest podpisywany i/lub szyfrowany przy użyciu tej samej strategii, która została skonfigurowana dla oryginalnej kolejki.

W poniższym przykładzie konfigurowane są dwie kolejki: QUEUE1 i QUEUE2. Atrybut QUEUE1 ma skonfigurowany atrybut **STREAMQ** , który służy do umieszczania komunikatów przesyłanych strumieniowo w kolejce QUEUE2:

```
DEFINE QLOCAL(QUEUE2)

DEFINE QLOCAL(QUEUE1) STREAMQ(QUEUE2)
```

Zabezpieczone komunikaty AMS są umieszczane w kolejce QUEUE1 przez użytkownika z certyfikatem `CN=bob,O=IBM,C=GB`.

Aplikacja z certyfikatem `CN=alice,O=IBM,C=GB` odbierze komunikaty z kolejki QUEUE1. Osobna aplikacja z certyfikatem `CN=fred,O=IBM,C=GB` odbierze komunikaty z kolejki QUEUE2.

Do kolejki QUEUE1 stosowana jest następująca strategia ochrony prywatności systemu AMS :

```
SET POLICY(QUEUE1) SIGNALG(SHA256) SIGNER('CN=bob,O=IBM,C=GB') ENCALG(AES256)
RECIP('CN=alice,O=IBM,C=GB') RECIP('CN=fred,O=IBM,C=GB') ACTION(ADD)
```

Jeśli algorytm szyfrowania został skonfigurowany w strategii dla QUEUE1, odbiorcy wymienieni w strategii muszą zawierać zarówno odbiorców oryginalnych komunikatów z kolejki QUEUE1, jak i odbiorców, którzy będą odbierać zduplikowane komunikaty z kolejki QUEUE2.

Gdy aplikacja próbuje pobierać komunikaty z kolejki QUEUE2 , wykonuje sprawdzenia integralności i/lub deszyfruje komunikat na podstawie strategii ustawionej w kolejce QUEUE2. Jeśli aplikacja chce korzystać z komunikatów przesyłanych strumieniowo z kolejki QUEUE2, należy ustawić odpowiednią strategię dla kolejki QUEUE2 , która umożliwia sprawdzanie integralności komunikatów i ich poprawne deszyfrowanie.

W szczególności algorytm podpisywania, osoba podpisująca i algorytm szyfrowania muszą być takie same, jak strategia zastosowana do kolejki QUEUE1. Odbiorcy strategii dla QUEUE2 muszą zawierać tożsamość odbiorcy odbierającego komunikat z kolejki QUEUE2.

Uwaga: Nie jest konieczne, aby strategia zastosowana do QUEUE2 wymieniała wszystkich odbiorców wymienionych w zestawie strategii QUEUE1.

Na przykład w kolejce QUEUE2 można ustawić następującą strategię, aby umożliwić aplikacji o nazwie wyróżniającej certyfikatu `CN=fred,O=IBM,C=GB` odczytywanie z niej komunikatów chronionych przez produkt AMS:

```
SET POLICY(QUEUE2) SIGNALG(SHA256) SIGNER('CN=bob,O=IBM,C=GB') ENCALG(AES256)
RECIP('CN=fred,O=IBM,C=GB') ACTION(ADD)
```

Pojęcia pokrewne

Kolejki przetwarzania strumieniowego

Nadawanie uprawnień OAM w AMS

Uprawnienia do pliku autoryzują wszystkich użytkowników do wykonywania komend `setmqspl` i `dspmqspl` . Jednak program Advanced Message Security bazuje na menedżerze uprawnień do obiektów (Object Authority Manager-OAM) i każda próba wykonania tych komend przez użytkownika, który nie należy do grupy mqm, która jest grupą administracyjną IBM MQ lub nie ma uprawnień do odczytu nadanych ustawień strategii bezpieczeństwa, powoduje wystąpienie błędu.

Procedura

Aby nadać niezbędne uprawnienia użytkownikowi, 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 planowane jest połączenie klientów z menedżerem kolejek przy użyciu programu Advanced Message Security 7.0.1.

Ostrzeżenie: Przeglądanie uprawnień do systemu SYSTEM.PROTECTION.POLICY.QUEUE nie jest obowiązkowa we wszystkich sytuacjach. Produkt IBM MQ optymalizuje wydajność, buforując strategie, dzięki czemu nie ma potrzeby przeglądania rekordów w poszukiwaniu szczegółów strategii w systemie SYSTEM.PROTECTION.POLICY.QUEUE we wszystkich przypadkach.

Program IBM MQ nie buforuje wszystkich dostępnych strategii. Jeśli istnieje duża liczba strategii, program IBM MQ buforuje ograniczoną liczbę strategii. Oznacza to, że jeśli dla menedżera kolejek zdefiniowano małą liczbę strategii, nie ma potrzeby udostępniania opcji przeglądania w systemie SYSTEM.PROTECTION.POLICY.QUEUE.

Należy jednak nadać uprawnienie do przeglądania tej kolejki w przypadku, gdy zdefiniowano dużą liczbę strategii lub gdy używane są stare klienty. SYSTEM SYSTEM.PROTECTION.ERROR.QUEUE służy do umieszczania komunikatów o błędach generowanych przez kod AMS. Uprawnienie do umieszczania dla tej kolejki jest sprawdzane tylko podczas próby umieszczenia komunikatu o błędzie w kolejce. Uprawnienia do umieszczania w kolejce nie są sprawdzane przy próbie umieszczenia lub pobrania komunikatu z kolejki zabezpieczonej AMS.

Nadawanie uprawnień w systemie AMS

W przypadku korzystania z ochrony zasobów za pomocą komend należy skonfigurować uprawnienia umożliwiające działanie produktu Advanced Message Security . W tym temacie użyto komend RACF w przykładach. Jeśli w przedsiębiorstwie używany jest inny zewnętrzny menedżer zabezpieczeń (ESM), należy użyć równoważnych komend dla tego menedżera ESM.

Istnieją trzy aspekty nadawania uprawnień zabezpieczeń:

- “Przestrzeń adresowa AMSM” na stronie 741
- “CSQ0UTIL” na stronie 742
- “Korzystanie z kolejek, dla których zdefiniowano strategię Advanced Message Security” na stronie 742

Uwagi: W przykładowych komendach używane są następujące zmienne.

1. *QMgrName* -nazwa menedżera kolejek.

   z/OS W systemie z/OSta wartość może być również nazwą grupy współużytkowania kolejek.
2. *username* -może to być nazwa grupy.
3. Przykłady przedstawiają klasę MQQUEUE. Może to być również MXQUEUE, GMQQUEUE lub GMXQUEUE. Więcej informacji na ten temat zawiera sekcja “Profile zabezpieczeń kolejki” na stronie 211.

Ponadto, jeśli profil już istnieje, komenda RDEFINE nie jest wymagana.

Przestrzeń adresowa AMSM

Należy wprowadzić pewne zabezpieczenia IBM MQ dla nazwy użytkownika, pod którą działa przestrzeń adresowa Advanced Message Security .

- W przypadku połączenia wsadowego z menedżerem kolejek należy wydać komendę

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
           PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Dostęp do systemu SYSTEM.PROTECTION.POLICY.QUEUE, problem:

```
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, gdzie 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)
```

- Dostęp do systemu SYSTEM.PROTECTION.POLICY.QUEUE, wymagana dla komendy **setmqpol** , wydaj komendę:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
             PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- Dostęp do systemu SYSTEM.PROTECTION.POLICY.QUEUE, wymagana dla komendy **dspmqpol** , wydaj 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

Jeśli aplikacja pracuje z kolejkami, które mają zdefiniowaną strategię, wymaga ona dodatkowych uprawnień, aby umożliwić produktowi Advanced Message Security zabezpieczanie komunikatów.

Aplikacja wymaga:

- Prawo do odczytu SYSTEM.PROTECTION.POLICY.QUEUE. W tym celu należy wydać komendę:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Dostęp do systemu SYSTEM.PROTECTION.ERROR.QUEUE. W tym celu należy wydać komendę:

```
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 dla systemu AMS w systemie IBM i

Pierwszym zadaniem podczas konfigurowania ochrony Advanced Message Security jest utworzenie certyfikatu i powiązanie go ze środowiskiem. Powiązanie jest konfigurowane za pomocą pliku przechowywanego w zintegrowanym systemie plików (IFS).

Procedura

1. Aby utworzyć certyfikat samopodpisany przy użyciu narzędzia OpenSSL dostarczanego z produktem IBM i, należy wydać następującą komendę w powłoce 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 w formacie PEM (Privacy Enhanced Mail).

W celu uproszczenia wystarczy wprowadzić wartości dla nazwy zwykłej, organizacji i kraju. Te atrybuty i wartości są ważne podczas tworzenia strategii.

Dodatkowe zachęty i atrybuty można dostosować, podając w wierszu komend niestandardowy plik konfiguracyjny openssl z parametrem **-config** . Więcej informacji na temat składni pliku konfiguracyjnego zawiera dokumentacja 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 zawierającym następujące elementy:

```
[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. Aby to osiągnąć, wykonaj następującą komendę:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

Plik `private.pem` w katalogu $HOME zawiera teraz zgodny klucz prywatny i certyfikat, a plik `mycert.pem` zawiera wszystkie certyfikaty publiczne, dla których można szyfrować komunikaty i sprawdzać poprawność podpisów.

Te dwa pliki należy powiązać ze środowiskiem, tworząc plik konfiguracyjny magazynu kluczy `keystore.conf`w położeniu domyślnym.

Domyślnie program AMS szuka konfiguracji magazynu kluczy w podkatalogu `.mqs` katalogu osobistego.

3. W powłoce 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 dla AMS w systemie IBM i*

Przed utworzeniem strategii należy utworzyć kolejkę do przechowywania chronionych komunikatów.

Procedura

1. W wierszu komend wpisz;

   ```
   CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
   ```

   gdzie mqmname jest nazwą menedżera kolejek.

   Użyj komendy DSPMQM, aby sprawdzić, czy menedżer kolejek może używać strategii bezpieczeństwa. Upewnij się, że w parametrze **Security Policy Capability** jest wyświetlana wartość **YES*.

   Najprostszą strategią, jaką można zdefiniować, jest strategia integralności, która jest realizowana przez utworzenie strategii z algorytmem podpisu cyfrowego, ale bez algorytmu szyfrowania.

   Komunikaty są podpisywane, ale nie są szyfrowane. Jeśli komunikaty mają być szyfrowane, należy określić algorytm szyfrowania i co najmniej jednego adresata komunikatu.

   Certyfikat w publicznym magazynie kluczy dla adresata 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 powłoce QShell:

   ```
   /QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
   ```

   Należy wprowadzić nazwę wyróżniającą jako adresata, 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 jest nazwą menedżera kolejek.

   Po utworzeniu strategii wszystkie komunikaty, które są umieszczane, przeglądane lub destrukcyjnie usuwane za pomocą tej nazwy kolejki, podlegają strategii AMS .

Odsyłacze pokrewne

Wyświetlenie menedżera kolejek komunikatów (Display Message Queue Manager-DSPMQM)

Ustawianie strategii bezpieczeństwa MQM (SETMQMSPL)

IBM i *Testowanie strategii dla systemu AMS w systemie IBM i*

Przykładowe aplikacje dostarczane z produktem służą do testowania strategii bezpieczeństwa.

O tym zadaniu

Można użyć przykładowych aplikacji dostarczonych z produktem IBM MQ , takich jak AMQSPUT4, AMQSGET4, AMQSGBR4i narzędzi, takich jak WRKMQMMSG, do umieszczania, przeglądania i pobierania komunikatów przy użyciu nazwy kolejki PROTECTED.

Pod warunkiem, że wszystko zostało poprawnie skonfigurowane, zachowanie aplikacji nie powinno różnić się od zachowania niechronionej kolejki dla tego użytkownika.

Użytkownik, który nie jest skonfigurowany dla Advanced Message Securitylub nie ma wymaganego klucza prywatnego do deszyfrowania komunikatu, nie będzie mógł jednak wyświetlić komunikatu. Użytkownik otrzymuje kod zakończenia RCFAIL, odpowiednik MQCC_FAILED (2) i kod przyczyny RC2063 (MQRC_SECURITY_ERROR).

Aby sprawdzić, czy ochrona AMS jest aktywna, należy umieścić niektóre komunikaty testowe w kolejce PROTECTED, na przykład za pomocą komendy AMQSPUT0. Następnie można utworzyć kolejkę aliasową w celu przeglądania surowych, chronionych danych w spoczynku.

Procedura

Aby nadać niezbędne uprawnienia użytkownikowi, 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 `scrambled` , w których podczas przeglądania kolejki PROTECTED wyświetlane są komunikaty jawnego tekstu.

Zakodowane komunikaty są widoczne, ale oryginalnego tekstu jawnego nie można odszyfrować przy użyciu kolejki ALIAS, ponieważ nie istnieje strategia wymuszania zgodności tej nazwy przez produkt AMS. Dlatego zwracane są surowe dane chronione.

Odsyłacze pokrewne

Ustawianie strategii bezpieczeństwa MQM (SETMQMSPL)

Praca z komunikatami MQ (Work with MQ Messages-WRKMQMMSG)

Zdarzenia komend i konfiguracji dla systemu AMS

Za pomocą programu Advanced Message Securitymożna generować komunikaty zdarzeń komend i konfiguracji, które mogą być rejestrowane i służyć jako zapis zmian strategii na potrzeby kontroli.

Zdarzenia komend i konfiguracji generowane przez program IBM MQ są komunikatami w formacie PCF wysyłanymi do dedykowanych kolejek w menedżerze kolejek, w którym wystąpiło zdarzenie.

Komunikaty o zdarzeniach konfiguracyjnych 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 używanych do zarządzania strategiami bezpieczeństwa systemu Advanced Message Security .

W programie Advanced Message Securityistnieją cztery typy zdarzeń generowanych przez różne działania w strategiach bezpieczeństwa:

- “Tworzenie strategii bezpieczeństwa w programie AMS” na stronie 734, który generuje dwa komunikaty zdarzeń IBM MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy
- Plik “Zmiana strategii bezpieczeństwa w programie AMS” na stronie 735, który generuje trzy komunikaty zdarzeń IBM MQ :
  - Zdarzenie konfiguracji, które zawiera stare wartości strategii bezpieczeństwa
  - Zdarzenie konfiguracji, które zawiera nowe wartości strategii bezpieczeństwa
  - Zdarzenie komendy
- “Wyświetlanie i zrzucanie strategii bezpieczeństwa w programie AMS” na stronie 736, który generuje jeden komunikat zdarzenia IBM MQ :
  - Zdarzenie komendy

- Plik “Usuwanie strategii bezpieczeństwa w programie AMS” na stronie 737, który generuje dwa komunikaty zdarzeń IBM MQ :
  - Zdarzenie konfiguracji
  - Zdarzenie komendy

Włączanie i wyłączanie rejestrowania zdarzeń w systemie AMS

Do sterowania zdarzeniami komendy i konfiguracji służą atrybuty menedżera kolejek **CONFIGEV** i **CMDEV**. Aby włączyć te zdarzenia, należy ustawić odpowiedni atrybut menedżera kolejek na wartość ENABLED. Aby wyłączyć te zdarzenia, należy ustawić odpowiedni atrybut menedżera kolejek na wartość DISABLED.

Procedura

Zdarzenia konfiguracji

Aby włączyć zdarzenia konfiguracji, należy ustawić właściwość **CONFIGEV** na wartość ENABLED. Aby wyłączyć zdarzenia konfiguracji, należy ustawić właściwość **CONFIGEV** na wartość DISABLED. Na przykład można włączyć zdarzenia konfiguracji za pomocą następującej komendy MQSC:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Zdarzenia komendy

Aby włączyć zdarzenia komend, należy ustawić parametr **CMDEV** na wartość ENABLED. Aby włączyć zdarzenia komend z wyjątkiem komend **DISPLAY MQSC** i komend Inquire PCF, należy ustawić parametr **CMDEV** na wartość NODISPLAY. Aby wyłączyć zdarzenia komend, należy ustawić parametr **CMDEV** na wartość DISABLED. Na przykład można włączyć zdarzenia komend za pomocą następującej komendy MQSC:

```
ALTER QMGR CMDEV (ENABLED)
```

Zadania pokrewne

Sterowanie konfiguracją, komendami i zdarzeniami programu rejestrującego w produkcie IBM MQ

Format komunikatu zdarzenia komendy dla AMS

Komunikat zdarzenia komendy składa się ze struktury MQCFH i następujących po niej parametrów PCF.

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 dwa, ponieważ zawsze istnieją dwa parametry typu MQCFGR (grupa). Każda grupa składa się z odpowiednich parametrów. Dane zdarzenia składają się z dwóch grup: CommandContext i CommandData.

CommandContext zawiera:

Identyfikator EventUser

Opis:	Identyfikator użytkownika, który wydał komendę lub wywołał, które wygenerowało zdarzenie. (Jest to ten sam identyfikator użytkownika, który jest używany do sprawdzania uprawnień do wydania komendy lub wywołania; w przypadku komend odebranych z kolejki jest to również identyfikator użytkownika (UserIdentifier) z deskryptora MD komunikatu komendy).
Identyfikator:	MQCACF_EVENT_USER_ID.

Typ danych: MQCFST.

Długość maksymalna: MQ_USER_ID_LENGTH.

Zwrócone: Zawsze.

EventOrigin

Opis: Źródło działania powodującego zdarzenie.

Identyfikator: MQIACF_EVENT_ORIGIN.

Typ danych: MQCFIN.

Wartości:

MQEVO_CONSOLE
Wiersz komend konsoli.

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 który generuje zdarzenie, znajduje się w MD komunikatu zdarzenia).

Identyfikator: MQCACF_EVENT_Q_MGR.

Typ danych: MQCFST.

Długość maksymalna: MQ_Q_MGR_NAME_LENGTH,

Zwrócone: Zawsze.

Znacznik EventAccounting

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), token rozliczania (AccountingToken) z deskryptora MD komunikatu komendy.

Identyfikator: MQBACF_EVENT_ACCOUNTING_TOKEN.

Typ danych: MQCFBS.

Długość maksymalna: MQ_ACCOUNTING_TOKEN_LENGTH,

Zwrócone: Tylko wtedy, gdy EventOrigin ma wartość MQEVO_MSG.

Dane EventIdentity

Opis: Dla komend odebranych jako komunikat (MQEVO_MSG), dane tożsamości aplikacji (daneApplIdentity) z deskryptora MD komunikatu komendy.

Identyfikator: MQCACF_EVENT_APPL_IDENTITY.

Typ danych: MQCFST.

Długość maksymalna: MQ_APPL_IDENTITY_DATA_LENGTH,

Zwrócone: Tylko wtedy, gdy EventOrigin ma wartość MQEVO_MSG.

Typ EventAppl

Opis:	Dla komend odebranych jako komunikat (MQEVO_MSG), typ aplikacji (PutApplType) z deskryptora MD komunikatu komendy.
Identyfikator:	MQIACF_EVENT_APPL_TYPE.
Typ danych:	MQCFIN.
Zwrócone:	Tylko wtedy, gdy EventOrigin ma wartość MQEVO_MSG.

EventApplNazwa

Opis:	W przypadku komend odebranych jako komunikat (MQEVO_MSG) jest to nazwa aplikacji (PutApplNazwa) z deskryptora MD komunikatu komendy.
Identyfikator:	MQCACF_EVENT_APPL_NAME.
Typ danych:	MQCFST.
Długość maksymalna:	DŁUGOŚĆ_NAZWY_APLIKACJI_MQ.
Zwrócone:	Tylko wtedy, gdy EventOrigin ma wartość MQEVO_MSG.

EventApplŹródło

Opis:	Dla komend odebranych jako komunikat (MQEVO_MSG), dane źródłowe aplikacji (daneApplOrigin) z deskryptora MD komunikatu komendy.
Identyfikator:	MQCACF_EVENT_APPL_ORIGIN.
Typ danych:	MQCFST.
Długość maksymalna:	MQ_APPL_ORIGIN_DATA_LENGTH.
Zwrócone:	Tylko wtedy, gdy EventOrigin ma wartość MQEVO_MSG.

Komenda

Opis:	Kod komendy.
Identyfikator:	MQIACF_COMMAND.
Typ danych:	MQCFIN.
Wartości:	**Wartość liczbowa MQCMD_INQUIRE_PROT_POLICY 205** **MQCMD_CREATE_PROT_POLICY wartość liczbowa 206** **Wartość liczbowa MQCMD_DELETE_PROT_POLICY 207** **MQCMD_CHANGE_PROT_POLICY wartość liczbowa 208** Są one definiowane w produkcie IBM MQ 8.0 `cmqcfc.h`
Zwrócone:	Zawsze.

CommandData zawiera elementy PCF składające się na komendę PCF.

Format komunikatu zdarzenia konfiguracji dla AMS

Zdarzenia konfiguracji są komunikatami PCF w standardowym formacie systemu 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 następującej po niej struktury parametrów. 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}
```

Następujące parametry MQCFH są następujące:

EventUserID

Opis: Identyfikator użytkownika, który wydał komendę lub wywołał, które wygenerowało zdarzenie. (Jest to ten sam identyfikator użytkownika, który jest używany do sprawdzania uprawnień do wydania komendy lub wywołania; w przypadku komend odebranych z kolejki jest to również identyfikator użytkownika (UserIdentifier) z deskryptora MD komunikatu komendy).

Identyfikator: **MQCACF_EVENT_USER_ID**

Typ danych: MQCFST.

Długość maksymalna: MQ_USER_ID_LENGTH.

Zwrócone: Zawsze.

SecurityId

Opis: Wartość MQMD.AccountingToken w przypadku komunikatu serwera komend lub identyfikatora SID Windows dla komendy lokalnej.

Identyfikator: **MQBACF_EVENT_SECURITY_ID**

Typ danych: MQCBS.

Długość maksymalna: DŁUGOŚĆ WŁAŚCIWOŚCI MQ_SECURITY_ID_LENGTH.

Zwrócone: Zawsze.

EventOrigin

Opis: Źródło działania powodującego zdarzenie.

Identyfikator: **MQIACF_EVENT_ORIGIN**

Typ danych: MQCFIN.

Wartości:

MQEVO_CONSOLE
Wiersz komend konsoli.

MQEVO_MSG
Komunikat komendy z wtyczki Eksploratora IBM MQ .

Zwrócone: Zawsze.

EventQMgr

Opis: Menedżer kolejek, w którym wprowadzono komendę lub wywołanie. (Menedżer kolejek, w którym wykonywana jest komenda i który generuje zdarzenie, znajduje się w MD komunikatu zdarzenia).

Identyfikator: **MQCACF_EVENT_Q_MGR**

Typ danych: MQCFST

Długość maksymalna: MQ_Q_MGR_NAME_LENGTH DŁUGOŚĆ

Zwrócone: Zawsze.

ObjectType

Opis: Typ obiektu.

Identyfikator: **MQIACF_OBJECT_TYPE**

Typ danych: Usługa MQCFIN

Wartość: **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` .

Długość maksymalna: DŁUGOŚĆ NAZWY OBIEKTU MQ_OBJECT_NAME_LENGTH.

Zwrócone: Zawsze.

PolicyVersion

Opis: Wersja strategii Advanced Message Security .

Identyfikator: **WERSJA_STRATEGII_MQIA**

Typ danych: Usługa MQCFIN

Wartość **238** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Zwrócone: Zawsze

TolerateFlag

Opis: Flaga tolerancji strategii Advanced Message Security .

Identyfikator: **MQIA_TOLERATE_UNPROTECTED**

Typ danych: Usługa 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: Usługa MQCFIN

Wartość: **236** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Zwrócone: Za każdym razem, gdy w strategii Advanced Message Security jest zdefiniowany algorytm podpisu.

EncryptionAlgorithm

Opis: Algorytm szyfrowania strategii Advanced Message Security .

Identyfikator: **MQIA_ENCRYPTION_ALGORITHM (mqia_encryption_algorithm)**

Typ danych: Usługa MQCFIN

Wartość: **237** -wartość liczbowa zdefiniowana w programie IBM MQ 8.0 lub w pliku `cmqc.h` .

Zwrócone: Za każdym razem, gdy w strategii 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 IBM MQ 8.0 lub w pliku `cmqc.h` .

Długość maksymalna: Najdłuższa nazwa wyróżniająca osoby podpisującej w strategii, ale nie dłużej niż przez MQ_DISTINGUISHED_NAME_LENGTH

Zwrócone: Za każdym razem, gdy jest zdefiniowany w strategii IBM MQ .

RecipientDNs

Opis: Temat DistinguishedName dozwolonych osób podpisujących.

Identyfikator: **MQCA_ODBIORCA_DN**

Typ danych: MQCFSL

Wartość: **2114** -wartość liczbowa zdefiniowana w produkcie IBM MQ 8.0 lub w pliku `cmqc.h` .

Długość maksymalna: Najdłuższa nazwa wyróżniająca (DN) odbiorcy w strategii, ale nie dłużej niż MQ_DISTINGUISHED_NAME_LENGTH.

Zwrócone: Za każdym razem, gdy jest zdefiniowany 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. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przesyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
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 oprogramowania, dział 49XA
3605 Autostrada 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 o interfejsie programistycznym, jeśli są dostępne, mają na celu pomóc w tworzeniu aplikacji do użycia z tym programem.

Podręcznik ten zawiera informacje na temat 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 o diagnostyce, modyfikacji i strojeniu nie należy używać jako interfejsu programistycznego, ponieważ mogą one ulec zmianie.

Znaki towarowe

IBM, logo IBM , ibm.comsą znakami towarowymi IBM Corporation zarejestrowanymi w wielu systemach prawnych na całym świecie. Aktualna lista znaków towarowych IBM dostępna jest w serwisie WWW IBM, 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 firmy Microsoft Corporation w Stanach Zjednoczonych i/lub 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 (https://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: