9.1

Protegendo o IBM MQ

Nota

Antes de usar estas informações e o produto suportado por elas, leia as informações em "Avisos" na página 663.

Esta edição se aplica à versão 9 liberação 1 do IBM® MQ e a todas as liberações e modificações subsequentes até que seja indicado de outra forma em novas edições.

Índice

ProtegendoIBM MQ

A segurança é uma consideração importante tanto para desenvolvedores de aplicativos do IBM MQ quanto para administradores de sistema do IBM MQ.

Atualizações de segurança

Assegure-se de que todos os hardwares e softwares dentro da zona segura e nas estações de trabalho do operador estejam dentro do ciclo de vida de suporte, que o upgrade tenha sido feito com atualizações de software obrigatórias e que eles tenham tido atualizações de segurança prontamente aplicadas.

É possível encontrar informações adicionais sobre atualizações de segurança para:

- Todas as plataformas em Boletins de segurança do IBM
- APARs de segurança e integridade do sistema no z/OS no portal de Integridade do IBM Z System.

Visão geral da segurança

Esta coleção de tópicos apresenta os conceitos de segurança do IBM MQ.

Os conceitos e mecanismos de segurança, conforme são aplicados a qualquer sistema de computador, são apresentados primeiro, seguido por uma discussão desses mecanismos de segurança, à medida que são implementados em IBM MQ.

Conceitos e Mecanismos de Segurança

Esta coleção de tópicos descreve aspecto de segurança para considerar em sua instalação do IBM MQ.

Os aspectos comumente aceitos de segurança são os seguintes:

- “Identificação e autenticação” na página 6
- “Autorização” na página 6
- “Auditoria” na página 6
- “Sigilosidade” na página 7
- “Integridade de dados” na página 7

Mecanismos de Segurança são ferramentas técnicas e métodos que são utilizados para implementar serviços de segurança. Um mecanismo pode operar por conta própria, ou com outros, para fornecer um serviço específico. Exemplos de mecanismos de segurança comuns são os seguintes:

- “Criptografia” na página 7
- “Trechos de mensagens e assinaturas digitais” na página 9
- “Certificados Digitais” na página 9
- “Infraestrutura da Chave Pública (PKI)” na página 14

Ao planejar uma implementação do IBM MQ, considere quais mecanismos de segurança serão necessários para implementar os aspectos de segurança que são importantes para você. Para obter informações sobre o que considerar depois de ler esses tópicos, consulte “Planejando para seus requisitos de segurança” na página 80.

Conceitos relacionados

“Trabalhando com SSL/TLS” na página 276
Estes tópicos fornecem instruções para executar tarefas únicas relacionadas ao uso do TLS com o IBM MQ.

Tarefas relacionadas

Conectando dois gerenciadores de filas usando TLS

Identificação e autenticação

Identificação é a capacidade de identificar exclusivamente um usuário de um sistema ou um aplicativo que esteja sendo executado no sistema. *Autenticação* é a capacidade de provar que um usuário ou um aplicativo é realmente quem essa pessoa ou o que esse aplicativo diz ser.

Por exemplo, considere um usuário que entre no sistema com um ID de usuário e uma senha. O sistema usa o ID de usuário para identificar o usuário. O sistema autentica o usuário no momento do logon verificando se a senha fornecida está correta.

Não repúdio

O serviço *não-repudiação* pode ser visto como uma extensão dos serviços de identificação e autenticação. Em geral, a não-repudiação é aplicada quando os dados são transmitidos eletronicamente; por exemplo, uma ordem ao corretor da bolsa para comprar ou vender ações, ou uma ordem a um banco para transferir fundos de uma conta a outra.

O objetivo geral do serviço de irrecusabilidade é poder provar que uma mensagem específica está associada a uma pessoa específica.

O serviço de não-repudiação pode conter mais de um componente, em que cada componente fornece uma função diferente. Caso o emitente da mensagem alguma vez se negue a enviá-la, o serviço de não-repudiação com a *prova de origem* pode fornecer ao receptor com completa certeza de que a mensagem foi enviada por aquele indivíduo específico. Caso o receptor da mensagem alguma vez se negue a enviá-la, o serviço de não-repudiação com a *prova de entrega* pode fornecer ao emitente com completa certeza de que a mensagem foi recebida por aquele indivíduo específico.

Na prática, provar com completa ou quase 100% de certeza, é uma tarefa difícil. No mundo real, nada é totalmente seguro. Gerenciamento de segurança está mais concentrado em gerenciar riscos a um nível que seja aceitável para os negócios. Em tal ambiente, uma expectativa mais realística do serviço de não-repudiação é ser capaz de fornecer provas que sejam admissíveis e que apóiem o seu caso em um tribunal de lei.

O não repúdio é um serviço de segurança relevante em um ambiente do IBM MQ porque o IBM MQ é um meio de transmitir dados eletronicamente. Por exemplo, você pode exigir provas contemporâneas de que uma mensagem específica foi enviada ou recebida por um aplicativo associado a um indivíduo em particular.

O IBM MQ com o Advanced Message Security não fornece um serviço de não repúdio como parte de sua função base. No entanto, esta documentação do produto traz sugestões sobre como é possível fornecer seu próprio serviço de não repúdio dentro de um serviço do IBM MQ elaborando seus próprios programas de saída.

Conceitos relacionados

"Identificação e autenticação em IBM MQ" na página 21
No IBM MQ, é possível implementar a identificação e autenticação usando informações de contexto da mensagem e autenticação mútua.

Autorização

A *autorização* protege os recursos críticos em um sistema, limitando o acesso somente a usuários autorizados e seus aplicativos. Ele previne o uso não autorizado de um recurso ou o uso de um recurso de maneira não autorizada.

Conceitos relacionados

"A autorização no IBM MQ" na página 22
É possível usar a autorização para limitar o que indivíduos ou aplicativos específicos podem fazer em seu ambiente do IBM MQ.

Auditoria

Auditoria é o processo de gravação e verificação de eventos para detectar se qualquer atividade inesperada ou desautorizada ocorreu, ou se nenhuma tentativa foi feita para executar essa atividade.

Para obter mais informações sobre como configurar a autorização, consulte "Planejando a autorização" na página 84 e os subtópicos associados.

Conceitos relacionados

"A auditoria no IBM MQ" na página 22
O IBM MQ pode emitir mensagens de eventos para registrar que uma atividade incomum ocorreu.

Sigilosidade

O serviço de *confidencialidade* protege informações sensitivas de exposições não autorizadas.

Quando dados sensíveis são armazenados localmente, os mecanismos de controle de acesso podem ser suficientes para protegê-lo na hipótese de não ser possível ler os dados caso não possam ser acessados. Caso um nível mais alto de segurança seja necessário, os dados podem ser critografados.

Criptografe dados sensíveis quando são transmitidos em uma rede de comunicações, especialmente em uma rede tão insegura quanto a Internet. Em um ambiente de rede, os mecanismos de controle de acesso não são efetivos contra tentativas de intercepção de dados, como grampeamento de linha.

Integridade de dados

O serviços *integridade dos dados* detecta se houve modificação não-autorizada dos dados.

Há duas maneiras nas quais os dados podem ser alterados: acidentalmente, por meio de erros de hardware ou transmissão ou em decorrência de um ataque deliberado. Muitos produtos de hardware e protocolos de transmissão possuem mecanismos para detectar e corrigir erros de hardware e de transmissão. O propósito de serviços de integridade de dados é detectar um ataque deliberado.

O serviço de integridade dos dados tem como objetivo somente detectar se algum dado foi modificado. Não tem a meta de restaurar dados ao seu estado original caso tenha sido modificado.

Mecanismos de controle de acesso podem contribuir para a integridade dos dados pois estes não podem ser modificados caso o acesso tenha sido negado. No entanto, como na confidencialidade, os mecanismos de controle de acesso não são efetivos em ambientes de rede.

Conceitos criptográficos

Esta coleção de tópicos descreve os conceitos de criptografia aplicáveis ao IBM MQ.

O termo *entidade* é usado para se referir a um gerenciador de fila, um IBM MQ MQI client, um usuário individual, ou qualquer outro sistema capaz de trocar mensagens.

Conceitos relacionados

"Criptografia no IBM MQ" na página 23
O IBM MQ fornece criptografia usando o protocolo Segurança da Camada de Transporte (TLS).

Criptografia

Criptografia é o processo de conversão entre texto legível, chamado *texto simples*, e uma forma ilegível, chamada *texto cifrado*.

Isso ocorre conforme a seguir:

1. O emissor converte a mensagem de texto corrido para texto cifrado. Esta parte do processo é chamada de *criptografia* (às vezes *codificação*).
2. O texto cifrado é transmitido ao receptor.
3. O receptor converte a mensagem de texto cifrado de volta à sua forma de texto corrido. Esta parte do processo é chamada de *decriptografia* (às vezes *decifração*).

A conversação envolve uma seqüência de operações matemáticas que alteram a aparência da mensagem durante a transmissão, mas não afetam o conteúdo. As técnicas criptográficas podem assegurar confidencialidade e proteger mensagens contra visualização não autorizada (escuta), porque uma mensagem criptografada não é compreensível. Assinaturas digitais, que fornecem uma garantia da

integridade da mensagem, usam técnicas de criptografia. Consulte a "Assinaturas digitais no SSL/TLS" na página 19 para obter mais informações.

Técnicas de criptografia envolvem um algoritmo geral, tornado específico pelo uso das chaves. Há duas classes de algoritmo:

- Aqueles que exigem que ambas as partes utilizem a mesma chave. Algoritmos que usam uma chave compartilhada são conhecidos como algoritmos *simétricos*. O Figura 1 na página 8 ilustra a criptografia de chave simétrica.
- Aqueles que utilizam uma chave para criptografia e uma chave diferente para decriptografia. Um destes deve ser mantido secreto mas o outro pode ser público. Algoritmos que usam pares de chaves públicas e privadas são conhecidos como algoritmos *assimétricos*. O Figura 2 na página 8 ilustra a criptografia de chave assimétrica, que também é conhecida como *criptografia de chave pública*.

Os algoritmos de criptografia e decriptografia utilizados podem ser públicos mas a chave secreta compartilhada e a chave privada devem ser mantidas secretas.

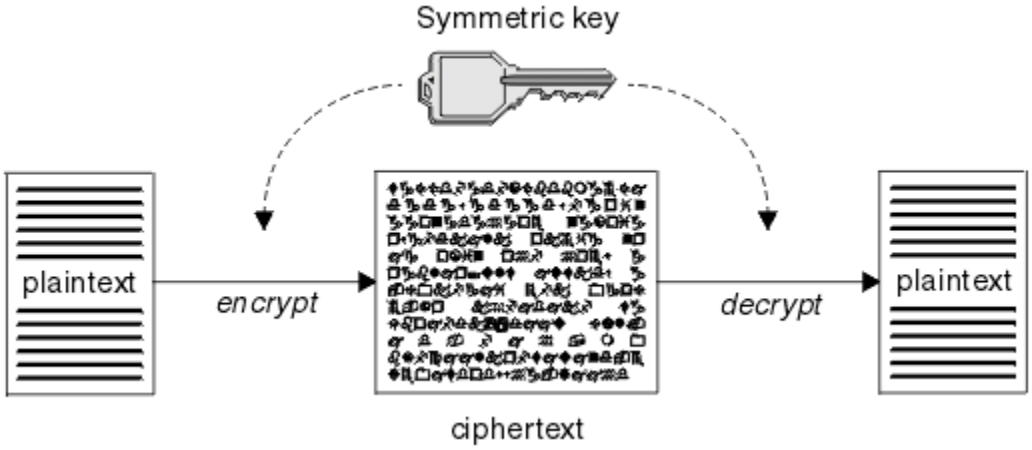


Figura 1. Criptografia de chave simétrica

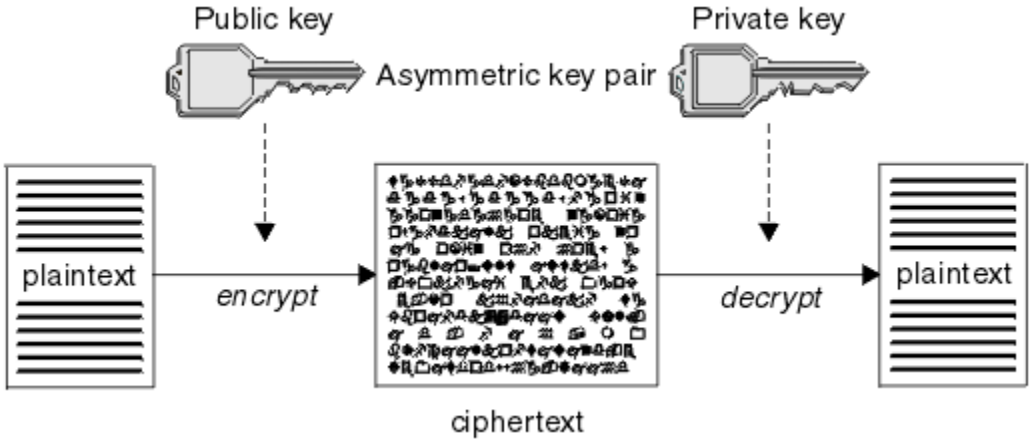


Figura 2. Criptografia de chave assimétrica

Figura 2 na página 8 mostra texto corrido criptografado com a chave pública do receptor e decriptografado com a chave privada do receptor. Somente o receptor pretendido tem a chave privada para decriptografar o texto cifrado. Observe que o emissor pode também criptografar mensagens com uma chave privada, que permite que qualquer um que tenha a chave pública do emissor decriptografe a mensagem, com a garantia de que a mensagem deve ter vindo do emissor.

Com algoritmos assimétricos, as mensagens são criptografadas com a chave pública ou privada mas podem ser decriptografados somente com a outra chave. Somente a chave privada é secreta, a chave pública pode ser conhecida por qualquer um. Com algoritmos simétricos, a chave compartilhada deve

ser conhecida somente pelas duas partes. Isso chama-se *problema de distribuição de chave*. Algoritmos assimétricos são mais lentos mas têm a vantagem de que não há problema de distribuição de chave.

Outra terminologia associada com a criptografia é:

Ponto Forte
A força da criptografia é determinada pelo tamanho da chave. Algoritmos assimétricos exigem chaves grandes, por exemplo:

1024 bits	Chave assimétrica de força baixa
2048 bits	Chave assimétrica de força média
4096 bits	Chave assimétrica de força alta

As chaves simétricas são menores: as chaves de 256 bits fornecem criptografia avançada.

Algoritmo de cifra de bloco
Estes algoritmos criptografam dados por blocos. Por exemplo, o algoritmo RC2 do RSA Data Security Inc. usa blocos de 8 bytes de comprimento. Algoritmos de bloco são geralmente mais lentos do que algoritmos de fluxo.

Algoritmo de cifra de fluxo
Estes algoritmos operam em cada byte de dados. Algoritmos de fluxo são geralmente mais rápidos do que algoritmos de bloco.

Trechos de mensagens e assinaturas digitais

O trecho da mensagem é uma representação numérica de tamanho fixo do conteúdo de uma mensagem. O trecho da mensagem é calculado por uma função hash e pode ser criptografado, formando uma assinatura digital.

A função hash usada para calcular uma trecho da mensagem deve atender a dois critérios:

- Ela deve ser de uma maneira. Não deve ser possível reverter a função para encontrar a mensagem correspondente a um trecho de mensagem específico, a não ser testando todas as mensagens possíveis.
- Deve ser computacionalmente impossível encontrar duas mensagens que executem hash para a mesma compilação.

A compilação de mensagens é enviada junto com a própria mensagem. O destinatário pode gerar uma compilação para a mensagem e compará-la com a compilação do emissor. A integridade da mensagem é verificada quando os dois trechos da mensagem são os mesmos. Qualquer violação da mensagem durante a transmissão quase certamente resultará em uma compilação de mensagem diferente.

Um trecho da mensagem criado usando uma chave simétrica secreta é conhecido como um código de autenticação de mensagem (MAC), pois ele pode fornecer garantia de que a mensagem não foi modificada.

O emissor pode também gerar um trecho da mensagem e, em seguida, criptografar a compilação usando a chave privada de um par de chaves assimétricas, formando uma assinatura digital. A assinatura deve, então, ser decriptografada pelo receptor, antes de compará-la com uma compilação gerada localmente.

Conceitos relacionados

“Assinaturas digitais no SSL/TLS” na página 19
Uma assinatura digital é formada pela criptografia de uma representação de uma mensagem. A criptografia utiliza a chave privada do assinante e, para eficiência, geralmente opera em uma compilação de mensagens, ao invés de na mensagem em si.

Certificados Digitais

Os certificados digitais são protegidos contra personificação, certificando que uma chave pública pertence a uma entidade especificada. Eles são emitidos por uma autoridade de certificação.

Certificados digitais fornecem proteção contra identidades falsas, porque um certificado digital liga uma chave pública a seu proprietário, seja este um indivíduo, um gerenciador de filas ou alguma outra

entidade. Certificados digitais também são conhecidos como certificados de chave pública, porque eles oferecem garantias sobre a propriedade de uma chave pública quando você utiliza um esquema de chave assimétrica. Um certificado digital contém a chave pública de uma entidade e é uma confirmação de que a chave pública pertence àquela entidade:

- Quando o certificado for para uma entidade individual, ele é chamado de *certificado pessoal* ou *certificado de usuário*.
- Quando o certificado for para uma Autoridade de Certificação, ele é chamado de *certificado de autoridade de certificação* ou *certificado de assinante*.

Se chaves públicas forem enviadas diretamente por seu proprietário a outra entidade, há um risco de que a mensagem possa ser interceptada e a chave pública ser substituída por outra. Isso é conhecido como *ataque humano intermediário* . A solução para este problema é trocar chaves públicas por meio de terceiros confiáveis, o que proporcionará ao usuário uma garantia segura de que a chave pública realmente pertence à entidade com a qual você está se comunicando. Em vez de enviar sua chave pública diretamente, peça aos terceiros confiáveis para incorporá-la a um certificado digital. Os terceiros confiáveis que emitem certificados digitais são chamados de Autoridade de Certificação (CA), conforme descrito em “Autoridades de Certificação” na página 11.

O Que é um Certificado Digital
Os certificados digitais contêm partes específicas de informações, conforme determinado pelo padrão de X.509.

Certificados digitais usados pelo IBM MQ são compatíveis com o padrão X.509, que especifica as informações que são necessárias e o formato para enviá-las. X.509 é a estrutura de Autenticação que faz parte da série X.500 de padrões.

Os certificados digitais contêm, no mínimo, as seguintes informações sobre a entidade que está sendo certificada:

- A chave pública do proprietário
- O Nome Distinto do proprietário
- O Nome Distinto da CA que emitiu o certificado
- A data a partir da qual o certificado é válido
- A data de vencimento do certificado
- O número da versão do formato de dados do certificado conforme definido no X.509. A versão atual do padrão X.509 é Versão 3, e a maioria dos certificados está em conformidade com essa versão.
- Um número de série. Esse é um identificador exclusivo designado pelo CA que emitiu o certificado. O número de série é exclusivo dentro do CA que emitiu o certificado: não há dois certificados assinados pelo certificado de CA que têm o mesmo número de série.

Um certificado X.509 Versão 2 também contém um Identificador do Emissor e um Identificador de Assunto, e um certificado X.509 Versão 3 pode conter várias extensões. Algumas extensões de certificado, como a extensão de Restrição Básica, são *padrão*, mas outras são específicas à implementação. Uma extensão pode ser *crítica*, no caso em que um sistema deve ser capaz de reconhecer o campo. Se ele não reconhecer o campo, deverá rejeitar o certificado. Se uma extensão não for crítica, o sistema pode ignorá-la se não a reconhecer.

A assinatura digital em um certificado pessoal é gerada usando a chave privada do CA que assinou esse certificado. Qualquer pessoa que precisa verificar o certificado pessoal pode usar a chave pública do CA para fazer isso. O certificado do CA contém sua chave pública.

Os certificados digitais não contêm sua chave privada. Você deve manter sua chave privada em segredo.

Requisitos para certificados pessoais
O IBM MQ suporta certificados digitais compatíveis com o padrão X.509. Ele requer a opção de autenticação de cliente.

Como o IBM MQ é um sistema ponto a ponto, ele é visualizado como autenticação de cliente na terminologia SSL/TLS. Portanto, qualquer certificado pessoal usado para autenticação de SSL/TLS precisa

permitir um uso principal de autenticação de cliente. Nem todos os certificados de servidor têm esta opção ativada, de forma que o fornecedor do certificado pode precisar ativar a autenticação de cliente no AC raiz do certificado seguro.

Além dos padrões que especificam o formato de dados para um certificado digital, há também os padrões para determinar se um certificado é válido. Essas normas foram atualizadas com o passar do tempo, a fim de evitar determinados tipos de violação de segurança. Por exemplo, os certificados mais antigos do X.509 versão 1 e 2 não indicam se o certificado pode ser legitimamente usado para assinar outros certificados. Era possível, portanto, para um usuário mal intencionado, obter um certificado pessoal de uma fonte legítima e criar novos certificados projetados para personificar outros usuários.

Ao usar certificados X.509 versão 3, o BasicConstraints e as extensões de certificado KeyUsage são usados para especificar quais certificados podem assinar legitimamente outros certificados. O padrão IETF RFC 5280 especifica uma série de regras de validação de certificado que o software de aplicativo compatível deve implementar para impedir ataques de personificação. Um conjunto de regras de certificado é conhecido como uma política de validação de certificado.

Para obter mais informações sobre as políticas de validação de certificado no IBM MQ, consulte "Políticas de validação de certificado no IBM MQ" na página 44.

Autoridades de Certificação
Uma autoridade de certificação (CA) é um terceiro confiável que emite certificados digitais para fornecer a garantia de que a chave pública de uma entidade verdadeiramente pertença àquela entidade.

As funções de uma CA são:

- Ao receber um pedido de um certificado digital, verifique a identidade do solicitante antes de construir, assinar e devolver o certificado pessoal
- Fornecer a chave pública da própria CA em seu certificado de CA
- Publicar listas de certificados que não são mais confiáveis em uma CRL (Lista de Revogação de Certificados). Para obter informações adicionais, consulte "Trabalhando com Certificados Revogados" na página 341
- Para fornecer acesso ao status de revogação de certificado, operando um respondente servidor de respondente do OCSP

Nomes Distintos
O DN (Distinguished Name) identifica de modo exclusivo uma entidade em um certificado X.509.

Atenção: Apenas os atributos na tabela a seguir podem ser usados em um filtro SSLPEER. Os DNs do certificado podem conter outros atributos, mas a filtragem não é permitida nesses atributos.

Tabela 1. Tipos de atributos localizados no DN que podem ser usados em um filtro SSLPEER

Tipo de atributo	**Descrição**
SERIALNUMBER	Número de série do certificado
MAIL	Endereço eletrônico
E	Endereço de e-mail (descontinuado na preferência para MAIL)
UID ou USERID	Identificador de usuário
CN	Nome Comum
T	Título
OU	Nome de Unidade Organizacional
DC	Componente de domínio
O	Nome da organização

Tabela 1. Tipos de atributos localizados no DN que podem ser usados em um filtro SSLPEER (continuação)	
Tipo de atributo	**Descrição**
STREET	Rua / Primeira linha do endereço
L	Nome da localidade
ST (ou SP ou S)	Nome do estado ou região
PC	Código Postal / Código de Endereçamento Postal
C	País
UNSTRUCTUREDNAME	Nome do host
UNSTRUCTUREDADDRESS	Endereço IP
DNQ	Qualificador de Nome Distinto

O padrão X.509 define outros atributos que normalmente não fazem parte do DN, mas podem fornecer extensões opcionais para o certificado digital.

O padrão X.509 faz com que um DN seja especificado em formato de cadeia. Por exemplo:

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

O Nome Comum (CN) pode descrever um usuário individual ou qualquer outra entidade, por exemplo, um servidor da Web.

O DN pode conter diversos atributos OU e DC. Apenas uma instância de cada um dos outros atributos é permitida. A ordem das entradas de OU é significante: ela especifica uma hierarquia de nomes de Unidades Organizacionais, com a unidade de mais alto nível primeiro. A ordem das entradas DC também é significativa.

IBM MQ tolera certos DNs malformados. Para obter mais informações, consulte as regras do IBM MQ para valores SSLPEER.

Conceitos relacionados

“O Que é um Certificado Digital” na página 10
Os certificados digitais contêm partes específicas de informações, conforme determinado pelo padrão de X.509.

Obtendo certificados pessoais a partir de uma autoridade de certificação
É possível obter um certificado a partir de uma autoridade de certificação (CA) externa confiável.

Você obtém um certificado digital enviando informações a um CA na forma de uma solicitação de certificado. O padrão X.509 define um formato para estas informações, mas alguns CAs têm seu próprio formato. Solicitações de certificado são geralmente geradas pela ferramenta de gerenciamento de certificados que seu sistema usa; por exemplo:

- Multi A ferramenta iKeyman em Multiplataformas.
- z/OS RACF no z/OS.

As informações contêm seu Nome Distinto e sua chave pública. Quando sua ferramenta de gerenciamento de certificados gera seu pedido de certificado, também gera sua chave privada, que você deve manter segura. Nunca distribua sua chave privada.

Quando a CA recebe seu pedido, a autoridade verifica sua identidade antes de construir o certificado e devolvê-lo a você como um certificado pessoal.

Figura 3 na página 13 ilustra o processo de obtenção de um certificado digital de uma CA.

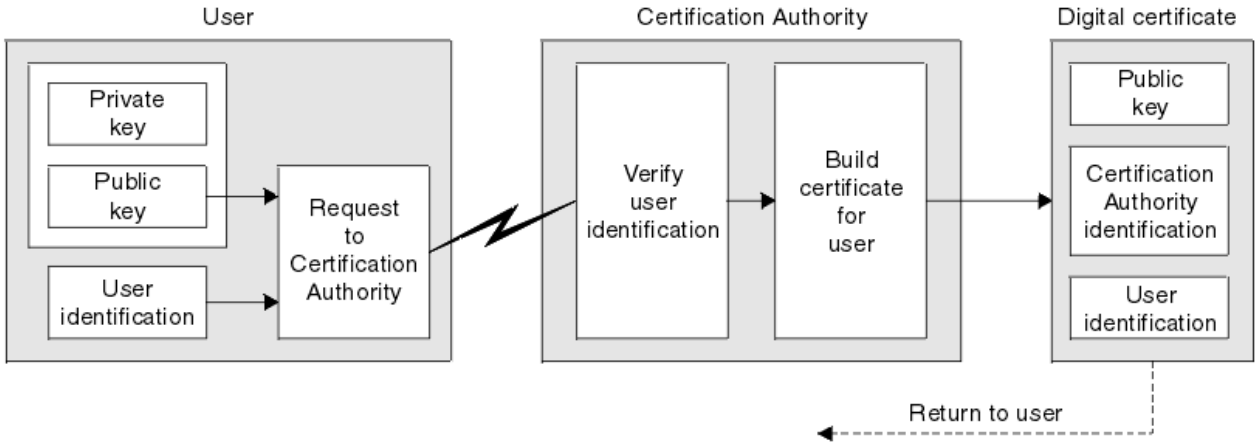


Figura 3. Obtendo um certificado digital

No diagrama:

- A identificação de usuário inclui o seu Nome distinto do assunto.
- A identificação de autoridade de certificação inclui o Nome distinto da autoridade de certificação que está emitindo o certificado.

Os certificados digitais contêm campos adicionais diferentes dos mostrados no diagrama. Para obter mais informações sobre os outros campos em um certificado digital, consulte "O Que é um Certificado Digital" na página 10.

Como Funcionam as Cadeias de Certificados
Quando você receber o certificado de outra entidade, você pode precisar utilizar uma *cadeia de certificados* para obter o certificado *CA raiz*.

A cadeia de certificados, também conhecida como *caminho de certificação*, é uma lista de certificados utilizada para autenticar uma entidade. A cadeia, ou caminho, começa com o certificado daquela entidade, e cada certificado na cadeia é assinado pela entidade identificada pelo próximo certificado na cadeia. A cadeia termina com um certificado de CA raiz. O certificado de autoridade de certificação raiz é sempre assinado pela própria autoridade de certificação (CA). As assinaturas de todos os certificados na cadeia devem ser verificadas até que o certificado de CA raiz seja alcançado.

Figura 4 na página 14 ilustra um caminho de certificação do proprietário do certificado para a CA raiz, onde a cadeia de confiança começa.

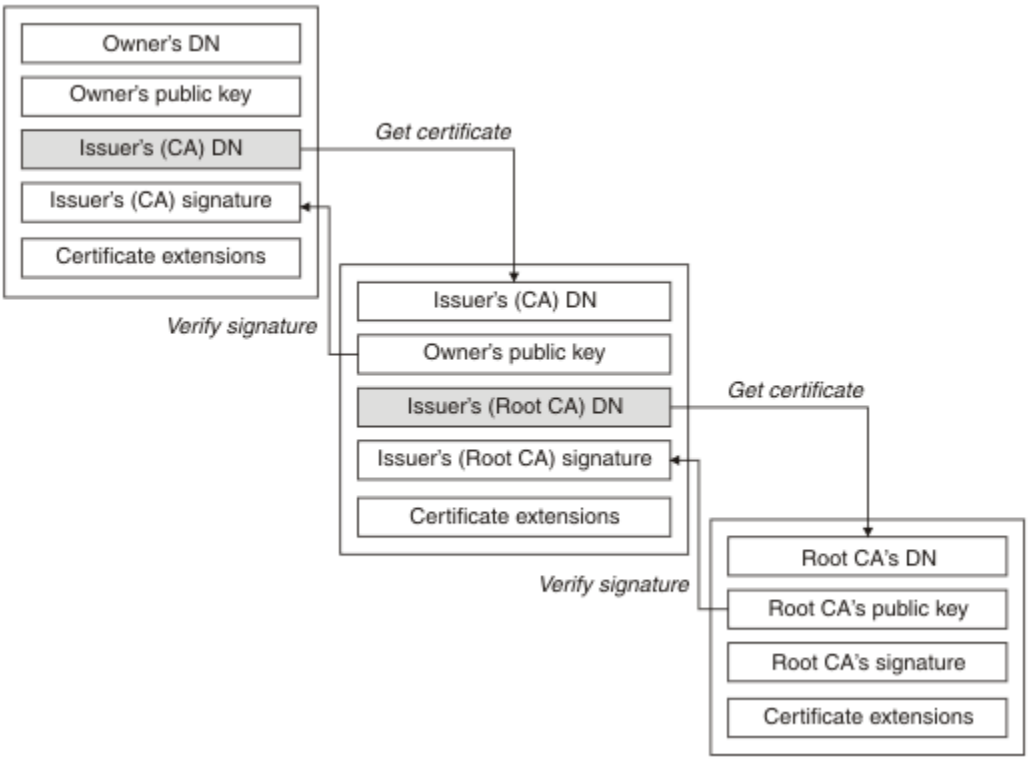


Figura 4. Cadeia de confiança

Cada certificado pode conter uma ou mais extensões. Um certificado pertencente a uma CA geralmente contém uma extensão BasicConstraints com o sinalizador isCA configurado para indicar que é permitido que ele assine outros certificados.

Quando os Certificados Não São Mais Válidos
Os certificados digitais podem vencer ou serem revogados.

Certificados digitais também são emitidos por um período fixo e não são válidos depois de suas datas de expiração.

Certificados podem ser revogados por várias razões, incluindo:

- O proprietário mudou para uma organização diferente.
- A chave privada não é mais secreta.

O IBM MQ pode verificar se um certificado foi revogado enviando uma solicitação para um respondente do Online Certificate Status Protocol (OCSP) (no UNIX, Linux®, and Windows somente). Como alternativa, eles podem acessar uma lista de revogação de certificado (CRL) em um servidor LDAP. A revogação do OCSP e as informações da CRL são publicadas por uma autoridade de certificação. Para obter mais informações, consulte "Trabalhando com Certificados Revogados" na página 341.

Infraestrutura da Chave Pública (PKI)

O PKI (Public Key Infrastructure) é um sistema de recursos, políticas, e serviços que suportam a utilização de criptografia de tecla pública para autenticar as partes envolvidas na transação.

Não há nem um único padrão que define os componentes de uma infraestrutura de chave pública, mas uma infraestrutura de chave pública geralmente inclui autoridades de certificação (CAs) e Autoridades de registro (RAs). Os CAs fornecem os serviços a seguir:

- Emissão de certificados digitais
- Validação de certificados digitais
- Revogação de certificados digitais

- Distribuição de teclas públicas

Os padrões X.509 fornecem a base para a infraestrutura de chave pública padrão de mercado.

Consulte “Certificados Digitais” na página 9 para obter mais informações sobre certificados digitais e autoridades de certificação (CAs). Os RAs verificam a informações fornecidas quando os certificados digitais são exigidos. Se o RA verificar a informação, o CA pode emitir um certificados digital ao solicitante.

Um PKI também pode fornecer as ferramentas para o gerenciamento de certificados digitais ou teclas públicas. Um PKI, às vezes, é descrito como uma *hierarquia de confiança* para o gerenciamento de certificados digitais, mas a maioria das definições incluem serviços adicionais. Algumas definições incluem serviços de criptografia e de assinatura digital, mas não são essenciais para a operação de um PKI.

Protocolos de segurança criptográficos: TLS

Os protocolos de criptografia fornecem conexões seguras, permitindo que dois grupos de comuniquem com privacidade e integridade de dados. O protocolo Transport Layer Security (TLS) surgiu desse do Secure Sockets Layer (SSL). O IBM MQ suporta o TLS.

Os objetivos principais dos dois protocolos é fornecer confidencialidade, (às vezes referida como *privacidade*), integridade de dados, identificação e autenticação, usando certificados digitais.

Embora os dois protocolos sejam semelhantes, as diferenças são suficientemente significantes que o SSL 3.0 e as várias outras versões do TLS não interoperam.

Conceitos relacionados

“Protocolos de segurança TLS no IBM MQ” na página 24
O IBM MQ suporta o protocolo da Segurança da Camada de Transporte (TLS) para fornecer segurança em nível de link para canais de mensagens e canais do MQI.

Conceitos de TLS (Transport Layer Security)

O protocolo TLS permite que duas partes identifiquem e autentiquem uma a outra e se comuniquem com confidencialidade e integridade de dados. O protocolo TLS surgiu do protocolo Netscape SSL 3.0, mas o TLS e o SSL não interoperam.

O protocolo TLS fornece segurança de comunicações sobre a Internet e permite que os aplicativos cliente/servidor se comuniquem de uma forma que seja confidencial e confiável. Os protocolo possuem duas camadas: um Protocolo de Registro e um Protocolo de Handshake e, eles são dispostos em camadas sobre um protocolo de transporte como TCP/IP. Ambos usam técnicas de criptografia assimétrica e simétrica.

Uma conexão do TLS é iniciada por um aplicativo, que se torna o cliente do TLS. O aplicativo que recebe a conexão se torna o servidor do TLS. Cada nova sessão se inicia com um handshake, conforme definido pelos protocolos do TLS.

Uma lista integral de CipherSpecs suportados por IBM MQ é fornecida em “Ativando CipherSpecs” na página 423.

Para obter mais informações sobre o protocolo SSL, consulte as informações fornecidas em https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt. Para obter mais informações sobre o protocolo TLS, consulte as informações fornecidas pelo Grupo de trabalho de TLS no website do Internet Engineering Task Force em https://www.ietf.org

Uma visão geral do handshake SSL/TLS

O handshake SSL/TLS permite que o cliente e o servidor TLS estabeleçam as chaves secretas com as quais se comunicam.

Esta seção fornece um resumo das etapas que permitem que o cliente e o servidor TLS se comuniquem entre si.

- Aceitar a versão do protocolo a ser usada.

- Selecionar algoritmos criptográficos, que são descritos em .
- Autenticar um ao outro com a troca e validação de certificados digitais.
- Utilizar técnicas de criptografia assimétrica para gerar uma chave compartilhada secreta, que evita o problema de distribuição de chaves. O TLS em seguida, usa a chave compartilhada para a criptografia simétrica das mensagens, que é mais rápida que a criptografia assimétrica.

Para obter mais informações sobre a importação de certificados, consulte a seção relevante para sua plataforma em .

Na visão geral, as etapas envolvidas no handshake do TLS são como a seguir:

1. O cliente do TLS envia uma mensagem "Olá, cliente" que lista as informações de criptografia como a versão do TLS e, na ordem de preferência do cliente, os CipherSuites suportados pelo cliente. A mensagem também contém uma cadeia de bytes aleatória que é utilizada em cálculos subsequentes. O protocolo permite que o "client hello" inclua métodos de compactação de dados suportados pelo cliente.
2. O servidor do TLS responde com uma mensagem "Olá, servidor" que contém o CipherSuite escolhido pelo servidor na lista fornecida pelo cliente, o ID da sessão e outra sequência de bytes aleatória. O servidor também envia seu certificado digital. Se o servidor exigir um certificado digital para a autenticação do cliente, o servidor envia um "pedido de certificado de cliente" que inclui uma lista dos tipos de certificados suportados e os Nomes Distintos de Autoridades de Certificação (CAs) aceitáveis.
3. O cliente do TLS verifica o certificado digital do servidor. Para obter mais informações, consulte “Como o TLS fornece identificação, autenticação, confidencialidade e integridade” na página 17.
4. O cliente do TLS envia a sequência de bytes aleatória que permite que ambos o cliente e o servidor calculem a chave secreta a ser usada para criptografar dados de mensagem subsequentes. A própria cadeia de bytes aleatória é criptografada com a chave pública do servidor.
5. Se o servidor do TLS enviou uma "solicitação de certificado de cliente", o cliente enviará uma sequência de bytes aleatória criptografada com a chave privada do cliente, junto com o certificado digital do cliente ou um "alerta de certificado não digital". Este alerta é apenas um aviso, mas com algumas implementações, o protocolo de reconhecimento falha em caso de obrigatoriedade da autenticação do cliente.
6. O servidor do TLS verifica o certificado de cliente. Para obter mais informações, consulte “Como o TLS fornece identificação, autenticação, confidencialidade e integridade” na página 17.
7. O cliente do TLS envia ao servidor uma mensagem de "concluído", que é criptografada com a chave secreta, indicando que a parte do handshake do cliente está concluída.
8. O servidor do TLS envia ao cliente uma mensagem de "concluído", que é criptografada com a chave secreta, indicando que a parte do servidor do handshake está concluída.
9. Para a duração da sessão do TLS, o servidor e o cliente agora podem trocar mensagens que são criptografadas simetricamente com a chave secreta compartilhada.

Figura 5 na página 17 ilustra o handshake do TLS.

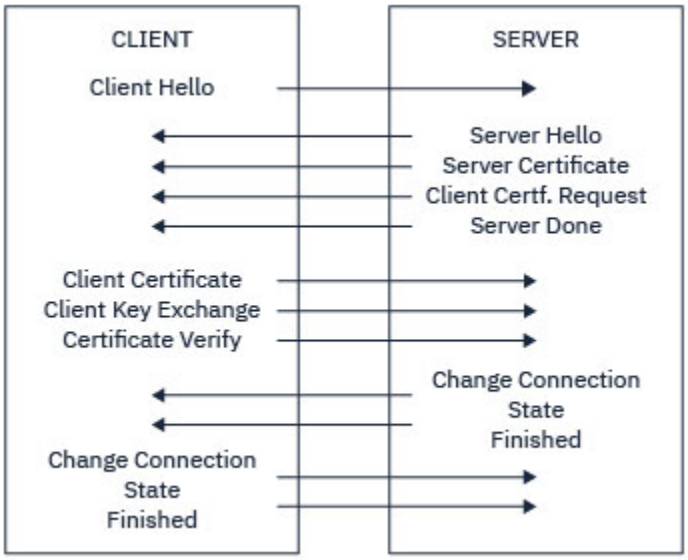


Figura 5. Visão geral do handshake do TLS

Como o TLS fornece identificação, autenticação, confidencialidade e integridade

Durante a autenticação do cliente e do servidor, existe uma etapa que requer que os dados sejam criptografados com uma das chaves de um par de chaves assimétricas e decriptografados com a outra chave do par. Um trecho da mensagem é usado para fornecer integridade.

Para obter uma visão geral das etapas envolvidas no handshake TLS, consulte "Uma visão geral do handshake SSL/TLS" na página 15..

Como o TLS fornece autenticação

Para autenticação do servidor, o cliente utiliza a chave pública do servidor para criptografar os dados que são utilizados para calcular a chave secreta. O servidor poderá gerar a chave secreta somente se puder descriptografar esses dados com a chave privada correta.

Para a autenticação do cliente, o servidor utiliza a chave pública do certificado do cliente para decriptografar os dados enviados pelo cliente durante a etapa "5" na página 16 do protocolo de reconhecimento. A troca de mensagens concluídas que são criptografadas com a chave secreta (etapas "7" na página 16 e "8" na página 16 na visão geral) confirma que a autenticação está completa.

Se alguma das etapas de autenticação falhar, o protocolo de reconhecimento falhará e a sessão será encerrada.

A troca de certificados digitais durante o handshake TLS faz parte do processo de autenticação. Para obter informações adicionais sobre como os certificados fornecem proteção contra personificação, consulte as informações relacionadas. Os certificados requeridos são os seguintes, em que CA X emite o certificado para o cliente TLS e CA Y emite o certificado para o servidor TLS:

Somente para autenticação de servidor, o servidor TLS precisa:

- O certificado pessoal emitido para o servidor pela autoridade de certificação Y
- Da chave privada do servidor

e o cliente TLS precisa:

- O certificado de CA para CA Y

Se o servidor TLS requerer autenticação de cliente, o servidor verificará a identidade do cliente verificando o certificado digital do cliente com a chave pública para a CA que emitiu o certificado pessoal para o cliente, neste caso, a CA X. Para autenticação de servidor e cliente, o servidor precisa:

- O certificado pessoal emitido para o servidor pela autoridade de certificação Y

- Da chave privada do servidor
- O certificado de CA para CA X

e o cliente precisa:

- O certificado pessoal emitido para o cliente pela autoridade de certificação X
- Da chave privada do cliente
- O certificado de CA para CA Y

O cliente e o servidor TLS podem precisar de outros certificados de CA para formarem uma cadeia de certificados para o certificado de CA raiz. Para obter informações adicionais sobre as cadeias de certificados, consulte as informações relacionadas.

O que Acontece Durante a Verificação de Certificado

Conforme observado nas etapas "3" na página 16 e "6" na página 16 da visão geral, o cliente TLS verifica o certificado do servidor e o servidor TLS verifica o certificado do cliente. Existem quatro aspectos para esta verificação:

1. A assinatura digital é verificada (consulte "Assinaturas digitais no SSL/TLS" na página 19).
2. A cadeia de certificados é verificada; é necessário ter certificados de autoridade de certificação intermediária (consulte "Como Funcionam as Cadeias de Certificados" na página 13).
3. As datas de expiração e de ativação e o período de validade são verificados.
4. O status de revogação do certificado é verificado (consulte "Trabalhando com Certificados Revogados" na página 341).

Reconfiguração de Chave Secreta

Durante um handshake TLS, uma *chave secreta* é gerada para criptografar dados entre o cliente e o servidor TLS. A chave secreta é utilizada em uma fórmula matemática que é aplicada aos dados para transformar o texto puro em texto criptografado ilegível, e texto criptografado em texto puro.

A chave secreta é gerada a partir do texto aleatório enviado como parte da handshake, e é usada para criptografar um texto simples para texto cifrado. A chave secreta também é utilizada no algoritmo MAC (Message Authentication Code), que é utilizado para determinar se uma mensagem foi alterada. Consulte a "Trechos de mensagens e assinaturas digitais" na página 9 para obter mais informações.

Caso a chave secreta seja descoberta, o texto puro de uma mensagem poderia ser decifrado a partir do texto criptografado, ou o resumo da mensagem poderia ser calculado, permitindo que mensagens sejam alteradas sem que isso seja detectado. Mesmo para um algoritmo complexo, o texto puro pode eventualmente ser descoberto aplicando todas as transformações matematicamente possíveis ao texto criptografado. Para minimizar a quantidade de dados que podem ser decifrados ou alterados caso a chave secreta seja descoberta, a chave secreta pode ser renegociada periodicamente. Quando a chave secreta for renegociada, a chave secreta anterior não poderá mais ser usada para decriptografar dados que foram criptografados com a nova chave secreta.

Como o TLS fornece confidencialidade

O TLS usa uma combinação de criptografia simétrica e assimétrica para assegurar a privacidade da mensagem. Durante o handshake TLS, o cliente e o servidor TLS concordam em relação a um algoritmo de criptografia e uma chave secreta compartilhada que serão usados somente para uma sessão. Todas as mensagens transmitidas entre o cliente e o servidor TLS serão criptografadas usando esse algoritmo e essa chave, o que assegura que a mensagem continuará sendo privada se for interceptada. Como o TLS usa criptografia assimétrica ao transportar a chave secreta compartilhada, não há nenhum problema de distribuição de chaves. Para obter mais informações sobre técnicas de criptografia, consulte "Criptografia" na página 7.

Como o TLS fornece integridade

O TLS fornece integridade de dados calculando um trecho da mensagem. Para obter informações adicionais, consulte “Integridade de dados de mensagens” na página 462.

O uso de TLS assegura integridade de dados, contanto que o CipherSpec na definição de canal use um algoritmo hash, conforme descrito na tabela em “Ativando CipherSpecs” na página 423.

Especificamente, se a integridade de dados for um problema, você deve evitar a escolha de um CipherSpec cujo algoritmo hash esteja listado como "Nenhum". O uso de MD5 também é fortemente desencorajado, pois isso agora é muito antigo e não é mais seguro para a maioria dos propósitos práticos.

CipherSpecs e CipherSuites

Os protocolos de segurança criptográficos devem concordar sobre os algoritmos usados por uma conexão segura. CipherSpecs e CipherSuites definem combinações específicas de algoritmos.

Um CipherSpec identifica uma combinação de algoritmo de criptografia e algoritmo de código de autenticação de mensagem (MAC). As extremidades de uma conexão TLS devem concordar com o mesmo CipherSpec para serem capazes de se comunicar.

O IBM MQ suporta o protocolo TLS 1.2. No entanto, será possível ativar CipherSpecs descontinuadas, se você precisar fazer isso.

Consulte “Ativando CipherSpecs” na página 423 para obter informações sobre:

- CipherSpecs suportados pelo IBM MQ
- Como ativar especificações de código descontinuadas do SSL 3.0 e do TLS 1.0

Importante: Ao lidar com canais do IBM MQ, você usa um CipherSpec. Ao lidar com canais do Java, canais do JMS ou canais do MQTT, especifique um CipherSuite.

Para obter mais informações sobre CipherSpecs, consulte “Ativando CipherSpecs” na página 423.

Um CipherSuite é um conjunto de algoritmos criptográficos usados por uma conexão TLS. Um conjunto compreende três algoritmos distintos:

- O algoritmo de troca de chave e autenticação, usado durante o handshake
- O algoritmo de criptografia, utilizado para codificar os dados
- O algoritmo MAC (Message Authentication Code), utilizado para gerar a compilação de mensagem

Há várias opções para cada componente do conjunto, mas somente certas combinações são válidas quando especificadas para uma conexão TLS. O nome de um CipherSuite válido define a combinação de algoritmos utilizada. Por exemplo, o CipherSuite TLS_RSA_WITH_AES_128_CBC_SHA especifica:

- O algoritmo de troca de chaves e autenticação RSA
- O algoritmo de criptografia AES, usando uma chave de 128 bits e o modo de encadeamento de blocos cifrados (CBC)
- O Código de Autenticação de Mensagem SHA-1 (MAC)

Assinaturas digitais no SSL/TLS

Uma assinatura digital é formada pela criptografia de uma representação de uma mensagem. A criptografia utiliza a chave privada do assinante e, para eficiência, geralmente opera em uma compilação de mensagens, ao invés de na mensagem em si.

Assinaturas digitais variam com os dados sendo assinados, diferente de com assinaturas manuscritas, que não dependem do conteúdo do documento sendo assinado. Se duas mensagens diferentes forem assinadas digitalmente pela mesma entidade, as duas assinaturas diferirão, mas ambas poderão ser verificadas com a mesma chave pública, ou seja, a chave pública da entidade que assinou as mensagens.

As etapas do processo de assinatura digital são as seguintes:

1. O emissor calcula uma compilação de mensagens, e então a criptografa, utilizando a chave privada do emissor, formando a assinatura digital.

2. O emissor transmite a assinatura digital com a mensagem.
3. O receptor decriptografa a assinatura digital utilizando a chave pública do emissor, gerando novamente a compilação de mensagens do emissor.
4. O receptor calcula uma compilação de mensagem recebida de dados de mensagem e verifica se as duas compilações são as mesmas.

Figura 6 na página 20 ilustra este processo.

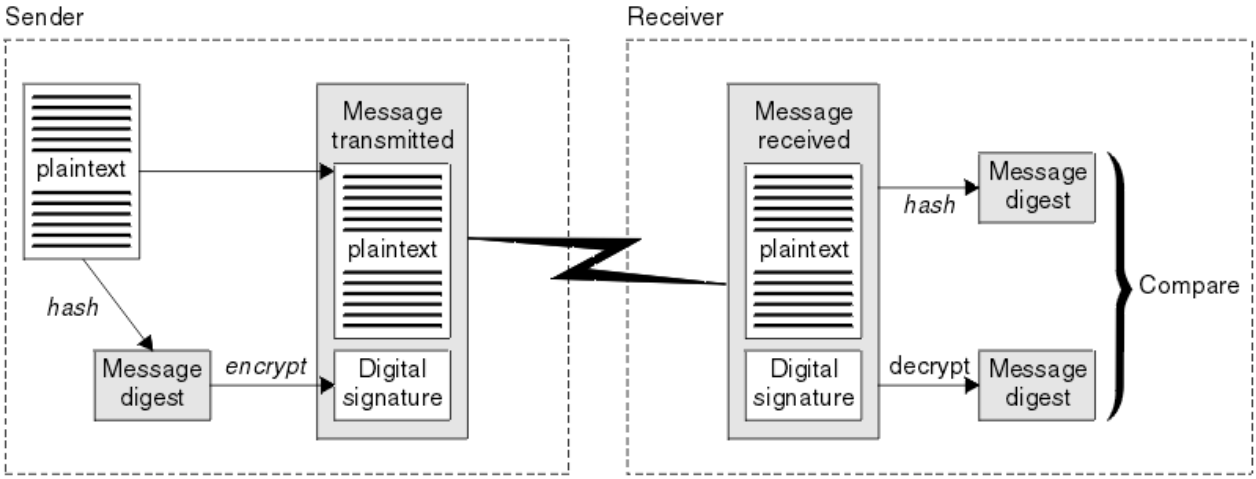


Figura 6. O processo de assinatura digital

Se a assinatura digital for verificada, o receptor saberá que:

- A mensagem não foi modificada durante a transmissão.
- A mensagem foi enviada pela entidade que declara tê-la enviado.

Assinaturas digitais são parte dos serviços de integridade e autenticação. Assinaturas digitais também proporcionam prova de origem. Somente o emissor conhece a chave privada, que fornece forte evidência de que o emissor é o originador da mensagem.

Nota: Você pode também criptografar a própria mensagem, que protegerá a confidencialidade das informações da mensagem.

Federal Information Processing Standards

O governo dos EUA produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. O National Institute for Standards and Technology (NIST) é um órgão importante ligado a sistemas e segurança de TI. O NIST produz recomendações e normas, inclusive Federal Information Processing Standards (FIPS).

Um dessas normas significativa é FIPS 140-2, que requer o uso de algoritmos criptográficos fortes. FIPS 140-2 também especifica requisitos para algoritmos hashing a serem usados para proteger pacotes contra modificação em trânsito.

O IBM MQ fornece suporte a FIPS 140-2 quando tiver sido configurado para tal.

Ao longo do tempo, analistas desenvolvem ataques contra algoritmos de criptografia e hashing existentes. Novos algoritmos são adotados para resistir a esses ataques. FIPS 140-2 é atualizada periodicamente para considerar essas mudanças.

Conceitos relacionados

“Criptografia do Conjunto B da Agência Nacional de Segurança (NSA)” na página 21
O governo dos Estados Unidos da América produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. A Agência Nacional de Segurança dos Estados Unidos (NSA) recomenda um conjunto de algoritmos criptográficos interoperável em seu padrão do Conjunto B.

Criptografia do Conjunto B da Agência Nacional de Segurança (NSA)

O governo dos Estados Unidos da América produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. A Agência Nacional de Segurança dos Estados Unidos (NSA) recomenda um conjunto de algoritmos criptográficos interoperável em seu padrão do Conjunto B.

O padrão do Conjunto B especifica um modo de operação no qual somente um conjunto específico de algoritmo criptográfico seguros são usados. O padrão do Conjunto B especifica:

- O algoritmo de criptografia (AES)
- O algoritmo de troca de chave (Diffie-Hellman da curva elíptica, também conhecido como ECDH)
- O algoritmo de assinatura digital (Algoritmo de assinatura digital da curva elíptica, também conhecido como ECDSA)
- Os algoritmos hash (SHA-256 ou SHA-384)

Além disso, o padrão de IETF RFC 6460 especifica o Conjunto B compatível com perfis que definem a configuração detalhada do aplicativo e o comportamento necessário para estar em conformidade com o padrão do Conjunto B. Ele define dois perfis:

1. Um perfil compatível com o Conjunto B para uso com o TLS 1.2. Quando configurado para operação compatível com o Conjunto B, somente o conjunto restrito de algoritmos criptográficos listados são usados.
2. Um perfil de transição para uso com o TLS 1.0 ou o TLS 1.1. Este perfil permite a interoperabilidade com servidores não compatíveis com o Conjunto B. Quando configurado para a operação transicional do Conjunto B, a criptografia adicional e os algoritmos de hash podem ser usados.

O padrão do Conjunto B é conceitualmente semelhante ao FIPS 140-2, porque restringe o conjunto de algoritmos criptográficos ativados, a fim de fornecer um nível de garantia de segurança.

Nos sistemas Windows, UNIX and Linux, o IBM MQ é pode ser configurado para se adequar ao Conjunto B compatível com o perfil do TLS 1.2, mas não suporta o perfil de transição do Conjunto B. Veja informações adicionais na publicação “Criptografia do Conjunto B da NSA no IBM MQ” na página 40.

Referências relacionadas

“Federal Information Processing Standards” na página 20
O governo dos EUA produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. O National Institute for Standards and Technology (NIST) é um órgão importante ligado a sistemas e segurança de TI. O NIST produz recomendações e normas, inclusive Federal Information Processing Standards (FIPS).

Mecanismo de segurança do IBM MQ

Esta coleção de tópicos explica como é possível implementar os vários conceitos de segurança no IBM MQ.

O IBM MQ fornece mecanismos para implementar todos os conceitos de segurança introduzidos no “Conceitos e Mecanismos de Segurança” na página 5. Eles são discutidos em mais detalhes nas seções a seguir.

Identificação e autenticação em IBM MQ

No IBM MQ, é possível implementar a identificação e autenticação usando informações de contexto da mensagem e autenticação mútua.

Aqui estão alguns exemplos da identificação e autenticação em um ambiente do IBM MQ:

- Toda mensagem pode conter informações sobre *contexto de mensagem*. Essas informações ficam retidas no descritor de mensagens. Elas podem ser geradas pelo gerenciador de filas quando uma mensagem é colocada em uma fila por um aplicativo. Como alternativa, o aplicativo pode fornecer a informação caso o ID de usuário associado ao aplicativo tenha autorização para assim fazê-lo.

A informação de contexto em uma mensagem permite à aplicação de recepção que descubra o originador da mensagem. Ela contém, por exemplo, o nome do aplicativo que colocou a mensagem e o ID de usuário associados ao aplicativo.

- Quando um canal de mensagens se inicia, é possível que o agente de canal de mensagens (MCA) autentique seu parceiro em cada extremidade do canal. Essa técnica é conhecida como *autenticação mútua*. Para o MCA emitente, essa é a garantia de que o parceiro ao qual ele está prestes a enviar mensagens é genuíno. Para o MCA receptor, há uma garantia semelhante de que ele está prestes a receber mensagens de um parceiro genuíno.

Conceitos relacionados

"Identificação e autenticação" na página 6
Identificação é a capacidade de identificar exclusivamente um usuário de um sistema ou um aplicativo que esteja sendo executado no sistema. *Autenticação* é a capacidade de provar que um usuário ou um aplicativo é realmente quem essa pessoa ou o que esse aplicativo diz ser.

A autorização no IBM MQ

É possível usar a autorização para limitar o que indivíduos ou aplicativos específicos podem fazer em seu ambiente do IBM MQ.

Aqui estão alguns exemplos de autorização em um ambiente do IBM MQ:

- Permitir somente um administrador autorizado a emitir comandos para gerenciar os recursos do IBM MQ.
- Permitir que um aplicativo se conecte a um gerenciador de filas somente se o ID de usuário associado ao aplicativo estiver autorizado a fazê-lo.
- Permitir que um aplicativo abra somente as filas que são necessárias para sua função.
- Permitir que um aplicativo assine apenas os tópicos que forem necessários para sua função.
- Permitir que um aplicativo execute apenas operações em uma fila que sejam necessárias à sua função. Por exemplo, é possível que um aplicativo necessite somente procurar mensagens em uma fila especifica, e não colocar ou receber mensagens.

Para obter mais informações sobre como configurar a autorização, consulte "Planejando a autorização" na página 84 e os subtópicos associados.

Conceitos relacionados

"Autorização" na página 6
A *autorização* protege os recursos críticos em um sistema, limitando o acesso somente a usuários autorizados e seus aplicativos. Ele previne o uso não autorizado de um recurso ou o uso de um recurso de maneira não autorizada.

A auditoria no IBM MQ

O IBM MQ pode emitir mensagens de eventos para registrar que uma atividade incomum ocorreu.

Aqui estão alguns exemplos de auditoria em um ambiente do IBM MQ:

- Um aplicativo tenta abrir uma fila para que ele não está autorizado a abrir. Uma mensagem do evento de instrumentação é emitida. Inspecionando a mensagem do evento, você descobre que essa tentativa ocorreu e pode decidir qual ação é necessária.
- Um aplicativo tenta abrir um canal, mas a tentativa falhou porque o SSL não permite a conexão. Uma mensagem do evento de instrumentação é emitida. Inspecionando a mensagem do evento, você descobre que essa tentativa ocorreu e pode decidir qual ação é necessária.

Conceitos relacionados

"Auditoria" na página 6
Auditoria é o processo de gravação e verificação de eventos para detectar se qualquer atividade inesperada ou desautorizada ocorreu, ou se nenhuma tentativa foi feita para executar essa atividade.

Confidencialidade em IBM MQ

É possível implementar a confidencialidade no IBM MQ, criptografando as mensagens.

A confidencialidade pode ser assegurada em um ambiente IBM MQ da seguinte forma:

- Depois que um MCA de envio obtém uma mensagem de uma fila de transmissão, o IBM MQ usa TLS para criptografar a mensagem antes de ser enviada pela rede para o MCA de recebimento. Na outra extremidade do canal, a mensagem é descodificada antes que o MCA receptor coloque-a em sua fila de destino.
- Enquanto as mensagens são armazenadas em uma fila local, os mecanismos de controle de acesso fornecidos pelo IBM MQ podem ser considerados suficientes para proteger seus conteúdos contra a divulgação não autorizada No entanto, para um maior nível de segurança, é possível usar o Advanced Message Security para criptografar as mensagens armazenadas nas filas.
- 

As mensagens armazenadas em filas locais podem ser criptografadas em repouso usando a criptografia do conjunto de dados do z/OS

  Consulte a seção Confidencialidade para dados em repouso no IBM MQ for z/OS com criptografia do conjunto de dados. para obter informações adicionais.

Conceitos relacionados

"Sigilosidade" na página 7
O serviço de *confidencialidade* protege informações sensitivas de exposições não autorizadas.

Integridade de dados no IBM MQ

É possível usar um serviço de integridade de dados para detectar se uma mensagem foi modificada.

A integridade de dados pode ser assegurada em um ambiente do IBM MQ, da seguinte forma:

- É possível usar TLS para detectar se o conteúdo de uma mensagem foi deliberadamente modificado enquanto estava sendo transmitido por uma rede. No TLS, o algoritmo de trecho da mensagem fornece detecção de mensagens modificadas em trânsito.

  Todos os IBM MQ CipherSpecs fornecem um algoritmo de trecho da mensagem, exceto para TLS_RSA_WITH_NULL_NULL, que não fornece a integridade dos dados da mensagem.

  O IBM MQ detecta mensagens modificadas ao recebê-las; no recebimento de uma mensagem modificada, o IBM MQ emitirá uma mensagem de erro AMQ9661 e o canal será interrompido.
- Enquanto as mensagens são armazenadas em uma fila local, os mecanismos de controle de acesso fornecidos pelo IBM MQ podem ser considerados suficientes para evitar a modificação intencional do conteúdo das mensagens.

  No entanto, para obter um nível de segurança maior, é possível usar o Advanced Message Security para detectar se o conteúdo de uma mensagem foi intencionalmente modificado entre o momento que a mensagem foi colocada na fila e o momento em que foi recuperada.

  Após detectar uma mensagem modificada, o aplicativo tentará considerar a mensagem que recebe um código de retorno 2063 e, se estiver usando uma chamada MQGET, a mensagem será movida para o SYSTEM.PROTECTION.ERROR.QUEUE

Conceitos relacionados

"Integridade de dados" na página 7
O serviços *integridade dos dados* detecta se houve modificação não-autorizada dos dados.

Criptografia no IBM MQ

O IBM MQ fornece criptografia usando o protocolo Segurança da Camada de Transporte (TLS).

Para obter informações adicionais, consulte "Protocolos de segurança TLS no IBM MQ" na página 24.

Conceitos relacionados

"Conceitos criptográficos" na página 7

Esta coleção de tópicos descreve os conceitos de criptografia aplicáveis ao IBM MQ.

Protocolos de segurança TLS no IBM MQ

O IBM MQ suporta o protocolo da Segurança da Camada de Transporte (TLS) para fornecer segurança em nível de link para canais de mensagens e canais do MQI.

Os canais de mensagem e os canais de MQI podem usar o protocolo do TLS para fornecer a segurança em nível de link. Um MCA do responsável pela chamada é um cliente TLS e um MCA do respondente é um servidor do TLS. O IBM MQ suporta TLS 1.0 e TLS 1.2. É possível especificar os algoritmos criptográficos que são usados pelo protocolo do TLS fornecendo um CipherSpec como parte da definição de canal.

Nota: No IBM MQ 8.0.0 Fix Pack 2, o protocolo SSLv3 e o uso de alguns IBM MQ CipherSpecs foi descontinuado. Para obter mais informações, veja Descontinuação: protocolo SSLv3.

É possível usar os parâmetros SECPROT e SSLCIPH para exibir o protocolo de segurança e o CipherSpec em uso em um canal.

Em cada extremidade de um canal de mensagens, e na extremidade do servidor de um canal do MQI, o MCA atua em nome do gerenciador de filas ao qual está conectado. Durante o handshake do TLS, o MCA envia o certificado digital do gerenciador de filas para seu MCA parceiro na outra extremidade do canal. O código do IBM MQ na extremidade do cliente de um canal de MQI age em nome do usuário do aplicativo cliente IBM MQ. Durante o handshake do TLS, o código do IBM MQ envia o certificado digital do usuário ao MCA na extremidade do servidor do canal do MQI.

Os gerenciadores de filas e os usuários do cliente do IBM MQ não têm que ter certificados digitais pessoais associados a eles quando estiverem atuando como clientes TLS, a menos que SSLCAUTH(REQUIRED) seja especificado no lado do servidor do canal.

Os certificados digitais são armazenados em um *repositório de chaves*. O atributo **SSLKeyRepository** do gerenciador de filas especifica a localização do repositório de chaves que mantém o certificado digital do gerenciador de filas. Em um sistema do cliente de IBM MQ, a variável de ambiente MQSSLKEYR especifica a localização do repositório de chaves que mantém o certificado digital do usuário. Como alternativa, um aplicativo cliente do IBM MQ pode especificar seu local no campo **KeyRepository** da estrutura de opções de configuração de TLS, MQSCO, em uma chamada MQCONNX. Consulte os tópicos relacionados para obter mais informações sobre repositórios de chaves e como especificar onde eles estão localizados.

Suporte para TLS

O IBM MQ fornece suporte para o TLS 1.0 e o TLS 1.2 de acordo com a plataforma que estiver usando. Para obter mais informações sobre o protocolo do TLS, consulte as informações nos subtópicos.

IBM i
O suporte do TLS é integral para o sistema operacional do IBM i.

Os clientes Java e JMS
Esses clientes usam a JVM para fornecer o suporte do TLS.

UNIX, Linux, and Windows
O suporte do TLS é instalado com o IBM MQ.

z/OS
O suporte do TLS é integral para o sistema operacional do z/OS. O suporte do TLS no z/OS é conhecido como *SSL do sistema*.

Para obter informações sobre quaisquer pré-requisitos para o suporte do TLS do IBM MQ, consulte Requisitos do sistema para IBM MQ.

Conceitos relacionados

“Protocolos de segurança criptográficos: TLS” na página 15

Os protocolos de criptografia fornecem conexões seguras, permitindo que dois grupos de comuniquem com privacidade e integridade de dados. O protocolo Transport Layer Security (TLS) surgiu desse do Secure Sockets Layer (SSL). O IBM MQ suporta o TLS.

O repositório de chaves SSL/TLS

Uma conexão TLS mutualmente autenticada requer um repositório de chaves em cada término da conexão. O repositório de chaves inclui certificados digitais e chaves privadas.

Estas informações usam o termo geral *repositório de chaves* para descrever o armazenamento para certificados digitais e suas chaves privadas associadas. O repositório de chaves é referido por diferentes nomes em diferentes plataformas e ambientes que suportam TLS:

- IBM i No IBM i: *armazenamento de certificados*
- No Java e no JMS: *keystore* e *armazenamento confiável*
- ULW No UNIX, Linux, and Windows: *Arquivo do banco de dados de chave*
- z/OS No z/OS: *conjunto de chaves*

Para obter mais informações, veja “Certificados Digitais” na página 9 e “Conceitos de TLS (Transport Layer Security)” na página 15.

Uma conexão TLS mutualmente autenticada requer um repositório de chaves em cada término da conexão. O repositório de chaves pode conter os seguintes certificados e solicitações:

- Vários certificados de CA de várias Autoridades de Certificação que permitem que o gerenciador de filas ou o cliente verifique certificados recebidos de seu parceiro na extremidade remota da conexão. Certificados individuais podem estar em uma cadeia de certificados.
- Um ou mais certificados pessoais recebidos de uma Autoridade de Certificação. É possível associar um certificado pessoal diferente a cada gerenciador de filas ou IBM MQ MQI client. Os certificados pessoais serão essenciais em um cliente TLS se a autenticação mútua for necessária. Se a autenticação mútua não for necessária, os certificados pessoais não serão necessários no cliente. O repositório de chaves também pode conter a chave privada correspondente a cada certificado pessoal.
- As solicitações de certificados que estão aguardando para serem assinadas por uma autoridade de certificação confiável.

Para obter mais informações sobre como proteger seu repositório de chaves, consulte “Protegendo repositórios de chaves do IBM MQ” na página 26.

A localização do repositório de chaves depende da plataforma que você está utilizando:

IBM i **IBM i**

O repositório de chaves é um armazenamento de certificados. O armazenamento de certificados padrão do sistema se localiza em `/QIBM/UserData/ICSS/Cert/Server/Default` no IFS (integrated file system). O IBM MQ armazena a senha para o armazenamento de certificados em um *arquivo stash de senha*. Por exemplo, o arquivo stash para o gerenciador de filas `QM1` é `/QIBM/UserData/mqm/qmgrs/QM1/ssl/Stash.sth`.

Como alternativa, é possível especificar que o armazenamento de certificados do sistema IBM i deve ser usado em seu lugar. Para fazer isso, mude o valor do atributo **SSLKEYR** do gerenciador de filas para `*SYSTEM`. Esse valor indica que o gerenciador de filas deve usar o armazenamento de certificados do sistema e que o gerenciador de filas seja registrado para ser usado como um aplicativo com o Digital Certificate Manager (DCM).

O armazenamento de certificados também contém a chave privada para o gerenciador de filas.

ULW **Sistemas UNIX, Linux, and Windows**

O repositório de chaves é um arquivo do banco de dados de chaves. O nome do arquivo do banco de dados de chave deve ter uma extensão de arquivo de `.kdb`. Por exemplo, no UNIX and Linux, o arquivo do banco de dados de chaves padrão para o `QM1` do gerenciador de filas

é `/var/mqm/qmgrs/QM1/ssl/key.kdb`. Se o IBM MQ estiver instalado na localização padrão, o caminho equivalente em Windows será `C:\ProgramData\IBM\MQ\Qmgrs\QM1\ssl\key.kdb`.

Cada arquivo do banco de dados de chaves tem um arquivo stash de senha associado. Este arquivo mantém senhas codificadas que permitem que o programa acesse o banco de dados de chaves. O arquivo stash de senha deve estar no mesmo diretório e ter o mesmo arquivo stem que o banco de dados de chaves e deve terminar com o sufixo `.sth`, por exemplo, `/var/mqm/qmgrs/QM1/ssl/key.sth`

Nota: As placas de hardware de criptografia PKCS #11 podem conter os certificados e chaves que são, em outras situações, armazenados em um arquivo do banco de dados de chaves. Quando os certificados e chaves são mantidos em placas PKCS #11, o IBM MQ ainda requer acesso a um arquivo do banco de dados de chaves e um arquivo stash de senha.

Nos sistemas UNIX e Windows, o banco de dados de chaves também contém a chave privada para o certificado pessoal associado ao gerenciador de filas ou IBM MQ MQI client.

z/OS **z/OS**

Os certificados são mantidos em um conjunto de chaves em z/OS.

Outros gerenciadores de segurança externa (ESMs) também usam conjuntos de chave para armazenar certificados.

As chaves privadas são gerenciadas pelo RACF.

Protegendo repositórios de chaves do IBM MQ

O repositório de chaves para o IBM MQ é um arquivo. Certifique-se de que somente o usuário pretendido possa acessar o arquivo repositório de chaves. Isso impede um intruso ou outro usuário não autorizado de copiar o arquivo repositório de chaves para outro sistema, e então configurar um ID de usuário idêntico naquele sistema para personificar o usuário pretendido.

As permissões sobre os arquivos dependem da umask do usuário e da ferramenta usada. No Windows, as contas do IBM MQ requerem permissão `BypassTraverseChecking`, que significa que as permissões das pastas no caminho de arquivo não têm efeito.

Verifique as permissões dos arquivos de repositório de chaves e certifique-se de que os arquivos e pasta recipiente não sejam globalmente legíveis, de preferência, nem legíveis por grupos.

Seja qual for o sistema usado, é uma boa prática tornar o keystore somente leitura, apenas com o administrador tendo permissão de ativar operações de gravação para executar manutenção.

Na prática, você deve proteger todos os keystores, seja qual for a localização e se forem protegidos por senha ou não; proteja os repositórios de chaves.

Rótulos de Certificados Digitais, Entendendo os Requisitos

Ao configurar o TLS para usar certificados digitais, pode haver requisitos de rótulo específicos que devem ser seguidos, dependendo da plataforma usada e do método usado para a conexão.

O que é rótulo certificado?

Um rótulo de certificado é um identificador exclusivo que representa um certificado digital armazenado em um repositório de chaves e que fornece um nome legível conveniente com o qual se referir a um determinado certificado ao executar funções de gerenciamento de chaves. Você designa o rótulo certificado ao incluir um certificado em um repositório de chaves pela primeira vez.

O rótulo do certificado é separado dos campos **`Subject Distinguished Name`** ou **`Subject Common Name`** do certificado Observe que **`Subject Distinguished Name`** e **`Subject Common Name`** são campos dentro do próprio certificado. Eles são definidos quando o certificado é criado e não pode ser alterado. Se necessário, entretanto, é possível mudar o rótulo associado a um certificado digital.

Sintaxe do rótulo certificado

Um rótulo certificado pode conter letras, números e pontuação com as condições a seguir:

- Multi O rótulo certificado pode conter até 64 caracteres.
- z/OS O rótulo certificado pode conter até 32 caracteres.
- O rótulo do certificado pode conter espaços
- Os rótulos fazem distinção entre maiúsculas e minúsculas.
- Nos sistemas que usam EBCDIC katakana, não é possível usar caracteres minúsculos.

Requisitos adicionais para os valores do rótulo certificado são especificados nas seções a seguir.

Como o rótulo certificado é usado?

O IBM MQ usa rótulos certificados para localizar um certificado pessoal que é enviado durante o handshake TLS. Isso elimina a ambiguidade quando existe mais de um certificado pessoal no repositório de chaves.

É possível configurar o rótulo certificado para um valor de sua escolha. Se você não configurar um valor, um rótulo padrão será usado, seguindo uma convenção de nomenclatura dependendo da plataforma que você está usando. Para obter detalhes, consulte as seções a seguir sobre plataformas específicas.

Notes:

1. Não é possível configurar o rótulo certificado você mesmo em sistemas Java ou JMS.
2. Os canais autodefinidos criados por uma saída de channel automatic definition (CHAD) não podem configurar o rótulo certificado, porque o handshake TLS ocorreu pelo tempo que o canal é criado. Configurar o rótulo certificado em uma saída CHAD para canais de entrada não terá efeito.

Neste contexto, um cliente TLS se refere ao parceiro de conexão que inicia o handshake, que pode ser um cliente IBM MQ ou outro gerenciador de filas.

Durante o handshake do TLS, o cliente do TLS sempre obtém e valida um certificado digital a partir do servidor. Com a implementação do IBM MQ, o servidor TLS sempre solicita um certificado do cliente e o cliente sempre fornece um certificado para o servidor, se for encontrado. Se o cliente não puder localizar um certificado pessoal, o cliente enviará uma resposta no `certificate` para o servidor

O servidor do TLS sempre valida o certificado de cliente, se um for enviado. Se o cliente não enviar um certificado, a autenticação falhará se a extremidade do canal que está agindo como o servidor TLS estiver definida com o parâmetro **SSLCAUTH** configurado como *REQUIRED* ou um valor de parâmetro **SSLPEER** configurado.

Observe que os canais de entrada (incluindo receptor, solicitante, receptor de cluster, servidor não qualificado e canais de conexão do servidor) enviarão o certificado configurado apenas se a versão do IBM MQ do peer remoto suportar totalmente a configuração do rótulo certificado e o canal estiver usando um CipherSpec de TLS.

Um canal do servidor não qualificado é aquele que não tem o campo CONNAME configurado.

Em todos os outros casos, parâmetro **CERTLABL** do gerenciador de filas determina o certificado enviado. Em particular, o seguinte somente sempre recebe o certificado configurado pelo parâmetro **CERTLABL** do gerenciador de filas, independentemente da configuração do rótulo do canal específico:

- Antes de IBM MQ 9.1.1, todos os clientes Java e JMS atuais.
- V 9.1.1 De IBM MQ 9.1.1, Java e JMS clientes que suportam Server Name Indication (SNI), ou seja, certificados em uma base canal por canal.
- Versões do IBM MQ anteriores à IBM MQ 8.0.
- Clientes .NET gerenciados

Além disso, o certificado usado por um canal deve ser apropriado para o canal CipherSpec - consulte “Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45 para obter mais informações.

O IBM MQ 8.0 e mais recente suportam o uso de vários certificados no mesmo Gerenciador de Filas, utilizando um rótulo de certificado por canal especificado por meio do atributo **CERTLABL** na definição de canal. Os canais de entrada para o gerenciador de filas (por exemplo, conexão ou receptor do servidor) dependem de detectar o nome do canal usando Name Server Indication (SNI) TLS, a fim de apresentar o certificado correto do gerenciador de filas.

Se um canal se conectar ao gerenciador de filas de destino por meio do IBM MQ Internet Pass-Thru (MQIPT) e a rota MQIPT tiver ambos **SSLServer** e **SSLClient** configurado, haverá duas sessões TLS separadas entre os terminais e os dados SNI não fluem na interrupção da sessão. Isso evita que um certificado individual de canal seja utilizado no gerenciador da fila de destino para a conexão TLS entre o MQIPT e o gerenciador de filas. Para usar um certificado por canal no gerenciador de filas de destino, para uma conexão TLS que passa pelo MQIPT, a rota MQIPT deve usar o modo de proxy TLS, que encaminha todos os fluxos de controle TLS intactos, incluindo o nome do SNI. Para obter informações adicionais sobre o suporte TLS em MQIPT, consulte Suporte SSL/TLS.

Os certificados que são usados para conexões TLS finalizadas ou iniciadas por MQIPT são configurados individualmente para cada rota, por exemplo usando as propriedades de rota **SSLServerSiteLabel** e **SSLClientSiteLabel**.

Para obter mais informações sobre como conectar um gerenciador de filas usando autenticação unilateral, ou seja, quando o cliente TLS não envia um certificado, veja Conectando dois gerenciadores de filas usando autenticação unilateral.

Sistemas multiplataformas

Em Multiplataformas, o servidor TLS envia um certificado para o cliente.

Para gerenciadores de filas e clientes respectivamente, as fontes a seguir são procuradas em sequência para um valor não vazio. O primeiro valor não vazio determina o rótulo certificado. O rótulo certificado deve existir no repositório de chaves. Se não for localizado um certificado correspondente nas maiúsculas e minúsculas e no formato corretos que corresponda a um rótulo, ocorrerá um erro e o handshake TLS falhará.

Gerenciadores de filas

1. Atributo **CERTLABL** do rótulo certificado do canal.
2. Atributo **CERTLABL** do rótulo certificado do gerenciador de filas.
3. Um padrão, que está no formato: `ibmwebspheremq` com o nome do gerenciador de filas anexado, tudo em minúsculas. Por exemplo, para um gerenciador de filas chamado `QM1`, o rótulo certificado padrão é `ibmwebspheremqqm1`.

Clientes do IBM MQ

1. Atributo de rótulo de certificado **CERTLABL** na definição de canal CLNTCONN.
2. Atributo **CertificateLabel** da estrutura MQSCO.
3. Variável de ambiente **MQCERTLABL**.
4. Arquivo `.ini` de cliente (em sua seção SSL) atributo **CertificateLabel**
5. Um padrão, que está no formato: `ibmwebspheremq` com o ID do usuário que o aplicativo cliente está executando como anexado, tudo em minúsculas. Por exemplo, para um ID do usuário de USER1, o rótulo certificado padrão é `ibmwebspheremquser1`.

Sistemas z/OS

Clientes IBM MQ não são suportados no z/OS. No entanto, um gerenciador de filas do z/OS pode agir na função de um cliente TLS ao iniciar uma conexão ou um servidor TLS ao aceitar uma solicitação de conexão. Os requisitos de rótulo certificado para gerenciadores de filas do z/OS se aplicam a ambas as funções e são diferentes dos requisitos em Multiplataformas.

Para gerenciadores de filas e clientes respectivamente, as fontes a seguir são procuradas em sequência para um valor não vazio. O primeiro valor não vazio determina o rótulo certificado. O rótulo certificado deve existir no repositório de chaves. Se não for localizado um certificado correspondente nas maiúsculas e minúsculas e no formato corretos que corresponda a um rótulo, ocorrerá um erro e o handshake TLS falhará.

1. Atributo de rótulo certificado do canal, **CERTLABL**.
2. Se compartilhado, o atributo do rótulo certificado do grupo de filas compartilhadas, **CERTQSGL**.

   Se não compartilhado, o atributo do rótulo certificado do gerenciador de filas, **CERTLABL**.
3. Um padrão, que está no formato: `ibmWebSphereMQ` com o nome do gerenciador de filas ou o grupo de filas compartilhadas anexado. Observe que esta sequência faz distinção entre maiúsculas e minúsculas deve ser escrita conforme mostrado. Por exemplo, para um gerenciador de filas chamado `QM1`, o rótulo certificado padrão é `ibmWebSphereMQQM1`.
4. Se não houver um certificado localizado com o formato na opção “3” na página 29, o IBM MQ tentará utilizar o certificado marcado como padrão no conjunto de chaves.

Para obter informações sobre como exibir o repositório de chaves, consulte “Localizando o repositório de chaves para um gerenciador de filas no z/OS” na página 323.

Os clientes IBM MQ Java e IBM MQ JMS

Os clientes IBM MQ Java e IBM MQ JMS usam os recursos de seu provedor de Java Secure Socket Extension (JSSE) para selecionar um certificado pessoal durante o handshake TLS e, portanto, não estão sujeitos a requisitos de rótulo certificado.

O comportamento padrão é que o cliente JSSE itere através de certificados no repositório de chaves, selecionando o primeiro certificado pessoal aceitável localizado. No entanto, esse comportamento é apenas um padrão, e depende da implementação do provedor JSSE.

Além disso, a interface JSSE é altamente customizável por meio de configuração e acesso direto no tempo de execução pelo aplicativo. Consulte a documentação fornecida pelo provedor JSSE para obter detalhes específicos.

Para resolução de problemas ou para entender melhor o handshake executado pelo aplicativo cliente do IBM MQ Java em combinação com o provedor JSSE específico, é possível ativar a depuração configurando `javax.net.debug=ssl` no ambiente JVM.

É possível configurar a variável dentro do aplicativo, através da configuração ou entrando em `-Djavax.net.debug=ssl` na linha de comandos.

Atualizando o repositório de chaves do gerenciador de filas
Ao mudar o conteúdo de um repositório de chaves, o gerenciador de filas não coleta imediatamente o novo conteúdo. Para um gerenciador de filas usar o novo conteúdo do repositório de chaves, deve-se emitir o comando REFRESH SECURITY TYPE(SSL).

Esse processo é intencional e evita a situação em que vários canais em execução poderia usar versões diferentes de um repositório de chaves. Como um controle de segurança, apenas uma versão de um repositório de chaves pode ser carregada pelo gerenciador de filas a qualquer momento.

Para obter mais informações sobre o comando REFRESH SECURITY TYPE(SSL), consulte REFRESH SECURITY.

Também é possível atualizar um repositório de chaves usando os comandos PCF ou o IBM MQ Explorer. Para obter mais informações, veja o comando MQCMD_REFRESH_SECURITY e o tópico *Atualizando a segurança TLS (Segurança da Camada de Transporte)* na seção do IBM MQ Explorer da documentação deste produto.

Conceitos relacionados
“Atualizando a visualização de um cliente do conteúdo do repositório de chaves SSL/TLS e configurações de SSl/TLS” na página 30

Para atualizar o aplicativo cliente com o conteúdo atualizado do repositório de chaves, deve-se parar e reiniciar o aplicativo cliente.

Atualizando a visualização de um cliente do conteúdo do repositório de chaves SSL/TLS e configurações de SSl/TLS
Para atualizar o aplicativo cliente com o conteúdo atualizado do repositório de chaves, deve-se parar e reiniciar o aplicativo cliente.

Não é possível atualizar a segurança em um cliente IBM MQ; não há equivalente do comando REFRESH SECURITY TYPE(SSL) para clientes (consulte REFRESH SECURITY) para obter mais informações.

Deve-se parar e reiniciar o aplicativo sempre que o certificado de segurança for mudado, para atualizar o aplicativo cliente com o conteúdo atualizado do repositório de chaves.

Se reiniciar o canal atualiza as configurações, e se o seu aplicativo tem reconexão lógica, é possível atualizar a segurança no cliente emitindo o comando STOP CHL STATUS(INACTIVE).

Conceitos relacionados
"Atualizando o repositório de chaves do gerenciador de filas" na página 29
Ao mudar o conteúdo de um repositório de chaves, o gerenciador de filas não coleta imediatamente o novo conteúdo. Para um gerenciador de filas usar o novo conteúdo do repositório de chaves, deve-se emitir o comando REFRESH SECURITY TYPE(SSL).

Proteção de senha do MQCSP
A partir do IBM MQ 8.0, é possível enviar as senhas que estão incluídas na estrutura MQCSP protegida, usando a funcionalidade do IBM MQ, ou criptografada, usando a criptografia TLS.

Importante: A proteção de senha MQCSP é útil para propósitos de teste e desenvolvimento, já que usar a proteção de senha MQCSP é mais simples do que configurar a criptografia TLS, mas não tão seguro. Para propósitos de produção, é necessário usar a criptografia TLS em preferência à proteção de senha do IBM MQ, especialmente quando a rede entre o cliente e o gerenciador de filas é não confiável, já que a criptografia TLS é mais segura.

Se a sua preocupação for exatamente sobre qual criptografia está sendo usada e quanta proteção ela oferece, será necessário usar a criptografia TLS integral. Nessa situação, os algoritmos são publicamente conhecidos e é possível selecionar aquele apropriado para sua empresa usando o atributo do canal **SSLCIPH**.

Para obter mais informações sobre a estrutura MQCSP, consulte Estrutura MQCSP.

A proteção com senha é usada quando todas as condições a seguir forem atendidas:

- Ambas as extremidades da conexão estão usando o IBM MQ 8.0 ou mais recente.
- O canal não está usando a criptografia TLS. Um canal não usará a criptografia TLS se o canal tiver um atributo **SSLCIPH** em branco ou o atributo **SSLCIPH** estiver configurado para uma CipherSpec que não fornece criptografia. Cifras nulas, por exemplo, NULL_SHA, não fornecem criptografia.
- Você configurou **MQCSPAuthenticationType** para MQCSP_AUTH_USER_ID_AND_PWD Configurar esse valor permite que mais verificações sejam avaliadas para decidir se a proteção de senha foi feita. O valor padrão de **MQCSP**.**AuthenticationType** é MQCSP_AUTH_NONE.. Com a configuração padrão nenhuma proteção de senha é feita. Para obter mais informações, consulte **AuthenticationType**..
- Se o cliente for o IBM MQ Explorer e o modo de compatibilidade de identificação do usuário não estiver ativado, o que não é o padrão. Essa condição é aplicável apenas ao IBM MQ Explorer.

Se essas condições não forem atendidas, a senha será enviada em texto simples, a menos que seja proibida pela definição de configuração **PasswordProtection**.

A definição de configuração `PasswordProtection`

O atributo **PasswordProtection** na seção Canais dos arquivos de configuração .ini do cliente e do gerenciador de filas pode evitar que as senhas sejam enviadas em texto simples. O atributo pode assumir um dos valores a seguir. O valor padrão é `compatible`:

compatíveis
A senha poderá ser enviada em texto simples se o gerenciador de filas ou cliente estiver executando uma versão do IBM MQ anterior à IBM MQ 8.0. Ou seja, as senhas de texto simples são permitidas para compatibilidade.

Portanto:

- A senha será enviada criptografada pelo CipherSpec do TLS se a criptografia do TLS for usada e o CipherSpec não for nulo.
- A senha será enviada em texto simples se o gerenciador de filas ou o cliente estiver executando uma versão do IBM MQ anterior à IBM MQ 8.0 e a criptografia TLS não for usada. A senha é enviada em texto simples porque as versões do IBM MQ anteriores à IBM MQ 8.0 podem enviar senhas somente em texto simples.
- A senha será enviada protegida se o gerenciador de filas e o cliente estiverem executando uma versão de IBM MQ em IBM MQ 8.0 ou posterior e um CipherSpec nulo for usado ou a criptografia TLS não for usada. **MQCSP**.O **AuthenticationType** deve ser configurado como MQCSP_AUTH_USER_ID_AND_PWD
- A conexão falhará antes que a senha seja enviada se o gerenciador de fila e o cliente estiverem executando uma versão de IBM MQ em IBM MQ 8.0 ou posterior e **MQCSP**.O **AuthenticationType** não está configurado como MQCSP_AUTH_USER_ID_AND_PWD

sempre
A senha deve ser criptografada com um CipherSpec que não seja um CipherSpecnulo ou **MQCSP**.O **AuthenticationType** deve ser configurado como MQCSP_AUTH_USER_ID_AND_PWD Caso contrário, a conexão falhará. Ou seja, senhas de texto simples não são permitidas.

Portanto:

- A senha será enviada criptografada pelo CipherSpec do TLS se a criptografia do TLS for usada e o CipherSpec não for nulo.
- A senha será enviada protegida se o gerenciador de filas e o cliente estiverem executando uma versão de IBM MQ em IBM MQ 8.0 ou mais recente e a criptografia TLS não for usada ou um CipherSpec nulo for usado. **MQCSP**.O **AuthenticationType** deve ser configurado como MQCSP_AUTH_USER_ID_AND_PWD
- A conexão falhará antes de a senha ser enviada se o gerenciador de filas ou o cliente estiver executando uma versão do IBM MQ anterior à IBM MQ 8.0 e a criptografia TLS não for usada. Como as versões do IBM MQ anteriores à IBM MQ 8.0 podem enviar senhas somente em texto simples e `always` requer que a senha seja criptografada ou protegida, a conexão falhará.

opcional
A senha pode, opcionalmente, ser enviada protegida, mas será enviada em texto simples se **MQCSP**.O **AuthenticationType** não está configurado como MQCSP_AUTH_USER_ID_AND_PWD Ou seja, senhas de texto simples são permitidas serem enviadas por qualquer cliente.

Portanto:

- A senha será enviada criptografada pelo CipherSpec do TLS se a criptografia do TLS for usada e o CipherSpec não for nulo.
- A senha será enviada em texto simples se um CipherSpec nulo for usado e **MQCSP**.O **AuthenticationType** não está configurado como MQCSP_AUTH_USER_ID_AND_PWD
- A senha será enviada em texto simples se o gerenciador de filas ou o cliente estiver executando uma versão do IBM MQ anterior à IBM MQ 8.0 e a criptografia TLS não for usada. A senha é enviada em texto simples porque as versões do IBM MQ anteriores à IBM MQ 8.0 podem enviar senhas somente em texto simples.
- A senha será enviada protegida se o gerenciador de filas e o cliente estiverem executando uma versão de IBM MQ em IBM MQ 8.0 ou posterior, a criptografia TLS não for usada ou um CipherSpec nulo for usado e **MQCSP**.O **AuthenticationType** é configurado como MQCSP_AUTH_USER_ID_AND_PWD

avisar
Senhas de texto simples são permitidas para serem enviadas por qualquer cliente. Se uma senha de texto sem formatação for recebida, uma mensagem de aviso (AMQ9297) será gravada nos logs de erros do gerenciador de filas.

Para clientes Java e JMS, o comportamento do atributo **PasswordProtection** mudará dependendo da escolha de usar o modo de compatibilidade ou o modo MQCSP:

- Se os clientes Java e JMS estiverem operando no modo de compatibilidade, uma estrutura MQCSP não será transmitida durante o processamento de conexão. Portanto, o comportamento do atributo **PasswordProtection** é o mesmo comportamento conforme descrito para clientes que estão executando uma versão do IBM MQ anterior à IBM MQ 8.0.
- Se os clientes Java e JMS estiverem operando no modo MQCSP, o comportamento do atributo **PasswordProtection** será o comportamento conforme descrito.

Para obter mais informações sobre a autenticação de conexão com clientes Java e JMS, veja "Autenticação de conexão com o cliente Java" na página 78.

Digital Certificate Manager (DCM)

Use o DCM para gerenciar certificados digitais e chaves privadas em IBM i.

O Digital Certificate Manager (DCM) permite gerenciar certificados digitais e usá-los em aplicativos seguros no servidor IBM i. Com o Digital Certificate Manager, é possível solicitar e processar certificados digitais das Autoridades de Certificação (CAs) ou de terceiros. Também é possível atuar como uma Autoridade de Certificação local para criar e gerenciar certificados digitais para seus usuários.

O DCM também suporta o uso de Listas de Revogação de Certificado para fornecer um certificado e um processo de validação de aplicativo mais consistentes. É possível usar o DCM para definir o local onde uma CRL de Autoridade de Certificação específica reside em um servidor LDAP, para que o IBM MQ possa verificar se um certificado específico ainda não foi revogado.

O DCM suporta e pode detectar automaticamente certificados em uma variedade de formatos. Quando o DCM detectar um certificado codificado pelo PKCS #12, ou um certificado PKCS #7 que contém dados criptografados, ele automaticamente solicitará ao usuário inserir a senha que foi utilizada para criptografar o certificado. O DCM não solicita os certificados PKCS #7 que não contém dados criptografados.

O DCM fornece uma interface com o usuário baseada em navegador que pode ser utilizada para gerenciar certificados digitais para os aplicativos e usuários. A interface com o usuário é dividida em dois quadros principais: um quadro de navegação e um quadro de tarefas.

Utilize o quadro de navegação para selecionar as tarefas para gerenciar os certificados ou os aplicativos que os utilizam. Algumas tarefas individuais são mostradas diretamente no quadro de navegação principal, mas a maioria das tarefas no quadro de navegação são organizadas em categorias. Por exemplo, Gerenciar Certificados é uma categoria de tarefa que contém várias tarefas individuais orientadas, tais como Visualizar Certificado, Renovar Certificado e Importar Certificado. Se um item no quadro de navegação for uma categoria que contém mais de uma tarefa, uma seta é exibida à esquerda dele. A seta indica que quando um link da categoria é selecionado, uma lista expandida de tarefas será exibida, permitindo escolher quais tarefas serão desempenhadas.

Para obter informações importantes sobre DCM, consulte as seguintes publicações do IBM Redbooks:

- Segurança de rede com fio do *IBM i: OS/400 V5R1 DCM e aprimoramentos criptográficos*, SG24-6168. Especificamente, consulte os apêndices para informações essenciais sobre como configurar seu sistema IBM i como um CA local.
- *segurança de internet AS/400: desenvolvendo uma infraestrutura de certificado digital*, SG24-5659. Especificamente, consulte o Capítulo 5. Gerenciador de certificado *digital para AS/400*, que explica o AS/400 DCM.

FIPS (Federal Information Processing Standards)

Este tópico apresenta o Federal Information Processing Standards (FIPS) Cryptomodule Validation Program do National Institute of Standards and Technology dos EUA e as funções criptográficas que podem ser usadas nos canais TLS.

Estas informações se aplicam às seguintes plataformas:

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

ULW Para obter mais informações sobre a conformidade com o FIPS 140-2 de uma conexão TLS do IBM MQ no UNIX, Linux, and Windows, consulte "Federal Information Processing Standards (FIPS) para UNIX, Linux, and Windows" na página 33.

z/OS Para obter mais informações sobre a conformidade com o FIPS 140-2 de uma conexão TLS do IBM MQ no z/OS, consulte "Federal Information Processing Standards (FIPS) para z/OS" na página 36.

Se o hardware de criptografia estiver presente, os módulos de criptografia usados pelo IBM MQ podem ser configurados para ser aqueles fornecidos pelo fabricante do hardware. Se isso for feito, a configuração só ficará em conformidade com o FIPS se esses módulos criptográficos forem certificados pelo FIPS.

Com o passar do tempo, os Federal Information Processing Standards são atualizados para refletirem novos ataques contra algoritmos de criptografia e protocolos. Por exemplo, alguns CipherSpecs podem deixar de ser certificados por FIPS. Quando tais mudanças ocorrem, o IBM MQ também é atualizado para implementar o padrão mais recente. Como um resultado, você poderá ver as mudanças no comportamento após a aplicação da manutenção.

Conceitos relacionados

"Especificando que Apenas CipherSpecs Certificados por FIPS São Usados no Tempo de Execução no Cliente de MQI" na página 272
Crie seus repositórios de chaves usando software compatível com FIPS e, em seguida, especifique que o canal deve usar CipherSpecs certificados por FIPS.

"Usando runmqckm, runmqakm e strmqikm para gerenciar certificados digitais" na página 289
Nos sistemas UNIX, Linux, and Windows, gerencie chaves e certificados digitais com a GUI do **strmqikm** (iKeyman) ou na linha de comandos usando **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

Tarefas relacionadas

Ativando o TLS no IBM MQ classes for Java

Usando Segurança da Camada de Transporte (TLS) com o IBM MQ classes for JMS

Referências relacionadas

Propriedades de TLS de objetos do JMS

"Federal Information Processing Standards" na página 20
O governo dos EUA produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. O National Institute for Standards and Technology (NIST) é um órgão importante ligado a sistemas e segurança de TI. O NIST produz recomendações e normas, inclusive Federal Information Processing Standards (FIPS).

ULW *Federal Information Processing Standards (FIPS) para UNIX, Linux, and Windows*

Quando a criptografia é necessária em um canal SSL/TLS em sistemas Windows, UNIX and Linux, o IBM MQ usa um pacote de criptografia chamado IBM Crypto for C (ICC). Nas plataformas Windows, UNIX and Linux, o software ICC passou no Federal Information Processing Standards (FIPS) Cryptomodule Validation Program do US National Institute of Standards and Technology, no nível 140-2.

A conformidade com o FIPS 140-2 de uma conexão TLS do IBM MQ em sistemas Windows e UNIX and Linux ocorre da maneira a seguir:

- Para todos os canais de mensagens do IBM MQ (exceto os tipos de canais CLNTCONN), a conexão será compatível com o FIPS se as seguintes condições forem atendidas:

  - A versão do ICC do GSKit instalada foi certificada como compatível com o FIPS 140-2 na versão do sistema operacional e arquitetura de hardware instaladas.
  - O atributo SSLFIPS do gerenciador de filas foi configurado para YES.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.
- Para todos os aplicativos do IBM MQ MQI client, a conexão usa GSKit e será compatível com o FIPS se as seguintes condições forem atendidas:
  - A versão do ICC do GSKit instalada foi certificada como compatível com o FIPS 140-2 na versão do sistema operacional e arquitetura de hardware instaladas.
  - Você especificou que somente a criptografia certificada para FIPS deve ser usada, conforme descrito no tópico relacionado para o cliente de MQI.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.
- Para aplicativos IBM MQ classes for Java que usam o modo cliente, a conexão usa as implementações TLS do JRE e será compatível com o FIPS se as condições forem atendidas:
  - O Java Runtime Environment usado para executar o aplicativo for compatível com o FIPS na versão do sistema operacional e arquitetura de hardware instaladas.
  - Você especificou que somente a criptografia certificada para FIPS deve ser usada, conforme descrito no tópico relacionado para o cliente do Java.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.
- Para aplicativos IBM MQ classes for JMS que usam o modo cliente, a conexão usa as implementações TLS do JRE e será compatível com o FIPS se as condições forem atendidas:
  - O Java Runtime Environment usado para executar o aplicativo for compatível com o FIPS na versão do sistema operacional e arquitetura de hardware instaladas.
  - Você especificou que somente a criptografia certificada para FIPS deve ser usada, conforme descrito no tópico relacionado para o cliente do JMS.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.
- Para aplicativos cliente não gerenciados do .NET, a conexão usa GSKit e será compatível com o FIPS se as seguintes condições forem atendidas:
  - A versão do ICC do GSKit instalada foi certificada como compatível com o FIPS 140-2 na versão do sistema operacional e arquitetura de hardware instaladas.
  - Você especificou que somente a criptografia certificada para FIPS deve ser usada, conforme descrito no tópico relacionado para o cliente do .NET.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.
- Para aplicativos cliente não gerenciados do .NET XMS, a conexão usa GSKit e será compatível com o FIPS se as seguintes condições forem atendidas:
  - A versão do ICC do GSKit instalada foi certificada como compatível com o FIPS 140-2 na versão do sistema operacional e arquitetura de hardware instaladas.
  - Você especificou que somente a criptografia certificada para FIPS deve ser usada, conforme descrito na documentação do .NET XMS.
  - Todos os repositórios de chaves foram criados e manipulados usando somente software compatível com FIPS, como **runmqakm** com a opção `-fips`.

Todas as plataformas suportadas são certificados pelo FIPS 140-2, exceto conforme observado no arquivo leia-me incluído com cada fix pack ou pacote de atualizações.

Para conexões TLS que usam o GSKit, o componente que é certificado pelo FIPS 140-2 é denominado *ICC*. É a versão desse componente que determina a conformidade com o FIPS do GSKit em qualquer plataforma fornecida. Para determinar a versão do ICC instalada atualmente, execute o comando **dspmqver -p 64 -v**.

Aqui está um exemplo de extrato da saída **dspmqver -p 64 -v** relacionada ao 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.
@ (#) Todos os direitos reservados. US Government Users
@(#)         Restricted Rights - Use, duplication or disclosure
@(#)         restricted by GSA ADP Schedule Contract with 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:
```

A instrução de certificação NIST para o GSKit ICC 8 (incluído no GSKit 8) pode ser localizada no endereço a seguir: Cryptographic Module Validation Program.

Se o hardware de criptografia estiver presente, os módulos de criptografia usados pelo IBM MQ podem ser configurados para ser aqueles fornecidos pelo fabricante do hardware. Se isso for feito, a configuração só ficará em conformidade com o FIPS se esses módulos criptográficos forem certificados pelo FIPS.

Nota: Os clientes SSL e TLS x86 de 32 bits do Solaris configurados para a operação compatível com FIPS 140-2 falham quando executados em sistemas Intel. Esta falha ocorre porque o arquivo de biblioteca GSKit-Crypto Solaris x86 32 bits compatível com FIPS 140-2 não carrega no Intel Chipset. Nos sistemas afetados, o erro AMQ9655 é relatado no log de erros do cliente. Para resolver esse problema, desative a conformidade com o FIPS 140-2 ou recompile o aplicativo cliente de 64 bits, porque o código de 64 bits não é afetado.

Restrições do Padrão de Criptografia de Dados triplo impostas ao operar em conformidade com o FIPS 140-2

Quando o IBM MQ está configurado para operar em conformidade com o FIPS 140-2, restrições adicionais são aplicadas no que se refere ao CipherSpecs do Padrão de Criptografia de Dados triplo (3DES). Essas restrições permitem a conformidade com a recomendação do US NIST SP800-67.

1. Todas as partes do Padrão de Criptografia de Dados triplo devem ser exclusivas.
2. Nenhuma parte do Padrão de Criptografia de Dados triplo pode ser uma chave Weak, Semi-Weak ou Possibly-Weak, de acordo com as definições no NIST SP800-67.
3. Não mais que 32 GB de dados podem ser transmitidos através da conexão antes que uma reconfiguração de chave secreta deva ocorrer. Por padrão, o IBM MQ não reconfigura a chave de sessão secreta, de modo que esta redefinição deve ser configurada. Falha ao ativar a reconfiguração da chave secreta ao usar um CipherSpec do Padrão de Criptografia de Dados triplo e resultados de conformidade com o FIPS 140-2 no fechamento da conexão com o erro AMQ9288 após a contagem máxima de bytes exceder. Para obter informações sobre como definir a reconfiguração de chave secreta, consulte “Reconfigurando as chaves secretas SSL e TLS” na página 450.

O IBM MQ gera chaves de sessão do Triple DES que já cumprem as regras 1 e 2. No entanto, para atender a terceira restrição, deve-se ativar a reconfiguração de chave secreta ao usar as CipherSpecs do Triple DES em uma configuração 140-2 do FIPS. Como alternativa, é possível evitar o uso do Padrão de Criptografia de Dados triplo.

Conceitos relacionados

“Especificando que Apenas CipherSpecs Certificados por FIPS São Usados no Tempo de Execução no Cliente de MQI” na página 272

Crie seus repositórios de chaves usando software compatível com FIPS e, em seguida, especifique que o canal deve usar CipherSpecs certificados por FIPS.

"Usando runmqckm, runmqakm e strmqikm para gerenciar certificados digitais" na página 289
Nos sistemas UNIX, Linux, and Windows, gerencie chaves e certificados digitais com a GUI do **strmqikm** (iKeyman) ou na linha de comandos usando **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

Tarefas relacionadas

Ativando o TLS no IBM MQ classes for Java

Usando Segurança da Camada de Transporte (TLS) com o IBM MQ classes for JMS

Referências relacionadas

Propriedades de TLS de objetos do JMS

"Federal Information Processing Standards" na página 20
O governo dos EUA produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. O National Institute for Standards and Technology (NIST) é um órgão importante ligado a sistemas e segurança de TI. O NIST produz recomendações e normas, inclusive Federal Information Processing Standards (FIPS).

z/OS *Federal Information Processing Standards (FIPS) para z/OS*

Quando a criptografia é necessária em um canal SSL/TLS no z/OS, o IBM MQ usa um serviço chamado SSL do Sistema. O objetivo do SSL do Sistema é fornecer a capacidade de executar com segurança em um modo projetado para seguir o Federal Information Processing Standards (FIPS) Cryptomodule Validation Program do US National Institute of Standards and Technology, no nível 140-2.

Ao implementar conexões compatíveis com FIPS 140-2 com conexões TLS do IBM MQ, existem vários pontos a considerar:

- Para ativar os canais de mensagem do IBM MQ para conformidade com o FIPS, assegure-se de que as seguintes condições sejam atendidas:
  - FMID do nível de segurança 3 do SSL do Sistema está instalado e configurado (consulte Planejando instalar o IBM MQ).
  - Módulos do SSL do Sistema são validados.
  - O atributo SSLFIPS do gerenciador de filas foi configurado como **YES**.

Ao executar no modo FIPS, o SSL do Sistema explora o Auxílio para função de criptografia (CPACF) quando disponível. As funções criptográficas executadas pelo hardware suportado por ICSF ao executar em um modo não FIPS a ser explorado ao executar no modo FIPS, com a exceção da geração de assinatura RSA que deve ser executada no software.

Tabela 2. Diferenças entre o suporte de algoritmo de modo FIPS e não FIPS.

	Não FIPS		**FIPS**	
Algoritmo	**Tamanhos de chave**	**Hardware**	**Tamanhos de chave**	**Hardware**
RC2	40 e 128			
RC4	40 e 128			
Padrão de Criptografia de Dados	56	x		
TDES	168	x	168	x
Padrão de Criptografia Avançado	128 e 256	x	128 e 256	x
MD5	48			

Tabela 2. Diferenças entre o suporte de algoritmo de modo FIPS e não FIPS. (continuação)				
	Não FIPS		**FIPS**	
Algoritmo	**Tamanhos de chave**	**Hardware**	**Tamanhos de chave**	**Hardware**
SHA-1	160	x	160	x
SHA-2	224, 256, 384 e 512	x	224, 256, 384 e 512	x
RSA	512-4096	x	1024-4096	x
DSA	512-1024		1024	
DH	512-2048		2048	

No modo FIPS, o SSL do sistema só pode utilizar certificados que utilizam os algoritmos e tamanhos de chave mostrados na Tabela 1. Durante a validação do certificado X.509, se um algoritmo que é incompatível com o modo FIPS for encontrado, o certificado não poderá ser usado e será tratado como inválido.

Para os aplicativos de classes do IBM MQ usando o modo cliente dentro do WebSphere Application Server, consulte o Suporte do Federal Information Processing Standard.

Para obter informações sobre a configuração do módulo SSL do sistema, consulte Configuração de verificação do módulo SSL do sistema.

Referências relacionadas

"Federal Information Processing Standards" na página 20
O governo dos EUA produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. O National Institute for Standards and Technology (NIST) é um órgão importante ligado a sistemas e segurança de TI. O NIST produz recomendações e normas, inclusive Federal Information Processing Standards (FIPS).

Multi

Verificando a configuração de TLS do seu gerenciador de filas com `mqcertck`

O comando **MQCERTCK** é uma ferramenta para procurar erros comuns na configuração de TLS do seu gerenciador de filas e fornece algumas sugestões para resolver problemas.

Introdução

O comando **`mqcertck`** verifica:

- Existência e permissões do repositório de chaves do gerenciador de filas, referenciado no atributo **SSLKEYR** do gerenciador de filas.
- Existência e validade do certificado para o certificado do gerenciador de filas, referenciado no atributo **CERTLABL** do gerenciador de filas.
- Existência e validade de quaisquer certificados referenciados nos atributos **CERTLABL** do canal ativado para TLS.
- o repositório de chaves e os certificados dos aplicativos clientes, incluindo a verificação de que os certificados estão autorizados com o gerenciador de filas.

Nota: O comando **`mqcertck`** não está disponível no z/OS ou no IBM i.

Uso

Para usar o comando **`mqcertck`**, execute o comando `mqcertck`, juntamente com os parâmetros necessários e quaisquer parâmetros opcionais requeridos em uma linha de comandos.

Veja mqcertck para obter uma descrição do comando e os parâmetros que o comando utiliza.

exemplo

Você acabou de configurar o QM1 do gerenciador de filas para permitir conexões TLS de clientes que se conectam ao canal SVRCONN do gerenciador de filas.

Você está usando o recurso de vários certificados e, portanto, o gerenciador de filas e o canal têm um rótulo de certificado especificado em seus atributos **CERTLABL**. Ao criar o canal, você cometeu um erro no atributo **CERTLABL** do canal, portanto, quando um cliente tenta se conectar, o gerenciador de filas retorna um código de retorno 2393 de MQRC_SSL_INITIALIZATION_ERROR.

Antes de ativar o gerenciador de filas, você usa o comando **mqcertck** para verificar a configuração de TLS do gerenciador de filas.

Você executa o comando `mqcertck QM1` e recebe a saída a seguir:

```
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.
|
+-----------------------------------------------------------
```

Essa saída solicita que você verifique a definição do seu canal para o canal de conexão do servidor MQCERTCK.CHANNEL. Aqui, você vê o erro que cometeu e pode corrigi-lo antes de executar o comando `mqcertck` novamente para verificar se resolveu o problema.

Verificando as conexões do cliente

O comando **mqcertck** tem a capacidade de verificar os repositórios de chaves do cliente, bem como a configuração de TLS do gerenciador de filas. Para fazer isso, o **mqcertck** precisa ser capaz de acessar o repositório de chaves do cliente na máquina executando o gerenciador de filas.

Ao executar o comando **mqcertck**, se você fornecer o parâmetro **-clientkeyr** com o local do repositório de chaves do cliente (exceto a extensão), o **mqcertck** verificará esse repositório de chaves com relação ao gerenciador de filas.

Se você souber qual canal o cliente usará para se conectar ao gerenciador de filas, poderá especificar isso com o sinalizador **-clientchannel**.

Se o cliente estiver usando a autenticação mútua para se conectar ao gerenciador de filas, será possível usar o parâmetro **-clientusername** ou **-clientlabel** para informar ao comando **mqcertck** qual certificado usar no repositório de chaves do cliente.

Se você estiver usando o certificado padrão e não fornecer um rótulo de certificado ao aplicativo cliente, poderá usar os parâmetros **-clientusername** e **username** que executam esse aplicativo.

Durante a operação do comando **mqcertck**, ele gera o rótulo certificado ibmwebspheremqXXXX, em que XXXX é o valor transmitido no parâmetro **-clientusername**.

Para verificar completamente o repositório de chaves do cliente, o comando **mqcertck** cria uma conexão simulada usando o GSKit. Para fazer isso, o comando precisa ter uma porta disponível à qual possa se ligar durante os testes do cliente. A porta padrão utilizada é 5857, porém, se esta já estiver em uso, é possível especificar uma porta diferente a ser usada durante os testes do cliente.

Nota: Embora o comando **mqcertck** seja ligado a uma porta, nenhuma comunicação externa é usada pelo **mqcertck** e todos os testes são realizados localmente.

SSL/TLS no IBM MQ MQI client

O IBM MQ suporta o TLS em clientes. É possível customizar o uso do TLS de várias formas.

O IBM MQ fornece o suporte do TLS para o IBM MQ MQI clients em sistemas Windows, UNIX and Linux. Se você estiver usando o IBM MQ classes for Java, consulte Usando o IBM MQ classes for Java e se você estiver usando o IBM MQ classes for JMS, consulte Usando o IBM MQ classes for JMS. O restante desta seção não se aplica aos ambientes do Java ou JMS.

É possível especificar o repositório de chaves para um IBM MQ MQI client com o valor MQSSLKEYR no arquivo de configuração do cliente do IBM MQ ou quando o aplicativo faz uma chamada MQCONNX. Você tem três opções para especificar que um canal usa o TLS:

- Utilizando uma tabela de definição de canais
- Usando a estrutura de opções de configuração do SSL, MQSCO, ou uma chamada de MQCONNX
- Usando o Active Directory (nos sistemas Windows)

Não é possível usar a variável de ambiente MQSERVER para especificar que um canal usa o TLS.

É possível continuar executando seus aplicativos IBM MQ MQI client existentes sem o TLS, contanto que o TLS não seja especificado na outra extremidade do canal.

Se as mudanças forem feitas em uma máquina do cliente no conteúdo do Repositório de chaves do TLS, do local do Repositório de chaves do TLS, das Informações de autenticação ou dos parâmetros de hardware criptográficos, será necessário encerrar todas as conexões do TLS para refletir essas mudanças nos canais de conexão do cliente que o aplicativo estiver usando para se conectar ao gerenciador de filas. Assim que todas as conexões tiverem sido encerradas, reinicie os canais do TLS. Todas as novas configurações do TLS são usadas. Essas configurações são análogas àquelas atualizadas pelo comando REFRESH SECURITY TYPE(SSL) em sistemas do Gerenciadores de Filas.

Quando o IBM MQ MQI client é executado em um sistema Windows, UNIX and Linux com hardware de criptografia, é possível configurar este hardware com a variável de ambiente MQSSLCRYP. Esta variável é equivalente ao parâmetro SSLCRYP no comando ALTER QMGR MQSC. Consulte ALTER QMGR para obter uma descrição do parâmetro SSLCRYP no comando ALTER QMGR MQSC. Se você usar a versão GSK_PCS11 do parâmetro SSLCRYP, o rótulo do token PKCS #11 deverá ser especificado inteiramente em minúsculas.

A reconfiguração de chave secreta do TLS e o FIPS são suportados no IBM MQ MQI clients. Para obter mais informações, consulte “Reconfigurando as chaves secretas SSL e TLS” na página 450 e “Federal Information Processing Standards (FIPS) para UNIX, Linux, and Windows” na página 33.

Consulte “Configurando a Segurança do IBM MQ MQI client” na página 271 para obter mais informações sobre o suporte do TLS para IBM MQ MQI clients.

Tarefas relacionadas

Configurando um Cliente Usando um Arquivo de Configuração

Especificando que um canal MQI usa SSL/TLS

Para um canal MQI usar TLS, o valor do atributo *SSLCipherSpec* do canal de conexão do cliente deve ser o nome de um CipherSpec que seja suportado pelo IBM MQ na plataforma do cliente.

É possível definir um canal de conexão do cliente com um valor para este atributo das seguintes maneiras. Eles são listados na ordem de precedência decrescente.

1. Quando uma saída PreConnect fornece uma estrutura de definição de canal para uso.

   Uma saída PreConnect pode fornecer o nome de um CipherSpec no campo *SSLCipherSpec* de uma estrutura de definição de canal, MQCD. Esta estrutura é retornada no campo **ppMQCDArrayPtr** da estrutura do parâmetro de saída MQNXP usada pela saída PreConnect.
2. Quando um aplicativo do IBM MQ MQI client emite uma chamada MQCONNX.

   O aplicativo pode especificar o nome de um CipherSpec no campo *SSLCipherSpec* de uma estrutura de definição de canal, MQCD.Esta estrutura é referenciada pela estrutura de opções de conexão, MQCNO, que é um parâmetro na chamada MQCONNX.
3. Usando uma Tabela de Definição de Canal de Cliente (CCDT).

   Uma ou mais entradas em uma tabela de definição de canal do cliente podem especificar o nome de um CipherSpec.Por exemplo, se você criar uma entrada usando o comando DEFINE CHANNEL MQSC, poderá usar o parâmetro SSLCIPH no comando para especificar o nome de um CipherSpec.
4. Usando um Active Directory no Windows.

   Nos sistemas Windows, é possível usar o comando de controle **setmqscp** para publicar as definições de canal de conexão do cliente no Active Directory. Uma ou mais destas definições podem especificar o nome de um CipherSpec.

Por exemplo, se um aplicativo cliente fornece uma definição de canal de conexão do cliente em uma estrutura MQCD em uma chamada MQCONNX, esta definição será usada como preferência em qualquer entrada em uma tabela de definição de canal do cliente que pode ser acessada pelo cliente IBM MQ.

Não é possível usar a variável de ambiente MQSERVER para fornecer a definição de canal na extremidade do cliente de um canal MQI que usa TLS.

Para verificar se um certificado de cliente fluiu, exiba o status do canal na extremidade do servidor de um canal para a presença de um valor de parâmetro de nome de mesmo nível.

Conceitos relacionados

"Especificando um CipherSpec para um IBM MQ MQI client" na página 439
Você tem três opções para especificar um CipherSpec para um IBM MQ MQI client.

CipherSpecs e CipherSuites no IBM MQ

O IBM MQ suporta especificações de código do TLS 1.2 e algoritmos RSA e Diffie-Hellman. No entanto, será possível ativar CipherSpecs descontinuadas, se você precisar fazer isso.

Consulte "Ativando CipherSpecs" na página 423 para obter informações sobre:

- CipherSpecs suportados pelo IBM MQ.
- Como ativar especificações de código descontinuadas do SSL 3.0 e do TLS 1.0.

O IBM MQ suporta o RSA e Diffie-Hellman Key Exchange e os algoritmos de autenticação. O tamanho da chave usada durante o handshake TLS pode depender do certificado digital usado, mas alguns CipherSpecs incluem uma especificação do tamanho de chave de handshake. Tamanhos maiores de chaves de handshake fornecem autenticação mais consistente. Com tamanhos de chaves menores, o protocolo de reconhecimento é mais veloz.

Conceitos relacionados

"CipherSpecs e CipherSuites" na página 19
Os protocolos de segurança criptográficos devem concordar sobre os algoritmos usados por uma conexão segura. CipherSpecs e CipherSuites definem combinações específicas de algoritmos.

Criptografia do Conjunto B da NSA no IBM MQ

Este tópico fornece informações sobre como configurar o IBM MQ no Windows, Linux e UNIX para adequação ao perfil do TLS 1.2 compatível com o Conjunto B.

Com o tempo, o Padrão do Conjunto B de Criptografia da NSA é atualizado para refletir novos ataques contra algoritmos de criptografia e protocolos. Por exemplo: alguns CipherSpecs podem deixar de serem certificados pelo Conjunto B. Quando tais mudanças ocorrem, o IBM MQ também é atualizado

para implementar o padrão mais recente. Como um resultado, você poderá ver as mudanças no comportamento após a aplicação da manutenção. O arquivo leia-me do IBM MQ lista a versão do Conjunto B cumprido por nível de manutenção do produto. Se você configurar o IBM MQ para aplicar conformidade do Conjunto B, sempre consulte o arquivo leia-me ao planejar aplicar manutenção. Consulte IBM MQ, WebSphere MQ, e MQSeries readmes do produto.

Nos sistemas Windows, UNIX e Linux, o IBM MQ pode ser configurado para conformidade com o perfil de TLS 1.2 compatível com o Conjunto B nos níveis de segurança mostrados na Tabela 1.

Tabela 3. Níveis de Segurança do Conjunto B com CipherSpecs Permitidos e Algoritmos de Assinatura Digital

Níveis de segurança	**CipherSpecs Permitidos**	**Algoritmos de assinatura digital**
128 bits	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA com SHA-256 ECDSA com SHA-384
192 bits	ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA com SHA-384
Ambos [1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA com SHA-256 ECDSA com SHA-384

1. É possível configurar ambos os níveis de segurança de 128 e 192 bits simultaneamente. Como a configuração do Conjunto B determina os algoritmos criptográficos mínimos aceitáveis, a configuração de ambos os níveis de segurança é equivalente a configurar apenas o nível de segurança de 128 bits. Os algoritmos criptográficos do nível de segurança de 192 bits são mais fortes do que o mínimo requerido para o nível de segurança de 128 bits, portanto, eles são permitidos para o nível de segurança de 128 bits, mesmo se o nível de segurança 192 bits não estiver ativado.

Nota: As convenções de nomenclatura usadas para o nível de segurança não representam necessariamente o tamanho da curva elíptica ou o tamanho da chave do algoritmo de criptografia AES.

configuração do Conjunto B para CipherSpec

Embora o comportamento padrão do IBM MQ não esteja em conformidade com o padrão do Conjunto B, o IBM MQ pode ser configurado para conformidade com qualquer um, ou ambos os níveis de segurança nos sistemas Windows, UNIX and Linux. Após a configuração bem-sucedida do IBM MQ para usar com o Conjunto B, qualquer tentativa de iniciar um canal de saída usando um CipherSpec que não seja compatível com o Conjunto B resulta no erro AMQ9282. Esta atividade também resulta no retorno do código de razão MQRC_CIPHER_SPEC_NOT_SUITE_B por parte do cliente do MQI. Assim como tentar iniciar um canal de entrada usando um CipherSpec que não esteja em conformidade com os resultados de configuração do Conjunto B no erro AMQ9616.

Para obter mais informações sobre o IBM MQ CipherSpecs, consulte “Ativando CipherSpecs” na página 423

Conjunto B e Certificados Digitais

O Conjunto B restringe os algoritmos de assinatura digital que podem ser usados para assinar certificados digitais. Conjunto B também restringe o tipo de chave pública que certificados pode conter. Portanto, o IBM MQ deve ser configurado para usar certificados digitais cujo algoritmo de assinatura digital e tipo de chave pública são permitidos pelo nível de segurança do Conjunto B configurado do parceiro remoto. Certificados digitais que não cumprirem os requisitos de nível de segurança serão rejeitados e a conexão falhará com o erro AMQ9633 ou AMQ9285.

Para o nível de segurança do Conjunto B de 128 bits, a chave pública do assunto do certificado é necessária para usar a curva elíptica P-256 NIST ou a curva elíptica P-384 NIST e ser assinada com a curva elíptica P-256 NIST ou a curva elíptica P-384 NIST. No nível de segurança de 192 bits do Conjunto B, a chave pública do assunto do certificado deve usar e ser assinada pela curva elíptica NIST P-384.

Para obter um certificado adequado a operações compatíveis com o Conjunto B, use o comando **runmqakm** e especifique o parâmetro **-sig_alg** para solicitar um algoritmo de assinatura digital apropriado. Os valores de parâmetro EC_ecdsa_with_SHA256 e EC_ecdsa_with_SHA384 **-sig_alg** correspondem às chaves de curva elíptica assinadas pelos algoritmos de assinatura digital permitidos peloConjunto B.

Para obter mais informações sobre o comando **runmqakm** , consulte opções runmqckm e runmqakm.

Nota: Os comandos **runmqckm** e **strmqikm** não suportam a criação de certificados digitais para operações compatíveis com Conjunto B.

Criando e Solicitando Certificados Digitais

Para criar um certificado digital autoassinado para testes com o Conjunto B, consulte "Criando um certificado pessoal autoassinado no UNIX, Linux, and Windows" na página 297

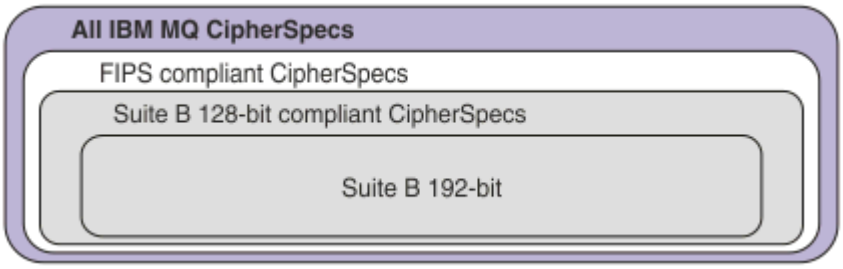
Para solicitar um certificado digital assinado pela CA para uso com o Conjunto B, consulte "Solicitando um certificado pessoal no UNIX, Linux, and Windows" na página 300.

Nota: A autoridade de certificação que está sendo usada deve gerar os certificados digitais que satisfazem os requisitos descritos em IETF RFC 6460.

FIPS 140-2 e Conjunto B

O padrão do Conjunto B é conceitualmente semelhante a FIPS 140-2, já que restringe o conjunto de algoritmos criptográficos ativados para fornecer um nível de garantia de segurança. Os CipherSpecs do Conjunto B atualmente suportados podem ser usados quando o IBM MQ é configurado para operação em conformidade com FIPS 140-2. Portanto, é possível configurar o IBM MQ para o FIPS e o Conjunto B em conformidade simultaneamente, em cujo caso os dois conjuntos de restrições se aplicam.

O diagrama a seguir ilustra a relação entre esses subconjuntos:



Configurando o IBM MQ para operação compatível com o Conjunto B.

Para obter informações sobre como configurar o IBM MQ no Windows, UNIX and Linux para operação compatível com o Conjunto B, consulte "Configurando o IBM MQ para o Conjunto B" na página 42.

O IBM MQ não suporta operação compatível com o Conjunto B nas plataformas IBM i e z/OS. Os clientes do IBM MQ Java e JMS também não suportam a operação compatível com o Conjunto B.

Conceitos relacionados

"Especificando que Apenas CipherSpecs Certificados por FIPS São Usados no Tempo de Execução no Cliente de MQI" na página 272
Crie seus repositórios de chaves usando software compatível com FIPS e, em seguida, especifique que o canal deve usar CipherSpecs certificados por FIPS.

Configurando o IBM MQ para o Conjunto B

O IBM MQ pode ser configurado para operar em conformidade com o padrão do Conjunto B da NSA nas plataformas Windows, UNIX and Linux.

O Conjunto B restringe o conjunto de algoritmos criptográficos ativados, a fim de fornecer um nível de segurança seguro. O IBM MQ pode ser configurado para operar em conformidade com o Conjunto B

para fornecer um nível de segurança aprimorado. Para obter informações adicionais sobre o Conjunto B, consulte “Criptografia do Conjunto B da Agência Nacional de Segurança (NSA)” na página 21. Para obter mais informações sobre a configuração do Conjunto B e seu efeito sobre os canais TLS, veja “Criptografia do Conjunto B da NSA no IBM MQ” na página 40.

Gerenciador de filas

Para um gerenciador de filas, use o comando **ALTER QMGR** com o parâmetro **SUITEB** para configurar os valores apropriados para o nível de segurança requerido. Para obter informações adicionais, consulte ALTER QMGR.

Também é possível usar o comando **MQCMD_CHANGE_Q_MGR** de PCF com o parâmetro **MQIA_SUITE_B_STRENGTH** para configurar o gerenciador de filas para operação compatível com o Conjunto B.

Nota: Se você alterar as configurações do Conjunto B de um gerenciador de filas, deverá reiniciar o serviço MQXR para que essas configurações entrem em vigor.

Cliente MQI

Por padrão, os clientes MQI não aplicam a conformidade do Conjunto B. É possível ativar o cliente MQI para conformidade com o Conjunto B, executando uma das seguintes opções:

1. Configurando o campo **EncryptionPolicySuiteB** na estrutura de MQSCO em uma chamada MQCONNX para um ou mais dos seguintes valores:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   Usar MQ_SUITE_B_NONE com qualquer outro valor é inválido.
2. Ao configurar a variável de ambiente MQSUITEB para um ou mais dos seguintes valores:
   - Nenhum
   - 128_BIT
   - 192_BIT

   É possível especificar vários valores usando uma lista separada por vírgula. Usar o valor NONE com qualquer outro valor é inválido.
3. Configurando o atributo **EncryptionPolicySuiteB** na sub-rotina de SSL do arquivo de configuração do cliente de MQI para um ou mais dos seguintes valores:
   - Nenhum
   - 128_BIT
   - 192_BIT

   É possível especificar vários valores usando uma lista separada por vírgula. Usar NONE com qualquer outro valor é inválido.

Nota: As configurações do cliente de MQI são listadas em ordem de prioridade. A estrutura de MSCO na chamada MQCONNX substitui a configuração na variável de ambiente MQSUITEB, que substitui o atributo na sub-rotina de SSL.

Para obter detalhes completos da estrutura de MQSCO, consulte MQSCO - Opções de configuração SSL.

Para obter mais informações sobre o uso do Conjunto B no arquivo de configuração do cliente, consulte Sub-rotina de SSL do arquivo de configuração do cliente.

Para obter informações adicionais sobre o uso da variável de ambiente MQSUITEB, consulte Descrições de variáveis de ambiente.

.NET

Para clientes não gerenciados do .NET, a propriedade **MQC.ENCRYPTION_POLICY_SUITE_B** indica o tipo de segurança do Conjunto B necessária.

Para obter informações sobre o uso do Conjunto B no IBM MQ classes for .NET, consulte Classe MQEnvironment do .NET.

AMQP

As configurações de atributo do Conjunto B para um gerenciador de filas são aplicadas a canais de AMQP nesse gerenciador de filas. Se você modificar as configurações do Conjunto B do gerenciador de filas, deverá reiniciar o serviço AMQP para que as mudanças entrem em vigor.

Políticas de validação de certificado no IBM MQ

A política de validação de certificado determina com qual precisão a validação de cadeia de certificados está em conformidade com os padrões de segurança do segmento de mercado.

A política de validação de certificado depende da plataforma e do ambiente, como a seguir:

- Para os aplicativos do Java e do JMS em todas as plataformas, a política de validação de certificado depende do componente JSSE do ambiente de tempo de execução do Java. Para obter informações adicionais sobre a política de validação de certificado, consulte a documentação do seu JRE.
- Para sistemas IBM i, a política de validação de certificado depende da biblioteca de soquetes seguros fornecida pelo sistema operacional. Para obter informações adicionais sobre a política de validação de certificado, consulte a documentação do sistema operacional.
- Para sistemas z/OS, a política de validação de certificado depende do componente SSL do Sistema fornecido pelo sistema operacional. Para obter informações adicionais sobre a política de validação de certificado, consulte a documentação do sistema operacional.
- Para sistemas UNIX, Linux, and Windows, a política de validação de certificado é fornecida pelo GSKit e pode ser configurada. Duas políticas de validação de certificado diferentes são suportadas:
  - Uma política de validação de certificado de legado, usada para máxima compatibilidade reversa e interoperabilidade com certificados digitais antigos que não estão em conformidade com os padrões de validação de certificado IETF atuais. Esta política é conhecida como a política Básica.
  - Uma política de validação de certificado rígida e em conformidade com padrões que impinge o padrão RFC 5280. Esta política é conhecida como a política Padrão.

Para obter informações sobre como configurar a política de validação de certificado no UNIX, Linux, and Windows, consulte “Configurando políticas de validação de certificado no IBM MQ” na página 44. Para obter mais informações sobre as diferenças entre as políticas de validação de certificado Básicas e Padrão, consulte Validação de certificado e design de política de confiança no UNIX, Linux, and Windows.

Configurando políticas de validação de certificado no IBM MQ

É possível especificar qual política de validação de certificado TLS é usada para validar certificados digitais recebidos de sistemas parceiros remotos de quatro maneiras.

No gerenciador de filas, a política de validação de certificado pode ser definida das seguintes maneiras:

- Usando o atributo do gerenciador de filas *CERTVPOL*. Para obter informações adicionais sobre a configuração desse atributo, consulte ALTER QMGR.

No cliente, existem vários métodos que podem ser usados para definir a política de validação de certificado. Se mais de um método é usado para definir a política, o cliente usará as configurações na seguinte ordem de prioridade:

1. Usando o campo *CertificateValPolicy* na estrutura MQSCO do cliente. Para obter informações adicionais sobre o uso desse campo consulte MQSCO - Opções de configuração SSL.
2. Usando a variável de ambiente do cliente, *MQCERTVPOL*. Para obter informações adicionais sobre o uso dessa variável, consulte MQCERTVPOL.

3. Usando a configuração para o parâmetro de ajuste da sub-rotina SSL do cliente, *CertificateValPolicy*. Para obter informações adicionais sobre o uso dessa configuração, consulte Sub-rotina de SSL do arquivo de configuração do cliente.

Para obter informações adicionais sobre as políticas de validação de certificado, consulte “Políticas de validação de certificado no IBM MQ” na página 44.

Certificados digitais e compatibilidade de CipherSpec no IBM MQ

Este tópico fornece informações sobre como escolher os certificados digitais e do CipherSpecs para sua política de segurança, delineando o relacionamento entre os certificados digitais e de CipherSpecs no IBM MQ.

Somente um subconjunto dos CipherSpecs suportados pode ser usado com todos os tipos suportados de certificado digital. Portanto, é necessário escolher um CipherSpec apropriado para o seu certificado digital. Da mesma forma, se a política de segurança de sua organização requer o uso de um CipherSpec específico, deve-se obter um certificado digital apropriado para esse CipherSpec.

Os algoritmos de assinatura digital MD5 e o TLS 1.2

Os certificados digitais assinados usando o algoritmo MD5 são rejeitados quando o protocolo TLS 1.2 é usado. Isso é porque o algoritmo MD5 é agora considerado fraco por muitos analistas de criptografia, e seu uso é normalmente desencorajado. Para usar as CipherSpecs mais recentes com base no protocolo TLS 1.2, assegure-se de que os certificados digitais não usem o algoritmo MD5 em suas assinaturas digitais. Os CipherSpecs mais antigos que usam os protocolos TLS 1.0 não estão sujeitos a essa restrição e podem continuar a usar certificados com assinaturas digitais MD5.

Para visualizar o algoritmo de assinatura digital para um certificado específico, é possível usar o comando **runmqakm**:

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

em que *cert_label* é o rótulo do certificado do algoritmo de assinatura digital a ser exibido. Consulte Rótulos de certificado digital para obter detalhes.

Nota: Embora a GUI do **runmqckm** (iKeycmd) e do **strmqikm** (iKeyman) possam ser usadas para visualizar uma seleção de algoritmos de assinatura digital, a ferramenta do **runmqakm** fornece um intervalo mais amplo.

A execução do comando **runmqakm** produz a saída exibindo o uso do algoritmo de assinatura especificado:

```
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
```

A linha `Signature Algorithm` mostra que o algoritmo `MD5WithRSASignature` é usado.. Este algoritmo é baseado em MD5 e, portanto, este certificado digital não pode ser usado com o CipherSpecs do TLS 1.2.

Interoperabilidade da curva elíptica e do RSA de CipherSpecs

V 9.1.4 Nem todos os CipherSpecs podem ser usados com todos os certificados digitais. CipherSpecs são denotados pelo prefixo do nome CipherSpec Cada tipo de CipherSpec impõe restrições diferentes sobre o tipo de certificado digital que pode ser utilizado Essas restrições são aplicadas a todas as conexões TLS do IBM MQ, mas são particularmente relevantes para os usuários da criptografia de Curva Elíptica.

A tabela a seguir resume os relacionamentos entre os certificados digital e de CipherSpecs:

Tabela 4. Relacionamentos entre os certificados digital e de CipherSpecs

tipo	Prefixo de nome do CipherSpec	Descrição	Tipo de chave pública requerido	Algoritmo de criptografia de assinatura digital	Método de estabelecimento de chave secreta
1	ECDHE_ECDSA_	Os CipherSpecs que usam as chaves públicas da Curva Elíptica, as chaves secretas da Curva Elíptica e os algoritmos de assinatura digital da Curva Elíptica.	Curva Elíptica	ECDSA	ECDHE
2	ECDHE_RSA_	CipherSpecs que usam chaves públicas RSA, chaves secretas de Curva Elíptica e algoritmos de assinatura digital RSA.	RSA	RSA	ECDHE
V 9.1.4 3	(Todos os TLS 1.3 CipherSpecs)	CipherSpecs que usam chaves públicas Elliptic Curve ou RSA, chaves secretas Elliptic Curve e algoritmos de assinatura digital Elliptic Curve ou RSA.	Curva elíptica ou RSA	ECDSA ou RSA	ECDHE ou RSA
4	(Todos os outros)	Os CipherSpecs que usam chaves públicas de RSA e algoritmos de assinatura digital de RSA.	RSA	RSA	RSA

Nota: Os CipherSpecs do tipo 1 e 2 não são suportados pelos gerenciadores de filas do IBM MQ e clientes do MQI na plataforma do IBM i.

A coluna de tipo de chave pública necessária mostra o tipo de chave pública que o certificado pessoal deve ter ao usar cada tipo de CipherSpec. O certificado pessoal é o certificado de entidade final que identifica o gerenciador de filas ou cliente para seu parceiro remoto.

Seria possível configurar um canal com um CipherSpec que requer um certificado de Curva Elíptica (CE) e um rótulo de certificado para um certificado RSA, ou o contrário. Deve-se assegurar que o certificado nomeado no rótulo certificado seja apropriado para o CipherSpec de canal.

Supondo que você tenha configurado corretamente o IBM MQ, será possível ter:

- Um gerenciador de filas único com uma mistura de certificados RSA e EC.
- Canais diferentes no mesmo gerenciador de filas usando um certificado RSA ou EC.

O algoritmo de criptografia de assinatura digital se refere ao algoritmo de criptografia usado para validar o peer. O algoritmo de criptografia é usado juntamente com um algoritmo hash, como MD5, SHA-1 ou SHA-256 para calcular a assinatura digital. Há vários algoritmos de assinatura digital que podem ser usados, por exemplo, RSA com MD5 ou ECDSA com SHA-256. Na tabela, ECDSA refere-se ao conjunto de algoritmos de assinatura digital que usam ECDSA; RSA refere-se ao conjunto de algoritmos de assinatura digital que usam RSA. Qualquer algoritmo de assinatura digital suportado no conjunto pode ser usado, contanto que seja baseado no algoritmo de criptografia indicado.

Os CipherSpecs do tipo 1 requerem que o certificado pessoal tenha uma chave pública da Curva Elíptica. Quando estes CipherSpecs são usados, o acordo da chave efêmera de Diffie Hellman de Curva Elíptica é usado para estabelecer a chave secreta para a conexão.

Os CipherSpecs do tipo 2 requerem que o certificado pessoal tenha uma chave pública de RSA. Quando estes CipherSpecs são usados, o acordo da chave efêmera de Diffie Hellman de Curva Elíptica é usado para estabelecer a chave secreta para a conexão.

Os CipherSpecs de tipo 3 requerem que o certificado pessoal tenha uma chave pública de RSA. Quando estes CipherSpecs são usados, a troca de chave de RSA é usada para estabelecer a chave secreta para a conexão.

Esta lista de restrições não é completa: dependendo da configuração, pode haver restrições adicionais que podem afetar ainda mais a capacidade de interoperar. Por exemplo, se IBM MQ for configurado para estar em conformidade com os padrões FIPS 140-2 ou Conjunto B da NSA, isto também limitará o intervalo de configurações permitidas. Consulte a seção seguinte para obter informações adicionais.

Se precisar usar diferentes tipos de CipherSpec no mesmo gerenciador de filas ou aplicativo cliente, configure um rótulo do certificado apropriado e a combinação do CipherSpec na definição do cliente.

Os três tipos de CipherSpec não interoperam diretamente: esta é uma limitação dos padrões de TLS atuais. Por exemplo, suponha que você tenha escolhido usar o ECDHE_ECDSA_AES_128_CBC_SHA256 CipherSpec para um canal receptor denominado TO.QM1 em um gerenciador de filas denominado QM1, então o receptor deve ter um certificado pessoal com uma chave de Curva Elíptica e uma assinatura digital baseada em ECDSA. Se o canal receptor não atender a esses requisitos, o canal falhará ao iniciar.

Outros canais que se conectam com o gerenciador de filas QM1 podem usar outros CipherSpecs, desde que cada canal use um certificado do tipo correto para o CipherSpec desse canal. Por exemplo, suponha que QM1 use um canal emissor denominado TO.QM2 para enviar mensagens para outro gerenciador de filas denominado QM2. O canal TO.QM2 pode usar o CipherSpec do tipo 3 TLS_RSA_WITH_AES_256_CBC_SHA256, desde que ambas as extremidades do canal usem certificados que contêm chaves públicas de RSA. O atributo do canal do rótulo de certificado pode ser usado para configurar um certificado diferente para cada canal.

Ao planejar as redes de seu IBM MQ, considere cuidadosamente quais canais requerem TLS e certifique-se de que o tipo de certificados usados para cada canal sejam apropriados para uso com o CipherSpec naquele canal.

Para visualizar o algoritmo de assinatura digital e o tipo de chave pública de um certificado digital, é possível usar o comando **runmqakm**:

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

em que *cert_label* é o rótulo do certificado cujo algoritmo de assinatura digital precisa ser exibido. Consulte Rótulos de certificado digital para obter detalhes.

A execução do comando **runmqakm** produzirá saída que exibe o Tipo de Chave Pública:

```
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
```

A linha Tipo de Chave Pública neste caso mostra que o certificado tem uma chave pública de Curva Elíptica. A linha de Algoritmo de Assinatura neste caso mostra que o algoritmo EC_ecdsa_with_SHA384 está em uso: isso é baseado no algoritmo de ECDSA. Esse certificado é, portanto, adequado apenas para uso com o CipherSpecs tipo 1.

Também é possível usar o comando **runmqckm** com os mesmos parâmetros. Além disso, a GUI do **strmqikm** poderá ser usada para visualizar algoritmos de assinatura digital se você abrir o repositório de chaves e der um clique duplo no rótulo do certificado. No entanto, é necessário usar a ferramenta **runmqakm** para visualizar certificados digitais porque ela suporta uma gama mais ampla de algoritmos.

TLS 1.3 CipherSpecs

V 9.1.4

TLS 1.3 CipherSpecs suportam certificados ECDSA e RSA.

Curva Elíptica de CipherSpecs e Conjunto B da NSA

Quando o IBM MQ é configurado para conformidade com o Conjunto B compatível com o perfil do TLS 1.2, os algoritmos de assinatura digital e de CipherSpecs permitidos são restringidos conforme descrito em “Criptografia do Conjunto B da NSA no IBM MQ” na página 40. Além disso, o intervalo de chaves aceitável do Elliptic Curve é reduzido de acordo com os níveis de segurança configurados.

No nível de segurança do Conjunto B de 128 bits, a chave pública do assunto do certificado é necessária para usar a curva elíptica de NIST P-256 ou NIST P-384 e ser assinada com a curva elíptica NIST P-256 ou NIST P-384. O comando **runmqakm** pode ser usado para solicitar certificados digitais para esse nível de segurança, usando um parâmetro -sig_alg de EC_ecdsa_with_SHA256 ou EC_ecdsa_with_SHA384.

No nível de segurança do Conjunto B de 192 bits, a chave pública do assunto do certificado é necessária para usar a curva elíptica de NIST P-384 e ser assinada com a curva elíptica NIST P-384. O comando **runmqakm** pode ser usado para solicitar certificados digitais para esse nível de segurança usando um parâmetro -sig_alg de EC_ecdsa_with_SHA384.

As curva elípticas de NIST suportadas são as seguintes:

Tabela 5. Curvas elípticas de NIST suportadas

Nome da curva NIST FIPS 186-3	**Nome da curva RFC 4492**	**Tamanho da chave da Curva Elíptica (bits)**
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Nota: A curva elíptica NIST P-521 não pode ser usado para operação compatível com o Conjunto B.

Conceitos relacionados

“Ativando CipherSpecs” na página 423
Ative um CipherSpec usando o parâmetro **SSLCIPH** no comando MQSC **DEFINE CHANNEL** ou no comando MQSC **ALTER CHANNEL** .

“Especificando que Apenas CipherSpecs Certificados por FIPS São Usados no Tempo de Execução no Cliente de MQI” na página 272
Crie seus repositórios de chaves usando software compatível com FIPS e, em seguida, especifique que o canal deve usar CipherSpecs certificados por FIPS.

“Criptografia do Conjunto B da NSA no IBM MQ” na página 40
Este tópico fornece informações sobre como configurar o IBM MQ no Windows, Linux e UNIX para adequação ao perfil do TLS 1.2 compatível com o Conjunto B.

“Criptografia do Conjunto B da Agência Nacional de Segurança (NSA)” na página 21
O governo dos Estados Unidos da América produz aconselhamento técnico sobre sistemas e segurança de TI, inclusive criptografia de dados. A Agência Nacional de Segurança dos Estados Unidos (NSA) recomenda um conjunto de algoritmos criptográficos interoperável em seu padrão do Conjunto B.

Registros de Autenticação de Canal

Para exercer um controle mais preciso sobre o acesso concedido à conexão de sistemas em um nível de canal, é possível usar registros de autenticação de canal.

Você pode achar que os clientes tentam se conectar ao seu gerenciador de filas usando um ID do usuário em branco ou um ID do usuário de alto nível que permitiria ao cliente executar ações indesejáveis. É possível bloquear o acesso a esses clientes usando os registros de autenticação de canal. Alternativamente, um cliente pode declarar um ID do usuário que seja válido na plataforma do cliente, mas é desconhecido ou de um formato inválido na plataforma do servidor. É possível usar um registro de autenticação de canal para mapear o ID do usuário declarado para um ID do usuário válido.

Você pode achar um aplicativo cliente que se conecta ao seu gerenciador de filas e se comporta indevidamente de algum modo. Para proteger o servidor contra os problemas que este aplicativo está causando, ele precisar ser bloqueado temporariamente usando o endereço IP no qual o aplicativo cliente está até o momento em que as regras de firewall são atualizadas ou o aplicativo cliente é corrigido. É possível usar um registro de autenticação de canal para bloquear o endereço IP a partir do qual o aplicativo cliente se conecta.

Se tiver configurado uma ferramenta de administração, tal como IBM MQ Explorer, e um canal para esse uso específico, você pode desejar assegurar que apenas computadores clientes específicos possam usá-lo. É possível usar um registro de autenticação de canal para permitir que o canal seja usado apenas a partir de determinados endereços IP.

Se você estiver apenas iniciando alguns aplicativos de amostra executando como clientes, consulte Preparando e executando os programas de amostra para obter um exemplo de como configurar o gerenciador de filas de maneira segura usando registros de autenticação de canal.

Para obter registros de autenticação de canal para controlar canais de entrada, use o comando MQSC **ALTER QMGR CHLAUTH(ENABLED)**.

As regras de **CHLAUTH** são aplicadas para um canal MCA que é criado em resposta a uma nova conexão de entrada. Para um canal MCA criado em resposta ao canal sendo iniciado localmente, nenhuma regra de **CHLAUTH** é aplicada.

Tabela 6. Quando as regras de CHLAUTH são aplicadas para pares de canais diferentes

Tipo de canal	**MCA no qual as regras CHLAUTH são aplicadas**
SDR-RCVR	RCVR
RQSTR-SVR (iniciado em SVR)	RQSTR
RQSTR-SVR (iniciado em RQSTR)	SVR
RQSTR-SDR (iniciado em SDR)	RQSTR
RQSTR-SDR (iniciado em RQSTR)	SDR para conexão inicial. RQSTR para conexão de retorno de chamada.

Os registros de autenticação de canal podem ser criados para executar as seguintes funções:

- Bloquear as conexões dos endereços IP específicos.
- Bloquear as conexões de IDs de usuário específicos.
- Configurar um valor MCAUSER a ser usado para qualquer canal que se conecta a partir de um endereço IP específico.
- Configurar um valor MCAUSER a ser usado para qualquer canal declarando um ID do usuário específico.
- Configurar um valor MCAUSER a ser usado para qualquer canal que tenha um SSL específico ou Nome Distinto TLS (DN).
- Configurar um valor MCAUSER a ser usado para qualquer canal que se conecta a partir de um gerenciador de filas específico.
- Bloquear as conexões consideradas de um certo gerenciador de filas, a menos que a conexão seja de um endereço IP específico.
- Bloquear conexões que apresentam um certo certificado SSL ou TLS, a menos que a conexão seja de um endereço IP específico.

Estas utilizações são explicadas em detalhes nas seções a seguir.

Você cria, modifica ou remove registros de autenticação de canais usando o comando MQSC **SET CHLAUTH** ou o comando PCF **Set Channel Authentication Record**.

Nota: Grandes números de registros de autenticação de canal podem ter um impacto negativo no desempenho de um gerenciador de filas.

Bloqueando endereços IP

Normalmente é a função de um firewall evitar o acesso de determinados endereços IP. No entanto, pode haver ocasiões nas quais você sofre tentativas de conexão de um endereço IP que não deve ter acesso ao seu sistema IBM MQ e deve bloquear temporariamente o endereço antes da atualização do firewall. Estas tentativas de conexão podem não estar vindo de canais do IBM MQ; essas tentativas de conexão podem vir de outros aplicativos de soquete que estão mal configurados para destinar seu listener do IBM MQ. Bloqueie os endereços IP configurando um registro de autenticação de canal do tipo BLOCKADDR. É possível especificar um ou mais endereços únicos, intervalos de endereços ou padrões, incluindo curingas.

Sempre que uma conexão de entrada é recusada porque o endereço IP está bloqueado desta maneira, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_ADDRESS é emitida, desde que os eventos do canal estejam ativados e o gerenciador de filas esteja em execução. Além disso, a conexão é mantida aberta por 30 segundos antes de retornar o erro para assegurar que o listener não estoure com tentativas repetidas de conexão que estão bloqueadas.

Para bloquear endereços IP somente em canais específicos ou para evitar o atraso antes do erro ser relatado, configure um registro de autenticação de canal do tipo ADDRESSMAP com o parâmetro USERSRC(NOACCESS).

Sempre que uma conexão de entrada é recusada por esta razão, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_NOACCESS é emitida, desde que os eventos do canal estejam ativados e o gerenciador de filas esteja em execução.

Consulte “Bloqueando Endereços IP Específicos” na página 388 para obter um exemplo.

Bloqueando IDs de usuário

Para evitar que determinados IDs do usuário se conectem por meio de um canal do cliente, configure o registro de autenticação de canal do tipo BLOCKUSER. Este tipo de registro de autenticação de canal se aplica somente a canais do cliente, não a canais de mensagens. É possível especificar um ou mais IDs de usuários individuais a serem bloqueados, mas você não pode usar curingas.

Sempre que uma conexão de entrada é recusada por esta razão, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_USERID é emitida, desde que os eventos do canal estejam ativados.

Consulte “Bloqueando IDs de Usuários Específicos” na página 390 para obter um exemplo.

Também é possível bloco qualquer acesso para IDs de usuários especificados em determinados canais configurando um registro de autenticação de canal do tipo USERMAP com o parâmetro USERSRC(NOACCESS).

Sempre que uma conexão de entrada é recusada por esta razão, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_NOACCESS é emitida, desde que os eventos do canal estejam ativados e o gerenciador de filas esteja em execução.

Consulte “Bloqueando o acesso para um ID de usuário cliente” na página 393 para obter um exemplo.

Bloqueando nomes do gerenciador de filas

Para especificar que qualquer canal que se conecta a partir de um gerenciador de filas especificado não deve ter acesso, configure um registro de autenticação de canal do tipo QMGRMAP com o parâmetro USERSRC(NOACCESS). É possível especificar um único nome do gerenciador de filas ou um padrão incluindo curingas. Não há equivalente da função BLOCKUSER para bloquear o acesso de gerenciadores de filas.

Sempre que uma conexão de entrada é recusada por esta razão, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_NOACCESS é emitida, desde que os eventos do canal estejam ativados e o gerenciador de filas esteja em execução.

Consulte “Bloqueando Acesso de um Gerenciador de Filas Remotas” na página 392 para obter um exemplo.

Bloqueando DNs de SSL ou TLS

Para especificar que qualquer usuário que apresenta um certificado pessoal de SSL ou TLS contendo um DN especificado não possui acesso, configure um registro de autenticação de canal do tipo SSLPEERMAP com o parâmetro USERSRC(NOACCESS). É possível especificar um único nome distinto ou um padrão incluindo curingas. Não há equivalente da função BLOCKUSER para bloquear o acesso para DNs.

Sempre que uma conexão de entrada é recusada por esta razão, uma mensagem do evento MQRC_CHANNEL_BLOCKED com o qualificador de razão MQRQ_CHANNEL_BLOCKED_NOACCESS é emitida, desde que os eventos do canal estejam ativados e o gerenciador de filas esteja em execução.

Consulte “Bloqueando o acesso para um Nome Distinto SSL ou TLS” na página 394 para obter um exemplo.

Mapeando endereços IP para IDs do usuário para serem usados

Para especificar se algum canal conectando-se a partir de um endereço IP especificado deve usar um MCAUSER específico, configure um registro de autenticação de canal do tipo ADDRESSMAP. É possível especificar um único endereço, um intervalo de endereços ou um padrão incluindo curingas.

Se você usar um encaminhador de porta, quebra da sessão DMZ ou qualquer outra configuração que mude o endereço IP apresentado ao gerenciador de filas, o mapeamento de endereços IP não será necessariamente adequado para uso.

Consulte “Mapeando um Endereço IP para um ID do Usuário MCAUSER” na página 394 para obter um exemplo.

Mapeando nomes do gerenciador de filas para IDs do usuário para serem usados

Para especificar se algum canal conectando-se a partir de um gerenciador de filas especificado deve usar um MCAUSER específico, configure um registro de autenticação de canal do tipo QMGRMAP. É possível especificar um único nome do gerenciador de filas ou um padrão incluindo curingas.

Consulte “Mapeando um Gerenciador de Filas Remoto para um ID do Usuário MCAUSER” na página 390 para obter um exemplo.

Mapeando IDs de Usuários Declarados por um Cliente para IDs de Usuários a Serem Usados

Para especificar que um determinado ID do usuário é usado por uma conexão a partir de um cliente IBM MQ MQI, um MCAUSER diferente especificado deve ser usado. configurar um registro de autenticação de canal do tipo USERMAP. O mapeamento do ID do usuário não usa curingas.

Consulte “Mapeando um ID de usuário cliente para um ID do usuário MCAUSER” na página 391 para obter um exemplo.

Mapeando DNs SSL ou TLS para IDs do usuário para serem usados

Para especificar se algum usuário apresentando um certificado pessoal de Secure Sockets Layer/ Segurança da Camada de Transporte contendo um Nome distinto especificado deve usar um MCAUSER específico, configure um registro de autenticação de canal do tipo SSLPEERMAP. É possível especificar um único nome distinto ou um padrão incluindo curingas.

Consulte “Mapeando um Nome Distinto de SSL ou TLS para um ID do Usuário MCAUSER” na página 392 para obter um exemplo.

Mapeamento de Gerenciadores de Filas, Clientes ou DNs de SSL ou TLS de acordo com Endereço IP

Em algumas circunstâncias, pode ser possível para um terceiro imitar um nome do gerenciador de filas. Um certificado SSL ou TLS ou arquivo do banco de dados de chave também pode ser deturpado e reutilizado. Para se proteger contra essas ameaças, é possível especificar que uma conexão a partir de um determinado gerenciador de filas ou cliente, ou usando um determinado Nome distinto deve ser estabelecida a partir de um endereço IP especificado. Configure um registro de autenticação de canal do tipo USERMAP, QMGRMAP ou SSLPEERMAP e especifique o endereço IP permitido, ou padrão de endereços IP, usando o parâmetro ADDRESS.

Consulte “Mapeando um Gerenciador de Filas Remoto para um ID do Usuário MCAUSER” na página 390 para obter um exemplo.

Interação entre registros de autenticação de canal

É possível que um canal ao tentar fazer uma conexão corresponda a mais de um registro de autenticação de canal e que isso tenha efeitos contraditórios. Por exemplo, um canal pode declarar um ID do usuário

que foi bloqueado por um registro de autenticação de canal BLOCKUSER, mas com um certificado SSL ou TLS que corresponde a um registro SSLPEERMAP que configura um ID do usuário diferente. Além disso, se registros de autenticação de canal usarem curingas, um único endereço IP, nome do gerenciador de filas ou Nome distinto Secure Sockets Layer ou de Segurança da Camada de Transporte pode corresponder a vários padrões. Por exemplo, o endereço IP 192.0.2.6 corresponde aos padrões 192.0.2.0-24, 192.0.2. *, e 192.0.*.6. A ação executada é determinada conforme a seguir.

- O registro de autenticação de canal usado é selecionado conforme a seguir:
  - Um registro de autenticação de canal que corresponde explicitamente ao nome de canal tem prioridade sobre um registro de autenticação de canal que corresponde ao nome de canal usando um curinga.
  - Um registro de autenticação de canal usando um DN SSL ou TLS tem prioridade sobre um registro que usa um ID do usuário, nome do gerenciador de filas ou endereço IP.
  - Um registro de autenticação de canal que usa um ID do usuário ou um nome do gerenciador de filas tem prioridade sobre um registro que usa um endereço IP.
- Se um registro de autenticação de canal correspondente for localizado e ele especificar um MCAUSER, este MCAUSER será designado ao canal.
- Se um registro de autenticação de canal correspondente for localizado e ele especificar que o canal não possui acesso, um valor de MCAUSER igual a *NOACCESS será designado ao canal. Este valor pode, posteriormente, ser alterado por um programa de saída de segurança.
- Se nenhum registro de autenticação de canal correspondente for localizado, ou um registro de autenticação de canal correspondente for localizado e ele especificar que o ID do usuário do canal deve ser usado, o campo MCAUSER será inspecionado.
  - Se o campo MCAUSER estiver em branco, o ID do usuário do cliente é designado ao canal.
  - Se o campo MCAUSER não estiver em branco, ele será designado ao canal.
- Qualquer programa de saída de segurança é executado. Este programa de saída pode configurar o ID do usuário do canal ou determinar que o acesso deve ser bloqueado.
- Se a conexão estiver bloqueada ou o MCAUSER estiver configurado para *NOACCESS, o canal é encerrado.
- Se a conexão não estiver bloqueada, para qualquer canal exceto um canal do cliente, o ID do usuário do canal determinado nas etapas anteriores será verificado com relação à lista de usuários bloqueados.
  - Se o ID do usuário estiver na lista de usuários bloqueados, o canal será encerrado.
  - Se o ID do usuário não estiver na lista de usuários bloqueados, o canal é executado.

A correspondência mais específica é usada quando um número de registros de autenticação de canal corresponde a um nome de canal, endereço IP, nome do host, nome do gerenciador de filas ou DN de SSL ou TLS. A correspondência considerada como sendo:

- A mais específica é um nome sem caracteres curinga, por exemplo:
  - Um nome de canal de A.B.C
  - Um endereço IP de 192.0.2.6
  - Um nome de host de `hursley.ibm.com`
  - Um nome do gerenciador de filas de 192.0.2.6
- O mais genérico é um asterisco (*) único que corresponde, por exemplo:
  - Todos os nomes de canais
  - Todos os endereços IP
  - Todos os nomes de hosts
  - Todos os nomes do gerenciador de filas
- Um padrão com um asterisco no início de uma sequência é mais genérico do que um valor definido no início de uma sequência:

  - Para canais, *.B.C é mais genérico que A.*
  - Para endereços IP, *.0.2.6 é mais genérico do que 192.*
  - Para nomes de host, `*.ibm.com` é mais genérico do que `hursley.*`
  - Para nomes de gerenciadores de filas, *QUEUEMANAGER é mais genérico do que QUEUEMANAGER*
- Um padrão com um asterisco em um local específico em uma sequência é mais genérico do que um valor definido no mesmo local em uma sequência, e de forma semelhante para cada local subsequente em uma sequência:
  - Para canais, A.*.C é mais genérico do que A.B.*
  - Para endereços IP, 192.*.2.6 é mais genérico do que 192.0.*.
  - Para nomes de host, `hursley.*.com` é mais genérico do que `hursley.ibm.*`
  - Para nomes de gerenciadores de filas, Q*MANAGER é mais genérico do que QUEUE*
- Onde dois ou mais padrões possuem um asterisco em um local específico em uma sequência, aquele com menos nós após o asterisco é mais genérico:
  - Para canais, A.* é mais genérico do que A.*.C
  - Para endereços IP, 192.* é mais genérico do que 192.*.2.*.
  - Para nomes de host, `hurlsey.*` é mais genérico do que `hursley.*.com`
  - Para nomes de gerenciadores de filas, Q* é mais genérico do que Q*MGR
- Além disso, para um endereço IP:
  - Um intervalo indicado com um hífen (-) é mais específico do que com um asterisco. Portanto, 192.0.2.0-24 é mais específico do que 192.0.2.*.
  - Um intervalo que é um subconjunto de um outro é mais específico do que o intervalo maior. Portanto, 192.0.2.5-15 é mais específico do que 192.0.2.0-24.
  - A sobreposição de intervalos não é permitida. Por exemplo, não é possível ter registros de autenticação de canal para 192.0.2.0-15 e 192.0.2.10-20.
  - Um padrão não pode ter menos do que o número necessário de partes, a menos que o padrão termine com um único asterisco final. Por exemplo 192.0.2 é inválido, mas 192.0.2 .* é válido
  - Um asterisco final deve ser separado do restante do endereço pelo separador de parte apropriado (um ponto (.) para IPv4, dois pontos (:) para IPv6). Por exemplo, 192.0* não é válido porque o asterisco não está em uma parte própria sua.
  - Um padrão pode conter asteriscos adicionais, contanto que nenhum asterisco seja adjacente ao asterisco final. Por exemplo, 192.*.2.* é válido, mas 192.0.*.* não é válido.
  - Um padrão de endereço IPv6 não pode conter dois pontos duplos e um asterisco final, pois o endereço resultante seria ambíguo. Por exemplo, 2001::* poderia expandir para 2001:0000:*, 2001:0000:0000:* e assim por diante.
- Para um Nome Distinto (DN) SSL ou TLS, a ordem de precedência das subsequências é a seguinte:

Tabela 7. Ordem de precedência de subsequências

Ordem	**Subsequência do DN**	**Nome**
1	SERIALNUMBER=	Número de série do certificado
2	MAIL=	Endereço de e-mail
3	E=	Endereço de e-mail (descontinuado na preferência para MAIL)
4	UID=, USERID=	Identificador de usuários
5	CN=	Nome comum
6	T =	Título

Tabela 7. Ordem de precedência de subsequências (continuação)		
Ordem	**Subsequência do DN**	**Nome**
7	OU=	unidade organizacional
8	DC=	Componente de domínio
9	O=	Organização
10	STREET=	Rua / Primeira linha do endereço
11	L=	Localidade
12	ST=, SP=, S=	Nome do estado ou território
13	PC=	Código Postal / Código de Endereçamento Postal
14	C=	País
15	UNSTRUCTUREDNAME=	Nome do host
16	UNSTRUCTUREDADDRESS=	endereço IP
17	DNQ=	Qualificador de Nome Distinto

Portanto, se um certificado SSL ou TLS for apresentado com um DN contendo as subsequências O=IBM e C=UK, o IBM MQ usará um registro de autenticação de canal para O=IBM em preferência a um para C=UK, se ambos estiverem presentes.

Um Nome distinto pode conter diversas OUs, que devem ser especificadas em ordem hierárquica com as maiores unidades organizacionais especificadas primeiro. Se dois Nomes distintos forem iguais em todos os aspectos, exceto por seus valores de OU, o Nome distinto mais específico será determinado conforme a seguir:

1. Se eles possuírem números diferentes de atributos de OU, o Nome distinto com a maioria dos valores de OU é mais específico. Isso porque o Nome distinto com mais Unidades Organizacionais qualifica integralmente o Nome distinto em mais detalhes e fornece mais critérios de correspondência. Mesmo se sua OU de nível superior for um curinga (OU=*), o DN com mais OUs ainda será considerado o mais específico no geral.
2. Se eles tiverem o mesmo número de atributos de OU, os pares correspondentes de valores de OU são comparados na sequência da esquerda-para-direita, em que a OU mais à esquerda é o nível mais superior (menos específico), de acordo com as seguintes regras.
   a. Uma OU sem nenhum valor curinga é a mais específica porque ela pode corresponder exatamente com uma sequência apenas.
   b. Uma OU com um único curinga no início ou no final (por exemplo, OU=ABC* ou OU=*ABC) é a próxima mais específica.
   c. Uma OU com dois curingas (por exemplo, OU=*ABC*) é a próxima mais específica.
   d. Uma OU que consiste em somente um asterisco (OU=*) é a menos específica.
3. Se a comparação de sequência tiver uma ligação entre dois valores de atributo com a mesma especificidade, a sequência de atributos mais longa será mais específica.
4. Se a comparação de sequência estiver empatada entre dois valores de atributo de mesma especificidade e comprimento, então o resultado será determinado por uma comparação de sequência sem distinção entre maiúsculas e minúsculas da parte do Nome distinto, excluindo quaisquer curingas.

Se dois DNs forem iguais em todos os aspectos, exceto por seus valores de DC, as mesmas regras de correspondência se aplicarão para OUs, exceto que em valores de DC, o DC mais à esquerda é o nível mais baixo (mais específico) e a ordenação de comparação difere em conformidade.

Exibindo registros de autenticação de canal

Para exibir registros de autenticação de canal, use o comando MQSC **DISPLAY CHLAUTH** ou o comando PCF **Inquire Channel Authentication Records**. É possível escolher para retornar todos os registros que correspondam ao nome de canal fornecido ou é possível escolher um correspondência explícita. A correspondência explícita informa qual registro de autenticação canal seria usado se um canal tentasse fazer uma conexão a partir de um endereço IP específico, a partir de um gerenciador de filas específico ou usando um ID do usuário específico e, opcionalmente, apresentando um certificado pessoal de Secure Sockets Layer/Segurança da Camada de Transporte contendo um Nome distinto especificado.

Conceitos relacionados

"Segurança para o Sistema de Mensagens Remoto" na página 96

Esta seção trata dos aspectos do sistema de mensagens remoto de segurança.

Interação de CHLAUTH e CONNAUTH

Como os registros de autenticação de canal (CHLAUTH) e a autenticação de conexão (CONNAUTH) interagem no IBM MQ, no caso de uma conversa única em um canal.

Tipos diferentes de ligações

O IBM MQ suporta dois métodos para que um aplicativo se conecte:

Ligações locais

Aplica-se quando o aplicativo e o gerenciador de filas estão na mesma imagem operacional. O CHLAUTH não é relevante para esse tipo de conexão de aplicativo.

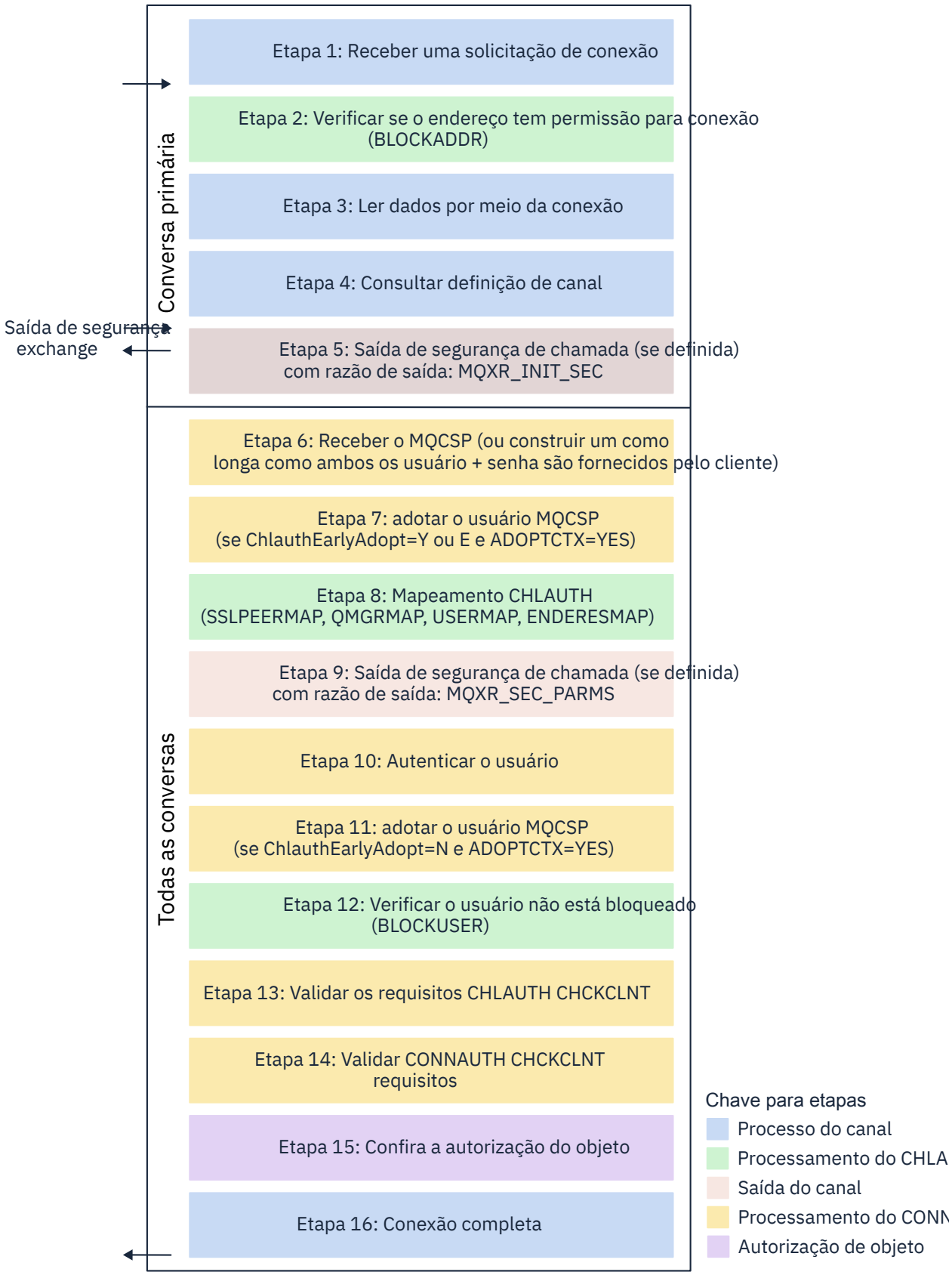
Ligações do Cliente

Aplica-se quando o aplicativo e o gerenciador de filas usam a rede para se comunicar. O aplicativo e o gerenciador de filas podem estar em execução na mesma máquina ou podem estar em máquinas diferentes. No IBM MQ, uma conexão do cliente é manipulada na forma de um canal de conexão do servidor (SVRCONN) e, nessa situação, tanto CONNAUTH quanto CHLAUTH são aplicáveis.

Etapas de ligação da extremidade de recebimento de um canal

Quando um aplicativo se conecta a um gerenciador de filas, uma quantia substancial de verificação é feita para assegurar que ambas as extremidades do canal entendam o que é suportado pela outra extremidade. A extremidade de recebimento do canal faz uma verificação extra, envolvendo CHLAUTH e CONNAUTH, para assegurar que o cliente tenha permissão para se conectar e esse processo também pode incluir uma saída de segurança, já que isso pode afetar o resultado. Essa fase de conexão de canal também é referida como *fase de ligação*.

O diagrama a seguir lista as etapas pelas quais um canal SVRCONN passa quando o encerramento do servidor (no Gerenciador de Filas) inicia:



Etapa 1: Receber uma solicitação de conexão
O inicializador ou o listener de canais recebe uma solicitação de conexão de algum lugar na rede.

Etapa 2: O endereço tem permissão para se conectar?
Antes que quaisquer dados sejam lidos, o IBM MQ verifica o endereço IP do parceiro com relação às regras do CHLAUTH, para ver se o endereço está na regra *BLOCKADDR*. Se o endereço não for localizado e, portanto, não estiver bloqueado, o fluxo continuará para a próxima etapa.

Etapa 3: Ler dados do canal
O IBM MQ agora lê os dados em um buffer e começa a processar as informações enviadas.

Etapa 4: Consultar a definição de canal
No primeiro fluxo de dados, o IBM MQ envia, dentre outras coisas, o nome do canal que a extremidade de envio está tentando iniciar. O gerenciador de filas de recebimento pode, então, consultar a definição de canal, que possui todas as configurações que são especificadas para o canal.

Etapa 5: Saída de segurança de chamada (se definida)
Se o canal tiver uma saída de segurança (SCYEXIT) definida, ela será chamada com o motivo da saída (MQCXP**ExitReason**) configure para MQXR_INIT_SEC.

Etapa 6: Receber MQCSP
Se necessário, construa um, desde que o ID do usuário e a senha sejam fornecidos pelo cliente.

Se o cliente for um aplicativo Java ou JMS executando em modo de compatibilidade, o cliente não passará uma estrutura MQCSP para o Gerenciador de Filas. Em vez disso, se o aplicativo tiver fornecido um ID do usuário e uma senha, uma estrutura do MQCSP será construída aqui.

Etapa 7: adotar usuário MQCSP (se `ChlauthEarlyAdopt` for *Y* e ADOPTCTX=YES)
O ID do usuário declarado pelo cliente é autenticado.

Se CONNAUTH estiver usando o LDAP para mapear um nome distinto declarado para um ID de usuário curto, o mapeamento acontecerá nessa etapa.

Se a autenticação for bem-sucedida, o ID do usuário será adotado pelo canal e usado pela etapa de mapeamento CHLAUTH.

Nota: A partir do IBM MQ 9.0.4, o parâmetro **`ChlauthEarlyAdopt=`** *Y* é automaticamente incluído na sub-rotina de canais do arquivo qm.ini para novos gerenciadores de filas.

Etapa 8: Mapeamento CHLAUTH
O cache CHLAUTH é inspecionado novamente para procurar as regras de mapeamento *SSLPEERMAP*, *USERMAP*, *QMGRMAP* e *ADDRESSMAP*.

A regra que corresponde ao canal de entrada mais especificamente é usada. Se a regra tiver **USERSRC***(CHANNEL)* ou *(MAP)*, o canal continua em vinculado.

Se as regras CHLAUTH forem avaliadas como uma regra com **USERSRC***(NOACCESS)*, o aplicativo será impedido de se conectar ao canal, a menos que as credenciais sejam substituídas posteriormente por um ID de usuário e senha válidos na Etapa 9.

Etapa 9: Chamar saída de segurança (se definida)
Se o canal tiver uma saída de segurança (SCYEXIT) definida, ela será chamada com o motivo da saída (MQCXP**ExitReason**) configurado para MQXR_SEC_PARMS.

Um ponteiro para MQCSP estará presente no campo **SecurityParms** da estrutura MQCXP.

A estrutura MQCSP tem ponteiros para o ID do usuário (MQCSP.**CSPUserIdPtr**) e senha (MQCSP.**CSPPasswordPtr**).

É possível mudar o ID do usuário e a senha na saída. O exemplo a seguir mostra como uma saída de segurança imprimiria os valores de ID do usuário e senha para um log de auditoria:

```
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);
```

A saída pode dizer IBM MQ para fechar o canal, retornando *MQXCC_CLOSE_CHANNEL* no MQCXP.campo **Exitresponse**. Caso contrário, o processamento do canal continuará com a fase de autenticação de conexão.

Nota: Se o usuário declarado for mudado pela saída de segurança, as regras de mapeamento de CHLAUTH não serão reaplicadas para o novo usuário.

Etapa 10: Autenticar o usuário

A fase de autenticação ocorre quando CONNAUTH é ativado no gerenciador de filas.

Para verificar isso, emita o comando 'DISPLAY QMGR CONNAUTH' do MQSC.

z/OS O exemplo a seguir mostra a saída do comando **DISPLAY QMGR CONNAUTH** de um gerenciador de filas em execução no 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 O exemplo a seguir mostra a saída do comando '**DISPLAY QMGR CONNAUTH**' de um gerenciador de filas em execução no IBM MQ for Multiplatforms.

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

O valor CONNAUTH é o nome de um objeto **AUTHINFO** IBM MQ.

Como a autenticação do sistema operacional (**AUTHTYPE**(*IDPWOS*)) é válida em ambos IBM MQ for Multiplatforms e IBM MQ for z/OS, os exemplos usam a autenticação do sistema operacional.

z/OS O exemplo a seguir mostra o objeto padrão enviado para **AUTHTYPE**(*IDPWOS*) a partir de um gerenciador de filas em execução no 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 O exemplo a seguir mostra o objeto padrão enviado para **AUTHTYPE**(*IDPWOS*) a partir de um gerenciador de filas em execução no 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)
```

O AUTHINFO TYPE(IDPWOS) tem um atributo chamado CHCKCLNT. Se o valor for mudado para *REQUIRED*, todos os aplicativos clientes terão que fornecer um ID de usuário e senha válidos.

Se o usuário tiver sido autenticado na Etapa 7, ele não será autenticado novamente, a menos que o usuário ou a senha no campo SecurityParms da estrutura do MQCXP tenha sido mudada por uma saída de segurança na Etapa 9.

Etapa 11: adotar o contexto do usuário MQCSP (Se `ChlauthEarlyAdopt=`*`N`* e ADOPTCTX=YES)
É possível configurar o atributo ADOPTCTX, que controla se o canal é executado sob MCAUSER ou o ID do usuário que o aplicativo forneceu.

Se o ID do usuário declarado no MQCSP ou no campo **`SecurityParms`** da estrutura MQXCP, foi autenticado com sucesso e **ADOPTCTX** é *YES*, então o contexto do usuário resultante das etapas 7 e 8 é adotado como o contexto a ser usado para esta aplicação, a menos que o usuário ou senha no campo **`SecurityParms`** da estrutura MQCXP foi alterado por uma saída de segurança na etapa 9.

Esse ID do usuário declarado é o ID do usuário que é verificado para autorização para usar os recursos do IBM MQ.

Por exemplo, você não tem um conjunto MCAUSER no canal SVRCONN e seu cliente está em execução no '`johndoe`' em sua máquina Linux. Seu aplicativo especifica o usuário '`fred`' no MQCSP, assim, o canal começa a ser executado com '`johndoe`' como o MCAUSER ativo. Após a verificação do CONNAUTH, o usuário '`fred`' é adotado, e o canal é executado com '`fred`' como o MCAUSER ativo.

Etapa 12: Verificar se o usuário não está bloqueado (BLOCKUSER)
Se a verificação **CONNAUTH** for bem-sucedida, o cache CHLAUTH será então inspecionado novamente para verificar se o MCAUSER ativo está bloqueado por uma regra *BLOCKUSER*. Se o usuário estiver bloqueado, o canal será encerrado.

Step13: Validar os requisitos de CHLAUTH CHCKCLNT
Se a regra CHLAUTH selecionada na etapa 8 especificar adicionalmente um valor CHCKCLNT de REQUIRED ou REQDADM, a validação será feita para assegurar que um ID do usuário CONNAUTH válido foi fornecido para atender ao requisito.

- Se CHCKCLNT (REQUIRED) estiver configurado, um usuário deverá ter sido autenticado na etapa 7 ou 10.. Caso contrário, a conexão será rejeitada
- Se CHCKCLNT (REQDADM) estiver configurado, um usuário deverá ter sido autenticado na etapa 7 ou 10 se for determinado que essa conexão é privilegiada Caso contrário, a conexão será rejeitada
- Se CHCKCLNT (ASQMGR) for configurado, esta etapa será ignorada.

Notes:

1. Se CHCKCLNT (REQUIRED) ou CHCKCLNT (REQDADM) estiver configurado, mas CONNAUTH não estiver ativado no gerenciador de filas, a conexão falhará com um código de retorno MQRC_SECURITY_ERROR (2063) devido ao conflito na configuração..
2. O usuário não é autenticado novamente nesta etapa

Etapa 14: Validar os requisitos de CONNAUTH CHCKCLNT.
A fase de autenticação ocorre quando CONNAUTH é ativado no gerenciador de filas.

O valor CONNAUTH CHCKCLNT é verificado para determinar quais requisitos são configurados para conexões de entrada:

- Se CHCKCLNT (NONE) for configurado, esta etapa será ignorada
- Se CHCKCLNT (OPTIONAL) for configurado, esta etapa será ignorada.
- Se CHCKCLNT (REQUIRED) for configurado, um usuário deverá ter sido autenticado na etapa 7 ou 10.. Caso contrário, a conexão será rejeitada
- Se CHCKCLNT (REQDADM) estiver configurado, um usuário deverá ter sido autenticado na etapa 7 ou 10 se for determinado que essa conexão é privilegiada Caso contrário, a conexão será rejeitada

Nota: O usuário não é autenticado novamente nesta etapa

Multi **Etapa 15: Verificar autorização de objeto**

Uma verificação é feita para assegurar que o MCAUSER ativo tenha a autoridade apropriada para se conectar ao gerenciador de filas.

ULW Consulte Gerenciador de autoridade de objeto para obter mais informações.

IBM i Consulte “Gerenciador de autoridade de objeto no IBM i” na página 157, para mais informações.

Etapa 16: A conexão é concluída

Se as etapas anteriores forem concluídas com sucesso, a conexão estará concluída.

Conceitos relacionados

CONNAUTH

Um gerenciador de filas pode ser configurado para usar um ID do usuário e senha fornecidos para verificar se um usuário tem autoridade para acessar recursos.

Referências relacionadas

SET CHLAUTH

ALTER AUTHINFO

Resolvendo problemas de acesso CHLAUTH

Sugestões sobre como resolver determinados problemas de acesso ao usar registros de autenticação de canal (CHLAUTH).

Regras CHLAUTH padrão

Há três regras padrão para o processamento de CHLAUTH:

- NO ACCESS para todos os canais por quaisquer usuários `MQ-admin*`
- NO ACCESS to all SYSTEM.* canais por todos os usuários
- Acesso ALLOW ao canal SYSTEM.ADMIN.SVRCONN (usuários não `MQ-admin`)

As duas primeiras regras bloqueiam o acesso a todos os canais. A terceira regra é mais específica e, portanto, tem precedência sobre as outras duas, caso o canal seja o canal SYSTEM.ADMIN.SVRCONN, permitindo, portanto, o acesso nesse canal.

Erros comuns de conexão

As regras CHLAUTH são usadas para determinar se um canal pode ser iniciado e permitem o mapeamento, por meio de MCAUSER, para outro ID do usuário. Se o canal não puder ser iniciado, os erros a seguir ocorrerão normalmente:

- RC 2035 MQRC_NOT_AUTHORIZED
- RC 2059 MQRC_Q_MGR_NOT_AVAILABLE
- AMQ4036 Acesso não permitido
- AMQ9776: O canal foi bloqueado pelo ID do usuário
- AMQ9777: O canal foi bloqueado
- MQJE001: Ocorreu uma MQException: Código de Conclusão 2, Razão 2035
- MQJE036: O gerenciador de filas rejeitou uma tentativa de conexão

É necessário bloquear o acesso estritamente e, em seguida, incluir mais regras CHLAUTH para controlar quem pode acessar e iniciar os canais. Como uma medida provisória e para solucionar os erros listados, é possível:

- “Desativar regras CHLAUTH” na página 62
- “Modificar ou remover regras CHLAUTH” na página 62

Desativar regras CHLAUTH

Como uma medida provisória e também para solucionar os erros acima, é possível desativar as regras CHLAUTH. As regras podem ser reativadas a qualquer momento e se a desativação das regras CHLAUTH resolver o problema de conexão, você sabe que essa foi a causa.

Para desativar as regras CHLAUTH, emita o comando a seguir:

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

Observe que também é possível configurar CHLAUTH como *WARN*, que permite o acesso e registra o resultado da regra.

Modificar ou remover regras CHLAUTH

Também é possível excluir ou modificar uma ou mais regras CHLAUTH, que causa seu problema.

Para modificar uma regra CHLAUTH, utilize o comando SET CHLAUTH com ACTION (REPLACE). Por exemplo, para modificar a regra padrão que causa nenhum acesso a todos os canais por quaisquer usuários `MQ-admin` para WARN, em vez do bloqueio, emita o comando a seguir:

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

Para excluir uma regra CHLAUTH, utilize o comando SET CHLAUTH com a ACTION (REMOVE). Por exemplo, para excluir a regra padrão que causa nenhum acesso a todos os canais por quaisquer usuários `MQ-admin`, emita o comando a seguir:

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

Testando o acesso usando MATCH (RUNCHECK)

É possível testar o resultado de suas regras CHLAUTH, usando a opção MATCH (*RUNCHECK*) da regra CHLAUTH em runmqsc. A opção **MATCH** (*RUNCHECK*) retorna o registro que é correspondido por um canal de entrada específico no tempo de execução, quando esse canal se conecta a esse gerenciador de filas. Deve-se fornecer:

- O nome do canal
- Atributo ADDRESS
- Atributo SSLPEER, apenas se o canal de entrada usar SSL ou TLS
- QMNAME, se o canal de entrada for um canal do gerenciador de filas ou
- Atributo CLNTUSER, se o canal de entrada for um canal do cliente

O exemplo a seguir verifica qual regra CHLAUTH, com as regras padrão em vigor, resulta em um usuário `MQ-admin` `johndoe` acessando um canal chamado `CHAN1`:

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

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

Para o usuário `johndoe`, o canal não é executado e o usuário será bloqueado devido à regra BLOCKUSER para usuários *MQADMIN.

O exemplo a seguir verifica qual regra CHLAUTH, com as regras padrão em vigor, resulta no usuário `alice`, que não é um usuário `MQ-admin`, acessando um canal denominado `CHAN1`:

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

```
('192.168.1.138')

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

Para o usuário `alice`, o canal é executado e transmite `alice` como o MCAUSER. O MCAUSER é o ID do usuário usado para verificar as autoridades de objetos do IBM MQ.

Referências relacionadas

SET CHLAUTH

DISPLAY CHLAUTH

Criando novas regras CHLAUTH para usuários

Alguns cenários comuns para usuários e regras CHLAUTH de exemplo para realizá-los.

Este tópico contém os cenários a seguir:

- “Controle de acesso para usuários MQ-admin específicos” na página 63
- “Controlando o acesso para um usuário e aplicativo cliente do IBM MQ específicos” na página 64
- “Controlando o acesso de um usuário específico usando o nome distinto (DN) de certificado desse usuário” na página 64
- “Mapeando um usuário específico para o usuário mqm” na página 65

Controle de acesso para usuários MQ-admin específicos

Para este cenário, configure um canal de conexão do servidor que deverá ser usado exclusivamente para uma perspectiva administrativa, ou seja, para conexão por meio do IBM MQ Explorer. Você tem um canal específico para esse uso, um ou mais endereços IP definidos de onde deseja que as conexões sejam aceitas e acesso bloqueado para o ID `'mqm'`, caso a conexão não seja de um dos endereços IP especificados.

Crie um canal SVRCONN para os usuários IBM MQ Explorer e `MQ-admin` chamados `ADMIN.CHAN`:

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

Para teste, assegure-se de que tenha um usuário definido que esteja no grupo `MQ-admin` e um que não esteja. Para este cenário, `mqadm` está no grupo `MQ-admin` e `alice` não está.

As regras CHLAUTH padrão estão no local. Inclua três regras para permitir que um usuário específico acesse ADMIN.CHAN como `MQ-admin` por meio de determinados endereços IP:

- Configure NOACCESS por meio de qualquer endereço
- Configure BLOCKUSER para esse canal para bloquear apenas o usuário `nobody`, que substitui o *MQADMIN BLOCKUSER
- Permita acesso ALLOW ao usuário `mqadm` em uma sub-rede de endereços específica e MAP para autoridade de usuário `mqadm`

```
runmqsc:
SET CHLAUTH (ADMIN.CHAN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS)
SET CHLAUTH('ADMIN.CHAN') TYPE(BLOCKUSER) +
DESCR('Rule to override *MQADMIN blockuser on this channel') +
USERLIST('nobody') ACTION(replace)
SET CHLAUTH('ADMIN.CHAN') TYPE(USERMAP) +
CLNTUSER('mqadm') USERSRC(MAP) MCAUSER('mqadm') +
ADDRESS('192.168.1.*') +
DESCR('Allow mqadm as mqadm on local subnet') ACTION(ADD)
```

Neste ponto, o usuário `mqadm` pode acessar e iniciar o canal ADMIN.CHAN, por meio de um intervalo de endereço IP especificado.

É possível executar MATCH (RUNCHECK) a qualquer momento para ver os resultados de cada um desses comandos:

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

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

Neste ponto, apenas os usuários que têm um registro CHLAUTH têm permissão para acessar usando o ADMIN.CHAN.

Controlando o acesso para um usuário e aplicativo cliente do IBM MQ específicos

Para este cenário, as regras CHLAUTH padrão são adequadas, supondo que a autoridade do IBM MQ deve ser configurada para um usuário específico, a fim de fornecer a autoridade correta do IBM MQ (usando setmqaut).

Neste cenário, as autoridades são configuradas para um usuário `mqapp1`, que não é um usuário `MQ-admin`. Faça com que um canal SVRCONN, APP1.CHAN, seja usado por um aplicativo e por um usuário específicos.

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

Com as regras CHLAUTH padrão em vigor, o usuário `mqapp1` pode iniciar o canal APP1.CHAN.

O ID do usuário proveniente do aplicativo cliente do IBM MQ é usado para verificação de autoridade de objeto do IBM MQ. Nesse caso, supondo que o usuário 'mqapp1' está executando o aplicativo do cliente do IBM MQ, isso é usado para verificação de autoridade de objeto do IBM MQ. Portanto, se `mqapp1` tiver acesso aos objetos do IBM MQ de que o aplicativo precisa, tudo estará normal, caso contrário, você obterá erros de autoridade.

É possível aumentar a segurança ainda mais ao criar regras CHLAUTH específicas para o ID do usuário `mqapp1`, no entanto, sob as regras padrão, nenhum membro do grupo `MQ-admin` pode acessar esse canal.

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

Controlando o acesso de um usuário específico usando o nome distinto (DN) de certificado desse usuário

Para este cenário, o usuário deve ter um certificado que seja encaminhado para o gerenciador de filas. O DN é, então, correspondido com a configuração SSLPEER da regra CHLAUTH e o SSLPEER pode utilizar caracteres curinga.

Se correspondido, o usuário também poderá ser mapeado para um MCAUSER diferente para propósitos de verificação das autoridades de objeto do IBM MQ. O mapeamento do MCAUSER pode minimizar o número de usuários que precisam ser gerenciados no gerenciador de autoridade de objeto (OAM) do IBM MQ.

Você tem um canal TLS com certificados em uso e requer regras para:

- Bloquear todos os usuários para um canal específico
- Permitir apenas usuários com um determinado SSLPEER que usam o cliente desse usuário para acesso do IBM MQ OAM.

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

O ID do usuário do cliente que está se conectando no canal é usado para a autoridade do IBM MQ OAM de objetos do IBM MQ, portanto, o ID do usuário deve ter autoridades apropriadas do IBM MQ.

Se desejar, será possível mapear para um ID do usuário do IBM MQ diferente usando:

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

em vez de USERSRC(CHANNEL).

Mapeando um usuário específico para o usuário `mqm`

Essa é uma inclusão ou modificação no “Controle de acesso para usuários MQ-admin específicos” na página 63.

Inclua a regra CHLAUTH a seguir para mapear usuários específicos para o usuário `mqm` ou um ID do usuário `MQ-admin`, que tenha a configuração de autoridade de objeto do IBM MQ no do IBM MQ OAM.

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

Isso permite e mapeia o usuário `johndoe` para o usuário `mqm` para o canal ADMIN.CHAN específico.

Conceitos relacionados

“Resolvendo problemas de acesso CHLAUTH” na página 61
Sugestões sobre como resolver determinados problemas de acesso ao usar registros de autenticação de canal (CHLAUTH).

“Criando novas regras CHLAUTH para canais” na página 65
Para ajudar a criar suas próprias regras CHLAUTH, aqui estão alguns cenários comuns para os canais, e, por exemplo, regras CHLAUTH para realizar isso.

Referências relacionadas

SET CHLAUTH
DISPLAY CHLAUTH

Criando novas regras CHLAUTH para canais
Para ajudar a criar suas próprias regras CHLAUTH, aqui estão alguns cenários comuns para os canais, e, por exemplo, regras CHLAUTH para realizar isso.

Este tópico contém os cenários a seguir:

- “Permitir acesso a um determinado canal por meio de um intervalo de endereços IP específico” na página 66
- “Para um canal específico, bloqueie todos os usuários, mas permita que usuários específicos se conectem.” na página 66

- “Usando CHLAUTH para canais receptores e emissores” na página 66

Permitir acesso a um determinado canal por meio de um intervalo de endereços IP específico

Para este cenário, você deseja:

- Configurar Nenhum acesso ao canal de qualquer lugar
- Permitir acesso por meio de um endereço IP ou de intervalo de endereços específico

```
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)
```

Isso permite que apenas o canal APP2.CHAN seja iniciado quando a condição é proveniente de um intervalo de endereço IP específico determinado.

O usuário que se conecta como MCAUSER é mapeado para `mqapp2` e, portanto, obtém a autoridade OAM do IBM MQ para esse usuário.

Para um canal específico, bloqueie todos os usuários, mas permita que usuários específicos se conectem.

Para este cenário, o acesso ao canal MY.SVRCONN tem as regras CHLAUTH padrão em vigor.

É necessário incluir o seguinte:

```
# 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)
```

Essa primeira parte do código impede que qualquer pessoa se conecte a MY.SVRCONN e, em seguida, o código permite que apenas o canal MY.SVRCONN seja iniciado quando a conexão é proveniente do ID do usuário específico `johndoe`.

O usuário que se conecta no canal `johndoe` é usado para a autoridade do OAM do IBM MQ de objetos do IBM MQ. Portanto, o ID do usuário deve ter as autoridades apropriadas do IBM MQ.

Se desejar, será possível mapear para um ID do usuário do IBM MQ diferente usando:

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

em vez de `USERSRC(CHANNEL)`.

Usando CHLAUTH para canais receptores e emissores

É possível usar regras CHLAUTH para incluir segurança extra nos canais receptores e emissores, para restringir o acesso ao canal receptor. Observe que, se você estiver incluindo ou fazendo mudanças nas regras CHLAUTH, as regras CHLAUTH atualizadas serão aplicadas apenas ao iniciar o canal, portanto, se os canais já estiverem em execução, será necessário pará-los e reiniciá-los, para que as atualizações CHLAUTH sejam aplicadas.

As regras CHLAUTH podem ser usadas em qualquer canal, mas há algumas restrições. Por exemplo, as regras USERMAP se aplicam apenas a canais SVRCONN.

Este exemplo permite uma conexão somente por meio de um endereço IP específico, para iniciar o canal TO.MYSVR1:

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

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

Este exemplo permite a conexão apenas de um gerenciador de filas específico:

```
# 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)
```

Conceitos relacionados

“Resolvendo problemas de acesso CHLAUTH” na página 61
Sugestões sobre como resolver determinados problemas de acesso ao usar registros de autenticação de canal (CHLAUTH).

“Criando novas regras CHLAUTH para usuários” na página 63
Alguns cenários comuns para usuários e regras CHLAUTH de exemplo para realizá-los.

Referências relacionadas

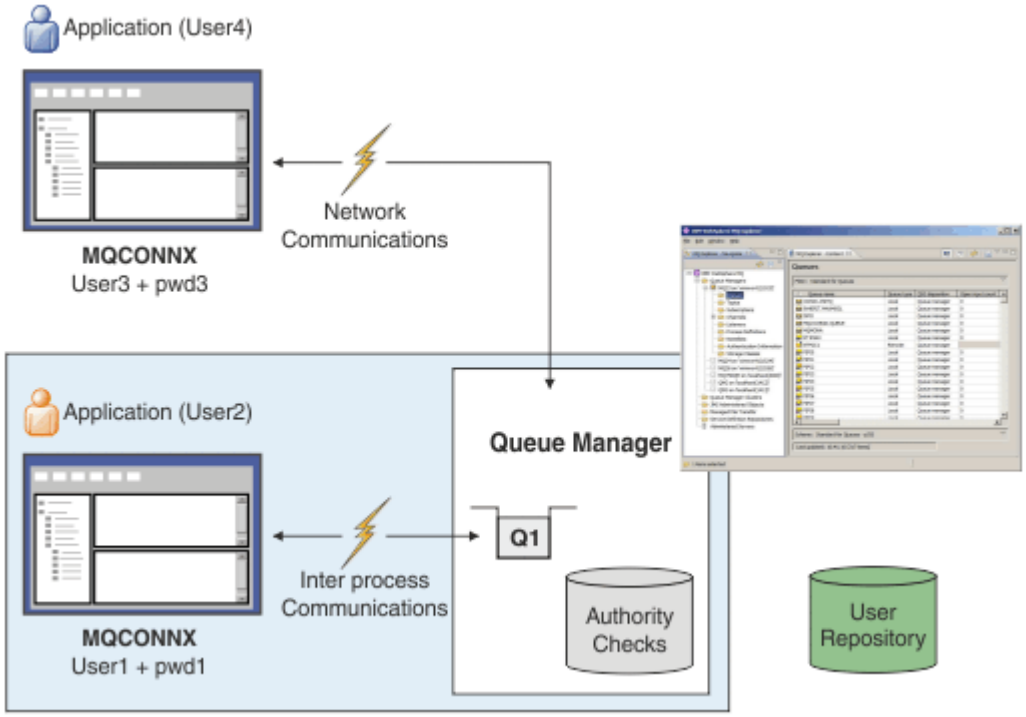
SET CHLAUTH

DISPLAY CHLAUTH

Autenticação de conexão

A autenticação de conexão pode ser alcançada de várias maneiras:

- Um aplicativo pode fornecer um ID do usuário e uma senha. O aplicativo pode ser um cliente ou pode usar ligações locais.
- Um gerenciador de filas pode ser configurado para agir em um ID do usuário e senha fornecidos.
- Um repositório pode ser usado para determinar se uma combinação de ID do usuário e senha é válida.



No diagrama, dois aplicativos estão fazendo conexões com um gerenciador de filas, um aplicativo como um cliente e um usando ligações locais. Os aplicativos podem usar uma variedade de APIs para se conectar ao gerenciador de filas, mas todos possuem a capacidade de fornecer um ID do usuário e uma senha. O ID do usuário sob o qual o aplicativo está em execução, `User2` e `User4` no diagrama, que é o ID do usuário do sistema operacional usual apresentado para o IBM MQ pode ser diferente do ID do usuário fornecido pelo aplicativo, `User1` e `User3`.

O gerenciador de filas recebe comandos de configuração (no diagrama, o IBM MQ Explorer está sendo usado) e gerencia a abertura de recursos e verifica a autoridade para acessar esses recursos. Há muitos recursos diferentes no IBM MQ que um aplicativo pode requerer autoridade para acessar. O diagrama ilustra como abrir uma fila para saída, mas os mesmos princípios também se aplicam a outros recursos.

Consulte Repositórios do usuário para obter detalhes sobre o repositório que é usado para verificação de IDs de usuário e senhas.

Conceitos relacionados

“Autenticação de conexão: configuração” na página 68
Um gerenciador de filas pode ser configurado para usar um ID do usuário e senha fornecidos para verificar se um usuário tem autoridade para acessar recursos.

“Autenticação de conexão: Mudanças no aplicativo” na página 72

“Autenticação de conexão: Repositórios do usuário” na página 73
Para cada um de seus gerenciadores de filas, é possível escolher diferentes tipos de objeto de informações sobre autenticação para autenticar os IDs do usuário e senhas.

Autenticação de conexão: configuração

Um gerenciador de filas pode ser configurado para usar um ID do usuário e senha fornecidos para verificar se um usuário tem autoridade para acessar recursos.

Ativando a autenticação de conexão em um gerenciador de filas

Em um objeto de gerenciador de filas, o atributo **CONNAUTH** pode ser definido para o nome de um objeto de informações sobre autenticação (AUTHINFO). Esse objeto pode ser de dois tipos (atributo AUTHTYPE):

IDPWOS
Indica que o gerenciador de filas usa o sistema operacional local para autenticar o ID do usuário e a senha.

IDPWLDAP
Indica que o gerenciador de filas usa um servidor LDAP para autenticar o ID do usuário e a senha.

Nota: Não é possível usar qualquer outro tipo de objeto de informações sobre autenticação no campo **CONNAUTH**.

IDPWOS e IDPWLDAP são semelhantes em inúmeros de seus atributos, que são descritos aqui. Outros atributos serão considerados mais tarde.

Para verificar conexões locais, use o atributo **CHCKLOCL** de AUTHINFO (verifique as conexões locais). Para verificar conexões do cliente, use o atributo **CHCKCLNT** de AUTHINFO (verifique as conexões do cliente). A configuração deve ser atualizada antes que o gerenciador de filas reconheça as mudanças.

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

Em que USE.PW no CONNAUTH é uma sequência que corresponde à definição de AUTHINFO.

CHCKLOCL e **CHCKCLNT** possuem o mesmo conjunto de valores possíveis que permitem que a exatidão da verificação seja variada:

NONE
Desativa a verificação.

OPCIONAL
Assegura que, se um ID do usuário e senha forem fornecidos por um aplicativo, eles sejam um par válido, mas que não seja obrigatório fornecê-los. Esta opção pode ser útil durante a migração, por exemplo.

Importante: OPTIONAL é o valor mínimo que é possível ser configurado, para usar regras CHLAUTH mais rigorosas.

Se você selecionar NONE e a conexão do cliente corresponder a um registro CHLAUTH com CHCKCLNT REQUIRED (ou REQDADM em plataformas diferentes de z/OS), a conexão falhará. Receba a mensagem AMQ9793 em plataformas diferentes de z/OS e a mensagem CSQX793E no z/OS.

REQUIRED
Exige que todos os aplicativos forneçam um ID do usuário e uma senha válidos. Consulte também a nota a seguir.

REQDADM
Os usuários privilegiados devem fornecer um ID do usuário e senha válidos, mas os usuários não privilegiados são tratados como com a configuração OPCIONAL. Consulte também a nota a seguir.
z/OS (Essa configuração não é permitida em sistemas z/OS.)

Nota:

Configurar **CHCKLOCL** como REQUIRED ou REQDADM significa que você não pode administrar localmente o gerenciador de filas usando **runmqsc** (erro AMQ8135: Não autorizado), a menos que o usuário especifique o parâmetro -u UserId na linha de comandos **runmqsc**. Com essa configuração, **runmqsc** solicita a senha do usuário no console.

Da mesma forma, um usuário que está executando o IBM MQ Explorer no sistema local verá o erro AMQ4036 ao tentar se conectar ao gerenciador de filas. Para especificar um nome de usuário e uma senha, clique com o botão direito no objeto do gerenciador de filas locais e selecione **Detalhes da Conexão** > **Propriedades ...** a partir do menu. Na seção **ID do Usuário**, insira o nome do usuário e a senha a serem usados e, em seguida, clique em **OK**.

Considerações semelhantes se aplicam às conexões remotas com **CHCKCLNT**.

CONNAUTH está em branco para gerenciadores de filas migrados, mas configurado como *SYSTEM.DEFAULT.AUTHINFO.IDPWOS* para novos gerenciadores de filas. A definição precedente **AUTHINFO** tem **CHCKCLNT** configurado para *REQDADM* por padrão.

Portanto, você precisará fornecer a senha correta do sistema operacional para quaisquer clientes existentes que usam um ID do usuário privilegiado para se conectar.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas apropriadamente, consulte “Proteção de senha do MQCSP” na página 30.

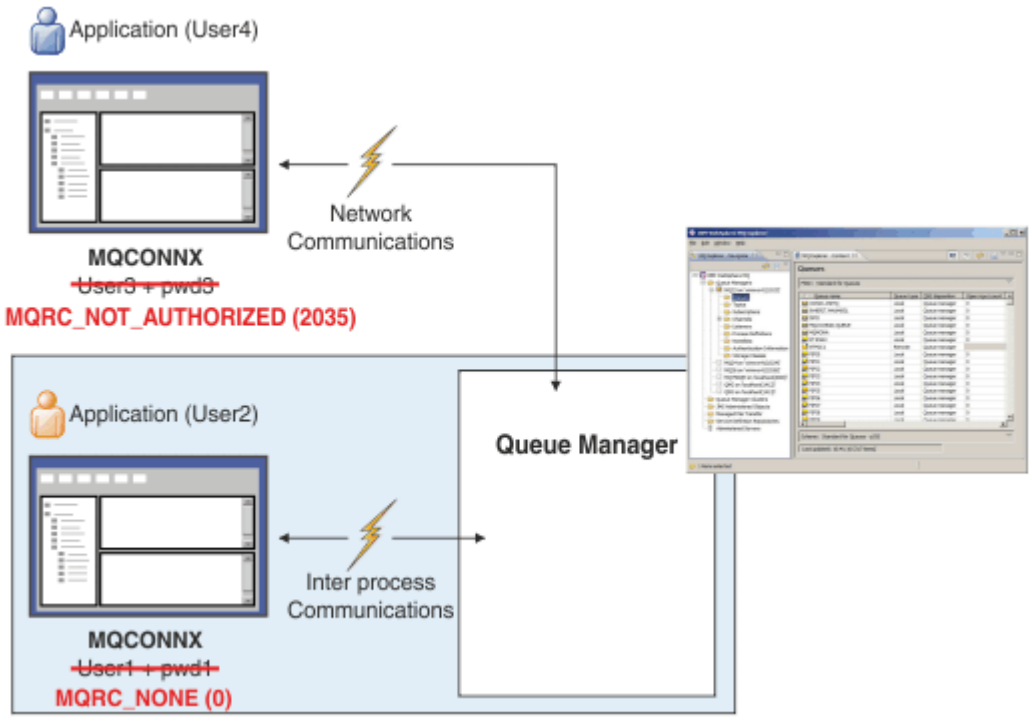
Granularidade de configuração

Além de **CHCKLOCL** e **CHCKCLNT** que são usados para ativar a verificação de ID do usuário e de senha, há aprimoramentos para as regras CHLAUTH para que uma configuração mais específica possa ser feita usando **CHCKCLNT**.

É possível configurar o valor geral **CHCKCLNT** para OPTIONAL, por exemplo, e, em seguida, fazer upgrade dele para ser mais rigoroso para determinados canais configurando **CHCKCLNT** como REQUIRED ou REQDADM na regra CHLAUTH. Por padrão, regras CHLAUTH serão executadas com CHCKCLNT(ASQMGR), portanto, essa granularidade não precisa ser usada. Por exemplo:

```
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)
```

Notificação de Erro



Um erro é registrado se um aplicativo não fornece um ID do usuário e senha quando necessário ou fornece uma combinação incorreta, mesmo quando é opcional.

Nota: Quando a verificação de senha está desativada, ao usar a opção NONE no **CHCKLOCL** ou **CHCKCLNT**, senhas inválidas não são detectadas.

Autenticações com falha são mantidas pelo número de segundos especificado pelo atributo **FAILDLAY** antes de o erro ser retornado ao aplicativo. Isso fornece alguma proteção contra um aplicativo tentar repetidamente se conectar.

O erro é registrado de várias maneiras:

Aplicativo
O aplicativo é retornado o erro de segurança padrão do IBM MQ, RC2035 - MQRC_NOT_AUTHORIZED.

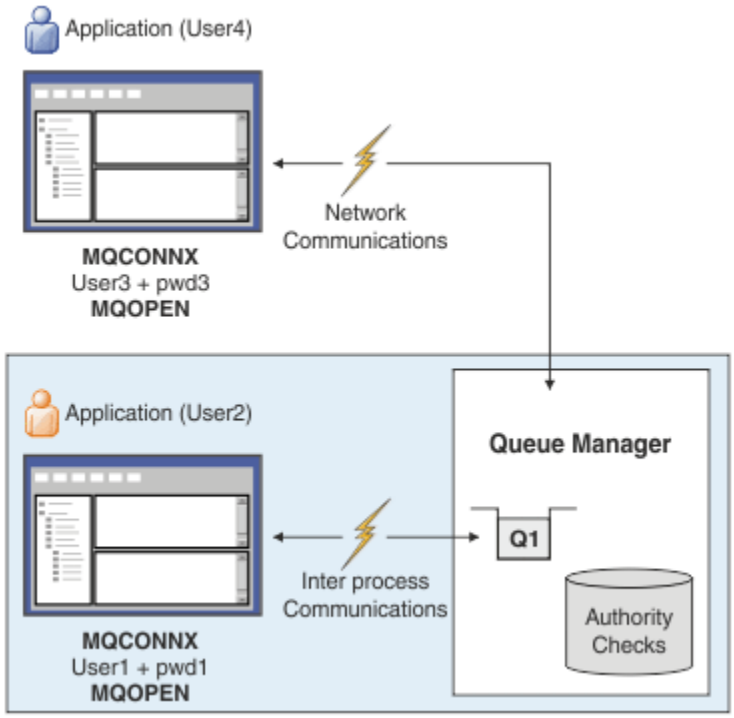
AdministraDor
Um administrador do IBM MQ vê o evento relatado no log de erros e pode, portanto, perceber que o aplicativo foi rejeitado porque o ID do usuário e a senha não passaram na verificação e não porque não houve autoridade de conexão, por exemplo .

Ferramenta de monitoração
Uma ferramenta de monitoramento também pode ser notificada da falha, se você ativar eventos de autoridade enviando uma mensagem de evento para a fila SYSTEM.ADMIN.QMGR.EVENT:

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

Este evento "Não Autorizado" é um evento de conexão Tipo 1, e fornece os mesmos campos que outros eventos Tipo 1, com um campo adicional, o ID do usuário MQCSP que foi fornecido. A senha não está especificada na mensagem do evento. Isso significa que há dois IDs de usuários na mensagem do evento: o ID que sob o qual o aplicativo está executando e o ID que o aplicativo apresentou para a verificação de ID de usuário e senha.

Relacionamento com autorização



É possível configurar um gerenciador de filas para exigir que IDs de usuário e senhas sejam fornecidos por determinados aplicativos, pois o ID do usuário no qual o aplicativo está sendo executado pode não ser o mesmo ID do usuário que foi apresentado pelo aplicativo juntamente com uma senha quando o aplicativo abre uma fila para saída, por exemplo:

```
ALTER QMGR CONNAUTH(USE.PWD)
```

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

Como IDs de usuário e senhas são tratados é controlado pelo atributo **ADOPTCTX** no objeto de informações sobre autenticação.

ADOPTCTX(YES)
Todas as verificações de autorização para um aplicativo são feitas com o mesmo ID do usuário que você autenticou por senha, selecionando para adotar o contexto como o contexto do aplicativo para o resto da vida da conexão.

Atenção: Ao utilizar o ADOPTCTX(YES) e os IDs de usuário do S.O., deve-se assegurar que o ID do usuário que está sendo adotado não exceda o comprimento máximo de IDs de usuário. Veja "IDs de Usuário" na página 83 para obter mais informações.

ADOPTCTX(NO)
Um aplicativo fornece um ID do usuário e senha para os propósitos de autenticá-los no momento da conexão, mas depois continua utilizando o ID do usuário no qual o aplicativo está em execução para verificações de autorização no futuro. Você pode achar essa opção útil ao migrar ou, se você planeja usar outros mecanismos, como registros de autenticação de canal, para designar o identificador de usuário do canal de mensagens (MCAUSER).

Atenção:

Ao usar o parâmetro **ADOPTCTX(YES)** em um objeto de informações sobre autenticação, outro contexto de segurança não pode ser adotado a menos que você configure o parâmetro **ChlauthEarlyAdopt** na sub-rotina de canais do arquivo `qm.ini`.

Por exemplo, o objeto de informações sobre autenticação padrão é configurado como **ADOPTCTX(YES)** e o usuário `fred` está com login efetuado. As duas regras CHLAUTH a seguir são configuradas:

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

O comando a seguir é emitido com a intenção de autenticar o comando como o contexto de segurança adotada do usuário `bob`:

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

Na verdade, o gerenciador de filas usa o contexto de segurança de `fred`, não de `bob`, e a conexão falha.

Para obter mais informações sobre **ChlauthEarlyAdopt**, consulte Atributos da sub-rotina de canais.

Conceitos relacionados
"Autenticação de conexão" na página 67

"Autenticação de conexão: Mudanças no aplicativo" na página 72

"Autenticação de conexão: Repositórios do usuário" na página 73
Para cada um de seus gerenciadores de filas, é possível escolher diferentes tipos de objeto de informações sobre autenticação para autenticar os IDs do usuário e senhas.

Autenticação de conexão: Mudanças no aplicativo

Um aplicativo pode fornecer um ID do usuário e uma senha dentro da estrutura de parâmetros de segurança de conexão (MQCSP) quando MQCONNX é chamado. O ID do usuário e a senha são transmitidos para verificação para o gerenciador de autoridade de objeto (OAM) fornecido com o

gerenciador de filas ou o componente de serviço de autorização fornecido com o gerenciador de filas nos sistemas z/OS. Você não tem que gravar sua própria interface customizada.

Se o aplicativo estiver em execução como um cliente, o ID do usuário e a senha também serão transmitidos para o lado do cliente e as saídas de segurança do lado do servidor para processamento. Eles também podem ser usados para configurar o atributo do ID do usuário do agente do canal de mensagens (MCAUSER) de uma instância do canal. A saída de segurança é chamada com a razão de saída MQXR_SEC_PARMS de para esse processamento. As saídas de segurança do lado do cliente e a saída de pré-conexão podem fazer mudanças no MQCONN antes que ele seja enviado para o Gerenciador de Filas.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas apropriadamente, consulte “Proteção de senha do MQCSP” na página 30.

Ao usar a sequência XAOPEN para fornecer um ID do usuário e senha, é possível evitar ter de fazer mudanças no código do aplicativo.

Nota:

No IBM WebSphere MQ 6.0 a saída de segurança permitiu que o MQCSP seja configurado. Portanto, os clientes nesse nível ou mais recente não precisam ser atualizados.

No entanto, em versões do IBM MQ anteriores à IBM MQ 8.0, o MQCSP não colocou restrições sobre o ID do usuário e a senha que foram fornecidos pelo aplicativo. Ao utilizar esses valores com recursos fornecidos pelo IBM MQ, há limites que se aplicam ao uso desses recursos, mas se você estiver apenas passando-os para as suas próprias saídas, esses limites não se aplicam.

Conceitos relacionados

“Autenticação de conexão” na página 67

“Autenticação de conexão: configuração” na página 68
Um gerenciador de filas pode ser configurado para usar um ID do usuário e senha fornecidos para verificar se um usuário tem autoridade para acessar recursos.

“Autenticação de conexão: Repositórios do usuário” na página 73
Para cada um de seus gerenciadores de filas, é possível escolher diferentes tipos de objeto de informações sobre autenticação para autenticar os IDs do usuário e senhas.

Autenticação de conexão: Repositórios do usuário

Para cada um de seus gerenciadores de filas, é possível escolher diferentes tipos de objeto de informações sobre autenticação para autenticar os IDs do usuário e senhas.

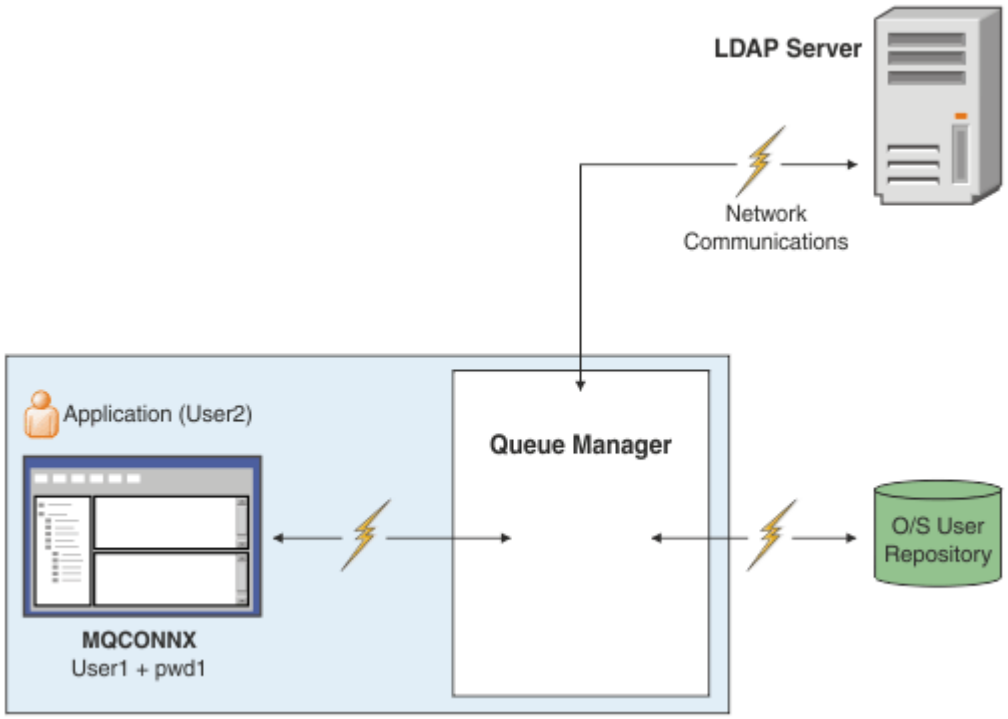


Figura 7. Tipos de objetos de informações de autenticação

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

Há dois tipos de objeto de informações sobre autenticação, conforme representado no diagrama:

- `IDPWOS` é usado para indicar que o gerenciador de filas usa o sistema operacional local para autenticar o ID do usuário e a senha. Se você optar por usar o sistema operacional local, será necessário configurar os atributos comuns, conforme descrito nos tópicos anteriores.
- `IDPWLDAP` é usado para indicar que o gerenciador de filas usa um servidor LDAP para autenticar o ID do usuário e a senha. Se você optar por usar um servidor LDAP, mais informações serão fornecidas nesse tópico.

Somente um tipo de objeto de informações sobre autenticação pode ser escolhido para cada gerenciador de filas usar nomeando o objeto apropriado no atributo **CONNAUTH** do gerenciador de filas.

Usando um servidor LDAP para autenticação.

Configure o campo **CONNAME** para o endereço do servidor LDAP para o gerenciador de filas. É possível fornecer mais endereços para o servidor LDAP em uma lista separada por vírgula, que pode ajudar com redundância se o servidor LDAP não fornecer esse recurso em si.

Configure o servidor LDAP necessários ID e senha nos campos **LDAPUSER** e **LDAPPWD** para que o gerenciador de filas possa acessar o servidor LDAP e procurar informações sobre registros do usuário.

Conexão segura para um servidor LDAP

Diferente dos canais, não há parâmetro **SSLCIPH** para ativar o uso do TLS para a comunicação com o servidor LDAP. Neste caso do IBM MQ está atuando como um cliente para o servidor LDAP, portanto muito da configuração é feito no servidor LDAP. Alguns parâmetros existentes no IBM MQ são usados para configurar como essa conexão funciona.

Configure o campo **SECCOMM** para controlar se a conectividade com o servidor LDAP usa o TLS.

Além desse atributo, os atributos **SSLFIPS** e **SUITEB** do gerenciador de filas restringem o conjunto de especificações de criptografia que são escolhidas. O certificado que é usado para identificar o gerenciador de filas para o servidor LDAP é o certificado do gerenciador de filas `ibmwebspheremq` *`qmgr-name`* ou o valor do atributo **CERTLABL**. Consulte Rótulos de certificado digital para obter detalhes.

Repositório de Usuário LDAP

Ao usar um repositório do usuário LDAP, existe mais alguma configuração a ser feita no gerenciador de filas diferente de apenas informar a ele onde localizar o servidor LDAP.

IDs de usuário definidos em um servidor LDAP têm uma estrutura hierárquica que os identificam exclusivamente. Portanto, um aplicativo pode se conectar ao gerenciador de filas e apresentar seu ID do usuário como o ID do usuário hierárquico completo.

Entretanto, para simplificar as informações que um aplicativo deve fornecer, é possível configurar o gerenciador de filas para presumir que a primeira parte da hierarquia seja comum a todos os IDs e para incluir automaticamente isso antes do ID reduzido fornecido pelo aplicativo. O gerenciador de filas pode, então, apresentar um ID completo ao servidor LDAP.

Configure BASEDNU como o ponto inicial que a procura do LDAP faz para o ID na hierarquia do LDAP. Ao configurar BASEDNU, deve-se assegurar de que somente um resultado será retornado quando procurar o ID na hierarquia do LDAP.

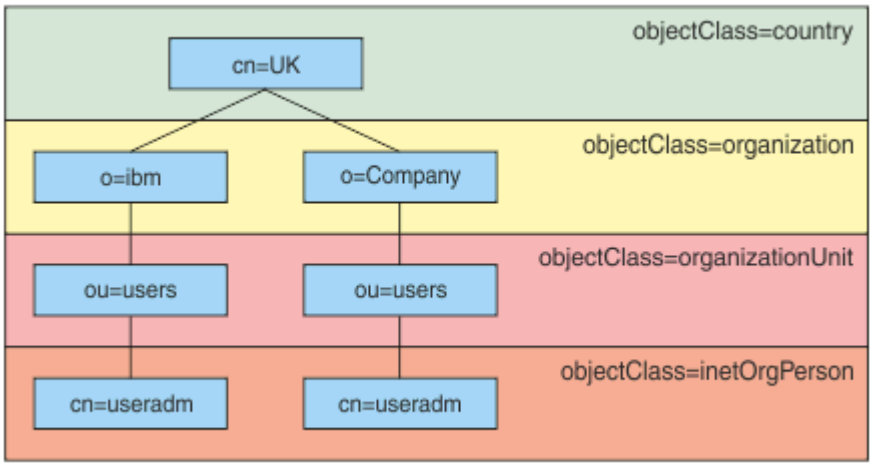


Figura 8. Uma hierarquia LDAP de exemplo

Por exemplo, em Figura 8 na página 75, BASEDNU pode ser configurado como "ou=users,o=ibm,c=UK" ou ",o=ibm,c=UK". Entretanto, como um nome distinto que contém "cn=useradm" existe em ambas as ramificações "o=ibm" e "o=Company", BASEDNU não pode ser configurado como "c=UK". Por motivos de desempenho e segurança, use o ponto mais alto em sua hierarquia de LDAP a partir do qual seja possível referenciar todos os IDs do usuário necessários. Neste exemplo, isso é "ou=users,o=ibm,c=UK".

Seu aplicativo pode enviar ao gerenciador de filas o ID do usuário sem fornecer o nome do atributo LDAP, CN=, por exemplo. Se você configurar USRFIELD para o nome do atributo LDAP, esse valor é incluído como um prefixo para o ID do usuário que vem do aplicativo. Isso pode ser um auxílio de migração útil ao mover dos IDs do usuário do sistema operacional para IDs do usuário LDAP, pois o aplicativo pode apresentar a mesma sequência em ambos os casos e é possível evitar mudar o aplicativo.

Portanto, o ID do usuário completo apresentado ao servidor LDAP é semelhante a:

```
USRFIELD = ID_from_application BASEDNU
```

Conceitos relacionados

“Autenticação de conexão” na página 67

“Autenticação de conexão: configuração” na página 68
Um gerenciador de filas pode ser configurado para usar um ID do usuário e senha fornecidos para verificar se um usuário tem autoridade para acessar recursos.

“Autenticação de conexão: Mudanças no aplicativo” na página 72

Saída de segurança do lado do cliente para inserir o ID do usuário e a senha (mqccred)

Se você tiver quaisquer aplicativos cliente que são necessários para enviar um ID do usuário ou senha, mas ainda não é possível mudar a origem, há uma saída de segurança fornecida com o IBM MQ 8.0 denominada **mqccred** que é possível usar. **mqccred** fornece um ID do usuário e senha em nome do aplicativo cliente, a partir de um arquivo `.ini`. Esse ID do usuário e a senha são enviados ao gerenciador de filas que, se configurado para fazer isso, os autenticará.

Visão Geral

mqccred é uma saída de segurança que é executada na mesma máquina que seu aplicativo cliente. Ela permite que informações de ID do usuário e senha sejam fornecidas em nome do aplicativo cliente, em que as informações não estão sendo fornecidas pelo próprio aplicativo. As informações do ID do usuário e senha são fornecidas em uma estrutura conhecida como Connection Security Parameters (MQCSP) e serão autenticados pelo gerenciador de filas, se a conexão de autenticação for configurada.

As informações do ID do usuário e senha são recuperadas de um arquivo `.ini` na máquina cliente. As senhas no arquivo são protegidas por ofuscação usando o comando **runmqccred** e também assegurando que as permissões de arquivo no arquivo `.ini` sejam configuradas de tal forma que somente o ID do usuário executando o aplicativo cliente (e, portanto, a saída) seja capaz de lê-las.

Local

mqccred é instalado:

Plataformas Windows
No diretório *installation_directory*\Tools\c\Samples\mqccred\

Plataformas UNIX
No diretório *installation_directory*/samp/mqccred

Notes: A saída:

1. Age apenas como uma saída de segurança do canal e precisa ser a única tal saída definida em um canal.
2. É geralmente chamada por meio do Client Channel Definition Table (CCDT), mas um cliente Java pode ter a saída mencionada diretamente nos objetos JNDI ou a saída pode ser configurada para aplicativos que constroem manualmente a estrutura MQCD.
3. Deve-se copiar os programas **mqccred** e **mqccred_r** para o diretório `var/mqm/exits`.

   Por exemplo, em uma máquina da plataforma UNIX de 64 bits, emita o comando:

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

   Consulte Um exemplo passo a passo de como testar mqccred para obter mais informações.
4. É capaz de executar em versões anteriores do IBM MQ, desde o IBM WebSphere MQ 7.0.1.

Configurando IDs do Usuário e Senhas

O arquivo `.ini` contém sub-rotinas para cada gerenciador de filas, com uma configuração global para gerenciadores de filas não especificados. Cada sub-rotina contém o nome do gerenciador de filas, um ID do usuário e um texto simples ou uma senha ofuscada.

Deve-se editar o arquivo `.ini` manualmente, usando o editor de sua escolha e incluir o atributo de senha de texto simples para as sub-rotinas. Execute o programa **runmqccred** fornecido, que usa o arquivo `.ini` e substitui o atributo **Password** com o atributo **OPW**, uma forma ofuscada da senha.

Consulte runmqccred para uma descrição do comando e seus parâmetros.

O arquivo `mqccred.ini` contém seu ID do usuário e senha.

Um arquivo de modelo `.ini` é fornecido no mesmo diretório que a saída para fornecer um ponto de início para sua empresa.

Por padrão, este arquivo será procurado em `$HOME/.mqs/mqccred.ini`. Se você gostaria de localizá-lo em outro lugar, é possível usar a variável de ambiente *MQCCRED* para apontar para ele:

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

Se você usar *MQCCRED*, a variável deve incluir o nome completo do arquivo de configuração, incluindo qualquer arquivo `.ini`. Como esse arquivo contém senhas (mesmo se ofuscadas), é esperado que você proteja o arquivo usando privilégios do sistema operacional para assegurar que as pessoas não autorizadas não possam lê-la. Se você não tem a permissão de arquivo correta, a saída não executará com êxito.

Se o aplicativo já tiver fornecido uma estrutura MQCSP a saída normalmente respeita isso e não irá inserir quaisquer informações a partir do arquivo `.ini`. Entretanto, você pode substituir esse usando o atributo **Force** na sub-rotina.

Configurar **Force** para o valor *TRUE* remove o ID do usuário e senha fornecidos pelo aplicativo e substitui aqueles com a versão do arquivo ini.

Também é possível configurar o atributo **Force** na seção global do arquivo para configurar o valor padrão desse arquivo.

O valor padrão para **Force** é *FALSE*.

Você pode fornecer um ID do usuário e uma senha para todos os gerenciadores de filas, ou para cada gerenciador de filas individual. Este é um exemplo de um arquivo `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
```

Notes:

1. As definições de gerenciador de filas individual têm precedência sobre a configuração global.
2. Os atributos fazem distinção entre maiúsculas e minúsculas.

Limitadores

Quando essa saída estiver em uso, o ID do usuário local da pessoa que está executando o aplicativo não fluirá do cliente para o servidor. As únicas informações de identidade disponíveis são a partir do conteúdo do arquivo ini.

Portanto, deve-se configurar o gerenciador de filas para usar **ADOPTCTX(YES)** ou mapear a solicitação de conexão de entrada para um ID do usuário apropriado por meio de um dos mecanismos disponíveis, por exemplo, “Registros de Autenticação de Canal” na página 49.

Importante: Se você incluir novas senhas ou atualizar antigas, o comando **runmqccred** somente processará quaisquer senhas de texto simples, deixando as ofuscadas intocadas.

Depurando

A saída grava para o rastreio do IBM MQ padrão quando ele está ativado.

Para ajudar na depuração de problemas de configuração, a saída também pode gravar diretamente para stdout.

Nenhuma configuração de dados da saída de segurança do canal (**SCYDATA**) é normalmente requerida para o canal. Entretanto, é possível especificar:

ERRO
Imprime somente informações sobre condições de erro, como não ser capaz de localizar o arquivo de configuração.

DEPURAÇÃO
Exibe estas condições de erro e algumas trilhas de auditoria adicionais.

NOCHECKS
Efetua bypass das restrições sobre as permissões de arquivo e a restrição adicional de que o arquivo `.ini` não deve conter quaisquer senhas desprotegidas.

É possível colocar um ou mais desses elementos no campo **SCYDATA**, separados por vírgulas, em qualquer ordem. Por exemplo, `SCYDATA=(NOCHECKS,DEBUG)`.

Observe que os itens fazem distinção entre maiúsculas e minúsculas e devem ser digitados em letras maiúsculas.

Usando o `mqccred`

Assim que tiver o seu arquivo configurado, é possível chamar a saída de canal atualizando a sua definição de canal de conexão do cliente para incluir o atributo `SCYEXIT('mqccred(ChlExit)')`:

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

Referências relacionadas
SCYDATA
SCYEXIT
runmqccred

Autenticação de conexão com o cliente Java

A autenticação de conexão é um recurso no IBM MQ que permite que o gerenciador de filas seja configurado para autenticar aplicativos, usando um ID do usuário e senha fornecidos. Quando o aplicativo for um aplicativo Java que está usando ligações de clientes, a autenticação de conexão poderá ser executada no modo de compatibilidade ou modo de autenticação MQCSP.

Compatibility Mode

Antes do IBM MQ 8.0, o cliente Java podia enviar um ID do usuário e senha por meio do canal de conexão do cliente para o canal de conexão do servidor e fornecer a eles uma saída de segurança nos campos **RemoteUserIdentifier** e **RemotePassword** da estrutura MQCD. No modo de compatibilidade, esse comportamento é retido.

Você pode usar este modo em combinação com a autenticação de conexão e migrar para fora de quaisquer saídas de segurança que foram anteriormente usadas para executar a mesma tarefa.

Deve-se usar ADOPTCTX(YES) ou ter outro método, por exemplo, uma regra CHLAUTH com base em um certificado TLS para configurar o MCAUSER em execução quando você está usando o modo de compatibilidade, uma vez que nesse modo o ID do usuário do lado do cliente não é enviado ao gerenciador de filas.

O modo de compatibilidade pode ser ativado em uma base de conexão por conexão ou globalmente:

- No IBM MQ classes for Java, configure a propriedade *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* para `false` na hashtable de propriedades que é passada para o construtor **`com.ibm.mq.MQQueueManager`**.
- No IBM MQ classes for JMS, configure a propriedade *JmsConstants.USER_AUTHENTICATION_MQCSP* para `false` no connection factory apropriado antes de criar a conexão.
- Globalmente, especifique a Java propriedade de sistema *-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication= N* na linha de comandos ao iniciar o aplicativo, conforme mostrado no exemplo a seguir:

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

O modo de compatibilidade é a configuração padrão.

Modo de autenticação MQCSP

Neste modo, o ID do usuário do lado do cliente é enviado, bem como o ID do usuário e a senha a serem autenticados, portanto, você é capaz de usar ADOPTCTX(NO). O ID do usuário e a senha estão disponíveis para uma saída de segurança de conexão do servidor na estrutura MQCSP que é fornecida na estrutura MQCXP.

Esse modo de operação pode ser ativado em uma base de conexão por conexão ou globalmente:

- No IBM MQ classes for Java, configure a propriedade *MQConstants.USE_MQCSP_AUTHENTICATION_PROPERTY* para `true` na hashtable de propriedades que é passada para o construtor **`com.ibm.mq.MQQueueManager`**.
- No IBM MQ classes for JMS, configure a propriedade *JmsConstants.USER_AUTHENTICATION_MQCSP* para `true` no connection factory apropriado antes de criar a conexão.
- Globalmente, configure a propriedade de sistema *com.ibm.mq.cfg.jmqi.useMQCSPauthentication* para um valor que indica true, por exemplo, incluindo `-Dcom.ibm.mq.cfg.jmqi.useMQCSPauthentication=Y` na linha de comandos.

Escolhendo o modo de autenticação no IBM MQ Explorer

Como o IBM MQ Explorer é um aplicativo Java, esses dois modos, o modo de compatibilidade e o modo de autenticação MQCSP, também são aplicáveis a ele.

V 9.1.0 A partir da IBM MQ 9.1.0, o modo de autenticação MQCSP é o padrão. Antes de IBM MQ 9.1, o modo de compatibilidade é o padrão.

Nos painéis nos quais a identificação de usuário é fornecida, há uma caixa de seleção para ativar ou desativar o modo de compatibilidade:

- V 9.1.0 Na IBM MQ 9.1.0, por padrão, essa caixa de seleção não está selecionada. Para usar o modo de compatibilidade, marque essa caixa de seleção.
- Antes da IBM MQ 9.1.0, por padrão, essa caixa de seleção está ativada. Para usar a autenticação MQCSP, limpe a caixa de seleção.

Conceitos relacionados

“Autenticação de conexão” na página 67

“Autenticação de conexão: Mudanças no aplicativo” na página 72

“Autenticação de conexão: Repositórios do usuário” na página 73
Para cada um de seus gerenciadores de filas, é possível escolher diferentes tipos de objeto de informações sobre autenticação para autenticar os IDs do usuário e senhas.

Segurança de mensagem no IBM MQ

A segurança de mensagem na infraestrutura do IBM MQ é fornecida pelo Advanced Message Security.

Advanced Message Security (AMS) expande os serviços de segurança do IBM MQ para fornecer assinatura e criptografia de dados no nível de mensagem. Os serviços expandidos garantem que os dados da mensagem não foram modificados entre quando foram originalmente colocados em uma fila e quando foram recuperados. Além disso, o AMS verifica se um emissor de dados da mensagem está autorizado a colocar mensagens assinadas em uma fila de destino.

Conceitos relacionados

“Advanced Message Security” na página 569
O Advanced Message Security (AMS) é um componente do IBM MQ que fornece um alto nível de proteção para dados sensíveis que fluem por meio da rede do IBM MQ, ao mesmo tempo em que não impacta os aplicativos finais.

Planejando para seus requisitos de segurança

Esta coleção de tópicos explica o que é necessário considerar ao planejar a segurança em um ambiente do IBM MQ.

É possível usar o IBM MQ para uma grande variedade de aplicativos em uma gama de plataformas. Os requisitos de segurança provavelmente serão diferentes para cada aplicativo. Para alguns, a segurança será uma consideração crítica.

O IBM MQ fornece um intervalo de serviços de segurança de nível de link, incluindo suporte para Segurança da Camada de Transporte (TLS).

Deve-se considerar determinados aspectos de segurança ao planejar a instalação do IBM MQ:

- Multi Em Multiplataformas, se você ignorar esses aspectos e não fizer nada, não poderá usar o IBM MQ.
- z/OS No z/OS, o efeito de ignorar esses aspectos é que os recursos do IBM MQ ficam desprotegidos. Ou seja, todos os usuários podem acessar e mudar todos os recursos do IBM MQ .

Autoridade para administrar o IBM MQ

Os administradores do IBM MQ precisam de autoridade para:

- Emita comandos para administrar o IBM MQ
- Usar o IBM MQ Explorer
- IBM i Usar comandos e painéis administrativos do IBM i.
- z/OS Use os painéis de operações e de controle no z/OS
- z/OS Use o programa utilitário IBM MQ, CSQUTIL, em z/OS
- z/OS Acesse os conjuntos de dados do gerenciador de filas no z/OS

Para obter informações adicionais, consulte:

- ULW “Autoridade para administrar o IBM MQ no UNIX, Linux, and Windows” na página 406
- IBM i “Autoridade para administrar o IBM MQ no IBM i” na página 85

- z/OS "Autoridade para administrar o IBM MQ no z/OS" na página 86

autoridade para trabalhar com objetos do IBM MQ

Os aplicativos podem acessar os seguintes objetos do IBM MQ, emitindo chamadas de MQI:

- Gerenciadores de filas
- Filas
- Processos
- Listas de Nomes
- tópicos

Os aplicativos podem também usar comandos de formato de comando programável (PCF) para acessar esses objetos do IBM MQ e para acessar os objetos de informações sobre autenticação de canais e autenticação também. Esses objetos podem ser protegidos pelo IBM MQ, de modo que os IDs de usuários associados ao aplicativo precisam de autoridade para acessá-los.

Para obter informações adicionais, consulte "Autorização para aplicativos usarem o IBM MQ" na página 88.

Segurança de canal

Os IDs de usuário associados a agentes do canal de mensagem (MCAs) necessitam de autoridade para acessar vários recursos do IBM MQ. Por exemplo, um MCA precisa ser capaz de conectar-se a um gerenciador de filas. Se estiver enviando MCA, deverá estar apto a abrir a fila de transmissão do canal. Se for um MCA de recepção, precisa ser capaz de abrir as filas de destino. Os IDs de usuário associados aos aplicativos que precisam administrar canais, inicializadores de canais e listeners precisam de autoridade para usar os comandos do PCF relevantes. No entanto, a maioria dos aplicativos não precisa desse acesso.

Para obter informações adicionais, consulte "Autorização de canal" na página 110.

Considerações Adicionais

É necessário considerar os seguintes aspectos de segurança apenas se você estiver usando certas funções do IBM MQ ou extensões do produto base:

- "Segurança para Clusters de Gerenciadores de Filas" na página 123
- "Segurança para o Publicar/assinar do IBM MQ" na página 124
- "Segurança para IBM MQ Internet Pass-Thru" na página 125

Planejando a identificação e a autenticação

Decida quais IDs do usuário usar e como e em que níveis você deseja aplicar controles de autenticação.

Deve-se como você identificará os usuários dos seus aplicativos IBM MQ, tendo em conta que os sistemas operacionais suportam diferentes IDs de usuário de comprimentos diferentes. É possível usar registros de autenticação de canal para mapear de um ID do usuário para outro, ou para especificar um ID do usuário com base em alguns atributos da conexão. Os canais do IBM MQ que usam TLS usam certificados digitais como um mecanismo para identificação e autenticação. Cada certificado digital tem um nome distinto do assunto que pode ser mapeado para identidades específicas usando registros de autenticação de canal. Além disso, os certificados de autoridade de certificação no repositório de chaves determinam quais certificados digitais podem ser usados para autenticar para o IBM MQ. Para obter informações adicionais, consulte:

- "Mapeando um Gerenciador de Filas Remoto para um ID do Usuário MCAUSER" na página 390
- "Mapeando um ID de usuário cliente para um ID do usuário MCAUSER" na página 391
- "Mapeando um Nome Distinto de SSL ou TLS para um ID do Usuário MCAUSER" na página 392

- “Mapeando um Endereço IP para um ID do Usuário MCAUSER” na página 394

Planejando a Autenticação para um Aplicativo Cliente

É possível aplicar controles de autenticação em quatro níveis: no nível de comunicações, em saídas de segurança, com registros de canal de autenticação, e em termos de identificação que é transmitida para uma saída de segurança.

Há quatro níveis de segurança a serem considerados. O diagrama mostra um IBM MQ MQI client que está conectado a um servidor. A segurança é aplicada em quatro níveis, conforme descrito no texto a seguir. MCA é um Agente do Canal de Mensagem.

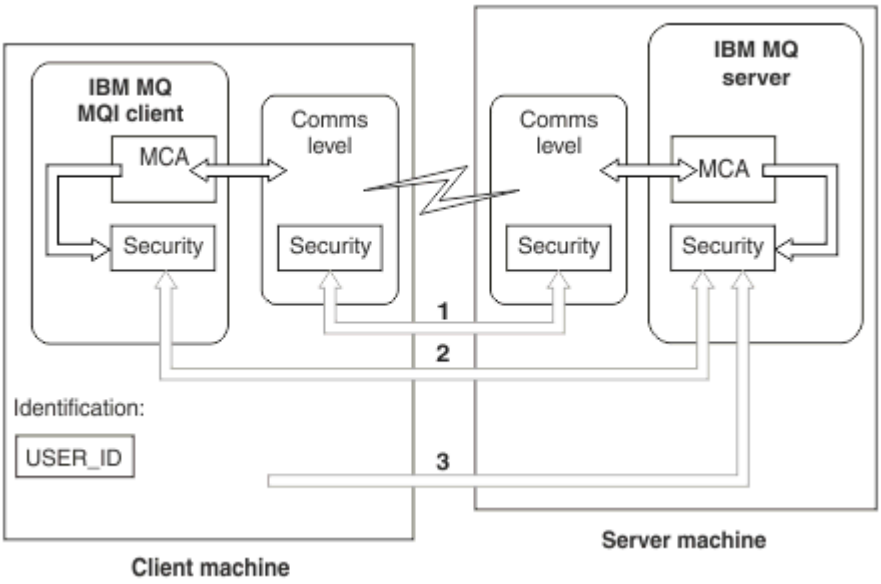


Figura 9. Segurança em uma Conexão de Cliente/Servidor

1. Nível de comunicações

   Veja a seta 1. Para implementar a segurança no nível de comunicações, use TLS. Para obter mais informações, consulte “Protocolos de segurança criptográficos: TLS” na página 15

2. Registros de Autenticação de Canal

   Ver as setas 2 e 3. A autenticação pode ser controlada com o uso do endereço IP ou nomes distintos TLS no nível de segurança. Um ID do usuário também pode ser bloqueado ou um ID do usuário declarado pode ser mapeado para um ID de usuário válido. Uma descrição completa é fornecida em “Registros de Autenticação de Canal” na página 49.

3. Autenticação de conexão

   Veja a seta 3. O cliente envia um ID e uma senha. Para obter informações adicionais, consulte “Autenticação de conexão: configuração” na página 68.

4. Saídas de Segurança do Canal

   Veja a seta 2. As saídas de segurança do canal para a comunicação do cliente para o servidor podem funcionar da mesma forma que para a comunicação do servidor para servidor. Um par de protocolos independentes de saída podem ser gravados para fornecer autenticação mútua entre o cliente e o servidor. Uma descrição completa é fornecida em Programas de saída de segurança de canal.

5. Identificação que é transmitida a uma saída de segurança do canal

   Veja a seta 3. Na comunicação do cliente para o servidor, as saídas de segurança do canal não têm que operar como um par. A saída no IBM MQ ao lado do cliente podem ser omitidos. Neste caso, o ID do usuário é colocado no descritor de canal (MQCD) e a saída de segurança do lado do servidor pode alterá-lo, se necessário.

Os clientes do Windows também enviam informações adicionais para ajudar na identificação.

- O ID do usuário que é transmitido ao servidor é o ID do usuário com login efetuado atualmente no cliente.
- O ID de segurança do usuário com logon efetuado atualmente.

Os valores do ID do usuário e, se disponível, o ID de segurança, podem ser usados por uma saída de segurança do servidor para estabelecer a identidade do IBM MQ MQI client.

No IBM MQ 8.0, é possível enviar senhas que são incluídas na estrutura do MQCSP.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas apropriadamente, consulte "Proteção de senha do MQCSP" na página 30.

IDs de Usuário

Quando você cria IDs de usuário para aplicativos clientes, os IDs de usuário não devem ser maiores que o comprimento máximo permitido. Não se deve usar os IDs de usuário reservados UNKNOWN e NOBODY. Se o servidor ao qual o cliente se conectar for um servidor IBM MQ for Windows, você deverá escapar o uso do sinal de arroba, @. O comprimento permitido de IDs de usuários é dependente da plataforma utilizada para o servidor:

- z/OS Linux UNIX No z/OS e UNIX and Linux, o comprimento máximo de um ID do usuário é 12 caracteres.
- IBM i No IBM i, o comprimento máximo de um ID do usuário é 10 caracteres.
- Windows No Windows, se o IBM MQ MQI client e o servidor IBM MQ estiverem ambos no Windows e o servidor tiver acesso ao domínio no qual o ID de usuário cliente está definido, o comprimento máximo de um ID do usuário será 20 caracteres. No entanto, se o servidor IBM MQ não for um servidor Windows, o ID do usuário será truncado para 12 caracteres.
- Se você usar a estrutura MQCSP para passar credenciais, o comprimento máximo de um ID do usuário será 1024 caracteres. O ID do usuário da estrutura MQCSP não pode ser usado para contornar o comprimento máximo de ID de usuário usado por IBM MQ para autorização. Para obter mais informações sobre a estrutura MQCSP, veja "Identificando e autenticando usuários usando a estrutura MQCSP" na página 337.

Em sistemas UNIX and Linux o padrão é que IDs de usuário são usados para autenticação, e grupos são usados para autorização. No entanto, é possível configurar esses sistemas para autorização com relação a IDs de usuário. Para obter mais informações, consulte "Permissões baseadas em usuário do OAM no UNIX and Linux" na página 355. Os sistemas Windows podem usar IDs de usuário para autenticação e autorização e grupos para autorização.

Se você criar contas de serviço, sem prestar atenção em grupos, e autorizar todos os IDs de usuário diferentes, cada usuário poderá acessar as informações dos outros usuários.

IDs de usuário restritos

Os IDs de usuário UNKNOWN e o grupo NOBODY têm significados especiais para IBM MQ. A criação de um ID de usuário no sistema operacional chamado UNKNOWN ou um grupo chamado NOBODY pode ter resultados indesejados.

IDs de usuário ao se conectar a um servidor IBM MQ for Windows

Windows

Um servidor IBM MQ for Windows não suporta a conexão de um cliente Windows se o cliente estiver em execução sob um ID do usuário que contém o caractere @, por exemplo, abc@d. O código de retorno para a chamada MQCONN no cliente é MQRC_NOT_AUTHORIZED.

No entanto, é possível especificar o ID do usuário usando dois caracteres @, por exemplo, `abc@@d`. Usar o formato `id@domain` é a prática preferencial para assegurar que o ID do usuário seja resolvido no domínio correto de forma consistente; portanto, `abc@@d@domain`.

Planejando a autorização

Planeje os usuários que terão autoridade administrativa e planeje como autorizar os usuários de aplicativos a usarem apropriadamente os objetos do IBM MQ, incluindo a conexão a partir de um IBM MQ MQI client.

Deve ser concedido acesso a indivíduos ou aplicações para usar o IBM MQ. O acesso que eles requerem depende das funções que eles realizam e das tarefas que eles precisam executar. A autorização no IBM MQ pode ser subdividida em duas categorias principais:

- Autorização para executar operações administrativas
- Autorização para aplicativos usarem o IBM MQ

As classes de operação são controladas pelo mesmo componente, e a um individual pode ser concedida a autoridade para executar ambas as categorias de operação.

Os tópicos a seguir fornecem informações adicionais sobre áreas específicas de autorização que deve ser consideradas:

Autoridade para administrar o IBM MQ

Os administradores do IBM MQ precisam de autoridade para executar várias funções. Essa autoridade é obtida de diferentes maneiras em diferentes plataformas.

Os administradores do IBM MQ precisam de autoridade para:

- Emitir comandos para administrar o IBM MQ.
- Windows Linux Use o IBM MQ Explorer.
- z/OS Usar os painéis de operações e de controle no z/OS.
- z/OS Usar o programa utilitário do IBM MQ, CSQUTIL, no z/OS.
- z/OS Acessar os conjuntos de dados do gerenciador de filas no z/OS.

Para obter mais informações, consulte o tópico apropriado para seu sistema operacional.

Windows UNIX *Autoridade para administrar o IBM MQ em sistemas UNIX e Windows*

Um administrador do IBM MQ é um membro do grupo mqm. Este grupo tem acesso a todos os recursos do IBM MQ e pode emitir comandos de controle do IBM MQ. Um administrador pode conceder autoridades específicas para outros usuários.

Para ser um administrador do IBM MQ no UNIX e Windows, um usuário deve ser membro do *grupo mqm*. Esse grupo é criado automaticamente quando você instala o IBM MQ. Para permitir que os usuários emitam comandos de controle, deve-se incluí-los no grupo mqm. Isso inclui o usuário raiz no UNIX.

Os usuários que não são membros do grupo mqm podem ser receber privilégios administrativos, mas eles não são capazes de emitir comandos de controle do IBM MQ e estão autorizados a executar apenas os comandos para os quais tiverem recebido acesso.

Além disso, em sistemas Windows , as contas SYSTEM e de Administrador têm acesso total aos recursos do IBM MQ

Todos os membros do grupo mqm têm acesso a todos os recursos do IBM MQ no sistema, incluindo ser capazes de administrar qualquer gerenciador de fila em execução no sistema. Esse acesso pode ser revogado somente com a remoção de um usuário do grupo mqm. Nos sistemas Windows, os membros do grupo de Administradores também têm acesso a todos os recursos do IBM MQ.

Os administradores podem usar o comando de controle **runmqsc** para emitir comandos IBM MQ Script (MQSC). Quando **runmqsc** é utilizado no modo indireto para enviar comandos MQSC para um gerenciador de fila remoto, cada comando será encapsulado dentro de um comando PCF Escape. Os administradores devem ter as autoridades requeridas para os comandos MQSC serem processados pelo gerenciador de fila remoto.

O IBM MQ Explorer emite comandos PCF (formato de comando programável) para executar tarefas de administração. Os administradores não requerem autoridades adicionais para usar o IBM MQ Explorer para administrar um gerenciador de filas no sistema local. Quando o IBM MQ Explorer é usado para administrar um gerenciador de filas em outro sistema, os administradores devem ter as autoridades necessárias para que os comandos PCF sejam processados pelo gerenciador de filas remoto.

Para obter mais informações sobre as verificações de autoridade efetuadas quando os comando de PCF e MQSC são processados, consulte os seguintes tópicos:

- Para comandos que operam em gerenciadores de filas, filas, canais, processos, listas de nomes e objetos de informações sobre autenticação, consulte “Autorização para aplicativos usarem o IBM MQ” na página 88.
- Para comandos que operam em canais, inicializadores de canais, listeners e clusters, consulte Segurança de canal.
- z/OS Para comandos MQSC que são processados pelo servidor de comando no IBM MQ for z/OS, consulte “Segurança do comando e segurança do recurso de comando no z/OS” na página 86.

Para obter mais informações sobre a autoridade que você precisa para administrar o IBM MQ nos sistemas UNIX e Windows, consulte as informações relacionadas.

IBM i *Autoridade para administrar o IBM MQ no IBM i*

Para ser um administrador do IBM MQ no IBM i, deve-se ser um membro do *grupo QMQMADM*. Este grupo tem propriedades semelhantes às do grupo mqm nos sistemas UNIX e Windows. Em particular, o grupo QMQMADM é criado ao se instalar o IBM MQ for IBM i, e os membros do grupo QMQMADM possuem acesso a todos os recursos do IBM MQ no sistema. Você também tem acesso a todos os recursos do IBM MQ se tiver a autoridade *ALLOBJ.

Os administradores podem usar comandos CL para administrar o IBM MQ.Um desses comandos de controle é GRTMQMAUT, que é utilizado para conceder autoridades a outros usuários. Outro comando, STRMQMMQSC, permite que um administrador emita comandos MQSC para um gerenciador de fila local.

Existem dois grupos do comando CL fornecidos pelo IBM MQ for IBM i:

Grupo 1
Para emitir um comando desta categoria, um usuário deve ser membro do grupo QMQMADM ou ter autoridade de *ALLOBJ. GRTMQMAUT e STRMQMMQSC pertencem a esta categoria, por exemplo.

Grupo 2
Para emitir um comando desta categoria, um usuário não precisa ser membro do grupo QMQMADM ou ter autoridade de *ALLOBJ. Em vez disso, são necessários dois níveis de autoridade:

- O usuário requer a autoridade do IBM i para usar o comando. Esta autoridade é concedida usando o comando GRTOBJAUT.
- O usuário requer a autoridade do IBM MQ para acessar qualquer objeto do IBM MQ associado ao comando. Esta autoridade é concedida usando o comando GRTMQMAUT.

Os exemplos a seguir mostram os comandos neste grupo:

- CRTMQMQ, Criar Fila do MQM
- CHGMQMPRC, Alterar Processo do MQM
- DLTMQMNL, Excluir Liste de Nomes do MQM
- DSPMQMAUTI, Exibir Informações de Autenticação do MQM
- CRTMQMCHL, Criar canal do MQM

Para obter mais informações sobre este grupo de comandos, consulte "Autorização para aplicativos usarem o IBM MQ" na página 88.

Para obter uma lista completa de comandos do grupo 1 e grupo 2, veja "Autoridades de acesso para objetos do IBM MQ no IBM i" na página 158

Para obter mais informações sobre a autoridade que você precisa para administrar o IBM MQ no IBM i, consulte Administrando o IBM i .

z/OS *Autoridade para administrar o IBM MQ no z/OS*

Esta coleção de tópicos descreve vários aspectos da autoridade necessária para administrar o IBM MQ for z/OS.

z/OS *Verificações de autoridade no z/OS*

O IBM MQ for z/OS usa o System Authorization Facility (SAF) para rotear solicitações de verificações de autoridade para um gerenciador de segurança externa (ESM) como o z/OS Security Server Resource Access Control Facility (RACF). O IBM MQ não faz autoverificações de autoridade.

Assume-se que você está usando o RACF como seu ESM. Se estiver usando um ESM diferente, pode ser necessário interpretar as informações fornecidas para o RACF de uma maneira que seja relevante para seu ESM.

É possível especificar se você deseja que as verificações de autoridade sejam ativadas ou desativadas para cada gerenciador de filas individualmente ou para cada gerenciador de filas em um grupo de filas compartilhadas.Este nível de controle chama-se *segurança do subsistema*. Se você desativar a segurança do subsistema de um determinado gerenciador de fila, nenhuma verificação de autoridade será realizada para esse gerenciador de fila.

Se você ativar a segurança do subsistema de um determinado gerenciador de fila, as verificações de autoridade poderão ser realizadas em dois níveis:

Segurança no nível do grupo de filas compartilhadas
As verificações de autoridade usam os perfis do RACF que são compartilhados por todos os gerenciadores de filas no grupo de filas compartilhadas. Isto significa que existem menos arquivos para definir e manter, tornando mais fácil a administração de segurança.

Segurança em Nível de Gerenciador de Fila
As verificações de autoridade usam perfis do RACF específicos para o gerenciador de filas.

É possível usar uma combinação de segurança no nível do grupo de filas compartilhadas e do gerenciador de filas. Por exemplo, é possível organizar perfis específicos para um gerenciador de filas para substituir os do grupo de filas compartilhadas ao qual ele pertence.

A segurança do subsistema, a segurança no nível do grupo de filas compartilhadas e a segurança no nível do gerenciador de filas são ativadas ou desativadas definindo *perfis do comutador*. Um perfil do comutador é um perfil normal do RACF que tem um significado especial para o IBM MQ.

z/OS *Segurança do comando e segurança do recurso de comando no z/OS*

A segurança de comando está relacionada à autoridade para emitir um comando; a autoridade do recurso de comando se refere à autoridade para executar uma operação em um recurso. Ambos são implementados usando classes do RACF.

As verificações de autoridade são realizadas quando um administrador do IBM MQ emite um comando de MQSC. Isso se chama *segurança do comando*.

Para implementar a segurança do comando, deve-se definir determinados perfis do RACF e conceder acesso aos IDs de grupos e usuários necessários nesses perfis nos níveis requeridos. O nome de um perfil de segurança do comando contém o nome de um comando MQSC.

Alguns comandos de MQSC executam uma operação em um recurso do IBM MQ, como o comando DEFINE QLOCAL para criar uma fila local. Quando um administrador emite um comando de MQSC, verificações de autoridade são realizadas para determinar se a operação solicitada pode ser executada no recurso especificado no comando. Isso é denominado *segurança de recurso do comando*.

Para implementar a segurança do recurso de comando, deve-se definir determinados perfis do RACF e conceder acesso aos IDs de grupos e usuários necessários nesses perfis nos níveis requeridos. O nome de um perfil de segurança do recurso de comando contém o nome de um recurso do IBM MQ e seu tipo (QUEUE, PROCESS, NAMELIST, TOPIC, AUTHINFO ou CHANNEL).

Segurança do comando e segurança de recurso do comando são independentes. Por exemplo, quando um administrador emite o comando:

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

são executadas as seguintes verificações de autoridade:

- A segurança do comando verifica se o administrador está autorizado a emitir o comando DEFINE QLOCAL.
- A segurança do recurso do comando verifica se o administrador está autorizado a executar uma operação na fila local denominada MOON.EUROPA.

A segurança do comando e a segurança de recurso do comando podem ser ativados ou desativados pela definição dos perfis de troca.

z/OS *Comandos MQSC e a fila de entrada de comando do sistema no z/OS*

Use este tópico para entender como o servidor de comandos processa os comandos MQSC direcionados à fila de entrada de comando do sistema no z/OS.

A segurança do comando e a segurança de recurso do comando também são utilizadas quando o servidor do comando recupera uma mensagem que contém um comando MQSC da fila de entrada de comandos do sistema.O ID do usuário utilizado para as verificações de autoridade é o encontrado no campo *UserIdentifier* , no descritor de mensagens da mensagem que contém o comando MQSC. Esse ID do usuário deve ter as autoridades requeridas no gerenciador de fila em que o comando é processado. Para obter mais informações sobre o campo *UserIdentifier* e como ele está definido, consulte Contexto da mensagem.

Mensagens que contêm comandos MQSC são enviadas à fila de entrada de comandos do sistema nas seguintes circunstâncias:

- Os painéis de operações e controle enviam comandos MQSC à fila de entrada de comandos do sistema do gerenciador de fila de destino. Os comandos MQSC correspondem às ações selecionadas nos painéis. O campo *UserIdentifier* de cada mensagem é definido no ID do usuário TSO do administrador.
- A função COMMAND do programa utilitário do IBM MQ, CSQUTIL, envia os comandos MQSC no conjunto de dados de entrada à fila de entrada de comandos do sistema do gerenciador de fila de destino. As funções COPY e EMPTY enviam comandos DISPLAY QUEUE e DISPLAY STGCLASS. O campo *UserIdentifier* de cada mensagem é definido com o ID do usuário do job.
- Os comandos MQSC nos conjuntos de dados CSQINPX são enviados à fila de entrada de comandos do sistema do gerenciador de fila ao qual o inicializador de canais está conectado. O campo *UserIdentifier* de cada mensagem é definido com o ID do usuário de espaço de endereçamento do inicializador de canais.

  Nenhuma verificação de autoridade é executada quando os comandos MQSC são emitidos a partir dos conjuntos de dados CSQINP1 e CSQINP2. É possível controlar quem tem permissão para atualizar esses conjuntos de dados usando a proteção do conjunto de dados do RACF.
- Dentro de um grupo de filas compartilhadas, um inicializador de canais pode enviar comandos START CHANNEL para a fila de entrada de comandos do sistema do gerenciador de filas ao qual ele está conectado. Um comando é enviado quando um canal de transmissão que utiliza uma fila de transmissão compartilhada é iniciada pelo disparo. O campo *UserIdentifier* de cada mensagem é definido com o ID do usuário de espaço de endereçamento do inicializador de canais.
- Um aplicativo pode enviar comandos MQSC a uma fila de entrada de comandos do sistema. Por padrão, o campo *UserIdentifier* de cada mensagem é definido como o ID do usuário associado ao aplicativo.
- Nos sistemas UNIX, Linux, and Windows, o comando de controle **runmqsc** pode ser usado no modo indireto para enviar comandos MQSC à fila de entrada de comando do sistema de um gerenciador

de filas no z/OS. O campo *UserIdentifier* de cada mensagem é definido com o ID do usuário do administrador que emitiu o comando **runmqsc**.

z/OS *Acesso aos conjuntos de dados do gerenciador de filas no z/OS*

Os administradores do IBM MQ for z/OS necessitam de autoridade para acessar os conjuntos de dados do gerenciador de filas. Use este tópico para entender quais conjuntos de dados precisam de proteção do RACF.

Esses conjuntos incluem:

- V 9.1.0 Os conjuntos de dados referidos por CSQINP1, CSQINP2 e CSQINPT no procedimento de tarefa iniciada do gerenciador de filas.
- Os conjuntos de páginas do gerenciador de fila, os conjuntos de dados dos logs ativos, os conjuntos de dados de log do arquivo e BSDS (Bootstrap Data Sets)
- Os conjuntos de dados referidos por CSQXLIB e CSQINPX no procedimento de tarefa iniciado do inicializador de canais

Você deve proteger os conjuntos de dados para que nenhum usuário sem autorização consiga iniciar um gerenciador de fila ou receba acesso a nenhum dado do gerenciador de fila. Para fazer isso, use a proteção do conjunto de dados do RACF.

Autorização para aplicativos usarem o IBM MQ

Quando os aplicativos acessam objetos, os IDs de usuário associados aos aplicativos precisam de autoridade apropriada.

Os aplicativos podem acessar os seguintes objetos do IBM MQ, emitindo chamadas de MQI:

- Gerenciadores de filas
- Filas
- Processos
- Listas de Nomes
- tópicos

Os aplicativos também podem usar comando de PCF para administrar objetos do IBM MQ. Quando o comando PCF é processado, ele usa o contexto de autoridade do ID do usuário que envia a mensagem de PCF.

Os aplicativos, neste contexto, incluem os gravados pelos usuários e fornecedores e os fornecidos com o IBM MQ for z/OS. Os aplicativos fornecidos com o IBM MQ for z/OS incluem:

- Os painéis de operações e controle
- O programa utilitário IBM MQ, CSQUTIL
- O utilitário CSQUDLQH (Dead Letter Queue Handler)

Os aplicativos que usam IBM MQ classes for Java, IBM MQ classes for JMS, IBM MQ classes for .NET ou o Message Service Clients for C/C++ e .NET usam o MQI indiretamente.

Os MCAs também emitem chamadas de MQI e os IDs do usuário associados a MCAs necessitam de autoridade para acessar esses objetos do IBM MQ. Para obter mais informações sobre esses IDs do usuário e as autoridades que eles requerem, consulte a seção “Autorização de canal” na página 110.

No z/OS, os aplicativos também podem usar comandos MQSC para acessar esses objetos do IBM MQ, porém, a segurança do comando e a segurança do recurso do comando fornecem as verificações de autoridade nesses casos. z/OS Para obter mais informações, consulte “Segurança do comando e segurança do recurso de comando no z/OS” na página 86 e “Comandos MQSC e a fila de entrada de comando do sistema no z/OS” na página 87.

No IBM i, um usuário que emite um comando CL no Grupo 2 pode requerer de autoridade para acessar um objeto do IBM MQ associado ao comando. Para obter mais informações, consulte “Quando as Verificações de Autoridade são Executadas” na página 89.

Quando as Verificações de Autoridade são Executadas

As verificações de autoridade são executadas quando um aplicativo tenta acessar um gerenciador de filas, uma fila, um processo ou uma lista de nomes.

No IBM i, as verificações de autoridade também podem ser realizadas quando um usuário emite um comando CL no Grupo 2 que acessa qualquer um destes objetos do IBM MQ. As verificações são executadas nas seguintes situações:

Quando um aplicativo estabelece conexão com um gerenciador de fila usando uma chamada MQCONN ou MQCONNX

O gerenciador de fila solicita o sistema operacional do ID do usuário associado ao aplicativo. Então, verifica se o ID do usuário tem autorização para estabelecer conexão com ele e o retém para verificações futuras.

Os usuários não têm que efetuar sign on para o IBM MQ. O IBM MQ assume que os usuários estão conectados ao sistema operacional subjacente e que foram autenticados por ele.

Quando um aplicativo abre um objeto do IBM MQ usando uma chamada MQOPEN ou MQPUT1

Todas as verificações de autoridade são executadas quando um objeto é aberto, não ao ser acessado posteriormente. Por exemplo, as verificações de autoridade são executadas quando um aplicativo abre uma fila. Elas não são executadas quando o aplicativo coloca mensagens na fila ou recebe mensagens da fila.

Quando um aplicativo abre um objeto, ele especifica os tipos de operação de que necessita executar nele. Por exemplo, um aplicativo pode abrir uma fila para consultar e obter mensagens, mas não para colocar mensagens nela. Para cada tipo de operação, o gerenciador de fila verifica se o ID do usuário associado ao aplicativo tem a autoridade para executar essa operação.

Quando um aplicativo abre uma fila, as verificações de autoridade são executadas no objeto nomeado no campo `ObjectName` do descritor de objeto. O campo `ObjectName` é usado nas chamadas `MQOPEN` ou `MQPUT1`. Se o objeto for uma fila de alias ou uma definição de fila remota, as verificações de autoridade serão executadas no próprio objeto. Elas não são executadas na fila para a qual a fila de alias ou a definição de fila remota é resolvida. Isso significa que o usuário não precisa de permissão para acessá-la. Limite a autoridade para criar filas a usuários privilegiados. Se você não fizer isto, os usuários podem efetuar bypass do controle de acesso normal simplesmente criando um alias.

Um aplicativo pode referenciar uma fila remota explicitamente. Ele configura os campos `ObjectName` e `ObjectQMgrName` no descritor de objetos para os nomes da fila remota e o gerenciador de filas remotas. As verificações de autoridade serão executadas na fila de transmissão com o mesmo nome que o gerenciador de filas remotas. No z/OS, uma verificação é feita no perfil de fila do RACF que corresponde ao nome do gerenciador de filas remotas. No Multiplataformas, uma verificação é feita com relação ao perfil RQMNAME que corresponde ao nome do gerenciador de filas remotas, se o armazenamento em cluster estiver sendo usado. Um aplicativo pode fazer referência a uma fila de clusters explicitamente, configurando o campo `ObjectName` no descritor de objeto com o nome da fila de clusters. As verificações de autoridade são executadas na fila de transmissão do cluster, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

A autoridade para uma fila dinâmica é baseada na fila modelo da qual se deriva, mas não é necessariamente a mesma; consulte nota 1.

O ID do usuário que o Gerenciador de Filas utiliza para as verificações de autoridade é obtido do sistema operacional. O ID do usuário é obtido quando o aplicativo estabelece conexão com o gerenciador de filas. Um aplicativo adequadamente autorizado pode emitir uma chamada `MQOPEN` especificando um ID do usuário alternativo; as verificações de controle de acesso são então feitas no ID do usuário alternativo. Usar um ID de usuário alternativo não muda o ID de usuário associado ao aplicativo, apenas o ID que é usado para verificações de controle de acesso.

Quando um aplicativo é subscrito para um tópico usando uma chamada MQSUB

Quando um aplicativo é subscrito para um tópico, ele especifica o tipo de operação que precisa executar. Ele estará criando uma assinatura, alterando uma assinatura existente ou continuando uma assinatura existente sem mudá-la. Para cada tipo de operação, o gerenciador de filas verifica se o ID do usuário que está associado ao aplicativo possui a autoridade para executar a operação.

Quando um aplicativo é subscrito para um tópico, as verificações de autoridade são executadas com relação a objetos de tópicos que estão localizados na árvore de tópicos. Os objetos do tópico estão em, ou acima do ponto na árvore de tópicos na qual o aplicativo foi inscrito. As verificações de autoridade podem envolver verificações em mais de um objeto de tópico. O ID do usuário que o Gerenciador de Filas utiliza para as verificações de autoridade é obtido do sistema operacional. O ID do usuário é obtido quando o aplicativo estabelece conexão com o gerenciador de filas.

O gerenciador de filas executa verificações de autoridade em filas de assinantes, mas não em filas gerenciadas.

Quando um aplicativo exclui uma fila dinâmica permanente usando uma chamada MQCLOSE

A manipulação de objetos especificada na chamada MQCLOSE não é necessariamente a mesma retornada pela chamada MQOPEN que criou a fila dinâmica permanente. Se for diferente, o gerenciador de filas verifica o ID do usuário associado ao aplicativo que emitiu a chamada MQCLOSE. Ele verifica se o ID de usuário tem autorização para excluir a fila.

Quando um aplicativo que fecha uma assinatura para removê-la não a criou, a autoridade apropriada é requerida para removê-la.

Quando um comando PCF que opera em um objeto do IBM MQ é processado pelo servidor de comandos

Essa regra inclui o caso em que um comando PCF opera em um objeto de informações sobre autenticação.

O ID do usuário utilizado para as verificações de autoridade é o encontrado no campo UserIdentifier , no descritor de mensagens do comando PCF. Esse ID do usuário deve ter as autoridades requeridas no gerenciador de fila em que o comando é processado. O comando MQSC equivalente encapsulado dentro de um comando PCF Escape é tratado da mesma forma. Para obter mais informações sobre o campo UserIdentifier e como ele está definido, consulte “Contexto da mensagem” na página 91.

IBM i **No IBM i, quando um usuário emite um comando CL no Grupo 2 que opera em um objeto do IBM MQ**

Essa regra inclui o caso em que um comando CL no Grupo 2 opera em um objeto de informações sobre autenticação.

As verificações são feitas para determinar se o usuário tem a autoridade para operar em um objeto do IBM MQ associado ao comando. As verificações são executadas, a menos que o usuário seja um membro do grupo QMQMADM ou tenha autoridade *ALLOBJ. A autoridade necessária depende do tipo de operação que o comando realiza sobre o objeto. Por exemplo, o comando **CHGMQMQ**, Change MQM Queue, requer autoridade para mudar atributos da fila especificada pelo comando. Em contraste, o comando **DSPMQMQ**, Display MQM Queue, requer a autoridade de exibir os atributos da fila especificada pelo comando.

Muitos comandos operam sobre mais de um objeto. Por exemplo, para emitir o comando **DLTMQMQ**, Delete MQM Queue, as seguintes autoridades são necessárias:

- A autoridade de conectar ao gerenciador de filas especificado pelo comando
- A autoridade de excluir a fila especificada pelo comando

Alguns comandos não operam sobre objeto algum. Neste caso, o usuário requer somente a autoridade do IBM i para emitir um desses comandos. **STRMQMLSR**, Start MQM Listener, é um exemplo de tal comando.

Alternar autoridade do usuário

Quando um aplicativo abre um objeto ou assina um tópico, o aplicativo pode fornecer um ID de usuário na chamada MQOPEN, MQPUT1 ou MQSUB. Ele pode solicitar ao gerenciador de filas para usar esse ID de usuário para verificações de autoridade, em vez daquele associado ao aplicativo.

O aplicativo será bem-sucedido ao abrir o objeto somente se as duas condições a seguir forem atendidas:

- O ID do usuário associado ao aplicativo tem autoridade para fornecer um ID de usuário diferente para verificações de autoridade. Diz-se que o aplicativo tem *autoridade de usuário alternativo*.
- O ID do usuário fornecido pelo aplicativo possui a autoridade para abrir o objeto para os tipos de operações solicitadas ou para assinar o tópico.

Contexto da mensagem

As informações sobre *contexto da mensagem* permitem que o aplicativo que recupera uma mensagem descubra o emissor dela. As informações ficam retidas em campos no descritor de mensagens e os campos são divididos em três partes lógicas

Essas partes são as seguintes:

contexto de identidade
Estes campos contêm informações sobre o usuário do aplicativo que colocou a mensagem na fila.

contexto de origem
Estes campos contêm informações sobre o aplicativo em si e quando foi que a mensagem foi colocada na fila.

contexto do usuário
Estes campos contêm propriedades de mensagens que os aplicativos utilizam para selecionar as mensagens que o gerenciador de filas deve entregar.

Quando um aplicativo coloca uma mensagem em uma fila, pode solicitar que o gerenciador de fila gere as informações de contexto na mensagem. Esta é a ação padrão. Alternativamente, ele pode especificar que os campos de contexto não contenham informações. O ID do usuário associado a um aplicativo não requer autoridade especial para nenhum desses.

Um aplicativo pode definir os campos de contexto de identidade em uma mensagem, permitindo que o gerenciador de fila gere o contexto de origem ou pode definir todos os campos de contexto. Pode também passar os campos de contexto de identidade de uma mensagem recuperada para uma mensagem que esteja colocando na fila ou passar todos os campos de contexto. Porém, o ID do usuário associado a um aplicativo requer autoridade para definir ou passar as informações de contexto. Um aplicativo especifica se pretende definir ou passar informações de contexto quando abrir a fila na qual está para colocar mensagens e sua autoridade é verificada nesse momento.

A seguir, uma descrição breve de cada campo de contexto:

Contexto de Identidade

UserIdentifier
O ID do usuário associado ao aplicativo que colocou a mensagem. Se o gerenciador de fila definir este campo, ele será definido com o ID obtido do sistema operacional de quando o aplicativo estabelece conexão com o gerenciador de fila.

AccountingToken
As informações podem ser utilizadas para cobrar o trabalho feito como resultado da mensagem.

ApplIdentityData
Se o ID do usuário associado ao aplicativo tiver autoridade para definir os campos de contexto de identidade ou todos os campos de contexto, o aplicativo poderá definir esse campo com qualquer valor relacionado à identidade. Se o gerenciador de fila definir esse campo, será deixado em branco.

Contexto de origem

PutApplType
O tipo do aplicativo que coloca a mensagem; uma transação do CICS, por exemplo.

PutApplName
O nome do aplicativo que coloca a mensagem.

PutDate
A data em que a mensagem foi colocada.

PutTime
A hora em que a mensagem foi colocada.

ApplOriginData
Se o ID do usuário associado ao aplicativo tiver autoridade para definir todos os campos de contexto, o aplicativo poderá definir esse campo com qualquer valor relacionado à origem. Se o gerenciador de fila definir esse campo, será deixado em branco.

Contexto de Usuário

Os seguintes valores são suportados para **MQINQMP** ou **MQSETMP**:

MQPD_USER _CONTEXT

A propriedade é associada com o contexto do usuário.

Não é necessária nenhuma autorização especial para poder definir uma propriedade associada ao contexto do usuário utilizando a chamada MQSETMP.

Em um gerenciador de filas V7.0 ou subsequente, uma propriedade associada ao contexto de usuário é salva conforme descrito para MQOO_SAVE_ALL_CONTEXT. Um MQPUT com MQOO_PASS_ALL_CONTEXT especificado faz com que a propriedade seja copiada do contexto salvo para a nova mensagem.

MQPD_NO_CONTEXT

A propriedade não é associada com um contexto de mensagem.

Um valor não reconhecido é rejeitado com um MQRC_PD_ERROR. O valor inicial deste campo é **MQPD_NO_CONTEXT**.

Para obter uma descrição detalhada de cada um dos campos de contexto, consulte MQMD - Descritor de mensagens. Para obter mais informações sobre como usar o contexto da mensagem, consulte Contexto da Mensagem.

ULW IBM i *Autoridade para trabalhar com objetos do IBM MQ em sistemas* IBM i *IBM i, UNIX, Linux, and Windows*

O componente de serviço de autorização fornecido com o IBM MQ é chamado de *gerenciador de autoridade de objeto* (OAM). Ele fornece controle de acesso por meio de verificações de autenticação e autorização.

Autenticação.
A verificação de autenticação executada pelo OAM fornecido com o IBM MQ é básico, e é executada apenas em circunstâncias específicas. Seu objetivo não é atender aos requisitos rígidos esperados em um ambiente altamente seguro.

O OAM realiza sua verificação de autenticação quando um aplicativo se conecta a um Gerenciador de Filas e as condições a seguir são verdadeiras:

- Se uma estrutura MQCSP tiver sido fornecida pelo aplicativo de conexão, e
- Ao atributo *AuthenticationType* na estrutura MQCSP é dado o valor MQCSP_AUTH_USER_ID_AND_AND_PWD, e
- O valor CHCKLOCL ou CHKCCLNT no objeto AUTHINFO configurado não é 'NONE'

As etapas de autenticação no OAM validam a senha usando os serviços do sistema operacional, que podem ter sido configurados para realizar verificações adicionais, como garantir que o nome de usuário não tenha tido muitas tentativas incorretas de teste de senha.

É possível que mecanismos de autenticação alternativos sejam usados se você escrever um novo componente de serviço de autorização ou obtiver um de um fornecedor.

Autorização.

As verificações de autorização são abrangentes e seu objetivo é atender a requisitos mais normais.

As verificações de autorização são executadas quando um aplicativo emite uma chamada MQI para acessar um gerenciador de filas, uma fila, um processo, um tópico ou uma lista de nomes. Elas também são executadas em outros momentos, por exemplo, quando um comando está sendo executado pelo Servidor de Comandos.

Em sistemas IBM i IBM i, UNIX, Linux, and Windows, o *serviço de autorização* fornecerá o controle de acesso quando um aplicativo emitir uma chamada MQI para acessar um objeto do IBM MQ que seja um gerenciador de filas, uma fila, um processo, um tópico ou uma lista de nomes. Isso inclui verificações da autoridade do usuário alternativo e a autoridade para definir ou passar informações de contexto.

Windows No Windows, o OAM fornece aos membros do grupo de Administradores a autoridade para acessar todos os objetos do IBM MQ, mesmo quando o UAC está ativado. Além disso, em sistemas Windows , a conta SYSTEM tem acesso total aos recursos do IBM MQ

O serviço de autorização também fornece verificações de autoridade quando um comando de PCF opera em um desses objetos do IBM MQ ou em um objeto de informações sobre autenticação. O comando MQSC equivalente encapsulado dentro de um comando PCF Escape é tratado da mesma forma.

IBM i No IBM i, a menos que o usuário seja um membro do grupo QMQMADM ou tenha autoridade *ALLOBJ, o serviço de autorização também fornece verificações de autoridade quando um usuário emite um comando CL no Grupo 2 que opera sobre qualquer um destes objetos do IBM MQ ou um objeto de informações sobre autenticação.

O serviço de autorização é um *serviço instalável* , que significa que é implementado por um ou mais *componentes de serviços instaláveis*. Cada componente é chamado por uma interface documentada. Isto permite que usuários e fornecedores forneçam componentes para aumentar ou substituir os fornecidos pelos produtos IBM MQ.

O componente de serviço de autorização fornecido com o IBM MQ é chamado de gerenciador de autoridade de objeto (OAM). O OAM é ativado automaticamente para cada gerenciador de fila criado.

O OAM mantém uma lista de controle de acesso (ACL) para cada objeto do IBM MQ para o qual ele está controlando o acesso. Em sistemas UNIX and Linux, somente IDs de grupos podem aparecer em uma ACL. Isto significa que todos os membros de um grupo possuem as mesmas autoridades. Em sistemas IBM i IBM i e Windows, os IDs do usuário e os IDs do grupo podem aparecer em uma ACL. Isto significa as autoridades podem ser concedidas para usuários individuais e grupos.

Uma limitação de 12 caracteres aplica-se ao grupo e ao ID do usuário. As plataformas UNIX geralmente restringem o comprimento de um ID do usuário a 12 caracteres. O AIX e o Linux emitiam esse limite, mas IBM MQ continua a observar uma restrição de 12 caracteres em todas as plataformas UNIX. Se você usar um ID do usuário com mais de 12 caracteres, o IBM MQ substitui-o com o valor de "UNKNOWN". Não defina um ID do usuário com um valor de "UNKNOWN".

O OAM pode autenticar um usuário e alterar os campos de contexto de identidade adequados. Você ativa isto especificando uma estrutura MQCSP (connection security parameters) em uma chamada MQCONNX. A estrutura é passada para a função de Autenticar Usuário OAM (MQZ_AUTHENTICATE_USER), que define campos de contexto de identidade adequados. Se uma conexão do MQCONNX a partir de um cliente IBM MQ, as informações no MQCSP são fluídas para o gerenciador de filas ao qual o cliente está se conectando através do canal de conexão do cliente e de conexão do servidor. Se as saídas de segurança estiverem definidas neste canal, a MQCSP é passada para cada saída de segurança e pode ser alterada pela saída. As saídas de segurança também podem criar a MQCSP. Para obter mais detalhes do uso das saídas de segurança neste contexto, consulte Programas de saída de segurança do canal.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas adequadamente, consulte IBM MQProteção de senha CSP.

Nos sistemas UNIX, Linux e Windows, o comando de controle **setmqaut** concede ou revoga autoridades e é usado para manter as ACLs. Por exemplo, o comando:

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

permite que membros do grupo VOYAGER procurem mensagens na fila MOON.EUROPA que é de propriedade do gerenciador de fila JUPITER. Permite também que os membros obtenham mensagens da fila. Para revogar estas autoridades posteriormente, insira o seguinte comando:

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

O comando:

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

permite que membros do grupo VOYAGER coloquem mensagens em qualquer fila com um nome que comece com os caracteres MOON.. MOON.* é o nome de um perfil genérico..Um *perfil genérico* permite conceder autoridades para um conjunto de objetos usando um único comando **setmqaut** .

O comando de controle **dspmqaut** está disponível para exibir as autoridades atuais que um usuário ou um grupo tem para um objeto especificado.O comando de controle **dmpmqaut** também está disponível para exibir as autoridades atuais associadas aos perfis genéricos.

IBM i No IBM i, um administrador usa o comando CL GRTMQMAUT para conceder autoridades e o comando CL RVKMQMAUT para revogar autoridades. Perfis genéricos também podem ser utilizados.Por exemplo, o comando CL:

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

fornece a mesma função que o exemplo anterior de um comando **setmqaut**. Ele permite que os membros do grupo VOYAGER coloquem mensagens em qualquer fila com um nome que inicia com os caracteres MOON.

IBM i O comando CL DSPMQMAUT exibe as autoridades atuais que o usuário ou grupo tem para um determinado objeto. Os comandos CL WRKMQMAUT e WRKMQMAUTD também estão disponíveis para trabalhar com as autoridades atualmente associadas a objetos e perfis genéricos.

Se você não desejar nenhuma verificação de autoridade, por exemplo, em um ambiente de teste, poderá desativar o OAM.

Multi *Usando PCF para acessar comandos OAM*

Nos sistemas IBM i, UNIX, Linux, and Windows, é possível usar comandos PCF para acessar comandos de administração OAM.

Os comando de PCF e seus comandos OAM equivalentes são os seguintes:

Tabela 8. Comandos PCF e seus comandos OAM equivalentes

comando PCF	**Comando OAM**
Consultar Registros de Autoridade	dmpmqaut
Solicitar Autoridade de Entidade	dspmqaut
Configurar Registro de Autoridade	setmqaut
Excluir Registro de Autoridade	setmqaut com opção -remove

Os comandos **setmqaut** e **dmpmqaut** são restritos a membros do grupo mqm. Os comandos de PCF equivalentes podem ser executados por usuários em qualquer grupo que tenha recebido as autoridades dsp e chg no gerenciador de filas.

Para obter mais informações sobre como usar esses comandos, consulte Introdução aos formatos de comando programável.

z/OS *Autoridade para trabalhar com objetos do IBM MQ no z/OS*

No z/OS, há sete categorias de verificação de autoridade associadas às chamadas para o MQI. Deve-se definir determinados perfis do RACF e conceder acesso apropriado a esses perfis. Use o perfil *RESLEVEL* para controlar quantos IDs de usuário são verificados.

As sete categorias de verificação de autoridade associadas às chamadas para MQI:

Segurança de Conexão
As verificações de autoridade que são executadas quando um aplicativo estabelece conexão com um gerenciador de fila.

Segurança da fila
As verificações de autoridade que são executadas quando um aplicativo abre uma fila ou exclui uma fila dinâmica permanente.

Segurança do processo
As verificações de autoridade que são executadas quando um aplicativo abre um objeto do processo.

Segurança da lista de nomes
As verificações de autoridade que são executadas quando um aplicativo abre um objeto da lista de nomes.

Segurança de usuário alternativo
As verificações de autoridade que são executadas quando um aplicativo solicita uma autoridade de usuário alternativo ao abrir um objeto.

Segurança de contexto
As verificações de autoridade que são executadas quando um aplicativo abre uma fila e especifica se pretende definir ou passar as informações de contexto nas mensagens que coloca na fila.

Segurança do tópico
As verificações de autoridade que são executadas quando um aplicativo abre um tópico

Cada categoria de verificação de autoridade é implementada da mesma forma que a segurança do comando e a segurança de recurso do comando. Deve-se definir determinados perfis do RACF e conceder acesso aos IDs de grupos e usuários necessários nesses perfis nos níveis requeridos. Para a segurança da fila, o nível de acesso determina os tipos de operação que o aplicativo pode executar em uma fila. Para segurança do contexto, o nível de acesso determina se o aplicativo pode:

- Passar todos os campos de contexto;
- Passar todos os campos de contexto e definir os campos de contexto da identidade;
- Passar e definir todos os campos de contexto.

Cada categoria de verificação de autoridade pode ser ativada ou desativada pela definição dos perfis de troca.

Todas as categorias, exceto a segurança de conexão, são conhecidas coletivamente como *Segurança de Recurso da API*.

Por padrão, quando uma verificação de segurança de recurso da API é executada como resultado de uma chamada MQI de um aplicativo, que utiliza uma conexão em batch, somente um ID do usuário é verificado. Quando uma verificação é executada como resultado de uma chamada MQI a partir de um aplicativo CICS ou IMS ou a partir do inicializador de canais, dois IDs de usuário serão verificados.

Contudo, com a definição de um *perfil RESLEVEL*, é possível controlar se serão verificados, zero, um ou dois IDs de usuários. O número de IDs do usuário verificado é determinado pelo ID do usuário associado ao tipo de conexão quando um aplicativo estabelece conexão com o gerenciador de fila e pelo nível de acesso que o ID tem ao perfil RESLEVEL. O ID associado a cada tipo de conexão é:

- O ID do usuário da tarefa conectada para conexões em batch;
- O ID do usuário do espaço de endereço do CICS para conexões do CICS
- O ID do usuário do espaço de endereço da região do IMS para conexões do IMS
- O ID do usuário do espaço de endereçamento do iniciador do canal das conexões do iniciador do canal.

Para obter mais informações sobre a autoridade para trabalhar com objetos do IBM MQ no z/OS, consulte “Autoridade para administrar o IBM MQ no z/OS” na página 86.

Segurança para o Sistema de Mensagens Remoto

Esta seção trata dos aspectos do sistema de mensagens remoto de segurança.

Você deve fornecer aos usuários a autoridade para usar os recursos do IBM MQ. Isto está organizado de acordo com as ações a serem obtidas em relação aos objetos e definições. Por exemplo:

- Os gerenciadores de fila podem ser iniciados ou parados por usuários autorizados
- Os aplicativos devem se conectar ao gerenciador de filas e ter autoridade para usar as filas
- Os canais de mensagens devem ser criados e controlados pelos usuários autorizados
- Os objetos são mantidos nas bibliotecas e o acesso a essas bibliotecas pode estar restrito

O agente do canal de mensagem em um site remoto deve verificar se a mensagem está sendo entregue originada de um usuário com autoridade para tal neste site remoto. Além disso, como os MCAs podem ser iniciados remotamente, pode ser necessário verificar se os processos remotos que tentam iniciar os seus MCAs estão autorizados a fazê-lo. Existem quatro maneira possíveis para tratar disso:

1. Fazer uso apropriado do atributo PutAuthority da sua definição de canal RCVR, RQSTR ou CLUSRCVR para controlar qual usuário é usado para as verificações de autorização no momento em que as mensagens recebidas são colocadas nas suas filas. Consulte a descrição do comando DEFINE CHANNEL na Referência de Comandos MQSC.
2. Implemente os registros de autenticação de canal para rejeitar as tentativas de conexão indesejadas ou para configurar um valor MCAUSER com base no seguinte: endereço IP remoto, ID do usuário remoto, Nome Distinto (DN) do assunto TLS fornecido ou nome do gerenciador de filas remotas.
3. Implemente a verificação de segurança de *saída de usuário* verificando se o canal de mensagem correspondente está autorizado. A segurança da instalação que hospeda o canal correspondente assegura que todos os usuários estejam corretamente autorizados, de modo que você não precise verificar as mensagens individuais.
4. Implemente o processamento de mensagens de *saída de usuário* para assegurar que as mensagens individuais sejam examinadas para autorização.

IBM i *Segurança de objetos do IBM MQ for IBM i*

Esta seção trata dos aspectos do sistema de mensagens remoto de segurança.

Deve-se fornecer aos usuários a autoridade para usar os recursos do IBM MQ for IBM i. Esta autoridade é organizada de acordo com as ações a serem obtidas em relação aos objetos e definições. Por exemplo:

- Os gerenciadores de fila podem ser iniciados ou parados por usuários autorizados
- Os aplicativos precisam se conectar ao gerenciador de filas, e ter autoridade para fazer uso de filas
- Os canais de mensagens precisam ser criados e controlados pelos usuários autorizados

O agente do canal de mensagens em um site remoto deve verificar se a mensagem que está sendo entregue é derivada de um usuário com autoridade para emitir mensagem neste site remoto. Além disso, como os MCAs podem ser iniciados remotamente, pode ser necessário verificar se os processos remotos que tentam iniciar os seus MCAs estão autorizados a fazê-lo. Existem quatro maneira possíveis para tratar disso:

- Decrete na definição de canal que as mensagens devem conter autoridade *context* aceitável, caso contrário, elas serão descartadas.

- Implemente os registros de autenticação de canal para rejeitar as tentativas de conexão indesejadas ou para configurar um valor MCAUSER com base no seguinte: endereço IP remoto, ID do usuário remoto, Nome Distinto (DN) do TLS ou nome do gerenciador de filas remotas.
- Implemente a verificação de segurança de saída de usuário para assegurar que o canal de mensagens correspondente está autorizado. A segurança da instalação que hospeda o canal correspondente assegura que todos os usuários estejam corretamente autorizados, de modo que você não precise verificar as mensagens individuais.
- Implemente o processamento de mensagens de saída de usuário para assegurar que as mensagens individuais sejam examinadas para autorização.

Aqui estão alguns fatos sobre a maneira como o IBM MQ for IBM i opera em relação à segurança:

- Os usuários são identificados e autenticados pelo IBM i.
- Os serviços do gerenciador de filas, chamados pelos aplicativos, são executados com a autoridade do perfil do usuário do gerenciador de filas, mas no processo do usuário.
- Os serviços do gerenciador de serviços, chamados por comandos do usuário, são executados com a autoridade do perfil do usuário do gerenciador de filas.

Linux UNIX *Segurança de objetos no UNIX and Linux*

Os usuários de Administração devem ser parte do grupo mqm em seu sistema (incluindo raiz), se este ID usar os comandos de administração do IBM MQ.

É necessário sempre executar amqcrsta como o ID do usuário "mqm".

IDs do Usuário no UNIX and Linux

O gerenciador de filas converte todos os identificadores com letras maiúsculas ou com letras maiúsculas e minúsculas em identificadores com letras minúsculas. O gerenciador de filas, então, insere os identificadores de usuário no contexto da parte de uma mensagem, ou verifica sua autorização. As autorizações são, portanto, baseadas apenas em identificadores com letras minúsculas.

Windows *A segurança de objetos em sistemas Windows*

Os usuários de Administração devem ser parte do grupo mqm e do grupo de administradores nos sistemas Windows se este ID usar os comandos de administração do IBM MQ.

Os IDs do usuário nos sistemas Windows

Em sistemas Windows, *se não houver saída de mensagem instalada*, o gerenciador de filas converte qualquer identificador de usuário com letras maiúsculas ou com letras maiúsculas e minúsculas em identificadores com letras minúsculas. O gerenciador de filas, então, insere os identificadores de usuário no contexto da parte de uma mensagem, ou verifica sua autorização. As autorizações são, portanto, baseadas apenas em identificadores com letras minúsculas.

IDs do usuário em sistemas

Plataformas diferentes dos sistemas Windows, UNIX and Linux usam caracteres maiúsculos para IDs de usuário em mensagens. Para permitir que os sistemas Windows, UNIX and Linux usem IDs do usuário em minúsculas em mensagens, o agente do canal de mensagens (MCA) deve executar as conversões apropriadas de caracteres alfabéticos.

Para permitir que os sistemas Windows, UNIX and Linux usem IDs de usuário com letras minúsculas em mensagens, as seguintes conversões são realizadas pelo agente do canal de mensagens (MCA) nestas plataformas:

Na extremidade de envio

Os caracteres alfabéticos em todos os IDs do usuário são convertidos em caracteres maiúsculos, se não houver nenhuma saída de mensagem instalada.

Na extremidade de recebimento
Os caracteres alfabéticos em todos os IDs de usuário são convertidos em caracteres minúsculos, se nenhuma saída de mensagem instalada.

As conversões automáticas não serão realizadas se você fornecer uma saída de mensagem no UNIX, Linux, and Windows por qualquer outra razão.

Usando um serviço de autorização customizado

O IBM MQ fornece um serviço de autorização instalável. É possível escolher instalar um serviço alternativo.

O componente de serviço de autorização fornecido com o IBM MQ é chamado Gerenciador de Autoridade de Objeto (OAM). Se o OAM não fornecer as instalações de autorização necessárias, será possível gravar seu próprio componente de serviço de autorização. As funções do serviço instalável, que deve ser implementado por um componente de serviço de autorização, são descritas em Informações de referência da interface de serviços instaláveis.

Controle de acesso para clientes

O controle de acesso é baseado nos IDs de usuário. Pode haver muitos IDs de usuário para administrar, e os IDs de usuário podem estar em diferentes formatos. É possível configurar a propriedade MCAUSER do canal de conexão do servidor com um valor de ID do usuário especial para uso pelos clientes.

O controle de acesso em IBM MQ é baseado nos IDs do usuário. O ID do usuário do processo que faz chamadas MQI é normalmente usado. Para os clientes do MQ MQI, o MCA de conexão do servidor faz chamadas MQI em nome de clientes do MQ MQI. É possível selecionar um ID do usuário alternativo para a conexão do servidor MCA para usar para fazer chamadas MQI. O ID do usuário alternativo pode ser associado à estação de trabalho do cliente ou a qualquer coisa escolhida para organizar e controlar o acesso dos clientes. O ID do usuário precisa ter as autoridades necessárias alocadas para ele no servidor para emitir chamadas MQI. Escolher um ID do usuário alternativo é preferível a permitir que clientes façam chamadas MQI com a autoridade da conexão do servidor MCA.

Tabela 9. O ID do usuário usado por um canal de conexão do servidor

ID do usuário	Quando usado
O ID do usuário que é configurado por uma saída de segurança	Usado a menos que seja bloqueado por uma regra **CHLAUTH TYPE(BLOCKUSER)**. Consulte a seção a seguir, “Configurando o ID do usuário em uma saída de segurança” na página 99, para obter mais informações.
O ID do usuário que é configurado por uma regra CHLAUTH	Usado a menos que substituído por uma saída de segurança. Consulte Registros de autenticação de canal para obter mais informações.
O ID do usuário que é definido no atributo **MCAUSER** na definição de canal SVRCONN	Usado a menos que substituído por uma saída de segurança ou uma regra CHLAUTH.
O ID do usuário que é transmitido a partir da máquina cliente	Usado quando nenhum ID do usuário é definido por qualquer outro meio.
O ID do usuário que iniciou o canal de conexão do servidor	Usado quando nenhum ID do usuário é configurado por qualquer outro meio e nenhum ID do usuário cliente é transmitido. Consulte a seção a seguir, “O ID do usuário que executa o programa do canal” na página 99 para obter mais informações.

Como o MCA de conexão do servidor faz chamadas de MQI em nome de usuários remotos, é importante considerar as implicações de segurança do MCA de conexão do servidor que emite chamadas de MQI

em nome de clientes remotos, e como administrar o acesso de um número potencialmente grande de usuários.

- Uma abordagem é para a conexão do servidor MCA emitir chamadas MQI em sua própria autoridade. Mas tenha cuidado, normalmente é indesejável para a conexão do servidor MCA, com seus recursos de acesso poderosos, emitir chamadas MQI em nome de usuários clientes.
- Outra abordagem é usar o ID do usuário que flui a partir do cliente. A conexão do servidor MCA pode emitir chamadas MQI usando os recursos de acesso do ID do usuário do cliente. Esta abordagem apresenta várias questões a considerar:
  1. Existem diferentes formatos para o ID do usuário em diferentes plataformas. Isto às vezes causa problemas se o formato do ID do usuário no cliente diferir dos formatos aceitáveis no servidor.
  2. Há potencialmente muitos clientes com IDs de usuário diferentes e em mudança. Os IDs precisam ser definidos e gerenciados no servidor.
  3. O ID do usuário é confiável? Qualquer ID do usuário pode fluir a partir de um cliente, não necessariamente o ID do usuário que efetuou logon. Por exemplo, o cliente pode fluir um ID com total autoridade `mqm` que foi intencionalmente definida apenas no servidor por razões de segurança.
- A abordagem preferencial é definir tokens de identificação de cliente no servidor e, portanto, limitar os recursos de aplicativos conectados pelo cliente. Isto é geralmente feito configurando a propriedade MCAUSER do canal de conexão do servidor com um valor de ID do usuário especial a ser usado pelos clientes, e definindo alguns IDs para uso por clientes com nível diferente de autorização no servidor.

Configurando o ID do usuário em uma saída de segurança

Para o IBM MQ MQI clients, o processo que emite as chamadas de MQI é o MCA de conexão do servidor MCA. O ID do usuário usado pela conexão do servidor MCA está contido nos campos `MCAUserIdentifier` ou `LongMCAUserIdentifier` do MQCD. O conteúdo destes campos é configurado por:

- Qualquer valor configurado pelas saídas de segurança
- O ID do usuário do cliente
- MCAUSER (na definição do canal de conexão do servidor)

A saída de segurança pode substituir os valores que estão visíveis para ela, quando ela é invocada.

- Se o atributo MCAUSER do canal de conexão do servidor estiver configurado como não-em branco, o valor MCAUSER será usado.
- Se o atributo MCAUSER do canal de conexão do servidor estiver em branco, o ID do usuário recebido do cliente será usado.
- Se o atributo MCAUSER do canal de conexão do servidor estiver em branco, e nenhum ID do usuário for recebido do cliente, o ID do usuário que iniciou o canal de conexão do servidor será usado.

O cliente do IBM MQ não flui o ID do usuário declarado para o servidor quando uma saída de segurança do lado do cliente está em uso.

O ID do usuário que executa o programa do canal

Quando os campos de ID do usuário forem derivados do ID do usuário que iniciou o canal de conexão do servidor, o seguinte valor será usado:

- z/OS Para o z/OS, o ID do usuário designado à tarefa iniciada pelo inicializador de canais pela tabela de procedimentos iniciados do z/OS.
- Para TCP/IP (não z/OS), o ID do usuário na entrada `inetd.conf` ou o ID do usuário que iniciou o listener.
- Para SNA (não z/OS), o ID do usuário na entrada do Servidor SNA ou (se não houver nenhum) a solicitação de conexão de entrada ou o ID do usuário que iniciou o listener.
- Para o NetBIOS ou SPX, o ID do usuário que iniciou o listener.

Se qualquer definição de canal de conexão do servidor existir tendo o atributo MCAUSER configurado como em branco, os clientes poderão usar esta definição de canal para se conectar ao gerenciador de filas com autoridade de acesso determinada pelo ID do usuário fornecido pelo cliente. Pode haver uma exposição de segurança se o sistema em que o gerenciador de filas está sendo executado permitir conexões de rede não-autorizadas. O canal de conexão do servidor padrão IBM MQ (SYSTEM.DEF.SVRCONN) possui o atributo MCAUSER configurado para em branco. Para evitar acesso não autorizado, atualize o atributo MCAUSER da definição padrão com um ID do usuário que não possui acesso aos objetos do IBM MQ MQ.

Caso de IDs de usuário

Quando você define um canal com `runmqsc`, o atributo MCAUSER é alterado para letra maiúscula a menos que o ID do usuário esteja contido entre aspas simples.

ULW Para servidores no UNIX, Linux, and Windows, o conteúdo do campo `MCAUserIdentifier` que é recebido do cliente muda para minúsculo.

IBM i Para servidores no IBM i, o conteúdo do campo `LongMCAUserIdentifier` que é recebido do cliente é mudado para letras maiúsculas.

Linux UNIX Para servidores nos sistemas UNIX and Linux, o conteúdo do campo `LongMCAUserIdentifier` que é recebido do cliente é mudado para letras minúsculas.

Por padrão, o ID do usuário, que é transmitido quando um aplicativo de ligação IBM MQ JMS é usado, é o ID do usuário para a JVM no qual o aplicativo está em execução.

Também é possível transmitir um ID de usuário por meio do método `createQueueConnection`.

Planejando a confidencialidade

Planeje como manter seus dados confidenciais.

É possível implementar confidencialidade no nível do aplicativo ou no nível de link. É possível escolher usar TLS nos casos em que se deve planejar o uso de certificados digitais. Também é possível usar programas de saída de canal se os recursos padrão não atenderem aos seus requisitos.

Conceitos relacionados

“Comparando a segurança no nível do link com a segurança no nível do aplicativo” na página 100
Este tópico contém informações sobre os diversos aspectos da segurança em nível de aplicativo e segurança em nível de link, e compara os dois níveis de segurança.

“Programas de Saída de Canal” na página 106
Os *programas de saída de Canal* são programas chamados em lugares definidos na seqüência do processamento de um MCA. Usuários e fornecedores podem desenvolver seus próprios programas de saída de canal. Alguns são fornecidos pelo IBM.

“Protegendo canais com SSL/TLS” na página 112
O suporte de TLS no IBM MQ usa o objeto de informações sobre autenticação do gerenciador de filas e vários comandos MQSC. Também se deve considerar o uso de certificados digitais.

Comparando a segurança no nível do link com a segurança no nível do aplicativo

Este tópico contém informações sobre os diversos aspectos da segurança em nível de aplicativo e segurança em nível de link, e compara os dois níveis de segurança.

A segurança em nível de link e de aplicativo é ilustrada na Figura 10 na página 101.

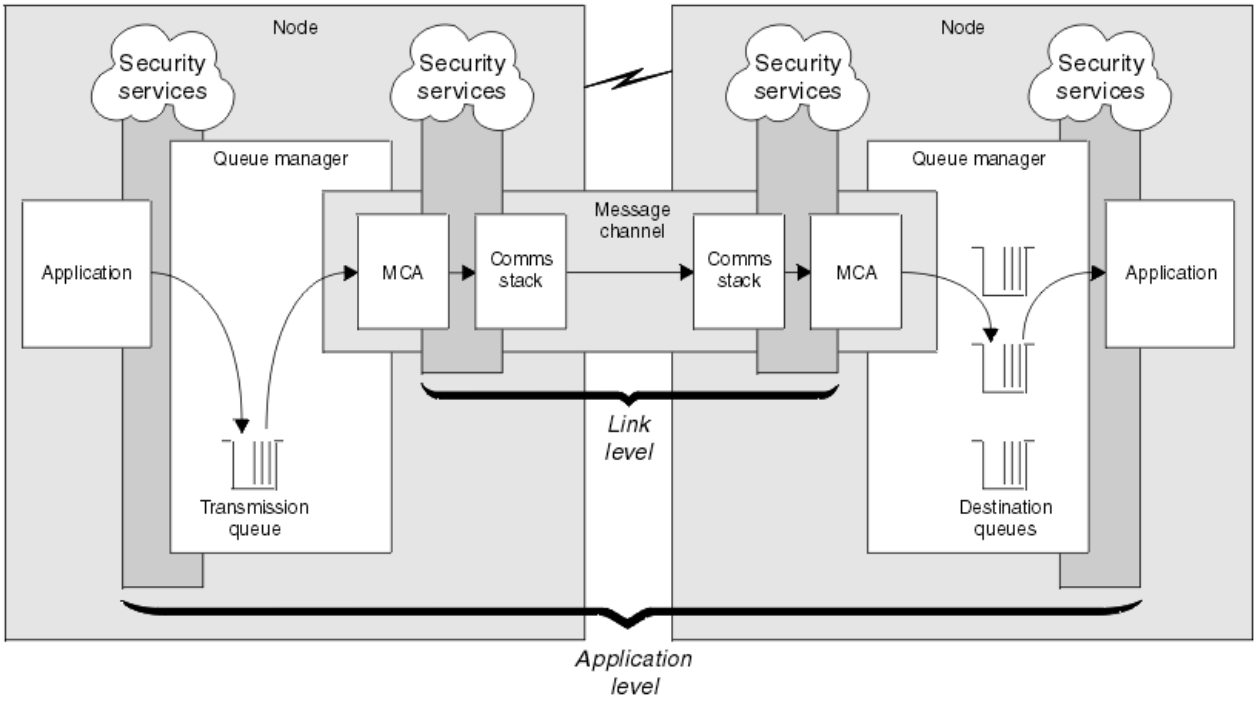


Figura 10. Segurança no nível do link e segurança no nível do aplicativo

Protegendo mensagens em filas

A segurança no nível do link pode proteger mensagens enquanto são transferidas de um gerenciador de filas para outro. É de particular importância quando as mensagens são transmitidas através de uma rede não protegida. Ela não pode, porém, proteger as mensagens enquanto elas estão armazenadas em filas em um gerenciador de filas de origem, de destino ou intermediário.

V 9.1.4 z/OS A criptografia do conjunto de dados do z/OS pode fornecer alguma proteção de mensagens armazenadas em filas, mas somente para dados em repouso em um gerenciador de filas locais. Consulte a seção Confidencialidade para dados em repouso no IBM MQ for z/OS com criptografia do conjunto de dados. para obter informações adicionais.

A segurança em nível de aplicativo, em comparação, pode proteger as mensagens enquanto elas estão armazenadas em filas e se aplica mesmo quando não está sendo utilizado enfileiramento distribuído. Essa é a principal diferença entre a segurança no nível do link e a segurança no nível do aplicativo, e é ilustrada na Figura 10 na página 101.

Gerenciadores de filas que não estão executando em ambientes controlados e de confiança

Se um gerenciador de filas estiver em execução em um ambiente controlado e confiável, os mecanismos de controle de acesso fornecidos pelo IBM MQ podem ser considerados suficientes para proteger as mensagens armazenadas em suas filas. Isso é especialmente verdadeiro se somente filas locais estiverem envolvidas e as mensagens nunca deixarem o gerenciador de filas. A segurança no nível do aplicativo neste caso pode ser considerada desnecessária.

Ela também pode ser considerada desnecessária se as mensagens forem transferidas para outro gerenciador de filas que também esteja executando em um ambiente controlado e de confiança, ou forem recebidas de um gerenciador de filas nessas condições. A necessidade de segurança em nível de aplicativo torna-se maior quando as mensagens são transferidas ou recebidas de um gerenciador de filas que não está sendo executado em um ambiente controlado e confiável.

Diferenças de custo

A segurança no nível do aplicativo pode custar mais que a segurança no nível do link em termos de administração e de desempenho.

É provável que o custo da administração seja maior porque existem mais restrições para configurar e manter. Por exemplo, você pode precisar assegurar que um determinado usuário envia somente certos tipos de mensagens e envia mensagens somente para certos destinos. Por outro lado, você pode precisar assegurar que um determinado usuário recebe somente certos tipos de mensagens e recebe mensagens somente de certas origens. Em vez de gerenciar os serviços de segurança no nível do link em um único canal de mensagem, você pode precisar configurar e manter regras para cada par de usuários que trocam mensagens através desse canal.

Pode haver um impacto no desempenho se os serviços de segurança forem chamados sempre que um aplicativo colocar ou obtiver uma mensagem.

As organizações tendem a considerar a segurança no nível do link primeiro porque ela pode ser mais fácil de implementar. Elas consideram a segurança em nível de aplicativo se descobrem que a segurança no nível do link não satisfaz todos os seus requisitos.

Disponibilidade de componentes

Geralmente, em um ambiente distribuído, um serviço de segurança requer um componente em pelo menos dois sistemas. Por exemplo, uma mensagem pode ser criptografada em um sistema e descriptografada em outro. Isso se aplica tanto à segurança no nível do link quanto à segurança em nível de aplicativo.

Em um ambiente heterogêneo, com diferentes plataformas em uso, cada uma delas com deferentes níveis de funções de segurança, os componentes necessários de um serviço de segurança podem não estar disponíveis para todas as plataformas nas quais eles são necessários e de uma forma fácil de utilizar. Isso provavelmente é um problema maior para a segurança em nível de aplicativo que para a segurança no nível do link, especialmente se você pretender fornecer sua própria segurança em nível de aplicativo comprando componentes de várias origens.

Mensagens em uma fila de cartas não entregues

Se uma mensagem for protegida pela segurança em nível de aplicativo, pode haver um problema se, por algum motivo, a mensagem não atingir seu destino e for colocada em uma fila de cartas não entregues. Se você não descobrir como processar a mensagem a partir das informações no descritor da mensagem e do cabeçalho da carta não entregue, poderá precisar inspecionar o conteúdo dos dados do aplicativo. Não é possível fazer isso se os dados do aplicativo estiverem criptografados e somente o destinatário pretendido poderá decriptografá-los.

O que a segurança em nível de aplicativo não pode fazer

A segurança no nível do aplicativo não é uma solução completa. Mesmo se você implementar a segurança em nível de aplicativo, alguns serviços da segurança no nível do link ainda podem ser necessários. Por exemplo:

- Quando um canal inicia, a autenticação mútua dos dois MCAs pode ainda ser uma exigência. Isso pode ser feito somente por um serviço de segurança no nível do link.
- A segurança em nível de aplicativo não pode proteger o cabeçalho da fila de transmissão, MQXQH, o qual inclui o descritor da mensagem incorporado. Também não se pode proteger os dados nos fluxos de protocolo do canal do IBM MQ diferentes dos dados da mensagem. Somente a segurança no nível do link pode fornecer essa proteção.
- Se os serviços da segurança em nível de aplicativo forem chamados na extremidade do servidor de um canal MQI, os serviços não poderão proteger os parâmetros das chamadas de MQI que forem enviadas pelo canal. Em particular, os dados do aplicativo em um chamada MQPUT, MQPUT1 ou MQGET não são protegidos. Somente a segurança no nível do link pode fornecer a proteção neste caso.

Segurança no nível do link

Segurança no nível do link se refere ao serviços de segurança que são chamados, direta ou indiretamente, por um MCA, pelo subsistema de comunicações ou por uma combinação dos dois trabalhando em conjunto.

A segurança em nível de link é ilustrada no Figura 10 na página 101.

Eis alguns exemplos de serviços de segurança no nível do link:

- O MCA em cada extremidade de um canal de mensagem pode autenticar seu parceiro. Isso é feito quando o canal iniciar e uma conexão de comunicações tiver sido estabelecido, mas antes que as mensagens comecem a fluir. Se a autenticação falhar em qualquer das extremidades, o canal será fechado e nenhuma mensagem será transferida. Este é um exemplo de um serviço de identificação e autenticação.
- Uma mensagem pode ser criptografada na extremidade de envio de um canal e decriptografada na extremidade de recepção. Este é um exemplo de um serviço de confidencialidade.
- Uma mensagem pode ser verificada na extremidade de recepção de um canal para determinar se seu conteúdo foi modificado deliberadamente enquanto ela estava sendo transmitida pela rede. Este é um exemplo de um serviço de integridade de dados.

A segurança em nível de link fornecida pelo IBM MQ

O meio primário de provisão de confidencialidade e integridade de dados no IBM MQ é pelo uso de TLS. Para obter mais informações sobre o uso de TLS no IBM MQ, veja “Protocolos de segurança TLS no IBM MQ” na página 24. Para autenticação, o IBM MQ fornece o recurso para usar registros de autenticação de canal. Os registros de autenticação de canal oferecem controle preciso sobre o acesso concedido à conexão de sistemas, no nível de canais individuais ou grupos de canais. Para obter informações adicionais, consulte “Registros de Autenticação de Canal” na página 49.

Fornecendo sua Própria Segurança em Nível de Link

É possível fornecer seus próprios serviços de segurança de nível de link. Gravar seus próprios programas de saída do canal é a principal forma de fornecer seus próprios serviços de segurança em nível de link.

Os programas de saída de canal são apresentados em “Programas de Saída de Canal” na página 106. O mesmo tópico também descreve o programa de saída do canal que é fornecido com o IBM MQ for Windows (o programa de saída do canal SSPI). Este programa de saída de canal é fornecido em formato de fonte para que você possa alterar o código-fonte para se adequar a suas necessidades. Se este programa de saída do canal, ou programas de saída do canal disponíveis a partir de outros fornecedores, não atenderem seus requisitos, será possível projetar e gravar seu próprio. Este tópico sugere maneiras nas quais os programas de saída do canal podem fornecer serviços de segurança. Para obter informações sobre como gravar um programa de saída do canal, consulte o Gravando programas de saída do canal.

Segurança em Nível de Link Usando uma Saída de Segurança

As saídas de segurança normalmente trabalham em pares; uma em cada extremidade de um canal. Elas são chamadas imediatamente após a conclusão da negociação de dados inicial na inicialização do canal.

Saídas de segurança podem ser usadas para fornecer identificação e autenticação, controle de acesso e confidencialidade.

Segurança em Nível de Link Usando uma Saída de Mensagem

Uma saída de mensagem pode ser utilizada apenas em um canal de mensagem, não em um canal MQI. Ela tem acesso ao cabeçalho da fila de transmissão, MQXQH, que inclui o descritor de mensagens internas e os dados do aplicativo em uma mensagem. Pode modificar o conteúdo da mensagem e alterar seu comprimento.

Uma saída de mensagem pode ser utilizada para qualquer objetivo que exija acesso à mensagem inteira, em vez de uma parte dela.

Saídas de mensagem podem ser usadas para fornecer identificação e autenticação, controle de acesso, confidencialidade, integridade de dados e irrecusabilidade, e por outros motivos que não segurança.

Segurança em Nível de Link Usando Saídas de Envio e Recebimento
As saídas de envio e recebimento podem ser utilizadas nos canais de mensagem e MQI. Podem ser chamadas para todos os tipos de dados que passam em um canal e para fluxos nas duas direções.

As saídas de envio e recebimento têm acesso a cada segmento de transmissão. Elas podem modificar seu conteúdo e alterar seu comprimento.

Em um canal de mensagens, se um MCA tem que dividir uma mensagem e enviá-la em mais de um segmento de transmissão, uma saída de envio poderá ser chamada para cada segmento de transmissão que contém uma parte da mensagem e, na extremidade de recebimento, uma saída de recebimento é chamada para cada segmento de transmissão. O mesmo ocorrerá em um canal MQI se os parâmetros de entrada ou saída de uma chamada MQI forem muito grandes para serem enviados em um único segmento de transmissão.

Em um canal MQI, o byte 10 de um segmento de transmissão identifica a chamada MQI e indica se o segmento de transmissão contém os parâmetros de entrada ou saída da chamada. As saídas de envio e recebimento podem examinar este byte para determinar se a chamada MQI contém dados do aplicativo que podem necessitar de proteção.

Quando uma saída de usuário é chamada pela primeira vez, para adquirir e inicializar os recursos de que necessita, pode solicitar que o MCA reserve uma quantidade específica de espaço no buffer que contém um segmento de transmissão. Quando é chamada posteriormente para processar um segmento de transmissão, ela pode usar esse espaço para incluir uma chave criptografada ou uma assinatura digital, por exemplo. A saída de recepção correspondente na outra extremidade do canal pode remover os dados incluídos pela saída de envio e utilizá-los para processar o segmento de transmissão.

As saídas de envio e recebimento são mais adequadas para propósitos em que não precisam entender a estrutura dos dados que estão manipulando, podendo, assim, tratar cada segmento de transmissão como um objeto binário.

As saídas de envio e recebimento podem ser usadas para fornecer confidencialidade e integridade de dados, e para outros usos que não segurança.

Tarefas relacionadas
Identificando uma chamada de API em um programa de saída de envio ou recebimento

Segurança em Nível de Aplicativo
Segurança no nível do aplicativo se refere aos serviços de segurança que são chamados na interface entre um aplicativo e um gerenciador de filas ao qual ele está conectado.

Esses serviços são chamados quando o aplicativo emite chamadas de MQI para o gerenciador de filas. Os serviços podem ser chamados direta ou indiretamente, pelo aplicativo, pelo gerenciador de filas, por outro produto que suporta o IBM MQ ou por uma combinação de qualquer um desses trabalhando em conjunto. A segurança em nível de aplicativo é ilustrada na Figura 10 na página 101.

A segurança em nível de aplicativo também é conhecida como *segurança ponta-a-ponta* ou *segurança no nível da mensagem*.

Eis alguns exemplos de serviços de segurança em nível de aplicativo:

- quando um aplicativo coloca uma mensagem em uma fila, o descritor da mensagem contém um ID de usuário associado ao aplicativo. Entretanto, não existem dados presentes, tais como uma senha criptografada, que possam ser utilizados para autenticar o ID do usuário. Um serviço de segurança pode incluir esses dados. Quando a mensagem for finalmente recuperada pelo aplicativo de recepção, outro componente do serviço pode autenticar o ID do usuário utilizando os dados que foram enviados com a mensagem. Este é um exemplo de um serviço de identificação e autenticação.
- Uma mensagem pode ser criptografada quando é colocada em uma fila por um aplicativo, e descriptografada quando é recuperada pelo aplicativo de recepção.Este é um exemplo de um serviço de confidencialidade.
- Uma mensagem pode ser verificada quando é recuperada pelo aplicativo de recepção. Essa verificação determina se seu conteúdo foi modificado deliberadamente desde que foi colocada pela primeira vez em uma fila pelo aplicativo de envio.Este é um exemplo de um serviço de integridade de dados.

Planejamento para o Advanced Message Security
O Advanced Message Security (AMS) é um componente do IBM MQ que fornece um alto nível de proteção para dados sensíveis que fluem por meio da rede do IBM MQ, ao mesmo tempo em que não impacta os aplicativos finais.

Se você estiver movendo informações altamente sigilosas ou de valor, informações especialmente confidenciais ou relacionadas a pagamento, como registros de paciente ou detalhes de cartão de crédito, deverá prestar muita atenção à segurança de informações. Assegurar que as informações que passam pela empresa retenham sua integridade e sejam protegidas contra acesso não autorizado é um desafio e uma responsabilidade contínua. É provável também que você seja obrigado a cumprir os regulamentos de segurança, sob o risco de penalidades por falta de conformidade.

É possível desenvolver suas próprias extensões de segurança para o IBM MQ. No entanto, essas soluções requerem qualificações de especialistas e podem ser complicadas e caras de se manter. O Advanced Message Security ajuda a lidar com esses desafios ao mover informações acerca da empresa entre cada tipo de sistema de TI comercial virtualmente.

O Advanced Message Security estende os recursos de segurança do IBM MQ das seguintes maneiras:

- Fornece proteção de dados de ponta a ponta no nível do aplicativo para sua infraestrutura do sistema de mensagens ponto a ponto, usando criptografia ou assinatura digital de mensagens.
- Fornece segurança abrangente sem gravar código de segurança complexo ou modificar ou recompilar aplicativos existentes.
- Usa a tecnologia de Infraestrutura de Chave Pública (PKI) para fornecer autenticação, autorização, confidencialidade e serviços de integridade de dados para mensagens.
- Fornece administração de políticas de segurança para servidores mainframe e distribuídos.
- Ele suporta servidores e clientes do IBM MQ.
- Ele se integra com o Managed File Transfer para fornecer uma solução do sistema de mensagens segura de ponta a ponta.

Para obter informações adicionais, consulte “Advanced Message Security” na página 569.

Fornecendo sua própria segurança de nível de aplicativo
É possível fornecer seus próprios serviços de segurança de nível de aplicativo. Para ajudar a implementar a segurança no nível do aplicativo, o IBM MQ fornece duas saídas, a saída da API e a saída cruzada da API.

A saída de API e a saída cruzada da API podem fornecer identificação e autenticação, controle de acesso, confidencialidade, integridade de dados, serviços de não repúdio e outras funções não relacionadas à segurança.

Se a saída API ou a saída de cruzamento de API não for suportada em seu ambiente de sistema, você pode desejar considerar outras maneiras de fornecer sua própria segurança de nível de aplicativo. Uma maneira é desenvolver uma API de nível mais alto que encapsule a MQI. Os programadores usam, então, essa API, em vez do MQI, para gravar aplicativos do IBM MQ.

As razões mais comuns para utilizar uma API de nível mais alto são:

- Para ocultar os recursos mais avançados da MQI dos programadores.
- Para reforçar padrões na utilização da MQI.
- Para incluir uma função à MQI. Esta função adicional pode ser serviços de segurança.

Alguns produtos de fornecedores usam esta técnica para fornecer segurança de nível do aplicativo para IBM MQ.

Se você estiver planejando fornecer serviços de segurança desta maneira, observe o seguinte em relação à conversão de dados:

- Se um token de segurança, tal como uma assinatura digital, tiver sido incluído aos dados de aplicativo na mensagem, qualquer código executando conversão de dados deve estar ciente da presença deste token.

- Um token de segurança pode ser derivado de uma imagem binária dos dados do aplicativo. Portanto, qualquer verificação do token deve ser feita antes de converter os dados.
- Se os dados do aplicativo na mensagem tiverem sido criptografados, eles devem ser decriptografados antes da conversão de dados.

Programas de Saída de Canal

Os *programas de saída de Canal* são programas chamados em lugares definidos na seqüência do processamento de um MCA. Usuários e fornecedores podem desenvolver seus próprios programas de saída de canal. Alguns são fornecidos pelo IBM.

Existem diversos tipos de programas de saída de canal, mas apenas quatro têm uma função de fornecer segurança em nível de link:

- Saída de Segurança
- Saída de mensagen
- Saída de envio
- Saída de recepção

Esses quatro tipos de programas de saída de canal são ilustrados na Figura 11 na página 106 e descritos nos tópicos a seguir.

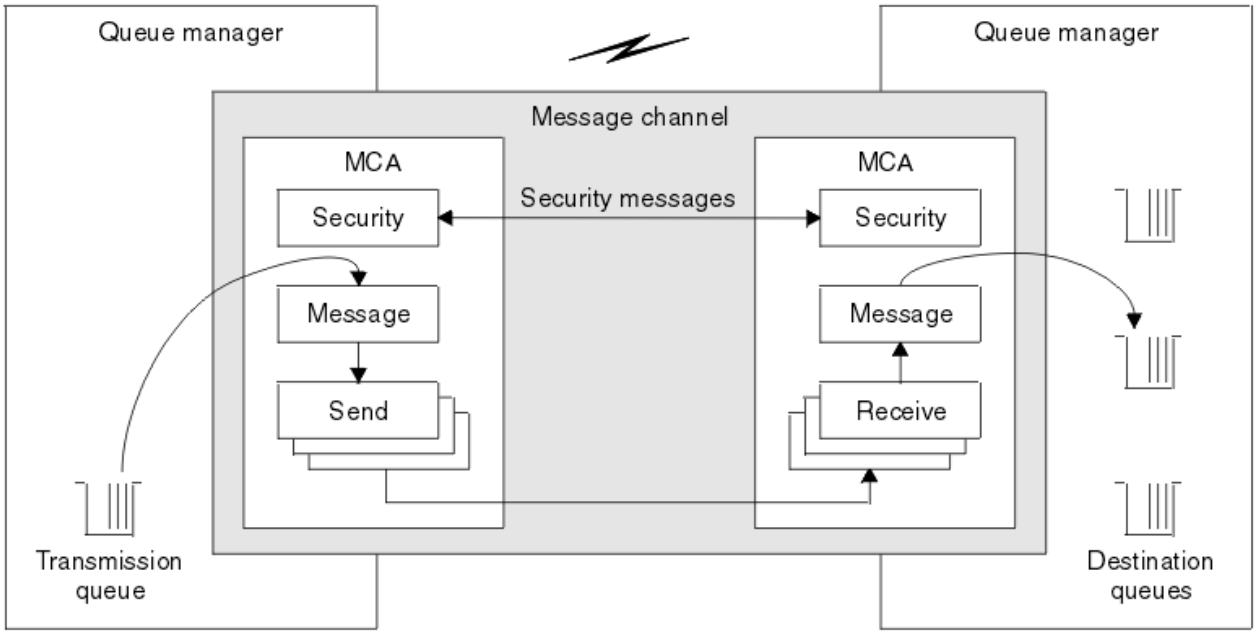


Figura 11. Saídas de segurança, mensagem, envio e recebimento em um canal de mensagens

Conceitos relacionados

Programas de Saída de Canal para Canais de Mensagens

Visão Geral da Saída de Segurança

As saídas de segurança normalmente trabalham em pares. Elas são chamadas antes dos fluxos de mensagens e seus propósitos são permitir que um MCA autentique seu parceiro.

As *Saídas de segurança* normalmente trabalham em pares; uma em cada extremidade de um canal. Elas são chamadas imediatamente após a conclusão da negociação de dados inicial na inicialização do canal, mas antes do início do fluxo de qualquer mensagem. A principal finalidade da saída de segurança é permitir ao MCA de cada extremidade de um canal autenticar o seu parceiro. No entanto, não há nada que possa evitar que uma saída de segurança efetue outra função, mesmo uma função que não tenha nada a ver com segurança.

As saídas de segurança podem se comunicar umas com as outras enviando *mensagens de segurança*. O formato de uma mensagem de segurança não é definido e é determinado pelo usuário. Um possível resultado da troca de mensagens de segurança é que uma das saídas de segurança pode decidir não prosseguir mais. Nesse caso, o canal é fechado e as mensagens não fluem. Se existir uma saída de segurança em apenas uma extremidade de um canal, a saída ainda é chamada e pode escolher se vai prosseguir ou fechar o canal.

As saídas de segurança podem ser chamadas em canais de mensagens e do MQI. O nome de uma saída de segurança é especificado como um parâmetro na definição do canal em cada extremidade de um canal.

Para obter mais informações sobre saídas de segurança, consulte “Segurança em Nível de Link Usando uma Saída de Segurança” na página 103.

Saída de mensagen

As saídas de mensagens operam apenas em canais de mensagens e normalmente funcionam em pares. Uma saída de mensagem pode operar em toda a mensagem e fazer várias mudanças nela.

As *Saídas de mensagens* nas extremidades de envio e de recebimento de um canal normalmente trabalham em pares. Uma saída de mensagens na extremidade de envio de um canal é chamada após o MCA ter recebido uma mensagem da fila de transmissão. Na extremidade de recebimento de um canal, uma saída de mensagens é chamada antes que o MCA coloque uma mensagem em sua fila de destino.

Uma saída de mensagens tem acesso ao cabeçalho da fila de transmissão, MQXQH, que inclui o descritor de mensagens embutidas, e os dados do aplicativo em uma mensagem. Uma saída de mensagens pode modificar o conteúdo da mensagem e alterar seu comprimento. Uma alteração no comprimento pode ser o resultado da compressão, descompressão, criptografia e decriptografia da mensagem. Também pode ser o resultado de incluir dados na mensagem ou remover dados dela.

As saídas de mensagens podem ser utilizadas para qualquer finalidade que exija acesso à mensagem inteira, em vez de parte dela, e não necessariamente para segurança.

Uma saída de mensagem pode determinar que a mensagem que está processando atualmente não deve continuar além da direção de seu destino. O MCA coloca a mensagem na fila dead-letter. Uma saída de mensagem pode também fechar o canal.

As saídas de mensagens podem ser chamadas apenas em canais de mensagens, não em canais do MQI. Isto ocorre porque o objetivo de um canal do MQI é permitir o fluxo de parâmetros de entrada e de saída de chamadas do MQI entre o aplicativo IBM MQ MQI client e o gerenciador de filas.

O nome de uma saída de mensagens é especificado como um parâmetro na definição do canal em cada extremidade de um canal. Você também pode especificar uma lista de saídas de mensagens para serem executadas sucessivamente.

Para obter mais informações sobre saídas de mensagem, consulte “Segurança em Nível de Link Usando uma Saída de Mensagem” na página 103.

Saídas de Envio e Recebimento

As saídas de envio e recebimento geralmente trabalham em pares. Elas operam em segmentos de transmissão e são melhor usadas onde a estrutura dos dados que estão processando não for relevante.

Uma *saída de envio* em uma extremidade de um canal e uma *saída de recebimento* na outra extremidade normalmente trabalham em pares. Uma saída de envio é chamada pouco antes de um MCA emitir um envio de comunicação para enviar dados para uma conexão de comunicação. Uma saída de recebimento é chamada logo depois que um MCA recuperou o controle após um recebimento de comunicação e recebeu dados de uma conexão de comunicação. Se as conversações compartilhadas estiverem em uso sobre um canal MQI, uma instância diferente de uma saída de envio e de recebimento será chamada para cada conversação.

Os fluxos de protocolo de canais do IBM MQ entre dois MCAs em um canal de mensagens contêm informações de controle, assim como dados das mensagens. Da mesma forma, em um canal do MQI, os fluxos contêm informações sobre controle assim como os parâmetros das chamadas do MQI. As saídas de envio e recebimento são chamadas para todos os tipos de dados.

Os dados de mensagens fluem em apenas uma direção em um canal de mensagens mas, em um canal do MQI, os parâmetros de entrada de uma chamada do MQI fluem em uma direção e os parâmetros de saída fluem na outra direção. Em canais de mensagens e do MQI, as informações de controle fluem em ambas as direções. Como resultado, as saídas de envio e recebimento podem ser chamadas em ambas as extremidades de um canal.

A unidade de dados que é transmitida em um único fluxo entre dois MCAs é denominada um *segmento de transmissão*. As saídas de envio e recebimento têm acesso a cada segmento de transmissão. Elas podem modificar seu conteúdo e alterar seu comprimento. No entanto, uma saída de envio não deve alterar os oito primeiros bytes de um segmento de transmissão. Esses 8 bytes fazem parte do cabeçalho do protocolo do canal do IBM MQ. Também existem restrições em relação a quanto uma saída de envio pode aumentar o comprimento de um segmento de transmissão. Especificamente, uma saída de envio não pode aumentar seu comprimento além do máximo negociado entre os dois MCAs na inicialização do canal.

Em um canal de mensagens, se uma mensagem for muito grande para ser enviada em um único segmento de transmissão, o MCA de envio divide a mensagem e a envia em mais de um segmento de transmissão. Como conseqüência, uma saída de envio é chamada para cada segmento de transmissão contendo uma parte da mensagem e, na extremidade de recebimento, uma saída de recebimento é chamada para cada segmento de transmissão. O MCA de recebimento reconstitui a mensagem a partir dos segmentos de transmissão após serem processados pela saída de recebimento.

Da mesma forma, em um canal do MQI, os parâmetros de entrada ou de saída de uma chamada do MQI são enviados em mais de um segmento de transmissão se forem muito grandes. Isso pode ocorrer, por exemplo, em uma chamada MQPUT, MQPUT1 ou MQGET se os dados do aplicativo forem grandes o suficiente.

Levando em conta essas considerações, é mais apropriado utilizar saídas de envio e recebimento para objetivos nos quais elas não precisem entender a estrutura dos dados que estão tratando e possam, assim, tratar cada segmento de transmissão como um objeto binário.

Uma saída de envio ou de recebimento pode fechar um canal.

Os nomes de uma saída de envio e de uma saída de recebimento são especificados como parâmetros na definição do canal em cada extremidade de um canal. Você também pode especificar uma lista de saídas de envio a serem executadas sucessivamente. Da mesma maneira, você pode especificar uma lista de saídas de recebimento.

Para obter mais informações sobre saídas de envio e recebimento, consulte “Segurança em Nível de Link Usando Saídas de Envio e Recebimento” na página 104.

Planejando a integridade de dados

Planeje como preservar a integridade dos dados.

É possível implementar a integridade dos dados no nível do aplicativo ou no nível de link.

No nível do aplicativo, é possível usar programas de saída de API se os recursos padrão não satisfizerem seus requisitos. É possível optar por usar o Advanced Message Security (AMS) para assinar mensagens digitalmente para proteção contra modificação não autorizada.

No nível de link, você pode escolher usar TLS. Nesse caso, deve-se planejar o uso de certificados digitais. Também é possível usar programas de saída de canal se os recursos padrão não atenderem aos seus requisitos.

Conceitos relacionados

“Protegendo canais com SSL/TLS” na página 112
O suporte de TLS no IBM MQ usa o objeto de informações sobre autenticação do gerenciador de filas e vários comandos MQSC. Também se deve considerar o uso de certificados digitais.

“Integridade de dados no IBM MQ” na página 23
É possível usar um serviço de integridade de dados para detectar se uma mensagem foi modificada.

“Planejamento para o Advanced Message Security” na página 105

O Advanced Message Security (AMS) é um componente do IBM MQ que fornece um alto nível de proteção para dados sensíveis que fluem por meio da rede do IBM MQ, ao mesmo tempo em que não impacta os aplicativos finais.

Chamadas de Saída do Canal e Estrutura de Dados

Referências relacionadas

Referência de saída de API

Planejando a auditoria

Decida quais dados são necessários para a auditoria e como as informações de auditoria serão capturadas e processadas. Considere como verificar se o sistema está configurado corretamente.

Há vários aspectos para o monitoramento de atividade. Os aspectos que devem ser considerados são frequentemente definidos por requisitos de auditoria, e esses requisitos são geralmente orientados por normas regulamentares, como o HIPAA (Health Insurance Portability and Accountability Act) ou o SOX (Sarbanes-Oxley). O IBM MQ fornece recursos destinados a ajudar na conformidade com tais normas.

Considere se você está interessado apenas em exceções ou se está interessado em todo o comportamento do sistema.

Alguns aspectos de auditoria também podem ser considerados como monitoramento operacional; uma distinção para a auditoria é que você está sempre olhando para dados históricos, e não apenas para alertas em tempo real. O monitoramento é abrangido na seção Monitoramento e desempenho.

Quais dados auditar

Considere quais tipos de dados ou atividade são necessários para auditar, conforme descrito nas seções a seguir:

As mudanças feitas no IBM MQ usando as interfaces do IBM MQ
: Configure o IBM MQ para emitir os eventos de instrumentação, especificamente os eventos de comando e eventos de configuração.

Mudanças feitas no IBM MQ fora de seu controle
: Algumas mudanças podem afetar como o IBM MQ se comporta, mas não podem ser monitoradas diretamente pelo IBM MQ. Exemplos de tais mudanças incluem mudanças nos arquivos de configuração `mqs.ini`, `qm.ini` e `mqclient.ini`, a criação e a exclusão de gerenciadores de filas, instalação de arquivos binários como programas de saída de usuários e alterações de permissões de arquivo. Para monitorar essas atividades, deve-se usar ferramentas em execução no nível do sistema operacional. Diferentes ferramentas estão disponíveis e são apropriadas para diferentes sistemas operacionais. Também é necessário ter logs criados por ferramentas associadas, tais como *sudo*.

Controle operacional do IBM MQ
: Talvez seja necessário usar as ferramentas do sistema operacional para auditar atividades, como iniciar e parar os gerenciadores de filas. Em alguns casos, IBM MQ pode ser configurado para emitir eventos de instrumentação.

Atividade do aplicativo no IBM MQ
: Para auditar as ações de aplicativos, por exemplo, abrir filas e enviar e receber mensagens, configure o IBM MQ para emitir eventos adequados.

Alertas de intruso
: Para auditar tentativas de violação de segurança, configure o sistema para emitir eventos de autorização. Os eventos do canal também podem ser úteis para mostrar a atividade, especialmente se um canal for encerrado inesperadamente.

Planejando a captura, exibição e arquivamento de dados de auditoria

Muitos dos elementos que são necessários são relatados como mensagens do evento do IBM MQ. Deve-se escolher ferramentas que podem ser lidas e formatar essas mensagens. Se você estiver interessado em armazenamento e análise de longo prazo, deverá movê-los para um mecanismo de armazenamento auxiliar, como um banco de dados. Se essas mensagens não forem processadas, elas permanecerão na

fila de eventos, possivelmente preenchendo a fila. É possível escolher implementar uma ferramenta que executa automaticamente uma ação com base em alguns eventos; por exemplo, para emitir um alerta quando uma falha de segurança ocorre.

Verificando se seu sistema está corretamente configurado

Um conjunto de testes é fornecido com o IBM MQ Explorer. Use estes testes para verificar problemas em suas definições de objeto.

Além disso, verifique periodicamente se a configuração do sistema está conforme o esperado. Embora eventos de comando e configuração possam relatar quando algo é mudado, eles também são úteis para fazer dump da configuração e compará-la com uma cópia correta conhecida.

Planejando a segurança por meio da topologia

Esta seção abrange a segurança em situações específicas, nomeadamente para os canais, clusters de gerenciadores de filas, publicação/assinatura e aplicativos multicast, e ao utilizar um firewall.

Consulte os subtópicos a seguir para obter mais informações:

Autorização de canal

Ao enviar ou receber uma mensagem por meio de um canal, será necessário fornecer acesso a diversos recursos do IBM MQ. Os agentes do canal de mensagens (MCAs) são essencialmente aplicativos do IBM MQ que movem mensagens entre gerenciadores de fila, e como tal, requerem acesso a vários recursos do IBM MQ para operar corretamente.

Para receber mensagens no tempo de PUT para MCAs, é possível usar o ID de usuário associado ao MCA ou o ID do usuário associado à mensagem.

No tempo CONNECT, é possível mapear o ID do usuário declarado para um usuário alternativo, usando registros de autenticação do canal **CHLAUTH**.

No IBM MQ, os canais podem ser protegidos pelo suporte de TLS.

Os IDs de usuário associados ao envio e recebimento de canais, excluindo o canal emissor em que o atributo MCAUSER não é usado, precisam ter acesso aos seguintes recursos:

- O ID do usuário associado a um canal de envio requer acesso ao gerenciador de filas, a fila de transmissão, a fila de mensagens não entregues e acesso a quaisquer outros recursos que são requeridos por saídas do canal.
- O ID do usuário MCAUSER de um canal receptor precisa da autoridade *+setall*. A razão é que o canal receptor tem que criar o MQMD completo, incluindo todos os campos de contexto, usando os dados que ele recebeu do canal emissor remoto. O gerenciador de filas, portanto, requer que o usuário que executa esta atividade tenha a autoridade *+setall*. Esta autoridade *+setall* deve ser concedida ao usuário para:
  - Todas as filas que o canal receptor coloca validamente as mensagens.
  - O objeto do gerenciador de filas. Para obter mais informações, veja Autorizações para contexto.
- O ID do usuário MCAUSER de um canal receptor no qual o originador solicitou uma mensagem de relatório COA precisa de autoridade *+passid* na fila de transmissão que retorna a mensagem de relatório. Sem essa autoridade, as mensagens de erro AMQ8077 são registradas.
- Com o ID do usuário associado ao canal de recebimento, é possível abrir as filas de destino para colocar mensagens nas filas. Isso envolve a Interface de enfileiramento de mensagens (MQI), portanto, as verificações de controle de acesso adicionais podem precisar ser feitas se você não estiver usando o gerenciador de autoridade de objeto (OAM) do IBM MQ. É possível especificar se as verificações de autorização são feitas em relação ao ID de usuário associado ao MCA (conforme descrito neste tópico) ou em relação ao ID de usuário associado à mensagem (a partir do campo MQMD UserIdentifier).

  Para os tipos de canais para os quais ele se aplica, o parâmetro **PUTAUT** de uma definição de canal especifica qual ID de usuário é usado para essas verificações.

- O canal é padronizado para usar a conta de serviço do gerenciador de filas, que tem direitos administrativos integrais e não requer autorizações especiais.
- No caso de canais de conexão do servidor, as conexões administrativas são bloqueadas por padrão pelas regras CHLAUTH e requerem fornecimento explícito.
- Canais do tipo receptor, solicitante e receptor de cluster permitem administração local por qualquer gerenciador de filas adjacente, a menos que o administrador execute as etapas para restringir esse acesso.
- Não é necessário conceder autoridade *dsp* e *ctrlx* para o ID do usuário MCAUSER de um canal receptor.
- Antes da IBM MQ 8.0.0 Fix Pack 4, se você usa um ID do usuário que não possui os privilégios administrativos do IBM MQ, deve-se conceder autoridade **dsp** e **ctrlx** para o canal a esse ID do usuário para que o canal funcione.

  A partir da IBM MQ 8.0.0 Fix Pack 4, não há verificações de autoridade quando um canal ressincroniza a si mesmo e corrige os números de sequência.

  No entanto, a emissão de um comando RESET CHANNEL manualmente ainda requer **+dsp** e **+ctrlx** em todas as liberações.

  Atenção: Quando a reconfiguração de um canal é necessária para confirmação do lote de mensagens, o IBM MQ tenta consultar o canal, o que requer autoridade **+dsp**.
- O atributo MCAUSER não é usado para o tipo de canal SDR.
- Se você usar o ID do usuário associado à mensagem, é provável que o ID do usuário seja de um sistema remoto. Esse ID do usuário do sistema remoto deve ser reconhecido pelo sistema de destino. Os comandos a seguir são exemplos do tipo de comando que é possível emitir para conceder autoridade a um ID do usuário de um sistema remoto:

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

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

em que *Profile* é um canal.

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

em que *Profile* é uma fila de mensagens não entregues, se configurada.

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

em que *Profile* é uma lista de filas autorizadas.

Atenção: Tome cuidado ao autorizar um ID do usuário a colocar mensagens na fila de comandos ou outras filas sensíveis do sistema.

O ID de usuário associado ao MCA depende do tipo de MCA. Há dois tipos de MCA:

MCA responsável pela chamada
MCAs que iniciam um canal. Os MCAs responsáveis pela chamada podem ser iniciados como processos individuais, como encadeamentos do inicializador de canais, ou como encadeamentos de um conjunto de processos. O ID do usuário usado é o ID do usuário associado ao processo pai (o inicializador de canais) ou o ID do usuário associado ao processo que inicia o MCA.

MCA respondente
MCAs respondentes são MCAs que são iniciados como resultado de uma solicitação feita por um MCA responsável pela chamada. MCAs respondentes podem ser iniciados como processos individuais, como encadeamentos do listener ou como encadeamentos de um conjunto de processos. O ID do usuário pode ser qualquer um dos tipos a seguir (nessa ordem, de preferência):

1. No APPC, o MCA responsável pela chamada pode indicar o ID de usuário a ser usado para o MCA respondente. Isso é chamado de ID do usuário da rede, e se aplica somente a canais iniciados

como processos individuais. Configure o ID do usuário de rede usando o parâmetro USERID da definição de canal.

2. Se o parâmetro **USERID** não for usado, a definição de canal do MCA respondente pode especificar o ID do usuário que o MCA deve usar. Configure o ID do usuário usando o parâmetro **MCAUSER** da definição de canal.
3. Se o ID do usuário não foi definido por um dos métodos anteriores (dois), o ID do usuário do processo que inicia o MCA ou o ID do usuário do processo pai (o listener) é usado.

Conceitos relacionados

"Registros de Autenticação de Canal" na página 49
Para exercer um controle mais preciso sobre o acesso concedido à conexão de sistemas em um nível de canal, é possível usar registros de autenticação de canal.

Propriedades de registro de autenticação de canal

Protegendo Definições do Inicializador de Canais

Apenas membros do grupo mqm podem manipular inicializadores de canais.

Os inicializadores de canais do IBM MQ não são objetos do IBM MQ; o acesso a eles não é controlado pelo OAM. O IBM MQ não permite que usuários ou aplicativos manipulem esses objetos, a menos que o ID do usuário seja um membro do grupo mqm. Se você tiver um aplicativo que emite o comando PCF **StartChannelInitiator**, o ID do usuário especificado no descritor de mensagens da mensagem PCF deve ser membro do grupo mqm no gerenciador de filas de destino.

Um ID de usuário também deverá ser um membro do grupo mqm na máquina de destino para emitir os comandos MQSC equivalentes por meio do comando PCF Escape ou usando `runmqsc` no modo indireto.

Filas de transmissão

Os gerenciadores de filas colocam mensagens remotas automaticamente em uma fila de transmissão; não é necessária nenhuma autoridade especial para isso.

No entanto, se for necessário colocar uma mensagem diretamente em uma fila de transmissão, isso exigirá autorização especial; consulte Tabela 12 na página 131.

Saídas do canal

Se registros de autenticação de canal não forem adequados, será possível usar saídas do canal para segurança incluída. Uma saída de segurança forma uma conexão segura entre dois programas de saída de segurança. Um programa é para o agente do canal de mensagens de envio (MCA) e o outro para o MCA de recebimento.

Consulte "Programas de Saída de Canal" na página 106 para obter mais informações sobre saídas do canal.

Protegendo canais com SSL/TLS

O suporte de TLS no IBM MQ usa o objeto de informações sobre autenticação do gerenciador de filas e vários comandos MQSC. Também se deve considerar o uso de certificados digitais.

Certificados digitais e repositórios de chaves

É uma boa prática configurar o atributo de rótulo do certificado do gerenciador de filas (**CERTLABL**) para o nome do certificado pessoal a ser usado para a maioria dos canais, e substituí-lo para exceções, configurando o rótulo certificado sobre os canais que requerem certificados diferentes.

Se são necessários muitos canais com certificados que diferem do certificado padrão definido no gerenciador de filas, deve-se considerar a divisão de canais entre os vários gerenciadores de filas ou usar um proxy MQIPT na frente do gerenciador de filas para apresentar um certificado diferente.

É possível usar um certificado diferente para cada canal, mas se você armazenar muitos certificados em um repositório de chaves, poderá esperar que o desempenho seja afetado ao iniciar os canais TLS. Tente manter o número de certificados em um repositório de chaves para menos de 50, e considere 100 como

um máximo à medida que o desempenho do GSKit diminui acentuadamente com repositórios de chaves maiores.

Permitir vários certificados no mesmo gerenciador de filas aumenta as chances de que vários certificados de autoridade de certificação sejam usados no mesmo gerenciador de filas. Isso aumenta as chances de o namespace Nome Distinto do Assunto do certificado entrar em conflito para certificados emitidos por autoridades de certificação separadas.

Enquanto autoridades de certificação profissionais são, provavelmente, mais cautelosas, autoridades de certificação internas muitas vezes não têm convenções de nomenclatura claras e você pode acabar com correspondências indesejadas entre uma CA e outra.

É necessário verificar o Nome Distinto do Emissor do certificado, além do Nome Distinto do Assunto. Para fazer isso, use um registro SSLPEERMAP de autenticação de canal e configure os campos **SSLPEER** e **SSLCERTI** para corresponder ao Nome Distinto do Assunto e Nome Distinto do Emissor respectivamente.

Certificados autoassinados e certificados assinados por CA

É importante planejar o uso de certificados digitais quando se está desenvolvendo e testando seu aplicativo, e para seu uso em produção. É possível usar os certificados assinados por CA ou os certificados autoassinados, dependendo do uso de seus gerenciadores de filas e aplicativos clientes.

Certificados assinados pelo CA
Para sistemas de produção, obtenha os certificados a partir de uma autoridade de certificação (CA) confiável. Ao se obter um certificado a partir de uma CA externa, você paga pelo serviço.

Certificados autoassinados
Enquanto você está desenvolvendo seu aplicativo, será possível usar certificados autoassinados ou certificados emitidos por uma autoridade de certificação local, dependendo da plataforma:

ULW Nos sistemas Windows, UNIX e Linux, é possível usar os certificados autoassinados. Consulte a seção “Criando um certificado pessoal autoassinado no UNIX, Linux, and Windows” na página 297 para obter instruções.

IBM i Em sistemas IBM i, é possível usar os certificados assinados pela autoridade de certificação local. Consulte a seção “Solicitando um certificado do servidor no IBM i” na página 281 para obter instruções.

z/OS No z/OS, é possível usar os certificados autoassinado ou assinado por CA local. Consulte “Criando um certificado pessoal autoassinado no z/OS” na página 325 ou “Solicitando um certificado pessoal no z/OS” na página 325 para obter instruções.

Os certificados autoassinados não são adequados para uso de produção, pelas seguintes razões:

- Certificados autoassinados não podem ser revogados, o que pode permitir que um invasor realize spoof em uma identidade após uma chave privada ter sido comprometida. CAs podem revogar um certificado comprometido, evitando seu uso adicional. O uso de certificados assinados por CA são, portanto, mais seguros em um ambiente de produção, embora certificados autoassinados sejam mais convenientes em um sistema de teste.
- Os certificados autoassinados nunca expirarão. Isso é conveniente e seguro em um ambiente de teste, mas em um ambiente de produção, isso os deixa abertos a eventuais violações de segurança. O risco é ainda composto pelo fato de os certificados autoassinados não poderem ser revogados.
- Um certificado autoassinado é usado como um certificado pessoal e como um certificado de autoridade de certificação raiz (ou âncora de confiança). Um usuário com um certificado pessoal autoassinado pode ser capaz de usá-lo para assinar outros certificados pessoais. Em geral, isso não é verdadeiro para certificados pessoais emitidos por uma autoridade de certificação, e representa uma exposição significativa.

CipherSpecs e certificados digitais

Somente um subconjunto dos CipherSpecs suportados pode ser usado com todos os tipos suportados de certificado digital. Portanto, é necessário escolher um CipherSpec apropriado para seus certificados digitais. Da mesma forma, se a política de segurança de sua organização requer que um determinado CipherSpec seja usado, deve-se obter os certificados digitais adequados.

Para obter mais informações sobre o relacionamento entre CipherSpecs e certificados digitais, consulte "Certificados digitais e compatibilidade de CipherSpec no IBM MQ" na página 45

Políticas de Validação de Certificado

O padrão IETF RFC 5280 especifica uma série de regras de validação de certificado que o software de aplicativo compatível deve implementar para impedir ataques de personificação. Um conjunto de regras de validação de certificado é conhecido como uma política de validação de certificado. Para obter mais informações sobre as políticas de validação de certificado no IBM MQ, consulte "Políticas de validação de certificado no IBM MQ" na página 44.

Planejando a verificação de revogação de certificado

Permitir vários certificados de autoridades de certificação diferentes causa, potencialmente, a verificação adicional de revogação de certificado desnecessária.

Em particular, se você tiver configurado explicitamente o uso de um servidor de revogação a partir de uma autoridade de certificação específica, por exemplo, usando um objeto AUTHINFO ou estrutura de registro de informações sobre autenticação (MQAIR), uma verificação de revogação falhará quando apresentada com um certificado a partir de uma autoridade de certificação diferente.

É necessário evitar a configuração do servidor de revogação de certificado explícito. Em vez disso, deve-se ativar a verificação implícita onde cada certificado contém seu próprio local de servidor de revogação em uma extensão de certificado, por exemplo, Ponto de Distribuição CRL ou OCSP AuthorityInfoAccess.

Para obter mais informações, consulte OCSPCheckExtensions e CDPCheckExtensions.

Comandos e atributos para o suporte de TLS

O protocolo Segurança da Camada de Transporte (TLS) fornece segurança de canal, com proteção contra espionagem do tráfego de rede, violação e personificação. O suporte do IBM MQ para TLS permite especificar, na definição de canal, que um determinado canal usa a segurança TLS. Também é possível especificar detalhes do tipo de segurança desejado, como o algoritmo de criptografia que você deseja usar.

- Os comandos do MQSC a seguir suportam TLS:

  ALTER AUTHINFO
  Modifica os atributos de um objeto de informações sobre autenticação.

  DEFINE AUTHINFO
  Cria um objeto de informações sobre autenticação.

  DELETE AUTHINFO
  Exclui um objeto de informações sobre autenticação.

  DISPLAY AUTHINFO
  Exibe os atributos para um objeto de informações sobre autenticação específico.

- Os parâmetros do gerenciador de filas a seguir suportam TLS:

  CERTLABL
  Define um rótulo de certificado pessoal a ser usado.

  SSLCRLNL
  O atributo SSLCRLNL especifica uma lista de nomes de objetos de informações sobre autenticação que são usados para fornecer locais de revogação de certificado para permitir verificação aprimorada de certificados TLS.

SSLCRYP
Nos sistemas Windows, UNIX and Linux, defina o atributo do gerenciador de filas **SSLCryptoHardware**. Esse atributo é o nome da sequência de parâmetros que pode ser usada para configurar o hardware criptográfico que você tem no sistema.

SSLEV
Determina se uma mensagem do evento TLS será relatada se um canal que usa TLS falhar ao estabelecer uma conexão TLS.

SSLFIPS
Especifica se apenas algoritmos certificados por FIPS devem ser usados se a criptografia for executada no IBM MQ, em vez de no hardware de criptografia. Se o hardware de criptografia for configurado, os módulos de criptografia fornecidos pelo produto de hardware são usados, e estes podem ser certificados por FIPS em um nível específico. Isto depende do produto de hardware em uso.

SSLKEYR
Em sistemas UNIX, Linux, and Windows, associa um repositório de chaves a um gerenciador de filas. O banco de dados de chaves fica retido em um banco de dados de chaves *GSKit*. O IBM Global Security Kit (GSKit) permite usar a segurança TLS em sistemas Windows, UNIX and Linux.

SSLRKEYC
O número de bytes a serem enviados e recebidos dentro de uma conversa TLS antes que a chave secreta seja renegociada. O número de bytes inclui informações de controle enviadas pelo MCA.

- Os parâmetros de canal a seguir suportam TLS:

CERTLABL
Define um rótulo de certificado pessoal a ser usado.

SSLCAUTH
Define se o IBM MQ requer e valida um certificado do cliente TLS.

SSLCIPH
Especifica a segurança da criptografia e a função (CipherSpec), por exemplo, TLS_RSA_WITH_AES_128_CBC_SHA. O CipherSpec deve corresponder em ambas as extremidades do canal.

SSLPEER
Especifica o nome distinto (identificador exclusivo) de parceiros permitidos.

Esta seção descreve os comandos **setmqaut**, **dspmqaut**, **dmpmqaut**, **rcrmqobj**, **rcdmqimg** e **dspmqfls** para suportar o objeto de informações sobre autenticação. Ela também descreve o comando **runmqckm** (iKeycmd) para gerenciamento de certificados em sistemas UNIX and Linux e a ferramenta **runmqakm** para gerenciamento de certificados no UNIX, Linux, and Windows. Consulte as seções a seguir:

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Gerenciando chaves e certificados

Para obter uma visão geral de segurança do canal usando TLS, veja

- “Protocolos de segurança TLS no IBM MQ” na página 24

Para obter detalhes de comandos MQSC associados ao TLS, veja

- ALTER AUTHINFO
- DEFINE AUTHINFO
- DELETE AUTHINFO

- DISPLAY AUTHINFO

Para obter detalhes de comandos PCF associados ao TLS, veja

- Mudar, copiar e criar objeto de informações sobre autenticação
- Excluir Objeto de Informações sobre Autenticação
- Investigar Objeto de Informações sobre Autenticação

z/OS *Canal de conexão do servidor IBM MQ for z/OS*

O canal SVRCONN do IBM MQ for z/OS não é seguro sem a implementação de autenticação de canal ou a inclusão de uma saída de segurança usando TLS. Os canais SVRCONN não tem uma saída de segurança definida por padrão.

Assuntos de segurança

Os canais SVRCONN não são seguros conforme definidos inicialmente, SYSTEM.DEF.SVRCONN por exemplo. Para assegurar um canal SVRCONN, deve-se configurar a autenticação de canal usando o comando SET CHLAUTH ou instalar uma saída de segurança e implementar o TLS.

Deve-se usar uma saída de segurança de amostra publicamente disponível, gravar uma saída de segurança ou comprar uma saída de segurança.

Existem várias amostras disponíveis que podem ser usadas como um bom ponto de partida para gravar sua própria saída de segurança do canal SVRCONN.

No IBM MQ for z/OS, o membro CSQ4BCX3 em sua biblioteca hlq.SCSQC37S é uma amostra de saída de segurança escrita na linguagem C. A amostra CSQ4BCX3 também é enviada pré-compilada em sua biblioteca hlq.SCSQAUTH.

É possível implementar a saída de amostra CSQ4BCX3 copiando o membro compilado hlq.SCSQAUTH (CSQ4BCX3) em uma biblioteca de carregamento que é alocada para o CSQXLIB DD em seu CHIN Proc. Observe que o CHIN requer que a biblioteca de carregamento seja configurada como "Programa controlado".

Altere o canal SVRCONN para configurar CSQ4BCX3 como a saída de segurança.

V 9.1.4 Quando um cliente se conecta usando esse canal SVRCONN, o CSQ4BCX3 será autenticado usando o par **RemoteUserIdentifier** e **RemotePassword** do MQCD ou na IBM MQ 9.1.4, o par **CSPUserIdPtr** e **CSPPasswordPtr** do MQCSP. Se a autenticação for bem-sucedida, ela copiará **RemoteUserIdentifier** em **MCAUserIdentifier**, mudando o contexto de identidade do encadeamento.

Para o Long Term Support e Continuous Delivery antes da IBM MQ 9.1.4, quando um cliente se conecta usando esse canal SVRCONN, o CSQ4BCX3 será autenticado usando o par **RemoteUserIdentifier** e **RemotePassword** do MQCD. Se a autenticação for bem-sucedida, ela copiará **RemoteUserIdentifier** em **MCAUserIdentifier**, mudando o contexto de identidade do encadeamento.

Se você estiver gravando um cliente IBM MQ Java, será possível usar pop-ups para consultar o usuário e configurar MQEnvironment.userID e MQEnvironment.password. Esses valores serão transmitidos quando a conexão for feita.

Agora que você tem uma saída de segurança funcional, há a preocupação adicional de que o ID de usuário e a senha estão sendo transmitidos em texto sem formatação pela rede quando a conexão é feita, assim como o conteúdo de quaisquer mensagens subsequentes do IBM MQ. É possível usar o TLS para criptografar essas informações de conexão iniciais, bem como o conteúdo de quaisquer mensagens do IBM MQ

exemplo

Para proteger o sistema IBM MQ Explorer canal SVRCONN SYSTEM.ADMIN.SVRCONN conclua as seguintes etapas:

1. Copie hlq.SCSQAUTH (CSQ4BCX3) em uma biblioteca de carregamento que está alocada para o CSQXLIB DD no CHINIT Proc.
2. Verifique se a biblioteca de carregamento é um Programa controlado.
3. Altere o ADMIN.SVRCONN SISTEMA para usar a saída de segurança CSQ4BCX3.
4. No IBM MQ Explorer, clique com o botão direito no nome do z/OS Queue Manager, selecione **Detalhes da conexão** > **Propriedades** > **ID do usuário** e insira seu ID do usuário do z/OS.
5. Conecte-se ao z/OS Queue Manager inserindo uma senha.

Informações Adicionais

Para a saída CSQ4BCX3 executar em um ambiente do Programa controlado, tudo carregado no espaço de endereço CHIN deve ser carregado a partir de uma biblioteca do Programa controlado, por exemplo, todas as bibliotecas no STEPLIB e quaisquer bibliotecas nomeadas no CSQXLIB DD. Para configurar uma biblioteca de carregamento como Programa controlado emita comandos do RACF. No exemplo a seguir, o nome da biblioteca de carregamento é MY.TEST.LOADLIB.

```
RALTER PROGRAM * ADDMEM('MY.TEST.LOADLIB'//NOPADCHK)
SETROPTS WHEN(PROGRAM)REFRESH
```

Para alterar o canal SVRCONN para implementar CSQ4BCX3, emita o seguinte comando IBM MQ :

```
ALTER CHANNEL(SYSTEM ADMIN.SVRCONN) CHLTYPE(SVRCONN) SCYEXIT(CSQ4BCX3)
```

No exemplo acima, o nome do canal SVRCONN que está sendo usado é SYSTEM ADMIN.SVRCONN.

Consulte “Programas de Saída de Canal” na página 106 para obter mais informações sobre saídas do canal.

Tarefas relacionadas

Gravando programas de saída de canal em z/OS

serviços de segurança do SNA LU 6.2

O SNA LU 6.2 oferece criptografia em nível de sessão, autenticação em nível de sessão e autenticação em nível de conversa.

Nota: Esta coleção de tópicos supõe que você tenha um entendimento básico de Systems Network Architecture (SNA). A outra documentação referida nesta seção contém uma breve introdução aos conceitos e terminologia relevantes. Se precisar de uma introdução técnica mais abrangente ao SNA, consulte *Systems Network Architecture Technical Overview*, GC30-3073.

O SNA LU 6.2 oferece três serviços de segurança:

- Criptografia em nível de sessão
- Autenticação em nível de sessão
- Autenticação em nível de conversação

Para criptografia em nível de sessão e autenticação em nível de sessão, o SNA utiliza o algoritmo do *DES (Data Encryption Standard)*. O algoritmo do DES é um algoritmo de cifra de bloco, que utiliza uma chave simétrica para criptografar e decriptografar dados. O bloco e a chave têm oito bytes de comprimento.

Criptografia em nível de sessão

A *Criptografia em nível de sessão* criptografa e decriptografa dados de sessão utilizando o algoritmo do DES. Ela pode portanto, ser utilizada para fornecer um serviço de confidencialidade em nível de link em canais do SNA LU 6.2.

LUs (Logical units) podem fornecer criptografia de dados obrigatória (ou necessária), criptografia de dados seletiva ou nenhuma criptografia de dados.

Em uma *sessão criptográfica obrigatória*, uma LU criptografa todas as unidades de pedido de dados de transmissão e decriptografa todas as unidades de pedido de dados de recepção.

Em uma *sessão criptográfica seletiva*, uma LU criptografa apenas as unidades de pedido de dados especificadas pelo TP (transaction program) de envio. A LU de envio indica que os dados são criptografados definindo um indicador no cabeçalho de pedido. Verificando esse indicador, a LU de recebimento pode definir quais unidades de pedido serão decriptografadas antes de transferi-las para o TP de recebimento.

Em uma rede SNA, os MCAs do IBM MQ são programas de transação. Os MCAs não solicitam criptografia para os dados que enviam. Portanto, a criptografia de dados seletiva não é uma opção; apenas a criptografia de dados obrigatória ou nenhuma criptografia de dados é possível em uma sessão.

Para obter informações sobre como implementar a criptografia de dados obrigatória, consulte a documentação para seu subsistema SNA. Consulte a mesma documentação para obter informações sobre formas mais fortes de criptografia que podem estar disponíveis para uso em sua plataforma, como a criptografia de 24 bytes do Padrão de Criptografia de Dados triplo no z/OS.

Para obter mais informações gerais sobre criptografia em nível de sessão, consulte *Systems Network Architecture LU 6.2 Reference: Peer Protocols* , SC31-6808.

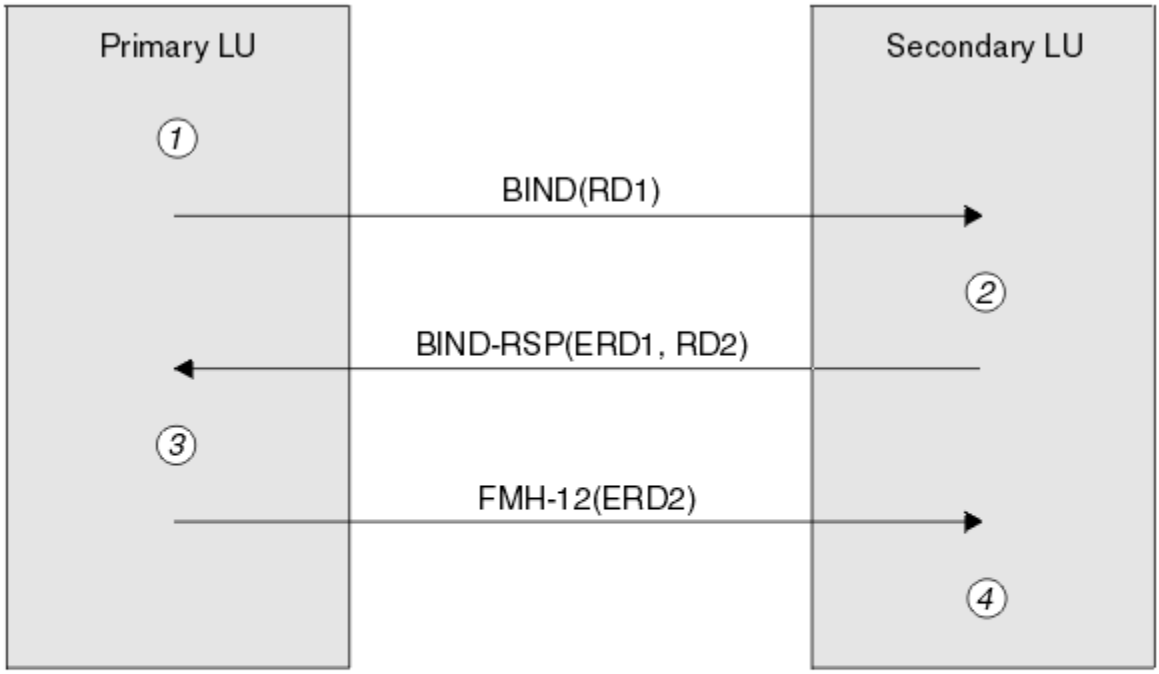
Autenticação em nível de sessão

A *Autenticação em nível de sessão* é um protocolo de segurança em nível de sessão que permite que duas LUs autentiquem uma à outra enquanto ativam a sessão. Também conhecida como *verificação de LU-LU*.

Como uma LU é efetivamente o "gateway" para um sistema a partir da rede, você pode considerar esse nível de autenticação como suficiente em certas circunstâncias. Por exemplo, se seu gerenciador de filas precisar trocar mensagens com um gerenciador de filas remoto sendo executado em um ambiente controlado e confiável, você pode estar preparado para confiar nas identidades dos componentes restantes do sistema remoto após a autenticação da LU.

A autenticação em nível de sessão é conseguida por cada LU verificando a senha de seu parceiro. A senha é denominada uma *senha de LU-LU* porque é estabelecida uma senha entre cada par de LUs. A maneira que uma senha de LU-LU é estabelecida depende da implementação e está fora do escopo do SNA.

Figura 12 na página 119 ilustra os fluxos para autenticação em nível de sessão.



Legend:

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

Figura 12. Fluxos para autenticação em nível de sessão

O protocolo para autenticação em nível de sessão é o seguinte. Os números no procedimento correspondem aos números em Figura 12 na página 119.

1. A LU primária gera um valor de dados aleatório (RD1) e o envia para a LU secundária no pedido BIND.
2. Quando a LU secundária recebe o pedido BIND com os dados aleatórios, ela criptografa os dados utilizando o algoritmo do DES com sua cópia da senha de LU-LU como a chave. A LU secundária, então, gera um segundo valor de dados aleatórios (RD2) e envia-o com os dados criptografados (ERD1) para a LU primária na resposta BIND.
3. Quando a LU primária recebe a resposta BIND, ela calcula sua própria versão dos dados criptografados a partir dos dados aleatórios gerados originalmente. Ela o faz utilizando o algoritmo do DES com sua cópia da senha de LU-LU como a chave. Então ela compara sua versão com os dados criptografados recebidos na resposta BIND. Se os dois valores forem iguais, a LU primária saberá que a LU secundária tem a mesma senha que ela e a LU secundária será autenticada. Se os dois valores não corresponderem, a LU primária encerrará a sessão.

   A LU primária criptografa os dados aleatórios recebidos na resposta BIND e envia os dados criptografados (ERD2) para a LU secundária em um FMH-12 (Function Management Header 12).
4. Quando a LU secundária recebe o FMH-12, ela calcula sua própria versão dos dados criptografados a partir dos dados aleatórios gerados por ela. Então ela compara sua versão com os dados criptografados recebidos no FMH-12. Se os dois valores forem iguais, a LU primária será autenticada. Se os dois valores não corresponderem, a LU secundária encerrará a sessão.

Em uma versão aperfeiçoada do protocolo, que fornece melhor proteção contra ataques humano intermediários, a LU secundária calcula um DES MAC (Message Authentication Code) a partir de RD1,

RD2 e o nome completo da LU secundária, utilizando sua cópia da senha de LU-LU como a chave. A LU secundária envia o MAC para a LU primária na resposta BIND em vez de ERD1.

A LU primária autentica a LU secundária calculando sua própria versão do MAC, a qual ela compara com o MAC recebido na resposta BIND. Em seguida a LU primária calcula um segundo MAC a partir de RD1 e RD2, e envia o MAC para a LU secundária no FMH-12 em vez do ERD2.

A LU secundária autentica a LU primária calculando sua própria versão do segundo MAC, a qual ela compara com o MAC recebido no FMH-12.

Para obter informações sobre como configurar a autenticação em nível de sessão, consulte a documentação para seu subsistema SNA. Para obter mais informações gerais sobre autenticação de nível de sessão, consulte *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Autenticação em nível de conversação
Quando um TP local tenta alocar uma conversação com um TP parceiro, a LU local envia um pedido de anexo para a LU parceira, pedindo que anexe o TP parceiro. Em certas circunstâncias, o pedido de anexo pode conter informações de segurança que a LU parceira pode utilizar para autenticar o TP local. Isso é conhecido como *autenticação em nível de conversação* ou *verificação do usuário final*.

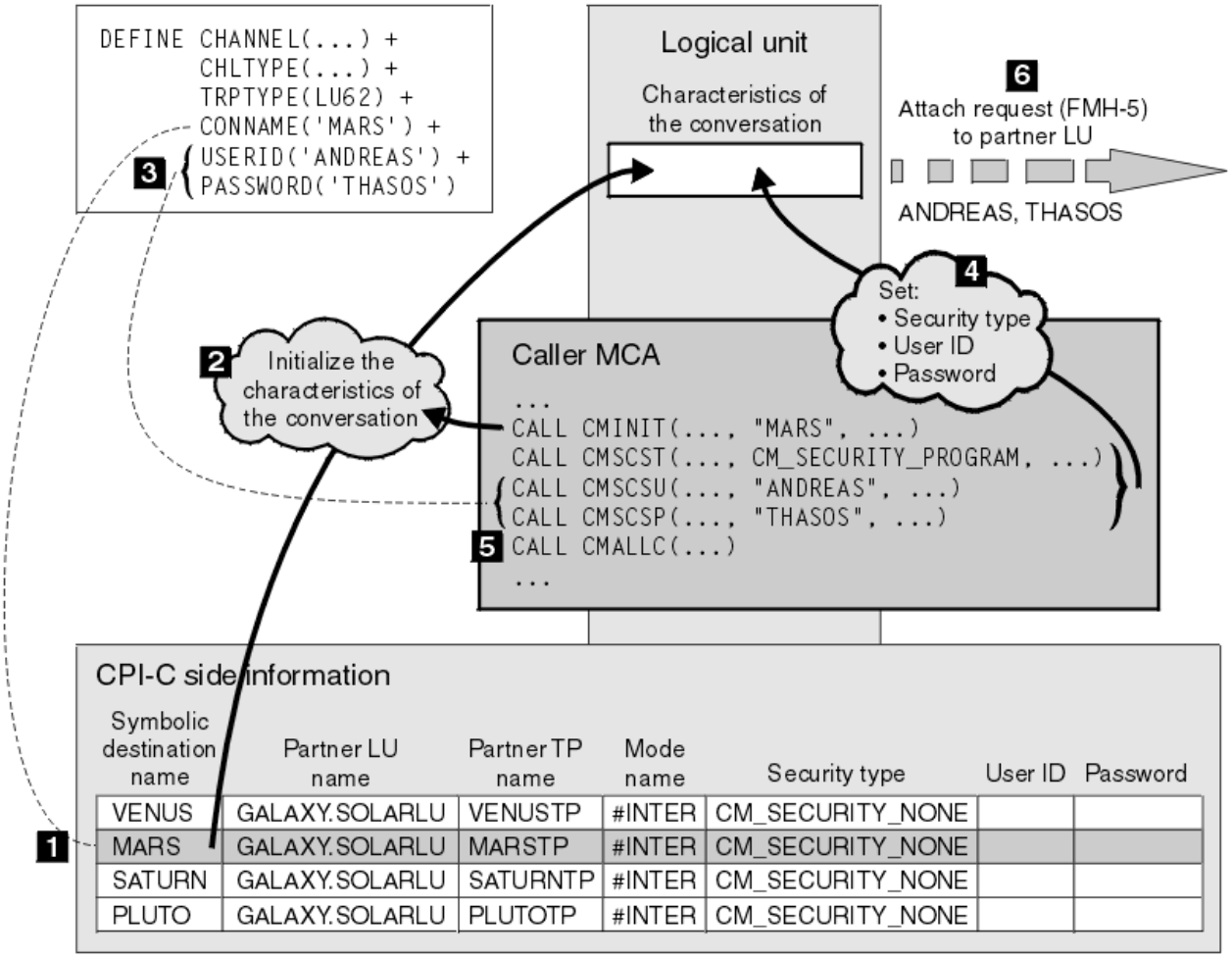
Os tópicos a seguir descrevem como o IBM MQ fornece suporte para autenticação em nível de conversação.

Para obter mais informações sobre autenticação em nível de conversação, consulte *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808. Para obter informações específicas para o z/OS, consulte *z/OS Planejamento de MVS: gerenciamento de APPC/MVS*, SA22-7599.

Para obter mais informações sobre o CPI-C, consulte *Common Programming Interface Communications CPI-C Specification*, SC31-6180. Para obter mais informações sobre APPC/MVS TP Conversation Callable Services, veja *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Suporte para autenticação de nível de conversa em IBM i, UNIXe Windows
Use este tópico para obter uma visão geral de como a autenticação em nível de conversa funciona no IBM i, UNIX e Windows.

O suporte para autenticação em nível de conversa no IBM i, UNIX e Windows é ilustrado em Figura 13 na página 121. Os números no diagrama correspondem aos números na descrição a seguir.



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		

Figura 13. Suporte do IBM MQ para autenticação de nível de conversa

No IBM i, UNIX e Windows, um MCA usa chamadas Common Programming Interface Communications (CPI-C) para se comunicar com um MCA parceiro por meio de uma rede SNA. Na definição de canal na extremidade do responsável pela chamada de um canal, o valor do parâmetro CONNAME é um nome de destino simbólico, que identifica uma entrada de informações secundárias de CPI-C (1). Essa entrada especifica:

- O nome da LU parceira
- O nome do TP parceiro, que é um MCA receptor da chamada
- O nome do modo a ser utilizado para a conversação

Uma entrada de informações secundárias também pode especificar as seguintes informações de segurança:

- Um tipo de segurança.

  Os tipos de segurança geralmente implementados são CM_SECURITY_NONE, CM_SECURITY_PROGRAM e CM_SECURITY_SAME, mas outros são definidos na especificação de CPI-C.
- Um ID do usuário.
- Uma senha.

Um MCA originador da chamada se prepara para alocar uma conversação com um MCA receptor da chamada emitindo a chamada de CPI-C CMINIT, utilizando o valor de CONNAME como um dos parâmetros na chamada. A chamada CMINIT identifica, para o benefício da LU local, a entrada de informações secundárias que o MCA pretende utilizar para a conversação. A LU local usa os valores nesta entrada para inicializar as características da conversa (2).

O MCA do responsável pela chamada verifica os valores dos parâmetros USERID e PASSWORD na definição de canal (3). Se USERID for definido, o MCA do responsável pela chamada emite as seguintes chamadas de CPI-C (4):

- CMSCST, para definir o tipo de segurança para a conversação para CM_SECURITY_PROGRAM.
- CMSCSU, para definir o ID de usuário para a conversação para o valor de USERID.
- CMSCSP, para definir a senha para a conversação para o valor de PASSWORD. CMSCSP não é chamado a menos que PASSWORD seja definido.

O tipo de segurança, ID de usuário e senha definidos por essas chamadas substituem quaisquer valores adquiridos anteriormente da entrada de informações secundárias.

O MCA do responsável pela chamada emite a chamada de CPI-C CMALLC para alocar a conversa (5). Em resposta a essa chamada, a LU local envia uma solicitação de conexão (Function Management Header 5 ou FMH-5) para a LU do parceiro (6).

Se a LU parceira aceitar um ID de usuário e uma senha, os valores de USERID e de PASSWORD serão incluídos no pedido de anexo. Se a LU parceira não aceitar um ID de usuário e uma senha, os valores não serão incluídos no pedido de anexo. A LU local descobre se a LU parceira aceitará um ID de usuário e uma senha como parte de uma troca de informações quando as LUs se ligarem para formar uma sessão.

Em uma versão posterior do pedido de anexo, um substituto de senha pode fluir entre as LUs em vez de uma senha propriamente dita. Um substituto de senha é um MAC (Message Authentication Code) ou uma compilação de mensagens SHA-1, formados a partir da senha. Substitutos de senha podem ser utilizados apenas se ambas as LUs os suportarem.

Quando a LU parceira recebe um pedido de anexo de entrada contendo um ID de usuário e uma senha, ela pode utilizar o ID de usuário e a senha para os objetivos de identificação e de autenticação. Referindo-se às listas de controle de acesso, a LU parceira também pode determinar se o ID de usuário tem autoridade para alocar uma conversação e anexar o MCA receptor da mensagem.

Além disso, o MCA receptor da mensagem pode ser executado sob o ID de usuário incluído no pedido de anexo.Nesse caso, o ID de usuário se torna o ID de usuário padrão para o MCA receptor da chamada e é utilizado para verificações de autoridade quando o MCA tenta se conectar ao gerenciador de filas. Ele também pode ser utilizado para verificações de autoridade subseqüentemente quando o MCA tenta acessar os recursos do gerenciador de filas.

A forma como um ID de usuário e uma senha em um pedido de anexo podem ser utilizados para identificação, autenticação e controle de acesso depende da implementação. Para obter informações específicas para seu subsistema SNA, consulte a documentação apropriada.

Se USERID não for definido, o MCA originador da chamada não chamará CMSCST, CMSCSU e CMSCSP. Nesse caso, as informações de segurança que circulam em um pedido de anexo são determinadas unicamente pelo que for especificado na entrada de informações secundárias e o que a LU parceira irá aceitar.

Autenticação em nível de conversa e IBM MQ for z/OS
Use este tópico para obter uma visão geral de como a autenticação em nível de conversa funciona, no z/OS.

No IBM MQ for z/OS, MCAs não usam CPI-C. Em vez disso, eles utilizam APPC/MVS TP Conversation Callable Services, uma implementação do APPC (Advanced Program-to-Program Communication), que tem alguns recursos do CPI-C. Quando um MCA originador da chamada aloca uma conversação, um tipo de segurança SAME é especificado na chamada. Portanto, como uma LU de APPC/MVS suporta verificação persistente apenas para conversações de recepção, não para conversações de transmissão, existem duas possibilidades:

- Se a LU parceira confiar na LU de APPC/MVS e aceitar um ID de usuário já verificado, a LU de APPC/MVS enviará um pedido de anexo contendo:
  - O ID de usuário do espaço de endereço inicializador de canais
  - Um nome de perfil de segurança o qual, se RACF for usado, será o nome do grupo de conexão atual do ID do usuário do espaço de endereço do inicializador de canais

  - Um indicador já verificado
- Se a LU parceira não confiar na LU de APPC/MVS e não aceitar um ID de usuário já verificado, a LU de APPC/MVS enviará um pedido de anexo não contendo informações de segurança.

No IBM MQ for z/OS, os parâmetros USERID e PASSWORD no comando DEFINE CHANNEL não podem ser usados para um canal de mensagens e só serão válidos na extremidade de conexão do cliente de um canal MQI. Portanto, um pedido de anexo de uma LU do APPC/MVS nunca contém valores especificados por esses parâmetros.

Segurança para Clusters de Gerenciadores de Filas

Embora o uso dos clusters de gerenciadores de filas possa ser conveniente, você deve prestar muita atenção à sua segurança.

Um *cluster de gerenciadores de filas* é uma rede de gerenciadores de filas que estão associados logicamente de alguma maneira. Um gerenciador de filas que seja um membro de um cluster é chamado um *gerenciador de filas de cluster*.

Uma fila que pertença a um gerenciador de filas de cluster pode ser tornada conhecida a outros gerenciadores de filas no cluster. Uma fila assim é chamada uma *fila de cluster*. Qualquer gerenciador de filas em um cluster pode enviar mensagens para filas do cluster sem precisar de nenhum dos seguintes:

- Uma definição explícita de fila remota para cada fila do cluster
- Canais explicitamente definidos para e de cada gerenciador de filas remotas
- Uma fila de transmissão separada para cada canal de transmissão

É possível criar um cluster no qual dois ou mais gerenciadores de filas são clones. Isso significa que eles possuem ocorrências das mesmas filas locais, incluindo quaisquer filas locais declaradas como filas de cluster, e podem suportar ocorrências dos mesmos aplicativos do servidor.

Quando um aplicativo conectado a um gerenciador de filas do cluster envia uma mensagem a uma fila de clusters que tem uma instância em cada um dos gerenciadores de filas clonados, o IBM MQ decide para qual gerenciador de filas enviá-la. Quando muitos aplicativos enviam mensagens para a fila de clusters, o IBM MQ equilibra a carga de trabalho entre todos os gerenciadores de filas que possuem uma instância da fila. Se um dos sistemas que hospedam um gerenciador de filas clonado falhar, o IBM MQ continuará a equilibrar a carga de trabalho entre os gerenciadores de filas restantes até que o sistema que falhou seja reiniciado.

Se você estiver utilizando clusters de gerenciadores de filas, precisará levar em consideração as seguintes questões de segurança:

- Permitir que somente gerenciadores de filas selecionados enviem mensagens a seu gerenciador de filas
- Permitir que somente usuários selecionados de um gerenciador de filas remoto enviem mensagens a uma fila no seu gerenciador de filas
- Permitir que aplicativos conectados a seu gerenciador de filas enviem mensagens somente a filas remotas selecionadas

Essas considerações são relevantes mesmo que você não esteja utilizando clusters, mas se tornam mais importantes se estiverem sendo utilizados clusters.

Se um aplicativo puder enviar mensagens a uma fila de cluster, ele poderá enviar mensagens a qualquer outra fila do cluster sem precisar de definições adicionais de filas remotas, filas de transmissão ou canais. Portanto, torna-se mais importante considerar se é preciso restringir o acesso às filas do cluster em seu gerenciador de filas, e restringir as filas do cluster às quais os aplicativos podem enviar mensagens.

Existem algumas considerações de segurança adicionais que são relevantes somente se você estiver utilizando clusters de gerenciadores de filas:

- Permitir que somente gerenciadores de filas selecionados se unam a um cluster
- Forçando Gerenciadores de Filas Indesejáveis a Sair de um Cluster

Para obter mais informações sobre todas essas considerações, consulte Mantendo os Clusters Seguros.

z/OS Para considerações específicas para o IBM MQ for z/OS, consulte “Segurança em clusters de gerenciadores de filas no z/OS” na página 266.

Tarefas relacionadas

“Impedindo que gerenciadores de filas recebam mensagens” na página 467
É possível evitar que um gerenciador de filas do cluster receba mensagens que ele não está autorizado a receber, usando programas de saída.

Segurança para o Publicar/assinar do IBM MQ

Há considerações de segurança adicionais se você estiver usando o publicar/assinar do IBM MQ.

Em um sistema de publicação/assinatura, há dois tipos de aplicativo: publicador e assinante. Os *publicadores* fornecem informações no formato de mensagens do IBM MQ. Quando um publicador publica uma mensagem, ele especifica um *tópico*, que identifica o assunto das informações dentro da mensagem.

Assinantes são os consumidores das informações que são publicadas. Um assinante especifica os tópicos nos quais está interessado inscrevendo-se neles.

O *gerenciador de filas* é um aplicativo fornecido com o Publicar/assinar do IBM MQ. Ele recebe as mensagens publicadas dos publicadores e pedidos de assinatura dos assinantes, e encaminha as mensagens publicadas aos assinantes. São enviadas a um assinante somente as mensagens sobre os tópicos que ele assinou.

Para obter mais informações, consulte Segurança da Publicação/Assinatura.

Segurança de multicast

Use estas informações para entender por que os processos de segurança podem ser necessários com o IBM MQ Multicast.

O IBM MQ Multicast não tem segurança integrada. As verificações de segurança são manipuladas no gerenciador de filas no tempo de MQOPEN, e a configuração do campo MQMD é manipulada pelo cliente. Alguns aplicativos na rede podem não ser os aplicativos IBM MQ (Por exemplo, os aplicativos LLM, consulte Interoperabilidade multicast com IBM MQ Sistema de mensagens de baixa latência para obter mais informações), portanto, você pode precisar implementar seus próprios procedimentos de segurança porque os aplicativos de recebimento não podem ter certeza da validade dos campos de contexto.

Há três processos de segurança a serem considerados:

Controle de Acesso

O controle de acesso em IBM MQ é baseado nos IDs do usuário. Para obter informações adicionais sobre este assunto, consulte “Controle de acesso para clientes” na página 98.

Segurança de rede

Uma rede isolada pode ser uma opção de segurança viável para evitar mensagens falsas. É possível para um aplicativo no endereço de grupo multicast publicar mensagens maliciosas usando as funções de comunicação nativa, que são indistinguíveis a partir das mensagens do MQ por virem de um aplicativo no mesmo endereço de grupo multicast.

Também é possível para um cliente no endereço de grupo multicast receber mensagens que foram destinadas a outros clientes no mesmo endereço de grupo multicast.

Isolar a rede multicast assegura que apenas clientes e aplicativos válidos possuam acesso. Esta precaução de segurança pode impedir as mensagens maliciosas de entrar e as informação confidenciais de sair.

Para obter informações sobre endereços de rede de grupo multicast, consulte: Configurando a rede apropriada para tráfego multicast

Assinaturas Digitais

Uma assinatura digital é formada pela criptografia de uma representação de uma mensagem. A criptografia utiliza a chave privada do assinante e, para eficiência, geralmente opera em uma compilação de mensagens, ao invés de na mensagem em si. Assinar digitalmente uma mensagem antes de um MQPUT é uma boa precaução de segurança, mas esse processo pode ter um efeito negativo no desempenho se houver um grande volume de mensagens.

As assinaturas digitais variam com os dados que estão sendo assinados. Se duas mensagens diferentes forem assinadas digitalmente pela mesma entidade, as duas assinaturas diferirão, mas ambas poderão ser verificadas com a mesma chave pública, ou seja, a chave pública da entidade que assinou as mensagens.

Conforme mencionado anteriormente nesta seção, pode ser possível para um aplicativo no endereço de grupo multicast publicar mensagens maliciosas usando funções de comunicação nativa, que são indistinguíveis a partir de mensagens do MQ. As assinaturas digitais fornecem prova de origem, e somente o emissor conhece a chave privada, que fornece forte evidência de que o emissor é o originador da mensagem.

Para obter informações adicionais sobre este assunto, consulte "Conceitos criptográficos" na página 7.

Firewalls e intermediário da Internet

Você normalmente usa um firewall para evitar o acesso a partir de endereços IP hostis, por exemplo, em um ataque de negação de serviço. No entanto, você pode precisar bloquear temporariamente endereços IP dentro do IBM MQ, talvez enquanto aguarda um administrador de segurança atualizar as regras de firewall.

Para bloquear um ou mais endereços IP, crie um registro de autenticação de canal do tipo ADDRESSMAP ou BLOCKADDR. Para obter informações adicionais, consulte "Bloqueando Endereços IP Específicos" na página 388.

Segurança para IBM MQ Internet Pass-Thru

O IBM MQ Internet Pass-Thru pode simplificar a comunicação por meio de um firewall, mas isso tem implicações de segurança.

O IBM MQ Internet Pass-Thru (MQIPT) é um componente opcional do IBM MQ que pode ser usado para implementar soluções do sistema de mensagens entre sites remotos através da Internet.

O MQIPT permite que dois gerenciadores de filas troquem mensagens ou que um aplicativo cliente do IBM MQ conecte-se a um gerenciador de filas através da Internet sem requerer uma conexão TCP/IP direta. Isso é útil se um firewall proibir uma conexão TCP/IP direta entre dois sistemas. Ele torna passagem de fluxos de protocolo do canal do IBM MQ para dentro e para fora de um firewall mais simples e mais gerenciável, tunelando os fluxos dentro do HTTP ou agindo como proxy. Usando a Segurança da Camada de Transporte (TLS), ela também pode ser usada para criptografar e decriptografar mensagens que são enviadas por meio da Internet.

Quando o seu sistema IBM MQ se comunica com o MQIPT, a menos que você esteja usando o modo de proxy SSL no MQIPT, certifique-se de que o CipherSpec usado por IBM MQ corresponde ao CipherSuite usado pelo MQIPT:

- Quando o MQIPT está agindo como o servidor TLS e o IBM MQ está se conectando como o cliente TLS, o CipherSpec usado pelo IBM MQ deve corresponder a um CipherSuite que está ativado no conjunto de chaves relevante do MQIPT.
- Quando o MQIPT está agindo como o cliente TLS e está se conectando a um servidor TLS do IBM MQ, o CipherSuite do MQIPT deve corresponder ao CipherSpec definido no canal de recebimento do IBM MQ.

Se você migrar do MQIPT para o suporte de TLS integrado do IBM MQ, transfira os certificados digitais do conjunto de chaves do MQIPT usando **mqiptKeyman** ou **mqiptKeycmd**.

Para obter mais informações, consulte IBM MQ Internet Pass-Thru.

z/OS Lista de verificação da implementação de segurança do IBM MQ for z/OS

Este tópico fornece um procedimento passo a passo que pode ser usado para descobrir e definir a implementação de segurança para cada um de seus gerenciadores de filas do IBM MQ.

O RACF fornece definições para as classes de segurança do IBM MQ em sua tabela descritora de classe estática (CDT) fornecida. Conforme você trabalha através da lista de verificação, é possível determinar quais dessas classes sua configuração requer. Deve-se assegurar que eles estejam ativados conforme descrito em "Classes de segurança do RACF" na página 185.

Consulte outras seções para obter detalhes, em particular "Perfis usados para controlar o acesso a recursos do IBM MQ" na página 196.

Se for necessária a verificação de segurança, siga esta lista de verificação para implementá-la:

1. Ative a classe RACF MQADMIN (perfis em maiúsculas) ou MXADMIN (perfis compostos por letras maiúsculas e minúsculas).
   - Deseja segurança no nível do grupo de filas compartilhadas, no nível do gerenciador de filas ou em uma combinação de ambos?

     Consulte "Perfis para controlar a segurança no nível do grupo de filas compartilhadas ou do gerenciador de filas" na página 191.
2. Você precisa de segurança de conexão?
   - **Sim**: Ative a classe MQCONN. Defina os perfis de conexão apropriados em qualquer nível do gerenciador de filas ou no nível do grupo de filas compartilhadas na classe MQCONN. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.

     Nota: Somente usuários da solicitação de API `MQCONN` ou IDs do usuário do espaço de endereço do CICS ou IMS precisam ter acesso ao perfil de conexão correspondente.
   - **Não**: defina um perfil hlq.NO.CONNECT.CHECKS em qualquer nível do gerenciador de filas ou nível do grupo de filas compartilhadas na classe MQADMIN ou MXADMIN.
3. Você precisa de verificação de segurança em comandos?
   - **Sim**: Ative a classe MQCMDS. Defina os perfis de comando apropriados em qualquer nível do gerenciador de filas ou no nível do grupo de filas compartilhadas na classe MQCMDS. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.

     Se você estiver usando um grupo de filas compartilhadas, poderá ser necessário incluir os IDs de usuário usados pelo próprio gerenciador de filas e o inicializador de canais. Consulte o "Configurando a segurança do recurso do IBM MQ for z/OS" na página 257.
   - **Não**: defina um perfil hlq.NO.CMD.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQADMIN ou MXADMIN.
4. Você precisa de segurança nos recursos usados em comandos?
   - **Sim**: assegure-se de que a classe MQADMIN ou MXADMIN esteja ativa. Defina os perfis apropriados para proteger recursos em comandos no nível do gerenciador de filas ou no nível do grupo de filas compartilhadas na classe MQADMIN ou MXADMIN. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis. Configure o parâmetro CMDUSER em CSQ6SYSP para o ID de usuário padrão a ser usado para verificações de segurança de comando.

     Se você estiver usando um grupo de filas compartilhadas, poderá ser necessário incluir os IDs de usuário usados pelo próprio gerenciador de filas e o inicializador de canais. Consulte o "Configurando a segurança do recurso do IBM MQ for z/OS" na página 257.
   - **Não**: Defina um perfil hlq.NO.CMD.RESC.CHECKS para o gerenciador de filas necessário ou grupo de filas compartilhadas na classe MQADMIN ou MXADMIN.
5. Você precisa de segurança da fila?

- **Sim**: ative a classe MQQUEUE ou MXQUEUE. Defina os perfis de fila apropriados para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQQUEUE ou MXQUEUE. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.
- **Não**: defina um perfil hlq.NO.QUEUE.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQADMIN ou MXADMIN.

6. Você precisa de segurança do processo?
   - **Sim**: ative a classe MQPROC ou MXPROC. Defina os perfis de processo apropriados no nível do gerenciador de filas ou no nível do grupo de filas compartilhadas e permita que os usuários ou grupos apropriados acessem esses perfis.
   - **Não**: defina um perfil hlq.NO.PROCESS.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas apropriado na classe MQADMIN ou MXADMIN.
7. Você precisa de segurança da lista de nomes?
   - **Sim**: ative a classe MQNLIST ou MXNLIST. Defina os perfis de lista de nomes apropriados no nível do gerenciador de filas ou no nível do grupo de filas compartilhadas na classe MQNLIST ou MXNLIST. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.
   - **Não**: defina um perfil hlq.NO.NLIST.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQADMIN ou MXADMIN.
8. Você precisa de segurança do tópico?
   - **Sim**: Ative a classe MXTOPIC. Defina os perfis de tópico apropriados em qualquer nível do gerenciador de filas ou no nível do grupo de filas compartilhadas na classe MXTOPIC. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.
   - **Não**: defina um perfil hlq.NO.TOPIC.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQADMIN ou MXADMIN.
9. Algum usuário precisa proteger o uso das opções `MQOPEN` ou `MQPUT1` com relação ao uso do contexto?
   - **Sim**: assegure-se de que a classe MQADMIN ou MXADMIN esteja ativa. Defina os perfis hlq.CONTEXT.queuename no nível da fila, do gerenciador de filas ou do grupo de filas compartilhadas na classe MQADMIN ou MXADMIN. Depois, permita aos usuários ou grupos apropriados o acesso a esses perfis.
   - **Não**: Defina um perfil hlq.NO.CONTEXT.CHECKS para o gerenciador de filas necessário ou grupo de filas compartilhadas na classe MQADMIN ou MXADMIN.
10. Você precisa proteger o uso de IDs de usuários alternativos?
    - **Sim**: assegure-se de que a classe MQADMIN ou MXADMIN esteja ativa. Defina os perfis hlq.ALTERNATE.USER *alternateuserid* apropriados para o gerenciador de filas ou grupo de filas compartilhadas necessário e permita que os usuários ou grupos necessários acessem esses perfis.
    - **Não**: defina o perfil hlq.NO.ALTERNATE.USER.CHECKS para o gerenciador de filas ou grupo de filas compartilhadas necessário na classe MQADMIN ou MXADMIN.
11. Você precisa customizar quais IDs de usuário devem ser usados para verificações de segurança do recurso por meio do RESLEVEL?
    - **Sim**: assegure-se de que a classe MQADMIN ou MXADMIN esteja ativa. Defina um perfil hlq.RESLEVEL em nível de gerenciador de filas ou nível de grupo de filas compartilhadas na classe MQADMIN ou MXADMIN. Em seguida, permita que os usuários ou grupos requeridos acessem o perfil.
    - **Não**: assegure-se de que não existam perfis genéricos na classe MQADMIN ou MXADMIN que podem se aplicar a hlq.RESLEVEL. Defina um perfil hlq.RESLEVEL para o gerenciador de filas ou grupo de filas compartilhadas necessário e certifique-se de que nenhum usuário ou grupo tenha acesso a ele.
12. Você precisa impor 'tempo limite' em IDs de usuários não usados a partir do IBM MQ?

- **Sim**: Determine quais valores de tempo limite você gostaria de usar e emita o comando MQSC ALTER SECURITY para alterar os parâmetros TIMEOUT e INTERVAL.
- **Não**: Emita o comando MQSC ALTER SECURITY para configurar o valor de INTERVAL para zero.

Nota: Atualize o conjunto de dados de entrada de inicialização do CSQINP1 usado pelo seu subsistema para que o comando MQSC ALTER SECURITY seja emitido automaticamente quando o gerenciador de filas for iniciado.

13. Você usa enfileiramento distribuído?
    - **Sim**: use os registros de autenticação de canal. Para obter mais informações, consulte "Registros de Autenticação de Canal" na página 49.
    - Também é possível determinar o valor de atributo MCAUSER apropriado para cada canal, ou fornecer as saídas de segurança de canais adequadas.
14. Deseja usar a Segurança da Camada de Transporte (TLS)?
    - **Sim**: para especificar que qualquer usuário que apresenta um certificado pessoal TLS contendo um DN especificado deve usar um MCAUSER específico, configure um registro de autenticação de canal do tipo SSLPEERMAP. É possível especificar um único nome distinto ou um padrão incluindo curingas.
    - Planeje sua infraestrutura do TLS. Instale o recurso de SSL do Sistema do z/OS. No RACF, configure seus filtros de nome de certificado (CNFs), se você os estiver usando, e seus certificados digitais. Configure o conjunto de chaves SSL. Certifique-se de que o atributo do gerenciador de filas SSLKEYR não esteja em branco e aponte para o conjunto de chaves de SSL. Além disso, assegure-se de que o valor de SSLTASKS seja pelo menos 2.
    - **Não**: Assegure-se de que SSLKEYR esteja em branco e SSLTASKS seja zero.

    Para obter detalhes adicionais sobre TLS, veja "Protocolos de segurança TLS no IBM MQ" na página 24.
15. Você usa clientes?
    - **Sim**: use os registros de autenticação de canal.
    - Também é possível determinar o valor de atributo MCAUSER apropriado para cada canal de conexão do servidor, ou fornecer saídas de segurança de canais adequadas, se necessário.
16. Verifique suas configurações do comutador.

    O IBM MQ emite mensagens quando o gerenciador de filas é iniciado que exibem suas configurações de segurança. Use essas mensagens para determinar se seus comutadores estão configurados corretamente.
17. Você envia senhas a partir de aplicativos clientes?
    - **Sim**: assegure-se de que o recurso z/OS esteja instalado e o Recurso de serviços criptográficos (ICSF) seja iniciado para melhor proteção.
    - **Não**: é possível ignorar a mensagem de erro relatando que o ICSF não foi iniciado.

    Para obter informações adicionais sobre o ICSF, consulte "Usando o Integrated Cryptographic Service Facility (ICSF)" na página 266

Configurar a segurança

Esta coleção de tópicos contém informações específicas para sistemas operacionais diferentes e para a utilização de clientes.

ULW Configurando a Segurança em UNIX, Linux, and Windows

Considerações de segurança específicas para sistemas UNIX, Linux, and Windows .

Gerenciadores de filas do IBM MQ transferem informações que são potencialmente de valor, portanto, é necessário usar um sistema de autoridade para assegurar que usuários não autorizados não possam acessar seus gerenciadores de filas. Considere os seguintes tipos de controles de segurança:

Quem pode administrar o IBM MQ
É possível definir o conjunto de usuários que pode emitir comandos para administrar o IBM MQ.

Quem pode usar objetos do IBM MQ
É possível definir quais usuários (geralmente aplicativos) podem usar chamadas MQI e comando de PCF para fazer o seguinte:

- Quem pode se conectar a um gerenciador de filas.
- Quem pode acessar objetos (filas, definições de processos, listas de nomes, canais, canais de conexão do cliente, listeners, serviços e objetos de informações sobre autenticação) e que tipo de acesso eles têm a esses objetos.
- Quem pode acessar mensagens do IBM MQ.
- Quem pode acessar as informações de contexto associadas a uma mensagem.

Segurança de canal
É necessário assegurar que os canais usados para enviar mensagens para sistemas remotos possam acessar os recursos necessários.

É possível usar recursos de operação padrão para conceder acesso a bibliotecas de programas, bibliotecas de link do MQI e comandos. No entanto, o diretório que contém as filas e outros dados do gerenciador de filas é privado ao IBM MQ; não use comandos do sistema operacional padrão para conceder ou revogar autorizações para recursos do MQI.

ULW Como as Autorizações funcionam no UNIX, Linux, and Windows

As tabelas de especificação de autorização nos tópicos desta seção definem precisamente como as autorizações funcionam e as restrições que se aplicam.

As tabelas aplicam-se a estas situações:

- Aplicativos que emitem chamadas MQI
- Programas de administração que emitem comandos MQSC como PCFs Escape
- Programas de administração que emitem comando de PCF

Nesta seção, as informações são apresentadas como um conjunto de tabelas que especificam o seguinte:

Ação a ser executada
Opção de MQI, comando MQSC ou comando PCF.

Objeto de controle de acesso
Fila, processo, gerenciador de filas, lista de nomes, informações sobre autenticação, canal, canal de conexão do cliente, listener ou serviço.

Authorization required
Expressa como uma constante MQZAO_.

Nas tabelas, as constantes prefixadas com MQZAO_ correspondem às palavras-chave na lista de autorização para o comando `setmqaut` da entidade específica. Por exemplo, MQZAO_BROWSE corresponde à palavra-chave `+browse`, MQZAO_SET_ALL_CONTEXT corresponde à palavra-chave `+setall`, etc. Essas constantes são definidas no arquivo de cabeçalho cmqzc.h, fornecido com o produto.

ULW *Autorizações para Chamadas MQI*

MQCONN, **MQOPEN**, **MQPUT1** e **MQCLOSE** podem requerer verificações de autorização. As tabelas deste tópico resumem as autorizações necessárias para cada chamada.

Um aplicativo terá permissão para emitir chamadas MQI e opções específicas somente se o identificador de usuário sob o qual estiver sendo executado (ou cujas autorizações puder assumir) tiver recebido a autorização relevante.

Quatro chamadas MQI podem requerer verificações de autorização: **MQCONN**, **MQOPEN**, **MQPUT1** e **MQCLOSE**.

Para **MQOPEN** e **MQPUT1**, a verificação de autoridade é feita no nome do objeto que está sendo aberto e não no nome ou nomes resultantes após a resolução de um nome. Por exemplo, um aplicativo pode receber autoridade para abrir uma fila de alias sem ter autoridade para abrir a fila de base para a qual o alias é resolvido. A regra é que a verificação seja realizada na primeira definição encontrada durante o processo de resolução de um nome que não é um alias do gerenciador de filas, a menos que a definição de alias do gerenciador de filas seja aberta diretamente; ou seja, seu nome é exibido no campo *ObjectName* do descritor de objeto. A autoridade é sempre necessária para o objeto que está sendo aberto. Em alguns casos, autoridade adicional independente da fila, obtida por meio de uma autorização para o objeto de gerenciador de filas, é necessária.

Tabela 10 na página 130, Tabela 11 na página 130, Tabela 12 na página 131 e Tabela 13 na página 131 resumem as autorizações necessárias para cada chamada. Nas tabelas, *Não aplicável* significa que a verificação de autorização não é relevante para essa operação; *Nenhuma verificação* significa que nenhuma verificação de autorização é executada.

Nota: Você não encontrará nenhuma menção a listas de nomes, canais, canais de conexão do cliente, listeners, serviços ou objetos de informações sobre autenticação nessas tabelas. Isso é porque nenhuma das autorizações se aplica a esses objetos, exceto MQOO_INQUIRE, para o qual as mesmas autorizações se aplicam como para os outros objetos.

A autorização especial MQZAO_ALL_MQI inclui todas as autorizações nas tabelas que são relevantes ao tipo de objeto, exceto MQZAO_DELETE e MQZAO_DISPLAY, que são classificados como autorizações de administração.

Para modificar qualquer uma das opções de contexto da mensagem, deve-se ter as autorizações apropriadas para emitir a chamada. Por exemplo, para usar MQOO_SET_IDENTITY_CONTEXT ou MQPMO_SET_IDENTITY_CONTEXT, deve-se ter a permissão `+setid`.

Tabela 10. Autorização de segurança necessária para chamadas MQCONN

Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQCONN	Não-aplicável	Não-aplicável	MQZAO_CONNECT

Tabela 11. Autorização de segurança necessária para chamadas MQOPEN

Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQOO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE
MQOO_BROWSE	MQZAO_BROWSE	Não-aplicável	Sem verificação
MQOO_INPUT_*	MQZAO_INPUT	Não-aplicável	Sem verificação
MQOO_SAVE_ ALL_CONTEXT **(“2” na página 132)**	MQZAO_INPUT	Não-aplicável	Não-aplicável
MQOO_OUTPUT (Fila normal) **(“3” na página 132)**	MQZAO_OUTPUT	Não-aplicável	Não-aplicável
MQOO_PASS_ IDENTITY_CONTEXT **(“4” na página 132)**	MQZAO_PASS_ IDENTITY_CONTEXT	Não-aplicável	Sem verificação
MQOO_PASS_ALL_ CONTEXT **(“4” na página 132, “5” na página 132)**	MQZAO_PASS _ALL_CONTEXT	Não-aplicável	Sem verificação

Tabela 11. Autorização de segurança necessária para chamadas MQOPEN (continuação)			
Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQOO_SET_ IDENTITY_CONTEXT **(“4” na página 132, “5” na página 132)**	MQZAO_SET_ IDENTITY_CONTEXT	Não-aplicável	MQZAO_SET_ IDENTITY_CONTEXT **(“6” na página 132)**
MQOO_SET_ ALL_CONTEXT **(“4” na página 132, “7” na página 132)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“6” na página 132)**
MQOO_OUTPUT (Fila de transmissão) **(“8” na página 132)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“6” na página 132)**
MQOO_SET	MQZAO_SET	Não-aplicável	Sem verificação
MQOO_ALTERNATE_ USER_AUTHORITY	**(“9” na página 132)**	**(“9” na página 132)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“9” na página 132, “10” na página 132)**

Tabela 12. Autorização de segurança necessária para chamadas MQPUT1			
Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQPMO_PASS_ IDENTITY_CONTEXT	MQZAO_PASS_ IDENTITY_CONTEXT **(“11” na página 132)**	Não-aplicável	Sem verificação
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **(“11” na página 132)**	Não-aplicável	Sem verificação
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **(“11” na página 132)**	Não-aplicável	MQZAO_SET_ IDENTITY_CONTEXT **(“6” na página 132)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **(“11” na página 132)**	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“6” na página 132)**
(Fila de transmissão) **(“8” na página 132)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“6” na página 132)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**(“12” na página 132)**	Não-aplicável	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” na página 132)**

Tabela 13. Autorização de segurança necessária para chamadas MQCLOSE			
Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQCO_DELETE	MQZAO_DELETE **(“13” na página 132)**	Não-aplicável	Não-aplicável

Tabela 13. Autorização de segurança necessária para chamadas MQCLOSE (continuação)			
Autorização necessária para:	**Objeto da fila (“1” na página 132)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQCO_DELETE _PURGE	MQZAO_DELETE **(“13” na página 132)**	Não-aplicável	Não-aplicável

Notas para as tabelas:

1. Se for abrir uma fila modelo:
   - A autoridade MQZAO_DISPLAY será necessária para a fila modelo, além da autoridade para abrir a fila modelo para o tipo de acesso para o qual você está abrindo.
   - A autoridade MQZAO_CREATE não é necessária para criar o fila dinâmica.
   - O identificador de usuários usado para abrir a fila modelo recebe automaticamente todas as autoridades específicas da fila (equivalente a MQZAO_ALL) para a fila dinâmica criada.
2. MQOO_INPUT_* também deve ser especificado. Isso é válido para uma fila local, modelo ou de alias.
3. Essa verificação é executada para todos os casos de saída, exceto para filas de transmissão (consulte a nota “8” na página 132).
4. MQOO_OUTPUT também deve ser especificado.
5. MQOO_PASS_IDENTITY_CONTEXT também é sugerido por essa opção.
6. Essa autoridade é necessária para o objeto de gerenciador de filas e a fila específica.
7. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT e MQOO_SET_IDENTITY_CONTEXT também são sugeridos por essa opção.
8. Essa verificação é executada para uma fila local ou modelo que tem um atributo de fila *Usage* de MQUS_TRANSMISSION e está sendo aberta diretamente para saída. Ela não será aplicada se uma fila remota estiver sendo aberta (especificando-se os nomes do gerenciador de filas remotas e da fila remota ou especificando-se o nome de uma definição local da fila remota).
9. Pelo menos um de MQOO_INQUIRE (para qualquer tipo de objeto) ou MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT ou MQOO_SET (para filas) também deve ser especificado. A verificação executada é como para as outras opções especificadas, usando-se o identificador de usuário alternativo fornecido para a autoridade de objeto com nome específico, e a autoridade de aplicativo atual para a verificação MQZAO_ALTERNATE_USER_IDENTIFIER.
10. Essa autorização permite que qualquer *AlternateUserId* seja especificado.
11. Uma verificação MQZAO_OUTPUT também será executada se a fila não tiver um atributo de fila *Usage* de MQUS_TRANSMISSION.
12. A verificação executada é como para as outras opções especificadas, usando-se o identificador de usuário alternativo fornecido para a autoridade de fila com nome específico, e a autoridade de aplicativo atual para a verificação MQZAO_ALTERNATE_USER_IDENTIFIER.
13. A verificação será realizada somente se ambas as instruções a seguir forem verdadeiras:
    - Uma fila dinâmica permanente está sendo fechada e excluída.
    - A fila não foi criada pela chamada MQOPEN que retornou a manipulação de objetos que estava sendo usada.

    Caso contrário, não haverá verificação.

ULW *Autorizações para Comandos MQSC em PCFs Escape*

Estas informações resumem as autorizações necessárias para cada comando MQSC contido no PCF Escape.

Não aplicável significa que esta operação não é relevante para esse tipo de objeto.

O ID de usuário com o qual o programa que envia o comando está sendo executado também deve ter as seguintes autoridades:

- Autoridade MQZAO_CONNECT para o gerenciador de filas
- Autoridade MQZAO_DISPLAY no gerenciador de filas para executar comandos de PCF
- Autoridade para emitir o comando MQSC dentro do texto do comando PCF Escape

ALTER *object*

Object	**Authorization required**
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	MQZAO_CHANGE
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE
Informações de comunicação	MQZAO_CHANGE

CLEAR *object*

Object	**Authorization required**
Fila	MQZAO_CLEAR
Tópico	MQZAO_CLEAR
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	Não-aplicável
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável
Informações de comunicação	Não-aplicável

DEFINE *object* NOREPLACE (“1” na página 137)

Object	**Authorization required**
Fila	MQZAO_CREATE **(“2” na página 137)**
Tópico	MQZAO_CREATE **(“2” na página 137)**
Processo	MQZAO_CREATE **(“2” na página 137)**
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CREATE **(“2” na página 137)**

Object	Authorization required
Informações sobre Autenticação	MQZAO_CREATE **(“2” na página 137)**
Canal	MQZAO_CREATE **(“2” na página 137)**
Canal de conexão do cliente	MQZAO_CREATE **(“2” na página 137)**
Listener	MQZAO_CREATE **(“2” na página 137)**
Serviço	MQZAO_CREATE **(“2” na página 137)**
Informações de comunicação	MQZAO_CREATE **(“2” na página 137)**

DEFINE *object* REPLACE (“1” na página 137, “3” na página 137)

Object	Authorization required
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE
Informações de comunicação	MQZAO_CHANGE

EXCLUIR *object*

Object	Authorization required
Fila	MQZAO_DELETE
Tópico	MQZAO_DELETE
Processo	MQZAO_DELETE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_DELETE
Informações sobre Autenticação	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de conexão do cliente	MQZAO_DELETE
Listener	MQZAO_DELETE
Serviço	MQZAO_DELETE
Informações de comunicação	MQZAO_DELETE

DISPLAY *object*

Object	Authorization required
Fila	MQZAO_DISPLAY
Tópico	MQZAO_DISPLAY
Processo	MQZAO_DISPLAY
Gerenciador de Filas	MQZAO_DISPLAY
Lista de Nomes	MQZAO_DISPLAY
Informações sobre Autenticação	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY
Canal de conexão do cliente	MQZAO_DISPLAY
Listener	MQZAO_DISPLAY
Serviço	MQZAO_DISPLAY
Informações de comunicação	MQZAO_DISPLAY

START *object*

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Listener	MQZAO_CONTROL
Serviço	MQZAO_CONTROL
Informações de comunicação	Não-aplicável

PARAR *object*

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL

Object	Authorization required
Canal de conexão do cliente	Não-aplicável
Listener	MQZAO_CONTROL
Serviço	MQZAO_CONTROL
Informações de comunicação	Não-aplicável

Comandos do Canal

Comando:	Object	Authorization required
PING CHANNEL	Canal	MQZAO_CONTROL
RESET CHANNEL	Canal	MQZAO_CONTROL_EXTENDED
RESOLVE CHANNEL	Canal	MQZAO_CONTROL_EXTENDED

Comandos de Assinatura

Comando:	Object	Authorization required
ALTER SUB	Tópico	MQZAO_CONTROL
DEFINE SUB	Tópico	MQZAO_CONTROL
DELETE SUB	Tópico	MQZAO_CONTROL
DISPLAY SUB	Tópico	MQZAO_DISPLAY

Comandos de Segurança

Comando:	Object	Authorization required
SET AUTHREC	Gerenciador de Filas	MQZAO_CHANGE
DELETE AUTHREC	Gerenciador de Filas	MQZAO_CHANGE
DISPLAY AUTHREC	Gerenciador de Filas	MQZAO_DISPLAY
DISPLAY AUTHSERV	Gerenciador de Filas	MQZAO_DISPLAY
DISPLAY ENTAUTH	Gerenciador de Filas	MQZAO_DISPLAY
SET CHLAUTH	Gerenciador de Filas	MQZAO_CHANGE
DISPLAY CHLAUTH	Gerenciador de Filas	MQZAO_DISPLAY
REFRESH SECURITY	Gerenciador de Filas	MQZAO_CHANGE

Exibições de status

Comando:	Object	Authorization required
DISPLAY CHSTATUS	Gerenciador de Filas	MQZAO_DISPLAY Observe que a autoridade `+inq` (ou equivalentemente MQZAO_INQUIRE) será necessária na fila de transmissão se o tipo de canal for CLUSSDR.
DISPLAY LSSTATUS	Gerenciador de Filas	MQZAO_DISPLAY

Comando:	Object	Authorization required
DISPLAY PUBSUB	Gerenciador de Filas	MQZAO_DISPLAY
DISPLAY SBSTATUS	Gerenciador de Filas	MQZAO_DISPLAY
DISPLAY SVSTATUS	Gerenciador de Filas	MQZAO_DISPLAY
DISPLAY TPSTATUS	Gerenciador de Filas	MQZAO_DISPLAY

Comandos do Cluster

Comando:	Object	Authorization required
EXIBIR CLUSQMGR	Gerenciador de Filas	MQZAO_DISPLAY
REFRESH CLUSTER	associação ao grupo 'mqm' necessária	
RESET CLUSTER	associação ao grupo 'mqm' necessária	
SUSPEND QMGR	associação ao grupo 'mqm' necessária	
RESUME QMGR	associação ao grupo 'mqm' necessária	

Outros comandos administrativos

Comando:	Object	Authorization required
PING QMGR	Gerenciador de Filas	MQZAO_DISPLAY
REFRESH QMGR	Gerenciador de Filas	MQZAO_CHANGE
RESET QMGR	Gerenciador de Filas	MQZAO_CHANGE
DISPLAY CONN	Gerenciador de Filas	MQZAO_DISPLAY
STOP CONN	Gerenciador de Filas	MQZAO_CHANGE

Nota:

1. Para comandos DEFINE, a autoridade MQZAO_DISPLAY também será necessária para o objeto LIKE, se houver um especificado, ou no objeto SYSTEM.DEFAULT.xxx apropriado, se LIKE for omitido.
2. A autoridade MQZAO_CREATE não é específica a um determinado objeto ou tipo de objeto. A autoridade Criar é concedida para todos os objetos de um gerenciador de filas especificado, especificando-se um tipo de objeto de QMGR no comando `setmqaut`.
3. Isso se aplicará se o objeto a ser substituído já existir. Caso contrário, a verificação será como para DEFINE *object* NOREPLACE.

Informações relacionadas

Armazenamento em Cluster: Usando Melhores Práticas de REFRESH CLUSTER

ULW *Autorizações para Comandos PCF*

Esta seção resume as autorizações necessárias para cada comando PCF.

Nenhuma verificação significa que nenhuma verificação de autorização é executada; *Não aplicável* significa que esta operação não é relevante para este tipo de objeto.

O ID de usuário com o qual o programa que envia o comando está sendo executado também deve ter as seguintes autoridades:

- Autoridade MQZAO_CONNECT para o gerenciador de filas
- Autoridade MQZAO_DISPLAY no gerenciador de filas para executar comandos de PCF

A autorização especial MQZAO_ALL_ADMIN inclui todas as autorizações na lista a seguir que são relevantes ao tipo de objeto, exceto MQZAO_CREATE, que não é específica a um determinado objeto ou tipo de objeto.

Mudar *object*

Object	**Autorização necessária**
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processar	MQZAO_CHANGE
Gerenciador de Filas	MQZAO_CHANGE
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Receptor	MQZAO_CHANGE
Serviço	MQZAO_CHANGE
Informações de Comunicação	MQZAO_CHANGE

Clear *object*

Object	**Autorização necessária**
Fila	MQZAO_CLEAR
Tópico	MQZAO_CLEAR
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	Não-aplicável
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável
Informações de comunicação	Não-aplicável

Copiar *object* (sem substituir) (1)

Object	**Autorização necessária**
Fila	MQZAO_CREATE **(2)**
Tópico	MQZAO_CREATE **(2)**
Processar	MQZAO_CREATE **(2)**
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CREATE **(2)**

Object	Autorização necessária
Informações sobre Autenticação	MQZAO_CREATE **(2)**
Canal	MQZAO_CREATE **(2)**
Canal de conexão do cliente	MQZAO_CREATE **(2)**
Receptor	MQZAO_CREATE **(2)**
Serviço	MQZAO_CREATE **(2)**
Informações de Comunicação	MQZAO_CREATE **("2" na página 144)**

Copie o *object* (com substituição) (1, 4)

Object	Autorização necessária
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processar	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Receptor	MQZAO_CHANGE
Serviço	MQZAO_CHANGE
Informações de Comunicação	MQZAO_CHANGE

Criar *object* (sem substituir) (3)

Object	Autorização necessária
Fila	MQZAO_CREATE **(2)**
Tópico	MQZAO_CREATE **(2)**
Processar	MQZAO_CREATE **(2)**
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CREATE **(2)**
Informações sobre Autenticação	MQZAO_CREATE **(2)**
Canal	MQZAO_CREATE **(2)**
Canal de conexão do cliente	MQZAO_CREATE **(2)**
Receptor	MQZAO_CREATE **(2)**
Serviço	MQZAO_CREATE **(2)**
Informações de Comunicação	MQZAO_CREATE **(2)**

Crie o *object* (com substituição) (3, 4)

Object	Autorização necessária
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processar	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Receptor	MQZAO_CHANGE
Serviço	MQZAO_CHANGE
Informações de Comunicação	MQZAO_CHANGE

Excluir *object*

Object	Autorização necessária
Fila	MQZAO_DELETE
Tópico	MQZAO_DELETE
Processar	MQZAO_DELETE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_DELETE
Informações sobre Autenticação	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de conexão do cliente	MQZAO_DELETE
Receptor	MQZAO_DELETE
Serviço	MQZAO_DELETE
Informações de Comunicação	MQZAO_DELETE

Inquire *object*

Object	Autorização necessária
Fila	MQZAO_DISPLAY
Tópico	MQZAO_DISPLAY
Processar	MQZAO_DISPLAY
Gerenciador de Filas	MQZAO_DISPLAY
Lista de Nomes	MQZAO_DISPLAY
Informações sobre Autenticação	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY

Object	Autorização necessária
Canal de conexão do cliente	MQZAO_DISPLAY
Receptor	MQZAO_DISPLAY
Serviço	MQZAO_DISPLAY
Informações de Comunicação	MQZAO_DISPLAY

Inquire *object* names

Object	Autorização necessária
Fila	Sem verificação
Tópico	Sem verificação
Processo	Sem verificação
Gerenciador de Filas	Sem verificação
Lista de Nomes	Sem verificação
Informações sobre Autenticação	Sem verificação
Canal	Sem verificação
Canal de conexão do cliente	Sem verificação
Listener	Sem verificação
Serviço	Sem verificação
Informações de comunicação	Sem verificação

Iniciar *object*

Object	Autorização necessária
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Receptor	MQZAO_CONTROL
Serviço	MQZAO_CONTROL
Informações de comunicação	Não-aplicável

Parar *object*

Object	Autorização necessária
Fila	Não-aplicável
Tópico	Não-aplicável

Object	Autorização necessária
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Receptor	MQZAO_CONTROL
Serviço	MQZAO_CONTROL
Informações de comunicação	Não-aplicável

Comandos do Canal

Comando:	Object	Autorização necessária
Executar ping no Canal	Canal	MQZAO_CONTROL
Redefinir Canal	Canal	MQZAO_CONTROL_EXTENDED
Resolver Canal	Canal	MQZAO_CONTROL_EXTENDED

Comandos de Assinatura

Comando:	Object	Autorização necessária
Change Subscription	Tópico	MQZAO_CONTROL
Criar assinatura	Tópico	MQZAO_CONTROL
Excluir assinatura	Tópico	MQZAO_CONTROL
Consultar Assinatura	Tópico	MQZAO_DISPLAY

Comandos de Segurança

Comando:	Object	Autorização necessária
Configurar Registro de Autoridade	Gerenciador de Filas	MQZAO_CHANGE
Excluir Registro de Autoridade	Gerenciador de Filas	MQZAO_CHANGE
Consultar Registros de Autoridade	Gerenciador de Filas	MQZAO_DISPLAY
Consultar Autoridade de Serviço	Gerenciador de Filas	MQZAO_DISPLAY
Solicitar Autoridade de Entidade	Gerenciador de Filas	MQZAO_DISPLAY
Configurar Registro de Autenticação de Canal	Gerenciador de Filas	MQZAO_CHANGE
Solicitar Registros de Autenticação de Canal	Gerenciador de Filas	MQZAO_DISPLAY
Atualizar segurança	Gerenciador de Filas	MQZAO_CHANGE

Exibições de status

Comando:	Object	Autorização necessária
Consultar Status do Canal	Gerenciador de Filas	MQZAO_DISPLAY Observe que a autoridade `+inq` (ou equivalentemente MQZAO_INQUIRE) será necessária na fila de transmissão se o tipo de canal for CLUSSDR.
Consulte o status do ouvinte de canal	Gerenciador de Filas	MQZAO_DISPLAY
Investigar Status da Pub/Ass	Gerenciador de Filas	MQZAO_DISPLAY
Inquire Subscription Status	Gerenciador de Filas	MQZAO_DISPLAY
Consultar Status do Serviço	Gerenciador de Filas	MQZAO_DISPLAY
Inquire Topic Status	Gerenciador de Filas	MQZAO_DISPLAY

Comandos do Cluster

Comando:	Object	Autorização necessária
Consultar Gerenciador de Filas de Clusters	Gerenciador de Filas	MQZAO_DISPLAY
Refresh Cluster	associação ao grupo 'mqm' necessária	associação ao grupo 'mqm' necessária
Reset Cluster	associação ao grupo 'mqm' necessária	associação ao grupo 'mqm' necessária
Suspender Cluster de Gerenciador de Filas	associação ao grupo 'mqm' necessária	associação ao grupo 'mqm' necessária
Retomar Cluster de Gerenciador de Filas	associação ao grupo 'mqm' necessária	associação ao grupo 'mqm' necessária

Outros comandos administrativos

Comando:	Object	Autorização necessária
Executar Ping do Gerenciador de Filas	Gerenciador de Filas	MQZAO_DISPLAY
Atualizar Gerenciador de Filas	Gerenciador de Filas	MQZAO_CHANGE
Reconfigurar Gerenciador de Filas	Gerenciador de Filas	MQZAO_CHANGE
Reconfigurar as Estatísticas de Fila	Fila	MQZAO_DISPLAY e MQZAO_CHANGE
Consultar Conexão	Gerenciador de Filas	MQZAO_DISPLAY
Para Conexão	Gerenciador de Filas	MQZAO_CHANGE

Nota:

1. Para comandos Copy, a autoridade MQZAO_DISPLAY também é necessária para o objeto De.

2. A autoridade MQZAO_CREATE não é específica a um determinado objeto ou tipo de objeto. A autoridade Criar é concedida para todos os objetos de um gerenciador de filas especificado, especificando-se um tipo de objeto de QMGR no comando `setmqaut`.
3. Para comandos de Criação, a autoridade MQZAO_DISPLAY também é necessária para o SYSTEM.DEFAULT.* objeto.
4. Isso se aplicará se o objeto a ser substituído já existir. Caso contrário, a verificação será como para Copy ou Create sem substituição.

AIX Criando e gerenciando grupos no AIX

No AIX, desde que você não esteja usando NIS ou NIS+, use SMITTY para trabalhar com grupos.

Sobre esta tarefa

No AIX, é possível usar SMITTY para criar um grupo, incluir um usuário em um grupo, exibir uma lista dos usuários que estão no grupo e remover um usuário de um grupo.

Procedimento

1. No SMITTY, selecione **Segurança e usuários** e pressione Enter.
2. Selecione **Grupos** e pressione Enter.
3. Para criar um grupo, conclua as etapas a seguir:
   a) Selecione **Incluir um grupo** e pressione Enter.
   b) Insira o nome do grupo e os nomes de usuários que você deseja incluir no grupo, separados por vírgulas.
   c) Pressione Enter para criar o grupo.
4. Para incluir um usuário em um grupo, conclua as etapas a seguir:
   a) Selecione **Mudar/mostrar características de grupos** e pressione Enter.
   b) Insira o nome do grupo para mostrar uma lista dos membros do grupo.
   c) Inclua os nomes dos usuários que você deseja incluir no grupo, separados por vírgulas.
   d) Pressione Enter para incluir os nomes no grupo.
5. Para exibir quem está em um grupo, conclua as etapas a seguir:
   a) Selecione **Mudar/mostrar características de grupos** e pressione Enter.
   b) Insira o nome do grupo para mostrar uma lista dos membros do grupo.
6. Para remover um usuário de um grupo, conclua as etapas a seguir:
   a) Selecione **Mudar/mostrar características de grupos** e pressione Enter.
   b) Insira o nome do grupo para mostrar uma lista dos membros do grupo.
   c) Exclua o nome do usuário que você deseja remover do grupo.
   d) Pressione Enter para remover o nome do grupo.

Linux Criando e gerenciando grupos no Linux

No Linux, desde que você não esteja usando NIS ou NIS+, use o arquivo `/etc/group` para trabalhar com grupos.

Sobre esta tarefa

No Linux, as informações do grupo são retidas no arquivo `/etc/group`. É possível usar comandos para criar um grupo, incluir um usuário em um grupo, exibir uma lista dos usuários que estão no grupo e remover um usuário de um grupo.

Procedimento

1. Para criar um novo grupo, use o comando **groupadd**.
   Digite o seguinte comando:

   ```
   groupadd -g group-ID group-name
   ```

   em que *group-ID* é o identificador numérico do grupo e *group-name* é o nome do grupo.
2. Para incluir um membro em um grupo complementar, use o comando **usermod** para listar os grupos complementares dos quais o utilizador é actualmente membro, e os grupos complementares que o usuário deve se tornar um membro do.
   Por exemplo, se o usuário já é um membro do grupo `groupa` e deve se tornar um membro de `groupb`, use o comando a seguir:

   ```
   usermod -G groupa,groupb user-name
   ```

   em que *user-name* é o nome do usuário.
3. Para exibir quem é um membro de um grupo, use o comando **getent**.
   Digite o seguinte comando:

   ```
   getent group group-name
   ```

   em que *group-name* é o nome do grupo.
4. Para remover um membro de um grupo complementar, use o comando **usermod** para listar os grupos complementares dos quais você deseja que o usuário permaneça um membro.
   Por exemplo, se o grupo primário do usuário for `users` e o usuário também for um membro dos grupos `mqm`, `groupa` e `groupb`, para remover o usuário do grupo `mqm`, use o comando a seguir:

   ```
   usermod -G groupa,groupb user-name
   ```

   em que *user-name* é o nome do usuário.

Solaris Criando e gerenciando grupos no Solaris

No Solaris, desde que você não esteja usando NIS ou NIS+, use o arquivo `/etc/group` para trabalhar com grupos.

Sobre esta tarefa

No Solaris, as informações do grupo são mantidas no arquivo do `/etc/group`. É possível usar comandos para criar um grupo, incluir um usuário em um grupo, exibir uma lista dos usuários que estão no grupo e remover um usuário de um grupo.

Procedimento

1. Para criar um novo grupo, use o comando **groupadd**.
   Digite o seguinte comando:

   ```
   groupadd -g group-ID group-name
   ```

   em que *group-ID* é o identificador numérico do grupo e *group-name* é o nome do grupo.
2. Para incluir um membro em um grupo complementar, use o comando **usermod** para listar os grupos complementares dos quais o utilizador é actualmente membro, e os grupos complementares que o usuário deve se tornar um membro do.
   Por exemplo, se o usuário já é um membro do grupo `groupa` e deve se tornar um membro de `groupb`, use o comando a seguir:

   ```
   usermod -G groupa,groupb user-name
   ```

em que *user-name* é o nome do usuário.

3. Para descobrir quem é um membro de um grupo, veja a entrada para esse grupo no arquivo `/etc/group`.
4. Para remover um membro de um grupo complementar, use o comando **usermod** para listar os grupos complementares dos quais você deseja que o usuário permaneça um membro.
   Por exemplo, se o grupo primário do usuário for `users` e o usuário também for um membro dos grupos `mqm`, `groupa` e `groupb`, para remover o usuário do grupo `mqm`, use o comando a seguir:

   ```
   usermod -G groupa,groupb user-name
   ```

   em que *user-name* é o nome do usuário.

Windows Criando e gerenciando grupos no Windows

No Windows, use o recurso Gerenciamento de computadores para administrar grupos em uma estação de trabalho ou máquina do servidor de membro.

Sobre esta tarefa

Para controladores de domínio, usuários e grupos são administrados por meio do Active Directory. Para obter mais detalhes sobre como usar o Active Directory, consulte as instruções apropriadas do sistema operacional.

Todas as mudanças feitas na associação ao grupo de um proprietário não são reconhecidas até que o gerenciador de filas seja reiniciado ou você emita o comando MQSC **REFRESH SECURITY** (ou o equivalente PCF).

Use o painel Gerenciamento de computadores do Windows para trabalhar com o usuário e os grupos. Quaisquer mudanças feitas no usuário com login efetuado atual podem não entrar em vigor até que o usuário efetue login novamente.

Windows *Criando um grupo no Windows*

Crie um grupo usando o painel de controle.

Procedimento

1. Abra o painel de controle
2. Dê um clique duplo em **Ferramentas Administrativas**.
   O painel Ferramentas Administrativas é aberto.
3. Dê um clique duplo em **Gerenciamento de Computadores**.
   O painel Gerenciamento de Computadores é aberto.
4. Expanda **Local Users and Groups**.
5. Clique com o botão direito do mouse em **Grupos** e selecione **Novo Grupo...**.
   O painel Novo Grupo é exibido.
6. Digite um nome apropriado no campo de nome Grupo e, em seguida, clique em **Criar**.
7. Clique em **Fechar (Close)**.

Windows *Incluindo um usuário em um grupo no Windows*

Inclua um usuário em um grupo usando o painel de controle.

Procedimento

1. Abra o painel de controle
2. Dê um clique duplo em **Ferramentas Administrativas**.
   O painel Ferramentas Administrativas é aberto.

3. Dê um clique duplo em **Gerenciamento de Computadores**.
   O painel Gerenciamento de Computadores é aberto.
4. No painel Gerenciamento de Computadores, expanda **Usuários e Grupos Locais**.
5. Selecione **Usuários**
6. Clique duas vezes no usuário que você deseja incluir em um grupo.
   O painel de propriedades do usuário é exibido.
7. Selecione a guia **Membro de**.
8. Selecione o grupo no qual você deseja incluir o usuário. Se o grupo desejado não estiver visível:
   a) Clique em **Incluir...**.
      O painel Selecionar Grupos é exibido.
   b) Clique em **Locais...**.
      O painel Locais é exibido.
   c) Selecione o local do grupo em que você deseja incluir o usuário na lista e clique em **OK**.
   d) Digite o nome do grupo no campo fornecido.

      Como alternativa, clique em **Avançado ...** .. e, em seguida, **Localizar Agora** para listar os grupos disponíveis no local atualmente selecionado Daqui, selecione o grupo em que deseja incluir o usuário e clique em **OK**.
   e) Clique em **OK**.
      O painel de propriedades do usuário é exibido, mostrando o grupo incluído.
   f) Selecionar o grupo.
9. Clique em **OK**.
   O painel Gerenciamento de Computadores é exibido.

Windows *Exibindo quem está em um grupo em Windows*

Exiba os membros de um grupo usando o painel de controle.

Procedimento

1. Abra o painel de controle
2. Dê um clique duplo em **Ferramentas Administrativas**.
   O painel Ferramentas Administrativas é aberto.
3. Dê um clique duplo em **Gerenciamento de Computadores**.
   O painel Gerenciamento de Computadores é aberto.
4. No painel Gerenciamento de Computadores, expanda **Usuários e Grupos Locais**.
5. Selecione **Grupos**.
6. Clique duas vezes em um grupo. O painel de propriedades do grupo é exibido.
   O painel de propriedades do grupo é exibido.

Resultados

Os membros do grupo são exibidos.

Windows *Removendo um usuário de um grupo em Windows*

Remova um usuário de um grupo usando o painel de controle.

Procedimento

1. Abra o painel de controle
2. Dê um clique duplo em **Ferramentas Administrativas**.

O painel Ferramentas Administrativas é aberto.

3. Dê um clique duplo em **Gerenciamento de Computadores**.
   O painel Gerenciamento de Computadores é aberto.
4. No painel Gerenciamento de Computadores, expanda **Usuários e Grupos Locais**.
5. Selecione **Usuários**.
6. Clique duas vezes no usuário que você deseja incluir em um grupo.
   O painel de propriedades do usuário é exibido.
7. Selecione a guia **Membro de**.
8. Selecione o grupo do qual você deseja remover o usuário e, em seguida, clique em **Remover**.
9. Clique em **OK**.
   O painel Gerenciamento de Computadores é exibido.

Resultados

Agora você removeu o usuário do grupo.

Windows Considerações especiais para segurança no Windows

Algumas funções de segurança se comportam de forma diferente em diferentes versões do Windows.

A segurança do IBM MQ depende de chamadas para a API do sistema operacional para obter informações sobre autorizações de usuários e associações de grupo. Algumas funções não se comportam de modo idêntico em sistemas Windows. Esta coleção de tópicos inclui descrições de como essas diferenças podem afetar a segurança do IBM MQ quando se está executando o IBM MQ em um ambiente do Windows.

Windows *Contas de usuário local e de domínio para o serviço IBM MQ Windows*

Quando o IBM MQ estiver em execução, ele deverá verificar se apenas usuários autorizados podem acessar gerenciadores de filas ou filas. Isso requer uma conta de usuário especial que o IBM MQ pode usar para consultar informações sobre o usuário que está tentando tal acesso.

- "Configurando contas de usuário especiais com o Prepare IBM MQ Wizard" na página 148
- "Usando o IBM MQ com o Active Directory" na página 149
- "Direitos de usuário necessários para um serviço do IBM MQ Windows" na página 149

Configurando contas de usuário especiais com o Prepare IBM MQ Wizard

O Prepare IBM MQ Wizard cria uma conta de usuário especial para que o serviço do Windows possa ser compartilhado por processos que precisam usá-lo (consulte Configurando o IBM MQ com o Assistente para preparar o IBM MQ).

Um serviço é compartilhado entre os processos do cliente Windows para uma instalação do IBM MQ. Um serviço é criado para cada instalação. Cada serviço é denominado `MQ_`*`InstallationName`* e possui um nome de exibição `IBM MQ(`*`InstallationName`*`)`.

Como cada serviço deve ser compartilhado entre as sessões de logon não interativas e interativas, deve-se ativar cada uma delas sob uma conta de usuário especial. É possível usar uma conta do usuário especial para todos os serviços ou criar contas do usuário especiais diferentes. Cada conta de usuário especial deve ter o direito de usuário para `Efetuar logon como um serviço`; para obter mais informações, consulte Tabela 14 na página 149. Se o ID do usuário não tiver a autoridade para executar o serviço, o serviço não será iniciado e retornará um erro no log de eventos do sistema Windows. Geralmente, você terá executado o Prepare IBM MQ Wizard e configurará o ID do usuário corretamente. No entanto, se você configurou o ID do usuário manualmente, possivelmente ocorrerá um problema que precisará ser resolvido.

Quando você instala o IBM MQ e executa o Prepare IBM MQ Wizard pela primeira vez, ele cria uma conta do usuário local para o serviço chamado MUSR_MQADMIN com as configurações e permissões necessárias, incluindo `Efetuar logon como um serviço`.

Para instalações subsequentes, o Prepare IBM MQ Wizard cria uma conta do usuário denominada MUSR_MQADMIN*x*, em que *x* é o próximo número disponível que representa um ID do usuário que não existe. A senha para MUSR_MQADMIN*x* é gerada aleatoriamente quando a conta é criada e usada para configurar o ambiente de logon para o serviço. A senha gerada não expira.

Esta conta do IBM MQ não é afetada por quaisquer políticas de conta que são configuradas no sistema para exigir que as senhas das contas sejam mudadas após um determinado período.

A senha não é conhecida fora desse processamento único e é armazenada pelo sistema operacional Windows em uma parte segura do registro.

Usando o IBM MQ com o Active Directory

Em algumas configurações de rede, em que as contas do usuário são definidas nos controladores de domínio que estão utilizando o serviço de diretório do Active Directory, a conta do usuário local sob a qual o IBM MQ está sendo executado pode não ter a autoridade necessária para consultar a associação ao grupo de outras contas de usuário de domínio. Quando você instala o IBM MQ, o Prepare IBM MQ Wizard identifica se esse é o caso executando testes e fazendo perguntas sobre a configuração de rede.

Se a conta do usuário local que o IBM MQ está executando sob não possui a autoridade necessária, o Prepare IBM MQ Wizard solicitará os detalhes da conta de um domínio conta do usuário com direitos de usuário específicos. Para obter informações sobre como criar e configurar uma conta de domínio do Windows, consulte Criando e configurando contas de domínio do Windows para o IBM MQ. Para obter os direitos de usuário que a conta do usuário do domínio requer, consulte Tabela 14 na página 149.

Quando você tiver inserido detalhes da conta válidos para a conta do usuário do domínio no Prepare IBM MQ Wizard, o assistente configurará um serviço IBM MQ Windows para ser executado na nova conta. Os detalhes da conta são retidos na parte segura do Registro e não podem ser lidos pelos usuários.

Quando o serviço está em execução, um serviço do IBM MQ Windows é iniciado e permanece em execução enquanto o serviço estiver em execução. Um administrador do IBM MQ que efetua logon no servidor depois que o serviço do Windows é ativado pode usar o IBM MQ Explorer para administrar gerenciadores de filas no servidor. Ele conecta o IBM MQ Explorer ao processo do serviço do Windows existente. Essas duas ações precisam de diferentes níveis de permissão para que possam trabalhar:

- O processo de ativação requer uma permissão de ativação.
- O administrador do IBM MQ requer permissão de acesso.

Direitos de usuário necessários para um serviço do IBM MQ Windows

A tabela a seguir lista os direitos de usuário necessários para as contas de usuário local e de domínio sob as quais o serviço do Windows para uma instalação do IBM MQ é executado.

Tabela 14. Direitos de usuário necessários para um serviço do Windows do IBM MQ

Permission	**Descrição**
Efetuar logon como uma tarefa em lote	Permite que um serviço do IBM MQ Windows execute sob essa conta do usuário.
Efetue logon como serviço	Permite que os usuários configurem o serviço do IBM MQ Windows para efetuar logon utilizando a conta configurada.
Desligar o sistema	Permite que o serviço IBM MQ Windows reinicie o servidor, se estiver configurado para fazer isso quando a recuperação de um serviço falhar.

Tabela 14. Direitos de usuário necessários para um serviço do Windows do IBM MQ (continuação)	
Permission	**Descrição**
Aumentar cotas	Necessário para chamada de `CreateProcessAsUser` do sistema operacional.
Aja como parte do sistema operacional	Requerido para a chamada de `LogonUser` do sistema operacional.
Verificação de passagem de desvio	Requerido para a chamada de `LogonUser` do sistema operacional.
Substituir um símbolo em nível de processo	Requerido para a chamada de `LogonUser` do sistema operacional.

Nota: Podem ser necessários direitos de programas de depuração em ambientes que executam os aplicativos ASP e IIS.

Sua conta de usuário de domínio deve ter esses direitos de usuário do Windows configurados como direitos de usuário efetivo, conforme listado no aplicativo Política de Segurança Local. Se eles não forem, configure-os usando o aplicativo Política de Segurança Local localmente no servidor ou usando o domínio de Aplicativo de Segurança do Domínio amplo.

Windows *Permissões de segurança do Windows Server*

A instalação do IBM MQ se comporta de forma diferente no Windows Server, dependendo se um usuário local ou um usuário do domínio executa a instalação.

Se um usuário *local* instala o IBM MQ, o Prepare IBM MQ Wizard detecta que o usuário local criado para o serviço do IBM MQ Windows pode recuperar as informações de associação ao grupo do usuário de instalação. O Prepare IBM MQ Wizard faz perguntas ao usuário sobre a configuração de rede para determinar se há outras contas do usuário definidas em controladores de domínio em execução no Windows 2000 ou mais recente. Se sim, o serviço do IBM MQ Windows precisar ser executado em uma conta de usuário do domínio com configurações e autoridades específicas. O Prepare IBM MQ Wizard solicita que o usuário para os detalhes da conta desse usuário, conforme descrito em Configurando o IBM MQ com o Assistente para preparar o IBM MQ.

Se um usuário *domain* instala o IBM MQ, o Prepare IBM MQ Wizard detecta que o usuário local criado para o serviço do IBM MQ Windows não pode recuperar as informações de associação ao grupo do usuário de instalação. Neste caso, o Prepare IBM MQ Wizard sempre solicita ao usuário os detalhes da conta da conta do usuário do domínio para o serviço do IBM MQ Windows usar.

Quando o serviço do IBM MQ Windows precisa usar uma conta de usuário de domínio, o IBM MQ não pode operar corretamente até que isso tenha sido configurado usando o Prepare IBM MQ Wizard. O Prepare IBM MQ Wizard não permite que o usuário continue com outras tarefas, até que o serviço do Windows tenha sido configurado com uma conta adequada.

Para obter mais informações, consulte Criando e configurando contas de domínio para o IBM MQ.

Windows *Mudando o nome do usuário associado ao serviço do IBM MQ*

É possível mudar o nome do usuário associado ao serviço do IBM MQ criando uma nova conta e inserindo seus detalhes usando o Prepare IBM MQ Wizard.

Sobre esta tarefa

Quando você instala o IBM MQ e executa o Prepare IBM MQ Wizard pela primeira vez, ele cria uma conta do usuário local para o serviço chamado MUSR_MQADMIN. Para instalações subsequentes, o Prepare IBM MQ Wizard cria uma conta do usuário denominada MUSR_MQADMIN*x*, em que *x* é o próximo número disponível que representa um ID do usuário que não existe.

Pode ser necessário mudar o nome do usuário associado ao serviço do IBM MQ de MUSR_MQADMIN ou MUSR_MQADMIN*x* para algo diferente. Por exemplo, talvez você precise fazer isso se seu gerenciador de filas estiver associado ao Db2, que não aceita nomes de usuário com mais de 8 caracteres.

Procedimento

1. Crie uma nova conta de usuário (por exemplo **NEW_NAME**)
2. Use o Prepare IBM MQ Wizard para inserir os detalhes do nova conta do usuário.

Tarefas relacionadas

Configurando o IBM MQ com o Assistente para preparar o IBM MQ

Windows *Mudando a senha da conta do usuário local do serviço IBM MQ Windows*

É possível mudar a senha da conta do usuário local do serviço IBM MQ Windows usando o painel Gerenciamento de computadores.

Sobre esta tarefa

Para mudar a senha do IBM MQ Windows de serviço da conta de usuário local, execute as seguintes etapas:

Procedimento

1. Identifique o usuário do serviço está sendo executado.
2. Pare o serviço do IBM MQ a partir do painel do Computer Management.
3. Mude a senha necessária da mesma maneira que você mudaria a senha de um indivíduo.
4. Acesse as propriedades para o serviço do IBM MQ a partir do painel do Computer Management.
5. Selecione a página **Efetuar Logon** .
6. Confirme se o nome da conta especificado corresponde ao usuário para o qual a senha foi modificada.
7. Digite a senha no **Senha** e **Confirmar Senha** os campos e clique em **OK**.

Windows *Mudando a senha para um serviço IBM MQ Windows para uma instalação em execução em uma conta de usuário do domínio*

Como uma alternativa ao uso do Prepare IBM MQ Wizard para inserir os detalhes da conta da conta do usuário do domínio, é possível usar o painel Gerenciamento do Computador para alterar os detalhes de **Logon** para o Serviço IBM MQ específico da instalação.

Sobre esta tarefa

Se o serviço IBM MQ Windows para uma instalação estiver em execução em uma conta de usuário do domínio, você poderá mudar a senha para a conta conforme a seguir:

Procedimento

1. Mude a senha para a conta de domínio no controlador de domínio. Talvez seja necessário solicitar ao seu administrador de domínio para fazer isso para você.
2. Conclua as etapas a seguir para modificar a página **Efetuar logon** para o serviço do IBM MQ.
   a) Identifique o usuário sob o qual o serviço está sendo executado.
   b) Pare o serviço do IBM MQ a partir do painel do Computer Management.
   c) Mude a senha necessária da mesma maneira que você mudaria a senha de um indivíduo.
   d) Acesse as propriedades para o serviço do IBM MQ a partir do painel do Computer Management.
   e) Selecione a página **Efetuar Logon** .
   f) Confirme se o nome da conta especificado corresponde ao usuário para o qual a senha foi modificada.

g) Digite a senha no **Senha** e **Confirmar Senha** os campos e clique em **OK**.

A conta do usuário sob a qual executa o serviço IBM MQ Windows executa quaisquer comandos MQSC que são emitidos por aplicativos de interface com o usuário ou executados automaticamente na inicialização, encerramento ou recuperação de serviço do sistema. Essa conta do usuário deve, portanto, ter direitos de administração do IBM MQ. Por padrão, ele é incluído no grupo mqm local no servidor. Se essa associação é removida, o serviço do IBM MQ Windows não funciona. Para obter mais informações sobre os direitos do usuário, consulte “Direitos de usuário necessários para um serviço do IBM MQ Windows” na página 149.

Se um problema de segurança surgir com a conta do usuário sob a qual o serviço do IBM MQ Windows executa, mensagens de erro e descrições aparecem no log de eventos do sistema.

Tarefas relacionadas

Configurando o IBM MQ com o Assistente para preparar o IBM MQ

Windows *Considerações ao promover servidores Windows para controladores de domínio*

Ao promover um servidor Windows para um domínio, é necessário considerar se a configuração de segurança relacionada às permissões de usuário e de grupo é apropriada. Ao mudar o estado de uma máquina do Windows entre o servidor e o controlador de domínio, é necessário levar em consideração que isso pode afetar a operação do IBM MQ porque o IBM MQ usa um grupo mqm definido localmente.

Configurações de segurança relacionadas a permissões de usuário e grupo de domínio

O IBM MQ conta com informações de associação ao grupo para implementar sua política de segurança, o que significa que é importante que o ID do usuário que está executando operações do IBM MQ possa determinar as associações ao grupo de outros usuários.

Ao promover um servidor Windows para um controlador de domínio, é apresentada uma opção para a configuração de segurança relacionada a permissões de usuário e de grupo. Essa opção controla se usuários arbitrários poderão recuperar associações do grupo do Active Directory. Se um controlador de domínio é configurado para que as contas locais tenham a autoridade para consultar a associação ao grupo das contas de usuário de domínio, o ID do usuário padrão criado pelo IBM MQ durante o processo de instalação pode obter associações de grupo para outros usuários, conforme necessário. No entanto, se um controlador de domínio for configurado para que as contas locais não tenham a autoridade para consultar a associação ao grupo das contas de usuário de domínio, isso impedirá que o IBM MQ conclua suas verificações de que os usuários que estão definidos no domínio estão autorizados a acessar gerenciadores de filas ou filas e o acesso falhará. Se você estiver usando o Windows em um controlador de domínio que tenha tiver sido configurado desta forma, uma conta de usuário do domínio especial com as permissões necessárias deve ser usada.

Neste caso, você precisa saber:

- Como as permissões de segurança para sua versão do Windows comporte-se.
- Como permitir que membros do grupo mqm de domínio leiam associação ao grupo.
- Como configurar um serviço do IBM MQ Windows para ser executado sob um usuário do domínio.

Para obter mais informações, consulte Configurando contas do usuário para o IBM MQ.

Acesso doIBM MQ para o grupo mqm local

Quando os servidores Windows são promovidos ou rebaixados para controladores de domínio, o IBM MQ perde o acesso ao grupo mqm local.

Quando um servidor é promovido para controlador de domínio, o escopo é alterado de local para domínio local. Quando a máquina é rebaixada para servidor, todos os grupos locais do domínio são removidos. Isso significa que alterar uma máquina de servidor para controlador de domínio e novamente para

servidor perde o acesso a um grupo mqm local. O sintoma é um erro indicando a perda de um grupo mqm local, por exemplo:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

Para resolver esse problema, recrie o grupo mqm local usando as ferramentas de gerenciamento padrão do Windows. Como todas as informações de associação ao grupo são perdidas, deve-se restabelecer os usuários privilegiados do IBM MQ no grupo mqm local recém criado. Se a máquina for um membro de domínio, também se deve incluir o grupo mqm de domínio no grupo mqm local, a fim de conceder aos IDs de usuário privilegiado de domínio do IBM MQ o nível de autoridade necessário.

Windows *Restrições em grupos aninhados no Windows*

Há restrições no uso de grupos aninhados. Estas resultam, em parte, do nível funcional do domínio e, em parte, das restrições do IBM MQ.

O Active Directory pode suportar diferentes tipos de grupos em um contexto de domínio, dependendo do nível funcional do domínio. Por padrão, os domínios Windows 2003 estão no nível funcional "Windows 2000 combinado". (Windows O Server 2008 e o Windows Server 2012 seguem o modelo de domínio Windows 2003.) O nível funcional do domínio determina os tipos de grupos suportados e o nível de aninhamento permitido ao configurar IDs do usuário e um ambiente de domínio. Consulte a documentação do Active Directory para obter detalhes sobre o Escopo de Grupo e os critérios de inclusão.

Além de requisitos de Active Directory, ainda se acrescentam restrições em IDs usados pelo IBM MQ. As APIs de rede usadas pelo IBM MQ não suportam todas as configurações que são suportadas pelo nível funcional de domínio. Como resultado, o IBM MQ não é capaz de consultar as associações do grupo de todos os IDs de Domínio presentes em um grupo de Domínio Local, que é então aninhado em um grupo local. Além disso, o aninhamento múltiplo de grupos globais e universais não é suportado. No entanto, grupos globais e universais imediatamente aninhados são suportados.

Windows *Autorizando Usuários a Usar o IBM MQ Remotamente*

Se você precisar criar e iniciar gerenciadores de filas quando conectado ao IBM MQ remotamente, deverá ter o acesso de usuário `Criar objetos globais`.

Sobre esta tarefa

Nota: Os administradores possuem o acesso de usuário `Create global objects` por padrão; portanto, se você for um administrador, será possível criar e iniciar gerenciadores de filas quando conectado remotamente, sem alterar seus direitos de usuário.

Se você estiver se conectando a uma máquina Windows usando os Serviços de terminal ou uma Conexão de área de trabalho remota e tiver problemas ao criar, iniciar ou excluir um gerenciador de filas, isso poderá ser porque você não tem o acesso de usuário `Criar objetos globais`.

O acesso de usuário `Create global objects` limita os usuários autorizados a criarem objetos no namespace global. Para que um aplicativo crie um objeto global, ele deve estar em execução no namespace global ou o usuário com o qual o aplicativo está sendo executado deve ter o acesso de usuário `Create global objects` aplicado a ele.

Quando você se conecta remotamente a uma máquina Windows utilizando os Serviços de terminal ou uma Conexão de área de trabalho remota, os aplicativos são executados em seus próprios namespaces locais. Se você tentar criar ou excluir um gerenciador de filas usando o IBM MQ Explorer ou o comando **crtmqm** ou **dltmqm**, ou iniciar um gerenciador de filas usando o comando **strmqm**, o resultado será uma falha de autorização. Isso cria um IBM MQ FDC com o ID de análise XY132002.

Iniciar um gerenciador de filas usando o IBM MQ Explorer ou usando o comando **amqmdain qmgr start** funciona corretamente porque esses comandos não iniciam diretamente o gerenciador de filas. Ao contrário, os comandos enviam um pedido para iniciar o gerenciador de filas em um processo separado em execução no espaço de nomes global.

Se os vários métodos de administração do IBM MQ não funcionarem ao usar serviços de terminal, tente configurar o direito de usuário `Criar objetos globais`.

Procedimento

1. Abra o painel Ferramentas Administrativas:

   Windows Server 2008 e Windows Server 2012
   Acesse esse painel usando **Painel de Controle** > **Sistema e Manutenção** > **Ferramentas Administrativas**.

   Windows 8.1
   Acesse esse painel utilizando **Ferramentas administrativas** > **Gerenciamento do computador**
2. Clique duas vezes em **Política de Segurança Local**.
3. Expanda **Políticas locais**.
4. Clique em **Atribuições de direitos de usuário**.
5. Inclua o novo usuário ou grupo na política `Criar objetos globais`.

Windows *O programa de saída do canal SSPI no Windows*

O IBM MQ for Windows fornece um programa de saída de segurança, que pode ser usado em canais de mensagens e canais de MQI. A saída é fornecida como código-fonte e de objeto, além de fornecer autenticação unilateral e de duas vias.

A saída de segurança usa o Security Support Provider Interface (SSPI), que fornece os recursos de segurança integrados das plataformas do Windows.

A saída de segurança fornece os seguintes serviços de identificação e de autenticação:

Autenticação de uma via
Este serviço usa o Windows NT suporte de autenticação do LAN Manager (NTLM). O NTLM permite que os servidores autentiquem seus clientes. Ele não permite que um cliente autentique um servidor, ou um servidor autentique outro servidor. O NTLM foi projetado para um ambiente de rede no qual supõe-se que os servidores sejam autênticos. NTLM é suportado em todas as plataformas do Windows que são suportadas pelo IBM WebSphere MQ 7.0.

Este serviço é usado geralmente em um canal de MQI para permitir que um gerenciador de filas do servidor autentique um aplicativo do IBM MQ MQI client. Um aplicativo cliente é identificado pelo ID de usuário associado ao processo em execução.

Para efetuar a autenticação, a saída de segurança na extremidade do cliente de um canal adquire um token de autenticação do NTLM e envia o token em uma mensagem de segurança para seu parceiro na outra extremidade do canal. A saída de segurança do parceiro transmite o token para o NTLM, que verifica se ele é autêntico. Se a saída de segurança do parceiro não for atendida quanto à autenticidade do token, ela instrui o MCA a fechar o canal.

Autenticação de duas vias ou mútua
Utiliza os serviços de autenticação do Kerberos. O protocolo Kerberos não supõe que os servidores em um ambiente de rede sejam autênticos. Servidores podem autenticar clientes e outros servidores, e clientes podem autenticar servidores. O Kerberos é suportado em todas as plataformas do Windows que são suportadas pelo IBM WebSphere MQ 7.0.

Este serviço pode ser utilizado em canais de mensagens e do MQI. Em um canal de mensagens, ele fornece autenticação mútua dos dois gerenciadores de filas. Em um canal de MQI, ele ativa o gerenciador de filas do servidor e o aplicativo do IBM MQ MQI client para autenticar um ao outro. Um gerenciador de filas é identificado por seu nome prefixado pela sequência `ibmMQSeries/`. Um aplicativo cliente é identificado pelo ID de usuário associado ao processo em execução.

Para efetuar a autenticação mútua, a saída de segurança iniciadora adquire um token de autenticação do servidor de segurança Kerberos e envia o token em uma mensagem de segurança para seu parceiro. A saída de segurança do parceiro transmite o token para o servidor de segurança do Kerberos, que verifica se é autêntico. O servidor de segurança do Kerberos gera um segundo token,

que é enviado pelo parceiro em uma mensagem de segurança para a saída de segurança iniciadora. A saída de segurança iniciadora solicita então ao servidor Kerberos que verifique se o segundo token é autêntico. Durante esta troca, se alguma das saídas de segurança não for atendida quanto à autenticidade do token enviado pela outra, ela instrui o MCA a fechar o canal.

A saída de segurança é fornecida no formato de fonte e de objeto. Você pode utilizar o código fonte como um ponto de início para criar seus próprios programas de saída de canal ou utilizar o módulo de objeto conforme fornecido. O módulo de objeto tem dois pontos de entrada, uma para autenticação de uma via utilizando o suporte para autenticação do NTLM e o outro para autenticação de duas vias utilizando os serviços de autenticação do Kerberos.

Para obter mais informações sobre como o programa de saída do canal SSPI funciona e para obter instruções sobre como implementá-lo, consulte Usando a saída de segurança SSPI em sistemas Windows.

Windows *Aplicando arquivos de modelo de segurança no Windows*

Aplicar um modelo pode afetar as configurações de segurança aplicadas aos arquivos e diretórios do IBM MQ. Se você usa o modelo altamente seguro, aplique-o antes de instalar o IBM MQ.

O Windows suporta arquivos de modelo de segurança baseados em texto que podem ser usados para aplicar as configurações de segurança uniformes para um ou mais computadores com o snap-in MMC de configuração e análise de segurança. Em particular, o Windows fornece vários modelos que incluem um intervalo de configurações de segurança com o objetivo de fornecer níveis específicos de segurança. Esses modelos incluem Compatível, Seguro e Altamente Seguro.

Aplicar um desses modelos pode afetar as configurações de segurança aplicadas aos arquivos e diretórios do IBM MQ. Se quiser usar o modelo Altamente Seguro, configure sua máquina antes de instalar o IBM MQ.

Se aplicar o modelo altamente seguro a uma máquina na qual o IBM MQ já está instalada, todas as permissões definidas nos arquivos e diretórios do IBM MQ serão removidas. Com a remoção dessas permissões, você perde acesso ao grupo de *Administradores*, *mqm* e, quando aplicável, ao grupo *Todos*, a partir dos diretórios de erro.

Windows *Configurando autoridade adicional para aplicativos Windows que se conectam ao IBM MQ*

A conta sob a qual os processos do IBM MQ são executados talvez precise de autorização adicional para que o acesso SYNCHRONIZE aos processos do aplicativo possa ser concedido.

Sobre esta tarefa

Pode haver problemas se você tiver aplicativos do Windows, por exemplo, as páginas ASP, que se conectam ao IBM MQ que são configuradas para executar em um nível de segurança mais alto do que o normal.

O IBM MQ requer o acesso SYNCHRONIZE aos processos do aplicativo para coordenar determinadas ações. Quando um aplicativo do servidor tenta primeiro se conectar a um gerenciador de filas, o IBM MQ modifica o processo para conceder autoridade SYNCHRONIZE para os administradores do IBM MQ. No entanto, a conta sob a qual os processos IBM MQ são executados pode precisar de autorização adicional antes que o acesso solicitado possa ser concedido.

Para configurar autoridade adicional para o ID do usuário sob o qual os processos do IBM MQ estão em execução, conclua as seguintes etapas:

Procedimento

1. Inicie a ferramenta Política de segurança local, clique em **Configurações de segurança**->**Políticas locais**->**Designações de direito do usuário**, clique em **Depurar programas**.
2. Dê um clique duplo em **Programas de depuração** e, em seguida, inclua seu ID do usuário do IBM MQ na lista

Se o sistema estiver em um domínio do Windows e a configuração de política efetiva ainda não estiver definida, mesmo que a configuração da política local esteja, o ID do usuário deve ser autorizado do mesmo modo no nível do domínio, usando a ferramenta Política de Segurança de Domínio.

IBM i Configurando a Segurança em IBM i

A segurança no IBM i é implementada usando o gerenciador de autoridade de objeto (OAM) do IBM MQ e a segurança no nível do objeto do IBM i.

Considerações de segurança que devem ser feitas ao determinar autoridade de acesso para objetos do IBM MQ.

Você precisa considerar os seguintes pontos ao configurar as autoridades para os usuários em sua empresa:

1. Conceda e revogue autoridades para os comandos do IBM MQ for IBM i usando os comandos IBM i GRTOBJAUT e RVKOBJAUT.

   Na biblioteca QMQM, certos objetos sem comando (*cmd) são configurados para ter autoridade ***PUBLIC** para ***USE**. Não altere as autoridades desses objetos, ou use uma lista de autorização para fornecer autoridade. Qualquer autoridade incorreta pode comprometer a funcionalidade do IBM MQ.
2. Durante a instalação do IBM MQ for IBM i, os seguintes perfis de usuário especial são criados:

   QMQM
   É usado principalmente para funções internas somente do produto. No entanto, ele pode ser usado para executar aplicativos confiáveis usando MQCNO_FASTPATH_BINDINGS. Consulte Conectando-se a um gerenciador de filas usando a chamada MQCONNX.

   QMQMADM
   É usado como um perfil de grupo para administradores do IBM MQ. O perfil do grupo fornece acesso a comandos CL e recursos do IBM MQ.

   Ao usar SBMJOB para enviar programas que chamam comandos do IBM MQ, USER não deve ser configurado explicitamente para QMQMADM. Em vez disso, configure USER para QMQM ou outro perfil do usuário que tenha QMQMADM especificado como um grupo.
3. Se você estiver enviando os comandos de canal para os gerenciadores de fila remotos, certifique-se de que o seu perfil de usuário é membro do grupo QMQMADM no sistema de destino. Para obter uma lista de comandos do canal PCF e MQSC, consulte os comandos da CL do IBM MQ for IBM i.
4. O conjunto de grupos associado a um usuário é armazenado em cache quando as autorizações do grupo são calculadas pelo OAM.

   As mudanças feitas nas associações do grupo de um usuário depois que o conjunto de grupos é armazenado em cache não são reconhecidas até que o gerenciador de filas seja reiniciado ou que RFRMQMAUT seja executado para atualizar a segurança.
5. Limite o número de usuários que possuem autoridade para trabalhar com comandos que são particularmente sigilosos. Esses comandos incluem:
   - Criar gerenciador da fila de mensagens (CRTMQM)
   - Excluir gerenciador da fila de mensagens (DLTMQM)
   - Iniciar gerenciador da fila de mensagens (STRMQM)
   - Finalizar gerenciador da fila de mensagens (ENDMQM)
   - Iniciar servidor de comandos (STRMQMCSVR)
   - Finalizar servidor de comandos (ENDMQMCSVR)
6. As definições de canal contêm uma especificação do programa de saída de segurança. A criação e a modificação do canal requerem considerações especiais. Os detalhes de saídas de segurança são fornecidos em “Visão Geral da Saída de Segurança” na página 106.
7. A saída de canal e os programas do monitor acionador podem ser substituídos. A segurança dessas substituições é de responsabilidade do programador.

IBM i Gerenciador de autoridade de objeto no IBM i

O gerenciador de autoridade de objeto (OAM) gerencia as autorizações dos usuários para manipular objetos do IBM MQ, incluindo filas e definições de processo. Ele também fornece uma interface de comandos pela qual é possível conceder ou revogar autoridade de acesso a um objeto para um grupo específico de usuários. A decisão de permitir acesso a um recurso é feita pelo OAM, e o gerenciador de filas segue essa decisão. Se o OAM não puder tomar uma decisão, o gerenciador de filas evitará o acesso a esse recurso.

Por meio do OAM, é possível controlar:

- O acesso a objetos do IBM MQ por meio do MQI. Quando um programa de aplicativo tenta acessar um objeto, o OAM verifica se o perfil do usuário que está fazendo a solicitação tem a autorização para a operação solicitada.

  Especificamente, isso significa que as filas, e as mensagens nas filas, podem ser protegidas contra acesso não autorizado.
- Permissão de usar comandos PCF e MQSC.

Diferentes grupos de usuários podem ter autoridade de acesso diferente para o mesmo objeto. Por exemplo, para uma fila específica, um grupo pode executar ambas as operações, put e get; outro grupo pode ter permissão apenas para navegar pela fila (MQGET com a opção de navegação). De forma semelhante, alguns grupos podem ter as autoridades get e put para uma fila, mas podem não ter permissão para alterar ou excluir a fila.

Comandos e operações de execução do IBM MQ for IBM i em objetos do IBM MQ for IBM i

IBM i Autoridades do IBM MQ no IBM i

Para acessar objetos do IBM MQ, é necessário ter a autoridade para emitir o comando e para acessar o objeto referenciado. Administradores têm acesso a todos os recursos do IBM MQ.

O acesso aos objetos do IBM MQ é controlado por autoridades para:

1. Emitir o comando do IBM MQ
2. Acessar os objetos do IBM MQ referenciados pelo comando

Todos os comandos de CL do IBM MQ for IBM i são fornecidos com um proprietário de QMQM, e a administração do perfil (QMQMADM) tem direitos *USE com o acesso *PUBLIC configurado como *EXCLUDE.

Nota: O programa QSRDUPER é usado pelo instalador do programa licenciado do IBM MQ for IBM i para duplicar objetos de Comando (*CMD) em QSYS. No IBM i V5R4 e posterior, o programa QSRDUPER foi mudado para que o comportamento padrão seja criar um comando proxy em vez de uma duplicação do comando original. Um comando proxy redireciona a execução do comando para outro comando e tem um atributo de PRX. Se existir um comando proxy com o mesmo nome do comando que está sendo copiado na biblioteca QSYS, as autoridades privadas para o comando proxy não serão concedidas ao comando na biblioteca do produto. Tentativas de solicitar ou de executar o comando proxy no QSYS verificam a autoridade do comando de destino na biblioteca do produto. Qualquer mudança na autoridade para objetos *CMD, portanto, precisa ser feita na biblioteca do produto (QMQM) e as do QSYS não precisam ser modificadas. Por exemplo:

```
GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
```

As mudanças na estrutura de autoridade de alguns dos comandos de CL do produto permitem o uso público destes comandos, se você tiver autoridade do OAM necessária para os objetos do IBM MQ para fazer essas mudanças.

Para ser um administrador do IBM MQ no IBM i, deve-se ser um membro do *grupo QMQMADM*. Este grupo tem propriedades como as propriedades do grupo mqm nos sistemas UNIX, Linux e Windows. Em particular, o grupo QMQMADM é criado ao se instalar o IBM MQ for IBM i, e os membros do grupo

QMQMADM possuem acesso a todos os recursos do IBM MQ no sistema. Você também tem acesso a todos os recursos do IBM MQ se tiver a autoridade *ALLOBJ.

Os administradores podem usar comandos CL para administrar o IBM MQ. Um desses comandos de controle é GRTMQMAUT, que é utilizado para conceder autoridades a outros usuários. Outro comando, STRMQMMQSC, permite que um administrador emita comandos MQSC para um gerenciador de fila local.

Conceitos relacionados

"Autoridade para administrar o IBM MQ no IBM i" na página 85

IBM i *Autoridades de acesso para objetos do IBM MQ no IBM i*

As autoridades de acesso necessárias para executar os comandos de CL do IBM MQ.

O IBM MQ for IBM i categoriza os comandos de CL do produto em dois grupos:

Grupo 1

Os usuários devem estar no grupo de usuários QMQMADM ou ter a autoridade *ALLOBJ, para processar esses comandos. Usuários com uma dessas autoridades podem processar todos os comandos em todas as categorias sem precisar de autoridade extra.

Nota: Essas autoridades substituem qualquer autoridade OAM.

Estes comandos podem ser agrupados da seguinte forma:

- Comandos do Servidor de Comandos
  - ENDMQMCSVR, Finalizar o servidor de comandos do IBM MQ
  - STRMQMCSVR, Iniciar o servidor de comandos do IBM MQ
- Comando do Manipulador da Fila de Devoluções
  - STRMQMDLQ, Iniciar o manipulador da fila de devoluções do IBM MQ
- Comando Listener
  - ENDMQMLSR, Terminar listener IBM MQ
  - STRMQMLSR, Iniciar listener de não objeto
- Comandos de Recuperação de Mídia
  - RCDMQMIMG, Registrar imagem do objeto IBM MQ
  - RCRMQMOBJ, Recriar o objeto do IBM MQ
  - WRKMQMTRN, Trabalhar com as transações Q do IBM MQ
- Comandos do Gerenciador de Filas
  - CRTMQM, Criar Gerenciador da Fila de Mensagens
  - DLTMQM, Excluir Gerenciador da Fila de Mensagens
  - ENDMQM, Terminar Gerenciador da Fila de Mensagens
  - STRMQM, Iniciar Gerenciador da Fila de Mensagens
- Comandos de Segurança
  - GRTMQMAUT, Conceder autoridade de objeto ao IBM MQ
  - RVKMQMAUT, Revogar autoridade de objeto do IBM MQ
- Comando de Rastreio
  - TRCMQM, Rastrear tarefa do IBM MQ
- Comandos de Transação
  - RSVMQMTRN, Resolve IBM MQ Transaction
- Comandos do Monitor Acionador
  - STRMQMTRM, Iniciar Monitor Acionador

- Comandos de SC do IBM MQ
  - RUNMQSC, Executar comandos de SC do IBM MQ
  - STRMQMMQSC, Iniciar comandos de SC do IBM MQ

Grupo 2

O restante dos comandos, para os quais dois níveis de autoridade são necessários:

1. Autoridade do IBM i para executar o comando. Um administrador do IBM MQ configura isto usando o comando **GRTOBJAUT** para substituir a restrição *PUBLIC(de *EXCLUDE) em um usuário ou grupo de usuários.

   Por exemplo:

   ```
   GRTOBJAUT OBJ(QMQM/DSPMQMQ) OBJTYPE(*CMD) USER(MQUSER) AUT(*USE)
   ```

2. Autoridade do IBM MQ para manipular os objetos do IBM MQ associados ao comando, ou comandos, dada a autoridade correta do IBM i na Etapa 1.

   Esta autoridade é controlada pelo usuário que tem a autoridade OAM apropriada para a ação necessária, definida por um administrador do IBM MQ usando o comando **GRTMQMAUT**

   Por exemplo:

   ```
   GRTMQMAUT *connect authority to the queue manager + *admchg authority to
           the queue
   ```

Os comandos podem ser agrupados da seguinte forma:

- Comandos do Canal
  - CHGMQMCHL, Alterar Canal IBM MQ

    Isso requer a autoridade *connect para o gerenciador de filas e a autoridade *admchg para o canal.
  - CPYMQMCHL, Copiar Canal IBM MQ

    Isso requer a autoridade *connect e *admcrt para o gerenciador de filas, a autoridade *admdsp para o tipo de canal padrão a ser copiado e a autoridade *admcrt para a classe de objeto do canal.

    Por exemplo, copiar um canal emissor precisa da autoridade *admdsp para o canal SYSTEM.DEF.SENDER
  - CRTMQMCHL, Criar Canal IBM MQ

    Isso requer a autoridade *connect e *admcrt para o gerenciador de filas, a autoridade *admdsp para o tipo de canal padrão a ser criado e a autoridade *admcrt para a classe de objeto do canal.

    Por exemplo, criar um canal emissor precisa da autoridade *admdsp para o canal SYSTEM.DEF.SENDER.
  - DLTMQMCHL, Excluir Canal IBM MQ

    Isso requer a autoridade *connect para o gerenciador de filas, e a autoridade *admdlt para o canal.
  - RSVMQMCHL, Resolver IBM MQ Canal

    Isso requer a autoridade *connect para o gerenciador de filas, e a autoridade *ctrlx para o canal.
- Comandos de Exibição

  Para processar os comandos DSP, você deve conceder ao usuário as autoridades `*connect` e `*admdsp` para o gerenciador de filas, juntamente com qualquer opção específica listada:
  - DSPMQM, Exibir Gerenciador da Fila de Mensagens
  - DSPMQMAUT, Display IBM MQ Object Authority

  - DSPMQMAUTI, Display IBM MQ Authentication Information - *admdsp para o objeto de informações sobre autenticação
  - DSPMQMCHL, Display IBM MQ Channel - *admdsp para o canal
  - DSPMQMCSVR, Exibir Servidor de Comandos IBM MQ
  - DSPMQMNL, Display IBM MQ Namelist - *admdsp para a lista de nomes
  - DSPMQMOBJN, Display IBM MQ Object Names
  - DSPMQMPRC, Display IBM MQ Process - *admdsp para o processo
  - DSPMQMQ, Display IBM MQ Queue - *admdsp para a fila
  - DSPMQMTOP, Display IBM MQ Topic - *admdsp para o tópico
- Trabalhar com comandos

  Para processar os comandos WRK e exibir o painel de opções, você deve conceder ao usuário as autoridades *connect e *admdsp para o gerenciador de filas, juntamente com qualquer opção específica listada:
  - WRKMQM, Trabalhar com Gerenciadores da Fila de Mensagens
  - WRKMQMAUT, Trabalhar com a Autoridade do Objeto IBM MQ
  - WRKMQMAUTD, Trabalhar com Dados de Autoridade do Objeto IBM MQ
  - WRKMQMAUTI, Trabalhar com IBM MQ Informações sobre Autenticação
    - *admchg para o comando Change IBM MQ Authentication Information Object.
    - *admcrt para o comando Create and Copy IBM MQ Authentication Information Object.
    - *admdlt para o comando Delete IBM MQ Authentication Information Object.
    - *admdsp para o comando Display IBM MQ Authentication Information Object.
  - WRKMQMCHL, Trabalhar com o canal do IBM MQ

    Isso requer as seguintes autoridades:
    - *admchg para o comando Change IBM MQ Channel.
    - *admclr para o comando Clear IBM MQ Channel.
    - *admcrt para o comando Create and Copy IBM MQ Channel.
    - *admdlt para o comando Delete IBM MQ Channel.
    - *admdsp para o comando Display IBM MQ Channel.
    - *ctrl para o comando Start IBM MQ Channel.
    - *ctrl para o comando End IBM MQ Channel.
    - *ctrl para o comando Ping IBM MQ Channel.
    - *ctrlx para o comando Reset IBM MQ Channel.
    - *ctrlx para o comando Resolve IBM MQ Channel.
  - WRKMQMCHST, Trabalhar com o Status do Canal IBM MQ

    Isso requer a autoridade *admdsp para o canal.
  - WRKMQMCL, Trabalhar com Clusters IBM MQ
  - WRKMQMCLQ, Trabalhar com IBM MQ Filas de Cluster
  - WRKMQMCLQM, Trabalhar com o Gerenciador de Filas do Cluster IBM MQ
  - WRKMQMLSR, Trabalhar com Listener IBM MQ
  - WRKMQMMSG, Trabalhar com Mensagens IBM MQ

    Isso requer a autoridade *browse para a fila
  - WRKMQMNL, Trabalhar com listas de nomes do IBM MQ

    Isso requer as seguintes autoridades:

- *admchg para o comando Change IBM MQ Namelist.
- *admcrt para o comando Create and Copy IBM MQ Namelist.
- *admdlt para o comando Delete IBM MQ Namelist.
- *admdsp para o comando Display IBM MQ Namelist.

– WRKMQMPRC, Trabalhar com processos do IBM MQ

Isso requer as seguintes autoridades:

- *admchg para o comando Change IBM MQ Process.
- *admcrt para o comando Create and Copy IBM MQ Process.
- *admdlt para o comando Delete IBM MQ Process.
- *admdsp para o comando Display IBM MQ Process.

– WRKMQMQ, Trabalhar com filas do IBM MQ

Isso requer as seguintes autoridades:

- *admchg para o comando Change IBM MQ Queue.
- *admclr para o comando Clear IBM MQ Queue.
- *admcrt para o comando Create and Copy IBM MQ Queue.
- *admdlt para o comando Delete IBM MQ Queue.
- *admdsp para o comando Display IBM MQ Queue.

– WRKMQMQSTS, Trabalhar com IBM MQ Status da fila

– WRKMQMTOP, Trabalhar com IBM MQ Tópicos

Isso requer as seguintes autoridades

- *admchg para o comando Change IBM MQ Topic.
- *admcrt para o comando Create and Copy IBM MQ Topic.
- *admdlt para o comando Delete IBM MQ Topic.
- *admdsp para o comando Display IBM MQ Topic.

– WRKMQMSUB, Trabalhar com assinaturas do IBM MQ

• Outros comandos de Canal

Para processar os comandos de canal, você deve conceder ao usuário as autoridades específicas listadas:

– ENDMQMCHL, Fim do Canal IBM MQ

Isso requer a autoridade *connect para o gerenciador de filas e a autoridade *allmqi para a fila de transmissão associada ao canal.

– ENDMQMLSR, Encerrar Listener IBM MQ

Isso requer a autoridade *connect para o gerenciador de filas e a autoridade *ctrl para o objeto de listener nomeado.

– PNGMQMCHL, Ping IBM MQ Canal

Isto requer a autoridade *connect e *inq para o gerenciador de filas, e a autoridade *ctrl para o objeto do canal.

– RSTMQMCHL, Reconfigurar Canal IBM MQ

Isso requer a autoridade *connect para o gerenciador de filas.

– STRMQMCHL, Iniciar Canal IBM MQ

Isso requer a autoridade *connect para o gerenciador de filas e a autoridade *ctrl para o objeto de canal.

– STRMQMCHLI, Iniciar Inicializador de Canais IBM MQ

Isso requer as autoridades `*connect` e `*inq` para o gerenciador de filas e a autoridade `*allmqi` para a fila de inicialização associada à fila de transmissão do canal.

– STRMQMLSR, Iniciar Listener IBM MQ

Isso requer a autoridade *connect para o gerenciador de filas e a autoridade *ctrl para o objeto de listener nomeado.

- Outros comandos:

Para processar os seguintes comandos, você deve conceder ao usuário as autoridades específicas listadas:

– CCTMQM, Conectar-se ao Gerenciador da Fila de Mensagens

Isso não requer autoridade de objeto do IBM MQ.

– CHGMQM, Alterar Gerenciador da Fila de Mensagens

Isso requer as autoridades `*connect` e `*admchg` para o gerenciador de filas.

– CHGMQMAUTI, Alterar IBM MQ Informações sobre Autenticação

Isso requer a autoridade `*connect` para o gerenciador de filas, e a autoridade `*admchg` e `*admdsp` para o objeto de informações sobre autenticação.

– CHGMQMNL, Alterar Lista de Nomes IBM MQ

Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admchg` para a lista de nomes.

– CHGMQMPRC, Alterar Processo IBM MQ

Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admchg` para o processo.

– CHGMQMQ, Alterar Fila IBM MQ

Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admchg` para a fila.

– CLRMQMQ, Limpar Fila IBM MQ

Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admclr` para a fila.

– CPYMQMAUTI, Copiar IBM MQ Informações sobre Autenticação

Isso requer a autoridade `*connect` para o gerenciador de filas, a autoridade `*admdsp` para o objeto de informações sobre autenticação e a autoridade `*admcrt` para a classe do objeto de informações sobre autenticação.

– CPYMQMNL, Lista de Nomes de Cópia IBM MQ

Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas.

– CPYMQMPRC, Copiar IBM MQ Processo

Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas.

– CPYMQMQ, Fila de Cópia IBM MQ

Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas.

– CRTMQMAUTI, Criar IBM MQ Informações sobre Autenticação

Isso requer a autoridade `*connect` para o gerenciador de filas, a autoridade `*admdsp` para o objeto de informações sobre autenticação e a autoridade `*admcrt` para a classe do objeto de informações sobre autenticação.

– CRTMQMNL, Criar Lista de Nomes IBM MQ

Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas e a autoridade `*admdsp` para a lista de nomes padrão.

– CRTMQMPRC, Criar Processo IBM MQ

Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas e a autoridade `*admdsp` para o processo padrão.

- CRTMQMQ, Criar Fila IBM MQ

  Isso requer as autoridades `*connect` e `*admcrt` para o gerenciador de filas e a autoridade `*admdsp` para a fila padrão.

- CVTMQMDTA, Converter Comando de Tipo de Dados IBM MQ

  Isso não requer autoridade de objeto do IBM MQ.

- DLTMQMAUTI, Excluir Informações sobre Autenticação IBM MQ

  Isso requer a autoridade `*connect` para o gerenciador de filas, e a autoridade `*ctrlx` para o objeto de informações sobre autenticação.

- DLTMQMNL, Excluir Namelist IBM MQ

  Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admdlt` para a lista de nomes.

- DLTMQMPRC, Excluir IBM MQ Processo

  Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admdlt` para o processo.

- DLTMQMQ, Excluir Fila IBM MQ

  Isso requer a autoridade `*connect` para o gerenciador de filas e a autoridade `*admdlt` para a fila.

- DSCMQM, Desconectar-se do Gerenciador da Fila de Mensagens

  Isso não requer autoridade de objeto do IBM MQ.

- RFRMQMAUT, Atualizar Segurança

  Isso requer a autoridade `*connect` para o gerenciador de filas.

- RFRMQMCL, Atualizar Cluster

  Isso requer a autoridade `*connect` para o gerenciador de filas.

- RSMMQMCLQM, Continuar o Gerenciador de Filas do Cluster

  Isso requer a autoridade `*connect` para o gerenciador de filas.

- RSTMQMCL, Reconfigurar Cluster

  Isso requer a autoridade `*connect` para o gerenciador de filas.

- SPDMQMCLQM, Suspender Gerenciador de Filas do Cluster

  Isso requer a autoridade `*connect` para o gerenciador de filas.

IBM i *Autorizações de acesso no IBM i*

Use estas informações para entender os comandos de autorização de acesso.

As autorizações definidas pela palavra-chave AUT nos comandos GRTMQMAUT e RVKMQMAUT podem ser categorizadas da seguinte forma:

- Autorizações relacionadas a chamadas MQI
- Comandos de administração relacionados à autorização
- Autorizações de contexto
- Autorizações gerais, isto é, para chamadas MQI, para comandos, ou ambos

As tabelas a seguir listam as diferentes autoridades, usando o parâmetro AUT para chamadas MQI, chamadas de Contexto, comandos MQSC e PCF e operações genéricas.

Tabela 15. Autorizações para Chamadas MQI	
AUT	**Descrição**
*ALTUSR	Permitir que a autoridade de um outro usuário seja usada para chamadas de MQOPEN e MQPUT1.
*BROWSE	Recuperar uma mensagem de uma fila, emitindo uma chamada MQGET com a opção BROWSE.
*CONNECT	Conecte o aplicativo ao gerenciador de filas especificado, emitindo uma chamada MQCONN.
*GET	Recuperar uma mensagem de uma fila, emitindo uma chamada MQGET.
*INQ	Fazer uma consulta em uma fila específica, emitindo uma chamada MQINQ.
*PUB	Abrir um tópico para publicar uma mensagem, usando uma chamada MQPUT.
*PUT	Colocar uma mensagem em uma fila específica, emitindo uma chamada MQPUT.
*RESUME	Continuar uma assinatura, usando uma chamada MQSUB.
*SET	Configurar atributos em uma fila a partir de MQI, emitindo uma chamada MQSET. Se você abrir uma fila para várias opções, deverá ter autorização para cada uma delas.
*SUB	Criar, Alterar ou Continuar uma assinatura para um tópico, usando uma chamada MQSUB.

Tabela 16. Autorizações para Chamadas de Contexto	
AUT	**Descrição**
*PASSALL	Passar todo o contexto na fila especificada. Todos os campos de contexto são copiados da solicitação original.
*PASSID	Passar contexto de identidade na fila especificada. O contexto de identidade é igual àquele da solicitação.
*SETALL	Configurar todo o contexto na fila especificada. Isso é usado por utilitários especiais do sistema.
*SETID	Configurar contexto de identidade na fila especificada. Isso é usado por utilitários especiais do sistema.

Tabela 17. Autorizações para Chamadas MQSC e PCF	
AUT	**Descrição**
*ADMCHG	Alterar os atributos do objeto especificado.
*ADMCLR	Limpar o objeto especificado (apenas o comando PCF Limpar objeto).
*ADMCRT	Criar objetos do tipo especificado.
*ADMDLT	Excluir o objeto especificado.
*ADMDSP	Exibir os atributos do objeto especificado.

Tabela 18. Autorizações para Operações Genéricas	
AUT	**Descrição**
*ALL	Usar todas as operações aplicáveis ao objeto. A autoridade `all` é equivalente à união das autoridades `alladm`, `allmqi` e `system` apropriadas ao tipo de objeto.

Tabela 18. Autorizações para Operações Genéricas (continuação)	
AUT	**Descrição**
*ALLADM	Executar todas as operações de administração aplicáveis ao objeto.
*ALLMQI	Usar todas as chamadas MQI aplicáveis ao objeto.
*CTRL	Controlar a inicialização e o encerramento de canais, listeners e serviços.
*CTRLX	Reconfigurar o número de sequência e resolver canais indeterminados.

IBM i *Usando os comandos de autorização de acesso no IBM i*

Use estas informações para aprender sobre os comandos de autorização de acesso e use os exemplos de comandos.

Usando o Comando GRTMQMAUT

Se você tiver a autorização necessária, poderá usar o comando GRTMQMAUT para conceder autorização de um perfil de usuário ou grupo de usuários para acessar um determinado objeto. Os seguintes exemplos ilustram como o comando GRTMQMAUT é usado:

1. ```
   GRTMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
             AUT(*BROWSE *PUT) MQMNAME('saturn.queue.manager')
   ```

   Nesse exemplo:

   - RED.LOCAL.QUEUE é o nome do objeto.
   - *LCLQ (fila local) é o tipo de objeto.
   - GROUPA é o nome de um perfil de usuário no sistema para o qual as autorizações devem ser mudadas. Esse perfil pode ser usado como um perfil do grupo para outros usuários.
   - *BROWSE e *PUT são as autorizações que estão sendo concedidas à fila especificada.

     *BROWSE inclui autorização para navegar pelas mensagens na fila (para emitir MQGET com a opção de navegação).

     *PUT inclui autorização para colocar (MQPUT) mensagens na fila.
   - saturn.queue.manager é o nome do gerenciador de filas.
2. O comando a seguir concede aos usuários JACK e JILL todas as autorizações aplicáveis, a todas as definições de processos, para o gerenciador de filas padrão.

   ```
   GRTMQMAUT OBJ(*ALL) OBJTYPE(*PRC) USER(JACK JILL) AUT(*ALL)
   ```
3. O comando a seguir concede ao usuário GEORGE autoridade para colocar uma mensagem na fila ORDERS, no gerenciador de filas TRENT.

   ```
   GRTMQMAUT OBJ(TRENT) OBJTYPE(*MQM) USER(GEORGE) AUT(*CONNECT) MQMNAME (TRENT)
   GRTMQMAUT OBJ(ORDERS) OBJTYPE(*Q) USER(GEORGE) AUT(*PUT) MQMNAME (TRENT)
   ```

Usando o Comando RVKMQMAUT

Se você tiver a autorização necessária, poderá usar o comando RVKMQMAUT para remover a autorização concedida anteriormente de um perfil de usuário ou grupo de usuários para acessar um determinado objeto. Os seguintes exemplos ilustram como o comando RVKMQMAUT é usado:

1. ```
   RVKMQMAUT OBJ(RED.LOCAL.QUEUE) OBJTYPE(*LCLQ) USER(GROUPA) +
   AUT(*PUT) MQMNAME('saturn.queue.manager')
   ```

A autoridade para colocar mensagens na fila especificada, que foi concedida no exemplo anterior, é removida de GROUPA.

2.
```
RVKMQMAUT OBJ(PAY*) OBJTYPE(*Q) USER(*PUBLIC) AUT(*GET) +
MQMNAME(PAYROLLQM)
```

A autoridade para obter mensagens de qualquer fila com um nome que começa com os caracteres PAY, pertencente ao gerenciador de filas PAYROLLQM, é removida de todos os usuários do sistema, a menos que eles, ou um grupo ao qual eles pertencem, tenham sido autorizados separadamente.

Usando o Comando DSPMQMAUT

O comando (DSPMQMAUT) da autoridade de MQM mostra, para o objeto e usuário especificados, a lista de autorizações que o usuário tem para o objeto. O seguinte exemplo ilustra como o comando é usado:

```
DSPMQMAUT OBJ(ADMINNL) OBJTYPE(*NMLIST) USER(JOE) OUTPUT(*PRINT) +
MQMNAME(ADMINQM)
```

Usando o Comando RFRMQMAUT

O comando de segurança do MQM de atualização (RFRMQMAUT) permite atualizar as informações do grupo de autorização do OAM imediatamente, refletindo as mudanças feitas no nível do sistema operacional, sem precisar parar e reiniciar o gerenciador de filas. O seguinte exemplo ilustra como o comando é usado:

```
RFRMQMAUT MQMNAME(ADMINQM)
```

IBM i Tabelas de especificação de autorização no IBM i

Use estas informações para determinar qual autorização é necessária para usar chamadas API específicas, e opções específicas dessas chamadas, em objetos de fila, objetos de processo e objetos de gerenciador de filas.

As tabelas de especificação de autorização, iniciadas na Tabela 19 na página 167, definem precisamente como as autorizações funcionam e as restrições que se aplicam. As tabelas aplicam-se a estas situações:

- Aplicativos que emitem chamadas MQI
- Programas de administração que emitem comandos MQSC como PCFs Escape
- Programas de administração que emitem comando de PCF

Nesta seção, as informações são apresentadas como um conjunto de tabelas que especificam os seguintes dados:

Ação a ser executada
Opção de MQI, comando MQSC ou comando PCF.

Objeto de controle de acesso
Fila, definição de processo, gerenciador de filas, lista de nomes, canal, canal de conexão do cliente, listener, serviço ou objeto de informações sobre autenticação.

Authorization required
Expressa como uma constante MQZAO_.

Nas tabelas, as constantes prefixadas com MQZAO_ correspondem às palavras-chave na lista de autorização para os comandos **GRTMQMAUT** e **RVKMQMAUT** da entidade específica. Por exemplo, MQZAO_BROWSE corresponde à palavra-chave *BROWSE; de forma semelhante, a palavra-chave MQZAO_SET_ALL_CONTEXT corresponde à palavra-chave *SETALL e assim por diante. Essas constantes são definidas no arquivo de cabeçalho cmqzc.h, fornecido com o produto.

autorizações MQI

Um aplicativo terá permissão para emitir chamadas MQI e opções específicas somente se o identificador de usuário sob o qual estiver sendo executado (ou cujas autorizações puder assumir) tiver recebido a autorização relevante.

Quatro chamadas MQI requerem verificações de autorização: MQCONN, MQOPEN, MQPUT1 e MQCLOSE.

Para MQOPEN e MQPUT1, a verificação de autoridade é feita no nome do objeto que está sendo aberto e não no nome ou nomes resultantes após a resolução de um nome. Por exemplo, um aplicativo pode receber autoridade para abrir uma fila de alias sem ter autoridade para abrir a fila de base para a qual o alias é resolvido. A regra é que a verificação seja realizada na primeira definição encontrada durante o processo de resolução do nome que não seja um alias do gerenciador de filas, a menos que a definição de alias do gerenciador de filas seja aberta diretamente; ou seja, seu nome apareça no campo *ObjectName* do descritor de objeto. A autoridade é sempre necessária para o objeto específico que está sendo aberto; em alguns casos, a autoridade independente de fila adicional, obtida por meio de uma autorização para o objeto do gerenciador de filas, é necessária.

Tabela 19 na página 167, Tabela 20 na página 167, Tabela 21 na página 168 e Tabela 22 na página 168 resumem as autorizações necessárias para cada chamada.

Nota: Essas tabelas não mencionam listas de nomes, canais, canais de conexão do cliente, listeners, serviços ou objetos de informações sobre autenticação. Isso é porque nenhuma das autorizações se aplica a esses objetos, exceto MQOO_INQUIRE, para o qual as mesmas autorizações se aplicam como para os outros objetos.

Tabela 19. Autorização de segurança necessária para chamadas MQCONN

Autorização necessária para:	Objeto da fila (“1” na página 169)	Objeto de processo	Objeto do gerenciador de filas
opção MQCONN	Não-aplicável	Não-aplicável	MQZAO_CONNECT

Tabela 20. Autorização de segurança necessária para chamadas MQOPEN

Autorização necessária para:	Objeto da fila (“1” na página 169)	Objeto de processo	Objeto do gerenciador de filas
MQOO_INQUIRE	MQZAO_INQUIRE (“2” na página 169)	MQZAO_INQUIRE (“2” na página 169)	MQZAO_INQUIRE (“2” na página 169)
MQOO_BROWSE	MQZAO_BROWSE	Não-aplicável	Sem verificação
MQOO_INPUT_*	MQZAO_INPUT	Não-aplicável	Sem verificação
MQOO_SAVE_ ALL_CONTEXT (“3” na página 169)	MQZAO_INPUT	Não-aplicável	Não-aplicável
MQOO_OUTPUT (fila Normal) (“4” na página 169)	MQZAO_OUTPUT	Não-aplicável	Não-aplicável
MQOO_PASS_ IDENTITY_CONTEXT (“5” na página 169)	MQZAO_PASS_ IDENTITY_CONTEXT	Não-aplicável	Sem verificação
MQOO_PASS_ALL_ CONTEXT (“5” na página 169, “6” na página 169)	MQZAO_PASS _ALL_CONTEXT	Não-aplicável	Sem verificação

Tabela 20. Autorização de segurança necessária para chamadas MQOPEN (continuação)			
Autorização necessária para:	**Objeto da fila (“1” na página 169)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQOO_SET_ IDENTITY_CONTEXT **(“5” na página 169, “6” na página 169)**	MQZAO_SET_ IDENTITY_CONTEXT	Não-aplicável	MQZAO_SET_ IDENTITY_CONTEXT **(“7” na página 169)**
MQOO_SET_ ALL_CONTEXT **(“5” na página 169, “8” na página 169)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“7” na página 169)**
MQOO_OUTPUT (Fila de transmissão) **(“9” na página 169)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“7” na página 169)**
MQOO_SET	MQZAO_SET	Não-aplicável	Sem verificação
MQOO_ALTERNATE_ USER_AUTHORITY	**(“10” na página 169)**	**(“10” na página 169)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(“10” na página 169, “11” na página 169)**

Tabela 21. Autorização de segurança necessária para chamadas MQPUT1			
Autorização necessária para:	**Objeto da fila (“1” na página 169)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQPMO_PASS_ IDENTITY_CONTEXT	MQZAO_PASS_ IDENTITY_CONTEXT **(“12” na página 169)**	Não-aplicável	Sem verificação
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **(“12” na página 169)**	Não-aplicável	Sem verificação
MQPMO_SET_ IDENTITY_CONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **(“12” na página 169)**	Não-aplicável	MQZAO_SET_ IDENTITY_CONTEXT **(“7” na página 169)**
MQPMO_SET_ ALL_CONTEXT	MQZAO_SET_ ALL_CONTEXT **(“12” na página 169)**	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“7” na página 169)**
(Fila de transmissão) **(“9” na página 169)**	MQZAO_SET_ ALL_CONTEXT	Não-aplicável	MQZAO_SET_ ALL_CONTEXT **(“7” na página 169)**
MQPMO_ALTERNATE_ USER_AUTHORITY	**(“13” na página 169)**	Não-aplicável	MQZAO_ALTERNATE_ USER_AUTHORITY **(“11” na página 169)**

Tabela 22. Autorização de segurança necessária para chamadas MQCLOSE			
Autorização necessária para:	**Objeto da fila (“1” na página 169)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQCO_DELETE	MQZAO_DELETE **(“14” na página 169)**	Não-aplicável	Não-aplicável

Tabela 22. Autorização de segurança necessária para chamadas MQCLOSE (continuação)			
Autorização necessária para:	**Objeto da fila (“1” na página 169)**	**Objeto de processo**	**Objeto do gerenciador de filas**
MQCO_DELETE _PURGE	MQZAO_DELETE **(“14” na página 169)**	Não-aplicável	Não-aplicável

Notas para as tabelas:

1. Se uma fila modelo estiver sendo aberta:
   - A autoridade MQZAO_DISPLAY será necessária para a fila modelo, além da autoridade para abrir a fila modelo para o tipo de acesso para o qual você está abrindo.
   - A autoridade MQZAO_CREATE não é necessária para criar o fila dinâmica.
   - O identificador de usuários usado para abrir a fila modelo recebe automaticamente todas as autoridades específicas da fila (equivalente a MQZAO_ALL) para a fila dinâmica criada.
2. O objeto de fila, de processo, de lista de nomes ou de gerenciador de filas é verificado, dependendo do tipo de objeto que está sendo aberto.
3. MQOO_INPUT_* também deve ser especificado. Essa opção é válida para uma fila local, modelo ou de alias.
4. Essa verificação é executada para todos os casos de saída, exceto para o caso especificado na nota “9” na página 169.
5. MQOO_OUTPUT também deve ser especificado.
6. MQOO_PASS_IDENTITY_CONTEXT também é sugerido por essa opção.
7. Essa autoridade é necessária para o objeto de gerenciador de filas e a fila específica.
8. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT e MQOO_SET_IDENTITY_CONTEXT também são sugeridos por essa opção.
9. Essa verificação é executada para uma fila local ou modelo que tem um atributo de fila *Usage* de MQUS_TRANSMISSION e está sendo aberta diretamente para saída. Ela não será aplicada se uma fila remota estiver sendo aberta (especificando-se os nomes do gerenciador de filas remotas e da fila remota ou especificando-se o nome de uma definição local da fila remota).
10. Pelo menos um de MQOO_INQUIRE (para qualquer tipo de objeto) ou (para filas) MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT ou MQOO_SET também deve ser especificado. A verificação executada é como para as outras opções especificadas, usando-se o identificador de usuário alternativo fornecido para a autoridade de objeto com nome específico, e a autoridade de aplicativo atual para a verificação MQZAO_ALTERNATE_USER_IDENTIFIER.
11. Essa autorização permite que qualquer *AlternateUserId* seja especificado.
12. Uma verificação MQZAO_OUTPUT também será executada se a fila não tiver um atributo de fila *Usage* de MQUS_TRANSMISSION.
13. A verificação executada é como para as outras opções especificadas, usando-se o identificador de usuário alternativo fornecido para a autoridade de fila nomeada, e a autoridade de aplicativo atual para a verificação MQZAO_ALTERNATE_USER_IDENTIFIER.
14. A verificação será realizada somente se ambas as instruções a seguir forem verdadeiras:
    - Uma fila dinâmica permanente está sendo fechada e excluída.
    - A fila não foi criada pela MQOPEN que retornou a manipulação de objetos que está sendo usada.

    Caso contrário, não haverá verificação.

Notas gerais:

1. A autorização especial MQZAO_ALL_MQI inclui todas as seguintes autorizações que são relevantes ao tipo de objeto:
   - MQZAO_CONNECT

- MQZAO_INQUIRE
- MQZAO_SET
- MQZAO_BROWSE
- MQZAO_INPUT
- MQZAO_OUTPUT
- MQZAO_PASS_IDENTITY_CONTEXT
- MQZAO_PASS_ALL_CONTEXT
- MQZAO_SET_IDENTITY_CONTEXT
- MQZAO_SET_ALL_CONTEXT
- MQZAO_ALTERNATE_USER_AUTHORITY

2. MQZAO_DELETE (consulte a nota “14” na página 169) e MQZAO_DISPLAY são classificados como autorizações de administração. Portanto, elas não são incluídas em MQZAO_ALL_MQI.
3. *Nenhuma verificação* significa que nenhuma verificação de autorização é executada.
4. *Não aplicável* significa que a verificação de autorização não é relevante para essa operação. Por exemplo, não é possível emitir uma chamada MQPUT para um objeto de processo.

IBM i *Autorizações para comandos MQSC em PCFs de escape no IBM i*

Essas autorizações permitem que um usuário emita comandos de administração como uma mensagem PCF Escape. Esses métodos permitem que um programa envie um comando de administração como uma mensagem para um gerenciador de filas, para execução em nome desse usuário.

Esta seção resume as autorizações necessárias para cada comando MQSC contido no PCF Escape.

Não aplicável significa que a verificação de autorização não é relevante para essa operação.

O ID de usuário com o qual o programa que envia o comando está sendo executado também deve ter as seguintes autoridades:

- Autoridade MQZAO_CONNECT para o gerenciador de filas
- Autoridade DISPLAY no gerenciador de filas para executar comando de PCF
- Autoridade para emitir os comandos MQSC dentro do texto do comando PCF Escape

ALTER *object*

Object	**Authorization required**
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	MQZAO_CHANGE
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE

CLEAR *object*

Object	Authorization required
Fila	MQZAO_CLEAR
Tópico	MQZAO_CLEAR
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	Não-aplicável
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

DEFINE *object* NOREPLACE ("1" na página 174)

Object	Authorization required
Fila	MQZAO_CREATE **("2" na página 174)**
Tópico	MQZAO_CREATE **("2" na página 174)**
Processo	MQZAO_CREATE **("2" na página 174)**
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CREATE **("2" na página 174)**
Informações sobre Autenticação	MQZAO_CREATE **("2" na página 174)**
Canal	MQZAO_CREATE **("2" na página 174)**
Canal de conexão do cliente	MQZAO_CREATE **("2" na página 174)**
Listener	MQZAO_CREATE **("2" na página 174)**
Serviço	MQZAO_CREATE **("2" na página 174)**

DEFINE *object* REPLACE ("1" na página 174, "3" na página 174)

Object	Authorization required
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE

Object	Authorization required
Serviço	MQZAO_CHANGE

EXCLUIR *object*

Object	Authorization required
Fila	MQZAO_DELETE
Tópico	MQZAO_DELETE
Processo	MQZAO_DELETE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_DELETE
Informações sobre Autenticação	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de conexão do cliente	MQZAO_DELETE
Listener	MQZAO_DELETE
Serviço	MQZAO_DELETE

DISPLAY *object*

Object	Authorization required
Fila	MQZAO_DISPLAY
Tópico	MQZAO_DISPLAY
Processo	MQZAO_DISPLAY
Gerenciador de Filas	MQZAO_DISPLAY
Lista de Nomes	MQZAO_DISPLAY
Informações sobre Autenticação	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY
Canal de conexão do cliente	MQZAO_DISPLAY
Listener	
Serviço	

PING CHANNEL

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL

Object	Authorization required
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

RESET CHANNEL

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL_EXTENDED
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

RESOLVE CHANNEL

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL_EXTENDED
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

START *object*

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável

Object	Authorization required
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Listener	MQZAO_CONTROL
Serviço	MQZAO_CONTROL

PARAR *object*

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Listener	MQZAO_CONTROL
Serviço	MQZAO_CONTROL

Nota:

1. Para comandos DEFINE, a autoridade MQZAO_DISPLAY também será necessária para o objeto LIKE, se houver um especificado, ou no objeto SYSTEM.DEFAULT.xxx apropriado, se LIKE for omitido.
2. A autoridade MQZAO_CREATE não é específica a um determinado objeto ou tipo de objeto. A autoridade Criar é concedida para todos os objetos de um gerenciador de filas especificado, especificando-se um tipo de objeto de QMGR no comando GRTMQMAUT.
3. Essa opção se aplicará se o objeto a ser substituído já existir. Caso contrário, a verificação será como para DEFINE *object* NOREPLACE.

IBM i *Autorizações para comandos de PCF no IBM i*

Essas autorizações permitem que um usuário emita comandos de administração como comando de PCF. Esses métodos permitem que um programa envie um comando de administração como uma mensagem para um gerenciador de filas, para execução em nome desse usuário.

Esta seção resume as autorizações necessárias para cada comando PCF.

Nenhuma verificação significa que nenhuma verificação de autorização é executada; *Não aplicável* significa que a verificação de autorização não é relevante para essa operação.

O ID de usuário com o qual o programa que envia o comando está sendo executado também deve ter as seguintes autoridades:

- Autoridade MQZAO_CONNECT para o gerenciador de filas
- Autoridade DISPLAY no gerenciador de filas para executar comando de PCF

A autorização especial MQZAO_ALL_ADMIN inclui as autorizações a seguir:

- MQZAO_CHANGE

- MQZAO_CLEAR
- MQZAO_DELETE
- MQZAO_DISPLAY
- MQZAO_CONTROL
- MQZAO_CONTROL_EXTENDED

A autoridade MQZAO_CREATE não é específica a um determinado objeto ou tipo de objeto

Mudar *object*

Object	**Authorization required**
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	MQZAO_CHANGE
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE

Clear *object*

Object	**Authorization required**
Fila	MQZAO_CLEAR
Tópico	MQZAO_CLEAR
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	Não-aplicável
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

Copiar *object* (sem substituição) (“1” na página 180)

Object	**Authorization required**
Fila	MQZAO_CREATE **(“2” na página 180)**
Tópico	MQZAO_CREATE **(“2” na página 180)**
Processo	MQZAO_CREATE **(“2” na página 180)**
Gerenciador de Filas	Não-aplicável

Object	Authorization required
NamelistMQZAO_CREATE	MQZAO_CREATE (**“2” na página 180**)
Informações sobre Autenticação	MQZAO_CREATE (**“2” na página 180**)
Canal	MQZAO_CREATE (**“2” na página 180**)
Canal de conexão do cliente	MQZAO_CREATE (**“2” na página 180**)
Listener	MQZAO_CREATE (**“2” na página 180**)
Serviço	MQZAO_CREATE (**“2” na página 180**)

Copiar *object* (com substituição) (“1” na página 180, “4” na página 180)

Object	Authorization required
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE
Processo	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE

Criar *object* (sem substituição) (“3” na página 180)

Object	Authorization required
Fila	MQZAO_CREATE (**“2” na página 180**)
Tópico	MQZAO_CREATE (**“2” na página 180**)
Processo	MQZAO_CREATE (**“2” na página 180**)
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CREATE (**“2” na página 180**)
Informações sobre Autenticação	MQZAO_CREATE (**“2” na página 180**)
Canal	MQZAO_CREATE (**“2” na página 180**)
Canal de conexão do cliente	MQZAO_CREATE (**“2” na página 180**)
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE

Criar *object* (com substituição) (“3” na página 180, “4” na página 180)

Object	Authorization required
Fila	MQZAO_CHANGE
Tópico	MQZAO_CHANGE

Object	Authorization required
Processo	MQZAO_CHANGE
Gerenciador de Filas	Não-aplicável
Lista de Nomes	MQZAO_CHANGE
Informações sobre Autenticação	MQZAO_CHANGE
Canal	MQZAO_CHANGE
Canal de conexão do cliente	MQZAO_CHANGE
Listener	MQZAO_CHANGE
Serviço	MQZAO_CHANGE

Excluir *object*

Object	Authorization required
Fila	MQZAO_DELETE
Tópico	MQZAO_DELETE
Processo	MQZAO_DELETE
Gerenciador de Filas	MQZAO_DELETE
Lista de Nomes	MQZAO_DELETE
Informações sobre Autenticação	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de conexão do cliente	MQZAO_DELETE
Listener	MQZAO_DELETE
Serviço	MQZAO_DELETE

Inquire *object*

Object	Authorization required
Fila	MQZAO_DISPLAY
Tópico	MQZAO_DISPLAY
Processo	MQZAO_DISPLAY
Gerenciador de Filas	MQZAO_DISPLAY
Lista de Nomes	MQZAO_DISPLAY
Informações sobre Autenticação	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY
Canal de conexão do cliente	MQZAO_DISPLAY
Listener	MQZAO_DISPLAY
Serviço	MQZAO_DISPLAY

Inquire *object* names

Object	Authorization required
Fila	Sem verificação
Tópico	Sem verificação
Processo	Sem verificação
Gerenciador de Filas	Sem verificação
Lista de Nomes	Sem verificação
Informações sobre Autenticação	Sem verificação
Canal	Sem verificação
Canal de conexão do cliente	Sem verificação
Listener	Sem verificação
Serviço	Sem verificação

Executar ping no Canal

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

Redefinir Canal

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL_EXTENDED
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável

Object	Authorization required
Serviço	Não-aplicável

Reconfigurar as Estatísticas de Fila

Object	Authorization required
Fila	MQZAO_DISPLAY e MQZAO_CHANGE
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	Não-aplicável
Canal de conexão do cliente	Não-aplicável
Listener	
Serviço	

Resolver Canal

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL_EXTENDED
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

Iniciar o Canal

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL

Object	Authorization required
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

Parar Canal

Object	Authorization required
Fila	Não-aplicável
Tópico	Não-aplicável
Processo	Não-aplicável
Gerenciador de Filas	Não-aplicável
Lista de Nomes	Não-aplicável
Informações sobre Autenticação	Não-aplicável
Canal	MQZAO_CONTROL
Canal de conexão do cliente	Não-aplicável
Listener	Não-aplicável
Serviço	Não-aplicável

Nota:

1. Para comandos Copy, a autoridade MQZAO_DISPLAY também é necessária para o objeto De.
2. A autoridade MQZAO_CREATE não é específica a um determinado objeto ou tipo de objeto. A autoridade Criar é concedida para todos os objetos de um gerenciador de filas especificado, especificando-se um tipo de objeto de QMGR no comando GRTMQMAUT.
3. Para comandos de Criação, a autoridade MQZAO_DISPLAY também é necessária para o SYSTEM.DEFAULT.* objeto.
4. Essa opção se aplicará se o objeto a ser substituído já existir. Caso contrário, a verificação será como para Copy ou Create sem substituição.

IBM i Perfis genéricos do OAM no IBM i

Os perfis genéricos Object authority manager (OAM) permitem configurar a autoridade que um usuário tem com vários objetos de uma vez, em vez de ter que emitir comandos **GRTMQMAUT** separados em cada objeto individual ao ser criado. O uso de perfis genéricos no comando **GRTMQMAUT** permite configurar uma autoridade genérica para todos os futuros objetos criados que se ajustarem a esse perfil.

O restante desta seção descreve o uso de perfis genéricos em mais detalhes:

- "Utilizando Caracteres Curinga" na página 180
- "Prioridades do Perfil" na página 181

Utilizando Caracteres Curinga

O que torna um perfil genérico é o uso de caracteres especiais (caracteres curinga) no nome do perfil. Por exemplo, o caractere curinga de ponto de interrogação (?) corresponde a qualquer caractere único em um nome. Portanto, se você especificar ABC.?EF, a autorização fornecida a esse perfil se aplicará a qualquer objeto criado com os nomes ABC.DEF, ABC.CEF, ABC.BEF, etc.

Os caracteres curinga disponíveis são:

?

Use o ponto de interrogação (?) em vez de qualquer caractere. Por exemplo, `AB.?D` seria aplicado aos objetos `AB.CD`, `AB.ED` e `AB.FD`.

*****

Use o asterisco (*) como:

- Um *qualificador* em um nome de perfil para corresponder a qualquer qualificador em um nome de objeto. Um qualificador é a parte de um nome de objeto delimitado por um ponto. Por exemplo, em `ABC.DEF.GHI`, os qualificadores são `ABC`, `DEF` e `GHI`.

  Por exemplo, `ABC.*.JKL` seria aplicado aos objetos `ABC.DEF.JKL` e `ABC.GHI.JKL`. (Observe que ele **não** seria aplicado ao `ABC.JKL`; * usado nesse contexto sempre indica um qualificador.)
- Um caractere dentro de um qualificador em um nome de perfil para corresponder a zero ou mais caracteres dentro do qualificador em um nome de objeto.

  Por exemplo, `ABC.DE*.JKL` seria aplicado aos objetos `ABC.DE.JKL`, `ABC.DEF.JKL` e `ABC.DEGH.JKL`.

******

Use o asterisco duplo (**) ***uma vez*** em um nome de perfil como:

- O nome do perfil inteiro para corresponder a todos os nomes de objeto. Por exemplo, se você usar a palavra-chave `OBJTYPE (*PRC)` para identificar processos e, em seguida, usar ** como o nome do perfil, irá alterar as autorizações de todos os processos.
- Como o qualificador inicial, do meio ou final em um nome de perfil para corresponder a zero ou mais qualificadores em um nome de objeto. Por exemplo, `**.ABC` identifica todos os objetos com o qualificador final ABC.

Prioridades do Perfil

Um ponto importante a ser entendido ao usar perfis genéricos é a prioridade que os perfis recebem ao decidirem quais autoridades aplicar a um objeto que está sendo criado. Por exemplo, suponha que você emitiu estes comandos:

```
GRTMQMAUT OBJ(AB.*) OBJTYPE(*Q) USER(FRED) AUT(*PUT) MQMNAME(MYQMGR)
GRTMQMAUT OBJ(AB.C*) OBJTYPE(*Q) USER(FRED) AUT(*GET) MQMNAME(MYQMGR)
```

O primeiro fornece autoridade put para todas as filas para o principal FRED com nomes que correspondem ao perfil AB. *; O segundo fornece autoridade get para os mesmos tipos de fila que correspondem ao perfil AB.C*.

Suponha que agora você crie uma fila chamada AB.CD. De acordo com as regras para correspondência de curinga, GRTMQMAUT poderia se aplicar a essa fila. Portanto, ele tem autoridade put ou get?

Para localizar a resposta, você aplica a regra que, sempre que vários perfis puderem se aplicar a um objeto, **apenas o mais específico será aplicado**. A maneira de aplicação dessa regra é comparando-se os nomes dos perfis da esquerda para a direita. Sempre que forem diferentes, um caractere não genérico será mais específico do que um genérico. Portanto, no exemplo anterior, o AB.CD da fila **possui** autoridade (AB.C* é mais específico do que AB.*).

Ao comparar os caracteres genéricos, a ordem de *especificidade* é:

1. ?
2. *
3. **

IBM i Especificando o serviço de autorização instalado no IBM i

É possível especificar qual componente de serviço de autorização usar.

O parâmetro **Service Component name** on **GRTMQMAUT** e **RVKMQMAUT** permite especificar o nome do componente de serviço de autorização instalado.

Selecionar **F24** no painel inicial, seguido de **F9=Todos os parâmetros** no próximo painel de um dos comandos, permite especificar o componente de autorização instalado (*DFT) ou o nome do componente de serviço de autorização necessário especificado na sub-rotina de Serviço do arquivo qm.ini do gerenciador de filas.

DSPMQMAUT também possui esse parâmetro extra. Esse parâmetro permite procurar todos os componentes de autorização instalados (*DFT) ou o nome do componente de serviço de autorização especificado, para o nome do objeto, o tipo de objeto e o usuário especificados

IBM i Trabalhando com e sem perfis de autoridade em IBM i

Use estas informações para aprender como trabalhar com perfis de autoridade e como trabalhar sem perfis de autoridade.

É possível trabalhar com perfis de autoridade, conforme explicado em "Trabalhando com Perfis de Autoridade" na página 182, ou sem eles, conforme explicado aqui:

Para trabalhar sem perfis de autoridade, use *NONE como um parâmetro de Autoridade em **GRTMQMAUT** para criar perfis sem autoridade. Isso deixa os perfis existentes inalterados.

Em **RVKMQMAUT**, use *REMOVE como um parâmetro de Autoridade para remover um perfil de autoridade existente.

Trabalhando com Perfis de Autoridade

Há dois comandos associados à criação de perfil de autoridade:

- **WRKMQMAUT**
- **WRKMQMAUTD**

É possível acessar esses comandos diretamente da linha de comandos ou do painel WRKMQM:

1. Digitando o nome do gerenciador de filas e pressionando a tecla Enter para acessar o painel de resultados **WRKMQM**.
2. Selecionando F23=More options neste painel

A Opção 24 seleciona o painel de resultados para o **WRKMQMAUT** comando e a opção 25 seleciona o comando **WRKMQMAUTI** , que é usado com a camada de ligações SSL

WRKMQMAUT

Este comando permite que você trabalhe com os dados de autoridade retido na fila de autoridades.

Nota: Para executar esse comando, você deve ter as autoridades *connect e *admdsp ao gerenciador de filas. No entanto, para criar ou excluir um perfil, é necessária a autoridade QMQMADM.

Se você fornecer as informações como saída para a tela, uma lista de nomes de perfis de autoridade, juntamente com seus tipos, será exibida. Se você imprimir a saída, receberá uma lista detalhada de todos os dados de autoridade, dos usuários registrados e de suas autoridades.

Inserir um nome de objeto ou perfil nesse painel e pressionar ENTER o leva ao painel de resultados para **WRKMQMAUT**

Se você selecionar 4=Delete, irá para um novo painel a partir do qual poderá confirmar que deseja excluir todos os nomes de usuário registrados para o nome do perfil de autoridade genérico especificado. Essa opção executa **RVKMQMAUT** com a opção *REMOVE para todos os usuários e aplica-se **apenas** a nomes de perfis genéricos.

Se você selecionar 12=Work with profile , acesse o painel de resultados do comando **WRKMQMAUTD** , conforme explicado em "WRKMQMAUTD" na página 183.

WRKMQMAUTD

Esse comando permite exibir todos os usuários registrados com um determinado nome de perfil de autoridade e tipo de objeto. Para executar esse comando, você deve ter as autoridades `*connect` e `*admdsp` ao gerenciador de filas. No entanto, para conceder, executar, criar ou excluir um perfil, é necessária a autoridade QMQMADM.

Selecionar `F24=More keys` no painel de entrada inicial, seguido pela opção `F9=All Parameters` exibe o Nome do Componente de Serviço para **GRTMQMAUT** e **RVKMQMAUT**.

Nota: A chave `F11=Display Object Authorizations` alterna entre os seguintes tipos de autoridades:

- Autorizações de objetos
- Autorizações de contexto
- autorizações MQI

As opções na tela são:

2=Grant
Leva-o ao painel **GRTMQMAUT** para incluir nas autoridades atuais.

3=Revoke
Leva-o ao painel **RVKMQMAUT** para remover algumas das definições atuais

4=Delete
Leva-o a um painel que permite excluir os dados de autoridade de usuários especificados. Isso executa **RVKMQMAUT** com a opção *REMOVE.

5=Display
Leva-o ao comando **DSPMQMAUT** existente

F6=Create
Leva-o ao painel **GRTMQMAUT** que permite criar um registro de autoridade de perfil.

IBM i Diretrizes do gerenciador de autoridade de objeto no IBM i

Dicas e sugestões adicionais para usar o gerenciador de autoridade de objeto (OAM)

Limitar o Acesso a Operações Sigilosas

Algumas operações são sigilosas; limite-as aos usuários privilegiados. Por exemplo,

- Acessando algumas filas especiais, como filas de transmissão ou a fila de comandos `SYSTEM.ADMIN.COMMAND.QUEUE`
- Execução de programas que usam opções de contexto completas de MQI
- Criando e copiando filas de aplicativos

Diretórios do Gerenciador de Filas

Os diretórios e as bibliotecas que contêm filas e outros dados do gerenciador de filas são privativos ao produto. Não use comandos padrão do sistema operacional para conceder ou revogar autorizações para recursos do MQI.

Filas

A autoridade para uma fila dinâmica baseia-se naquela da fila modelo da qual é derivada, mas não é necessariamente a mesma.

Para filas de alias e filas remotas, a autorização é aquela do próprio objeto, não da fila à qual a fila do alias ou a fila remota é resolvida. É possível autorizar um perfil de usuário para acessar uma fila de alias que é resolvida para uma fila local à qual o perfil do usuário não possui permissões de acesso.

Limite a autoridade para criar filas a usuários privilegiados. Se você não fizer isso, os usuários podem ignorar o controle de acesso normal criando um alias.

Autoridade de Usuário Alternativo

A autoridade de usuário alternativo controla se um perfil do usuário pode usar a autoridade de outro perfil do usuário ao acessar um objeto do IBM MQ. Essa técnica é essencial onde um servidor recebe solicitações de um programa e deseja assegurar-se de que o programa possui a autoridade necessária para a solicitação. O servidor pode ter a autoridade necessária, mas precisa saber se o programa tem a autoridade para as ações solicitadas.

Por exemplo:

- Um programa do servidor em execução com um perfil de usuário PAYSERV recupera uma mensagem de solicitação de uma fila que foi colocada na fila pelo perfil de usuário USER1.
- Quando o programa do servidor recebe a mensagem de solicitação, ele processa a solicitação e coloca a resposta de volta na fila de resposta especificada com a mensagem de solicitação.
- Em vez de usar seu próprio perfil de usuário (PAYSERV) para autorizar a abertura da fila de resposta, o servidor pode especificar algum outro perfil de usuário, neste caso, USER1. Neste exemplo, é possível usar a autoridade de usuário alternativo para controlar se PAYSERV tem permissão para especificar USER1 como um perfil de usuário alternativo ao abrir a fila de resposta.

O perfil de usuário alternativo é especificado no campo *AlternateUserId* do descritor de objeto.

Nota: É possível usar perfis de usuário alternativo em qualquer objeto do IBM MQ. O uso de um perfil de usuário alternativo não afeta o perfil do usuário usado por nenhum outro gerenciador de recursos.

Autoridade de Contexto

Contexto são informações que se aplicam a uma determinada mensagem e está contido no descritor de mensagens, MQMD, que faz parte da mensagem.

Para obter descrições dos campos do descritor de mensagens relacionados ao contexto, consulte Visão geral do MQMD.

Para obter informações sobre as opções de contexto, consulte Contexto da mensagem.

Considerações de Segurança Remota

Para segurança remota, considere:

Autoridade de transmissão
Para segurança em gerenciadores de filas, é possível especificar a autoridade put usada quando um canal recebe uma mensagem enviada de outro gerenciador de filas.

Este parâmetro é válido somente para os tipos de canal RCVR, RQSTR ou CLUSRCVR. Especifique o atributo de canal PUTAUT da seguinte forma:

DEF
Perfil do usuário padrão. Este é o perfil do usuário QMQM sob o qual o agente do canal de mensagens está em execução.

CTX
O perfil do usuário no contexto da mensagem.

Filas de transmissão
Os gerenciadores de filas colocam mensagens remotas automaticamente em uma fila de transmissão; não é necessária nenhuma autoridade especial. No entanto, a colocação de uma mensagem diretamente em uma fila de transmissão exige autorização especial.

Saídas do canal
É possível usar saídas de canais para aumentar a segurança.

Registros de Autenticação de Canal
Use para exercer um controle mais preciso sobre o acesso concedido para conectar-se aos sistemas em um nível de canal.

Para obter mais informações sobre segurança remota, consulte “Autorização de canal” na página 110.

Protegendo canais com SSL/TLS

O protocolo Segurança da Camada de Transporte (TLS) fornece segurança de canal, com proteção contra espionagem do tráfego de rede, violação e personificação. O suporte do IBM MQ para TLS permite especificar, na definição de canal, que um determinado canal usa a segurança TLS. Também é possível especificar detalhes da segurança desejada, como o algoritmo de criptografia que você deseja usar.

O suporte de TLS no IBM MQ usa o *objeto de informações sobre autenticação* do gerenciador de filas e vários comandos de CL e MQSC e parâmetros de gerenciador de filas e de canal que definem o suporte do TLS requerido em detalhe.

Os comandos de CL a seguir suportam TLS:

WRKMQMAUTI
Trabalhar com os atributos de um objeto de informações sobre autenticação.

CHGMQMAUTI
Modificar os atributos de um objeto de informações sobre autenticação.

CRTMQMAUTI
Criar um objeto de informações sobre autenticação.

CPYMQMAUTI
Criar um objeto de informações sobre autenticação copiando um existente.

DLTMQMAUTI
Excluir um objeto de informações sobre autenticação.

DSPMQMAUTI
Exibe os atributos para um objeto de informações sobre autenticação específico.

Para obter uma visão geral de segurança do canal usando TLS, veja

- Protegendo canais com TLS

Para obter detalhes de comandos PCF associados ao TLS, veja

- Mudar, copiar e criar objeto de informações sobre autenticação
- Excluir Objeto de Informações sobre Autenticação
- Investigar Objeto de Informações sobre Autenticação

z/OS Configurando a Segurança em z/OS

Considerações de segurança específicas para z/OS.

A segurança em IBM MQ for z/OS é controlada usando o RACF ou um gerenciador de segurança externa equivalente (ESM).

As instruções a seguir presumem que você esteja usando o RACF.

Referências relacionadas
Cenário de segurança: dois gerenciadores de filas no z/OS
Cenário de segurança: grupo de filas compartilhadas no z/OS

z/OS Classes de segurança do RACF

As classes do RACF são usadas para manter os perfis necessários para a verificação de segurança do IBM MQ. Muitas das classes de membro possuem classes de grupo equivalentes. Você deve ativar as classes e ativá-las para aceitar perfis genéricos

Cada classe do RACF mantém um ou mais perfis usados em algum momento na sequência de verificação, conforme mostrado em Tabela 23 na página 186.

Tabela 23. As classes do RACF usadas pelo IBM MQ

Classe de membro	Classe de grupo	Conteúdos
MQADMIN	GMQADMIN	Perfis: Usado principalmente para reter perfis para funções do tipo administração. Por exemplo: • Os perfis para os comutadores de segurança do IBM MQ • O perfil de segurança RESLEVEL • Perfis para segurança de usuário alternativo • O perfil de segurança do contexto • Perfis para segurança do recurso de comando
MXADMIN	GMXADMIN	Perfis: Usado principalmente para reter perfis para funções do tipo administração. Por exemplo: • Os perfis para os comutadores de segurança do IBM MQ • O perfil de segurança RESLEVEL • Perfis para segurança de usuário alternativo • O perfil de segurança do contexto • Perfis para segurança do recurso de comando Essa classe pode manter perfis do RACF tanto em letras maiúsculas como em letras maiúsculas e minúsculas.
MQCONN		Perfis usados para segurança de conexão
MQCMDS		Perfis usados para segurança de comando
MQQUEUE	GMQQUEUE	Perfis usados em segurança do recurso de comando
MXQUEUE	GMXQUEUE	Perfis compostos por maiúsculas e por letras maiúsculas e minúsculas usados em segurança do recurso de fila
MQPROC	GMQPROC	Perfis usados em segurança do recurso do processo
MXPROC	GMXPROC	Perfis compostos por maiúsculas e por letras maiúsculas e minúsculas usados em segurança do recurso do processo
MQNLIST	GMQNLIST	Perfis usados em segurança do recurso de lista de nomes
MXNLIST	GMXNLIST	Perfis compostos por maiúsculas e por letras maiúsculas e minúsculas usados em segurança do recurso de lista de nomes
MXTOPIC	GMXTOPIC	Perfis compostos por maiúsculas e por letras maiúsculas e minúsculas usados em segurança do tópico

Algumas classes possuem uma *classe de grupo* relacionada que permite colocar juntos os grupos de recursos que possuem requisitos de acesso semelhantes. Para obter detalhes sobre a diferença entre as classes de membro e de grupo e quando usar uma classe de membro ou de grupo, consulte o z/OS Security Server RACF Security Administrator's Guide.

As classes devem ser ativadas antes que as verificações de segurança possam ser feitas. Para ativar todas as classes do IBM MQ, é possível usar esse comando: RACF

```
SETROPTS CLASSACT(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                  MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

Você também deve assegurar-se de configurar as classes de modo que possam aceitar perfis genéricos. Também é possível fazer isso com o comando SETROPTS do RACF, por exemplo:

```
SETROPTS GENERIC(MQADMIN,MXADMIN,MQQUEUE,MXQUEUE,MQPROC,MXPROC,
                 MQNLIST,MXNLIST,MXTOPIC,MQCONN,MQCMDS)
```

z/OS Perfis do RACF

Todos os perfis do RACF usados pelo IBM MQ contêm um prefixo, que é o nome do gerenciador de filas ou o nome do grupo de filas compartilhadas. Tome cuidado quando usar o sinal de percentual como um curinga.

Todos os perfis do RACF usados pelo IBM MQ contém um prefixo. Para a segurança no nível do grupo de filas compartilhadas, esse é o nome do grupo de filas compartilhadas. Para segurança no nível do gerenciador de filas, o prefixo é o nome do gerenciador de filas. Se você estiver usando uma combinação de segurança no nível do gerenciador de filas e do grupo de filas compartilhadas, você usará perfis com ambos os tipos de prefixo. (A segurança no nível do gerenciador de filas e no grupo de compartilhamento de filas está descrita em Conceitos do IBM MQ for z/OS: segurança.)

Por exemplo, se você desejar proteger uma fila chamada QUEUE_FOR_SUBSCRIBER_LIST no grupo de filas compartilhadas QSG1 no nível do grupo de filas compartilhadas, o perfil apropriado será definido para o RACF como:

```
RDEFINE MQQUEUE QSG1.QUEUE_FOR_SUBSCRIBER_LIST
```

Se quiser proteger uma fila chamada QUEUE_FOR_LOST_CARD_LIST, que pertence ao gerenciador de filas STCD no nível do gerenciador de filas, o perfil apropriado será definido para o RACF como:

```
RDEFINE MQQUEUE STCD.QUEUE_FOR_LOST_CARD_LIST
```

Isso significa que diferentes gerenciadores de filas e grupos de filas compartilhadas podem compartilhar o mesmo banco de dados do RACF e ainda ter opções de segurança diferentes.

Não use nomes de gerenciadores de filas genéricos em perfis para evitar acesso de usuário não previsto.

O IBM MQ permite o uso do sinal de porcentagem (%) em nomes de objetos. No entanto, o RACF usa o caractere % como um caractere curinga único. Isso significa que quando você define um nome de objeto com um caractere % em seu nome, deve considerar isso ao definir o perfil correspondente.

Por exemplo, para a fila %_RATE_INQUIRY CREDIT_CARD_, no gerenciador de filas CRDP, o perfil será definido para o RACF conforme a seguir:

```
RDEFINE MQQUEUE CRDP.CREDIT_CARD_%_RATE_INQUIRY
```

Essa fila não pode ser protegida por um perfil genérico, tal como, CRDP.**.

O IBM MQ permite o uso de caracteres maiúsculos e minúsculos nos nomes do objeto. É possível proteger esses objetos definindo:

1. Perfis compostos por letras maiúsculas e minúsculas nas classes apropriadas do RACF compostas por letras maiúsculas e minúsculas, ou

2. Perfis genéricos nas classes apropriadas do RACF compostas por letras maiúsculas.

Para usar perfis de casos e classes RACF compostos por letras maiúsculas e minúsculas deve-se seguir as etapas descritas em "z/OS Migrando um Gerenciador de Filas para Segurança Composta por Letras Maiúsculas e Minúsculas" na página 271.

Há alguns perfis, ou partes de perfis, que permanecem somente com letras maiúsculas, já que os valores são fornecidos pelo IBM MQ. São elas:

- Perfis do comutador.
- Todos os qualificadores de alto nível (HLQ), incluindo identificadores de subsistema e de grupo de filas compartilhadas.
- Perfis para objetos SYSTEM.
- Perfis para objetos Padrão.
- A classe **MQCMDS**, portanto, todos os perfis de comando são somente em maiúsculas.
- A classe **MQCONN**, portanto, todos os perfis de conexão são somente em maiúsculas.
- Perfis **RESLEVEL**.
- A qualificação `'object'` em perfis de recurso de comando; por exemplo, `hlq.QUEUE.queuename`. Apenas o nome do recurso é composto por letras maiúsculas e minúsculas.
- Os perfis de fila dinâmica `hlq.CSQOREXX.*`, `hlq.CSQUTIL.*` e `CSQXCMD.*`.
- A parte `'CONTEXT'` de `hlq.CONTEXT.resourcename`.
- A parte `'ALTERNATE.USER'` de `hlq.ALTERNATE.USER.userid`.

Por exemplo, se você tiver uma fila chamada `PAYROLL.Dept1` no Gerenciador de Filas `QM01` e estiver usando:

- Perfis compostos por letras maiúsculas e minúsculas; é possível definir um perfil na IBM MQ classe RACF `MXQUEUE`

```
RDEFINE MXQUEUE MQ01.PAYROLL.Dept1
```

- Perfis em maiúsculas; é possível definir um perfil na IBM MQ classe RACF `MQQUEUE`

```
RDEFINE MQQUEUE MQ01.PAYROLL.*
```

O primeiro exemplo, usando perfis compostos por letras maiúsculas e minúsculas, fornece um controle mais granular sobre a concessão de autoridade para acessar o recurso.

z/OS Perfis do Comutador

Para controlar a verificação de segurança executada pelo IBM MQ, use *perfis do comutador*. Um perfil do comutador é um perfil normal do RACF que tem um significado especial para o IBM MQ. A lista de acesso em perfis do comutador não será usada pelo IBM MQ.

O IBM MQ mantém um comutador interno para cada tipo de comutador mostrado nas tabelas Perfis de comutador para segurança de nível de subsistema, Perfis de comutador para grupo de filas compartilhadas ou segurança de nível de Gerenciador de Filas e Perfis de comutador para verificação de recursos. Os perfis do comutador podem ser mantidos no nível do grupo de filas compartilhadas, no nível do gerenciador de filas ou em uma combinação de ambos. Usando um único conjunto de perfis do comutador de segurança do grupo de filas compartilhadas, é possível controlar a segurança em todos os gerenciadores de filas dentro de um grupo de filas compartilhadas.

Quando um comutador de segurança é configurado como ligado, as verificações de segurança associadas ao comutador são executadas. Quando um comutador de segurança é configurado como desligado, é efetuado bypass das verificações de segurança associadas ao comutador. O padrão é que todos os comutadores de segurança sejam configurados como ativados.

z/OS *Comutadores e Classes*

Ao iniciar um gerenciador de filas ou atualizar a segurança, os conjuntos do IBM MQ são alternados de acordo com o estado de várias classes do RACF.

Quando um gerenciador de filas é iniciado (ou quando a classe MQADMIN ou MXADMIN é atualizada pelo comando IBM MQ REFRESH SECURITY), o IBM MQ primeiro verifica o status de RACF e a classe apropriada:

- A classe MQADMIN se você estiver usando perfis em maiúsculas
- A classe MXADMIN se você estiver usando um perfil composto por letras maiúsculas e minúsculas.

Ele configura o comutador de segurança do subsistema como desligado se uma destas condições for verdadeira:

- O RACF está inativo ou não instalado.
- A classe MQADMIN ou MXADMIN não está definida (essas classes são sempre definidas para RACF porque são incluídas na tabela descritora de classe (CDT)).
- A classe MQADMIN ou MXADMIN não foi ativada.

Se RACF e a classe MQADMIN ou MXADMIN estiverem ativos, o IBM MQ verificará a classe MQADMIN ou MXADMIN para ver se qualquer um dos perfis do comutador foram definidos. Ele verifica primeiramente os perfis descritos em "Perfis para Controlar a Segurança do Subsistema" na página 190. Se a segurança do subsistema não for necessária, o IBM MQ configura o comutador de segurança do subsistema interno como desligado, e não executa verificações adicionais.

Os perfis determinam se o comutador IBM MQ correspondente está ativado ou desativado.

- Se o comutador estiver desligado, o tipo de segurança será desativado.
- Se qualquer comutador do IBM MQ for configurado como ligado, o IBM MQ verifica o status da classe do RACF associada ao tipo de segurança correspondente ao comutador do IBM MQ. Se a classe não estiver instalada ou não estiver ativa, o comutador do IBM MQ é desativado. Por exemplo, as verificações de segurança do processo não serão executadas se a classe MQPROC ou MXPROC não tiver sido ativada. A classe que não está sendo ativa é equivalente a definir o perfil NO.PROCESS.CHECKS para cada gerenciador de filas e grupo de filas compartilhadas que usa este banco de dados do RACF.

z/OS *Como os Comutadores Funcionam*

Para desativar um comutador de segurança, defina um NO.* perfil de comutação para ele É possível substituir um NO.* perfil configurado no nível do grupo de filas compartilhadas definindo um YES.* para um gerenciador de filas.

Para desativar um comutador de segurança, é necessário definir um NO.* perfil de comutação para ele A existência de um NO.* O perfil significa que as verificações de segurança **não** são executadas para esse tipo de recurso, a menos que você escolha substituir uma configuração de nível do grupo de filas compartilhadas em um gerenciador de filas específico. Isso é descrito no "Substituindo Configurações de Nível de Grupo de Compartilhamento de" na página 190.

Se o seu gerenciador de filas não for um membro de um grupo de filas compartilhadas, não será necessário definir nenhum perfil de nível do grupo de filas compartilhadas nem perfis de substituição. No entanto, deve-se lembrar-se de definir esses perfis se o gerenciador de filas se unir a um grupo de filas compartilhadas em uma data posterior.

Cada NO.* que o IBM MQ detecta desliga a verificação para esse tipo de recurso. Os perfis do comutador são ativados durante a inicialização do gerenciador de filas. Se você mudar os perfis do comutador enquanto quaisquer gerenciadores de filas afetadas estiverem em execução, será possível obter o IBM MQ para reconhecer as mudanças emitindo o comando IBM MQ REFRESH SECURITY.

Os perfis do comutador devem ser sempre definidos na classe MQADMIN ou MXADMIN. Não defina-os na classe GMQADMIN ou GMXADMIN. As tabelas Alternar perfis para a segurança no nível do subsistema e Alternar perfis para verificação de recursos mostram os perfis do comutador válido e o tipo de segurança que controlam.

Substituindo Configurações de Nível de Grupo de Compartilhamento de

É possível substituir as configurações de segurança no nível do grupo de filas compartilhadas para um gerenciador de filas específico que é um membro desse grupo. Se desejar executar verificações do gerenciador de filas em um gerenciador de filas individual que não sejam executadas em outros gerenciadores de filas no grupo, use o (qmgr-name.YES. *) Perfis do comutador.

Por outro lado, se você não desejar executar uma determinada verificação em um gerenciador de filas específico em um grupo de filas compartilhadas, defina um (qmgr-name.NO. *) para esse tipo de recurso específico no gerenciador de filas, e não defina um perfil para o grupo de filas compartilhadas (IBM MQ somente verifica um perfil de nível do grupo de filas compartilhadas se ele não localizar um perfil de nível do gerenciador de filas.)

z/OS *Perfis para Controlar a Segurança do Subsistema*

O IBM MQ verifica se as verificações de segurança do subsistema são necessárias para o subsistema, para o gerenciador de filas e para o grupo de filas compartilhadas.

A primeira verificação de segurança feita pelo IBM MQ é usada para determinar se as verificações de segurança são necessárias para todo o subsistema IBM MQ. Se você especificar que não deseja a segurança do subsistema, nenhuma verificação adicional será feita.

Os perfis do comutador a seguir são verificados para determinar se a segurança do subsistema é necessária. A Figura 14 na página 190 mostra a ordem na qual eles são verificados.

Tabela 24. Perfis do Comutador para Segurança no Nível do Subsistema

Nome do perfil do comutador	**Tipo de recurso ou verificação que é controlado**
qmgr-name.NO.SUBSYS.SECURITY	Segurança do subsistema para este gerenciador de filas
qsg-name.NO.SUBSYS.SECURITY	Segurança do subsistema para este grupo de filas compartilhadas
qmgr-name.YES.SUBSYS.SECURITY	Substituição de segurança do subsistema para este gerenciador de filas

Se o seu gerenciador de filas não for um membro de um grupo de filas compartilhadas, o IBM MQ verificará apenas o perfil do comutador qmgr-name.NO.SUBSYS.SECURITY.

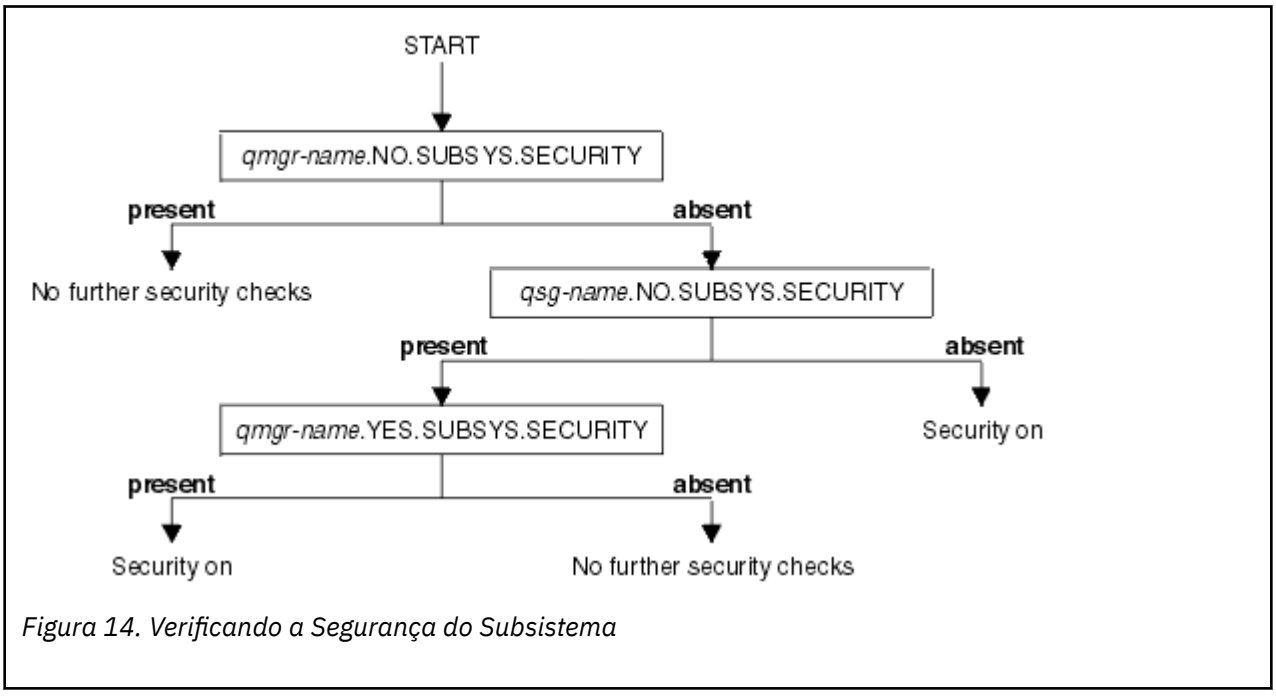


Figura 14. Verificando a Segurança do Subsistema

z/OS *Perfis para controlar a segurança no nível do grupo de filas compartilhadas ou do gerenciador de filas*

Se a verificação de segurança do subsistema for necessária, o IBM MQ verificará se a verificação de segurança é necessária no nível do grupo de filas compartilhadas ou do gerenciador de filas.

Quando o IBM MQ determina que a verificação de segurança é necessária, ele determina se a verificação é necessária no nível do grupo de filas compartilhadas, do nível do gerenciador de filas ou ambos. Estas verificações não são executadas se seu gerenciador de filas não é um membro de um grupo de filas compartilhadas.

Os perfis do comutador a seguir são verificados para determinar o nível necessário. Figura 15 na página 191 e Figura 16 na página 192 mostram a ordem na qual eles são verificados.

Tabela 25. Alternar perfis para segurança no nível do grupo de filas compartilhadas ou do gerenciador de filas

Nome do perfil do comutador	**Tipo de recurso ou verificação que é controlado**
qmgr-name.NO.QMGR.CHECKS	Nenhuma verificação no nível do gerenciador de filas para este gerenciador de filas
qsg-name.NO.QMGR.CHECKS	Nenhum nível de gerenciador de filas verifica para este grupo de filas compartilhadas
qmgr-name.YES.QMGR.CHECKS	As verificações no nível do gerenciador de filas são substituídas para este gerenciador de filas
qmgr-name.NO.QSG.CHECKS	Nenhuma verificação de nível de grupo de filas compartilhadas para este gerenciador de filas
qsg-name.NO.QSG.CHECKS	Nenhuma verificação no nível do grupo de filas compartilhadas para este grupo de filas compartilhadas
qmgr-name.YES.QSG.CHECKS	O nível do grupo de filas compartilhadas verifica a substituição para este gerenciador de filas

Se a segurança do subsistema estiver ativa, não será possível desativar a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas. Se você tentar fazer isso, o IBM MQ configura a verificação de segurança em ambos os níveis.

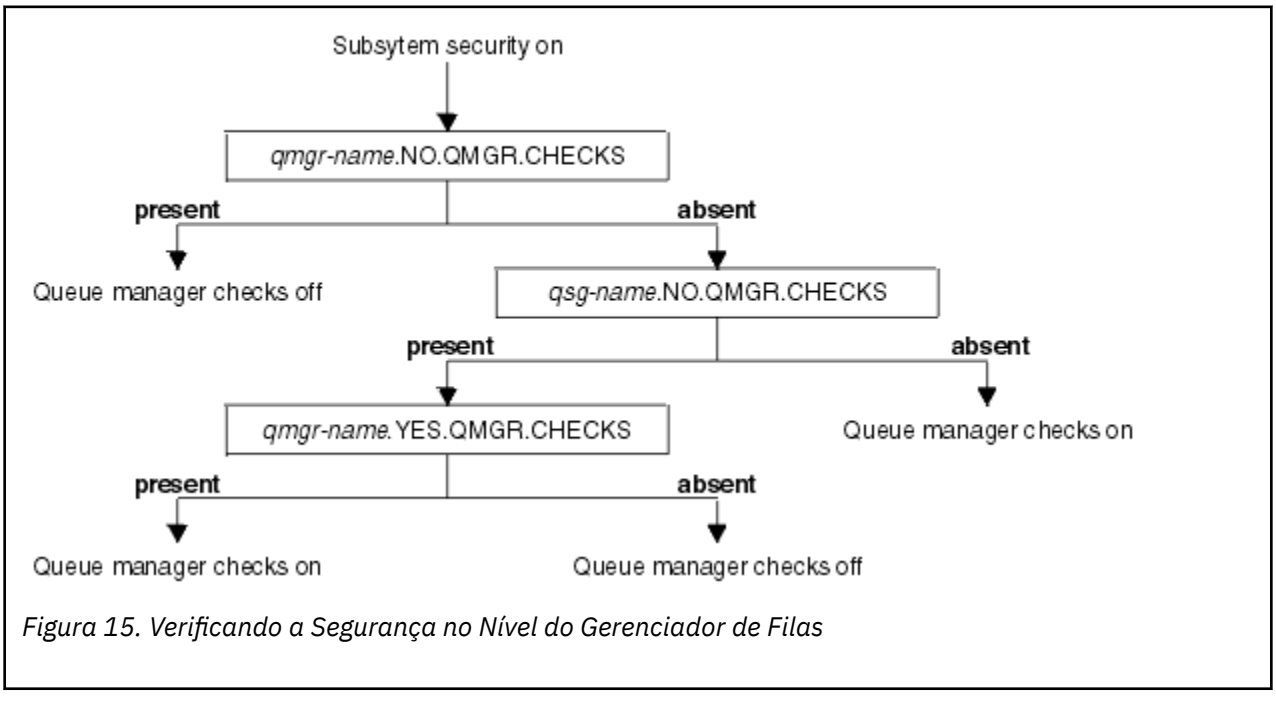


Figura 15. Verificando a Segurança no Nível do Gerenciador de Filas

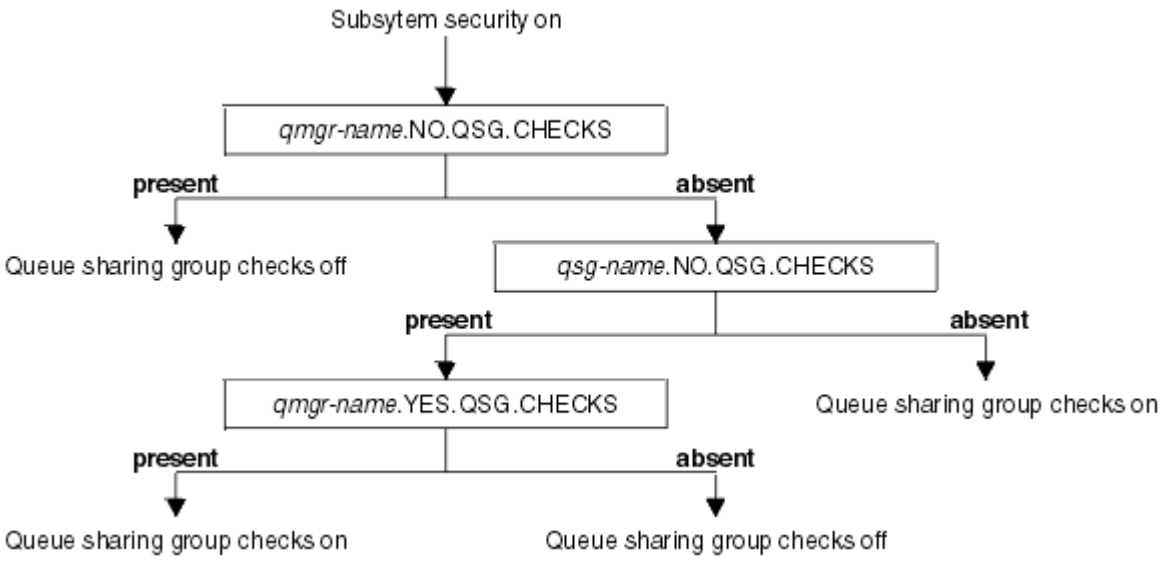


Figura 16. Verificando a segurança no nível do grupo de filas compartilhadas

z/OS *Combinações Válidas de Comutadores de Segurança*

Somente determinadas combinações de comutadores são válidas. Se você usar uma combinação de configurações do comutador que não é válida, a mensagem CSQH026I será emitida e a verificação de segurança será configurada como em ambos os níveis de grupo de filas compartilhadas e de gerenciador de filas.

A Tabela 26 na página 192, Tabela 27 na página 192, Tabela 28 na página 193 e Tabela 29 na página 193 mostram os conjuntos de combinações de configurações de comutador que são válidos para cada tipo de nível de segurança.

Tabela 26. Combinações de Comutador de Segurança Válidas para Segurança no Nível do Gerenciador de Filas

Combinações
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. Combinações do comutador de segurança válidas para segurança no nível do grupo de filas compartilhadas

Combinações
qmgr-name.NO.QMGR.CHECKS
qsg-name.NO.QMGR.CHECKS

Tabela 27. Combinações do comutador de segurança válidas para segurança no nível do grupo de filas compartilhadas (continuação)
Combinações
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. Combinações de comutador de segurança válidas para o gerenciador de filas e o nível do grupo de filas compartilhadas segurança
Combinações
qsg-name.NO.QMGR.CHECKS qmgr-name.YES.QMGR.CHECKS Nenhum perfil QSG.* definido
Nenhum perfil QMGR.* definido 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
Nenhum perfil definido para qualquer um dos comutadores

*Tabela 29. Outras Combinações de Comutador de Segurança Válidas que Alternam Ambos os Níveis de Verificação para **Ligado**.*
Combinações
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 *Verificações em Nível de Recurso*

Vários perfis do comutador são usados para controlar o acesso a recursos. Alguns param a verificação que está sendo executada em um gerenciador de filas ou em um grupo de filas compartilhadas. Eles podem ser substituídos por perfis que permitem a verificação de gerenciadores de filas específicos.

O Tabela 30 na página 194 mostra os perfis do comutador usados para controlar o acesso aos recursos do IBM MQ.

Se o gerenciador de filas fizer parte de um grupo de filas compartilhadas e você tiver a segurança do gerenciador de filas e do grupo de filas compartilhadas ativa, será possível usar um YES.* para substituir os perfis de nível do grupo de filas compartilhadas e ativar especificamente a segurança para um gerenciador de filas específico.

Alguns perfis se aplicam a ambos os gerenciadores de filas e grupos de filas compartilhadas. Eles são prefixados pela sequência *hlq* e é necessário substituir o nome de seu grupo de filas compartilhadas ou gerenciador de filas, conforme aplicável. Os nomes de perfil mostrados como prefixados por *qmgr-name* são perfis de substituição do gerenciador de filas; é necessário substituir o nome de seu gerenciador de filas.

Tabela 30. Perfis do Comutador para Verificação de Recursos

Tipo de verificação de recursos que é controlado	**Nome do perfil do comutador**	**Perfil de substituição para um gerenciador de filas específico**
Segurança de Conexão	hlq.NO.CONNECT.CHECKS	qmgr-name.YES.CONNECT.CHECKS
Segurança da fila	hlq.NO.QUEUE.CHECKS	qmgr-name.YES.QUEUE.CHECKS
Segurança do processo	hlq.NO.PROCESS.CHECKS	qmgr-name.YES.PROCESS.CHECKS
Segurança da lista de nomes	hlq.NO.NLIST.CHECKS	qmgr-name.YES.NLIST.CHECKS
Segurança de contexto	hlq.NO.CONTEXT.CHECKS	qmgr-name.YES.CONTEXT.CHECKS
Segurança de usuário alternativo	hlq.NO.ALTERNATE.USER.CHECKS	qmgr-name.YES.ALTERNATE.USER.CHECKS
Segurança de Comando	hlq.NO.CMD.CHECKS	qmgr-name.YES.CMD.CHECKS
Segurança do Recurso de Comando	hlq.NO.CMD.RESC.CHECKS	qmgr-name.YES.CMD.RESC.CHECKS
Segurança do tópico	hlq.NO.TOPIC.CHECKS	qmgr-name.YES.TOPIC.CHECKS
Nota: Perfis do comutador genérico, como hlq.NO. * * são ignorados por IBM MQ		

Por exemplo, se você desejar executar verificações de segurança do processo no gerenciador de filas QM01, que é um membro do grupo de filas compartilhadas QSG3, mas não desejar executar verificações de segurança do processo em nenhum dos outros gerenciadores de filas no grupo, defina os perfis do comutador a seguir:

```
QSG3.NO.PROCESS.CHECKS
QM01.YES.PROCESS.CHECKS
```

Se você desejar ter verificações de segurança de fila executadas em todos os gerenciadores de filas no grupo de filas compartilhadas, exceto QM02, defina o perfil do comutador a seguir:

```
QM02.NO.QUEUE.CHECKS
```

(Não há necessidade de definir um perfil para o grupo de filas compartilhadas porque as verificações serão ativadas automaticamente se não houver um perfil definido.)

z/OS *Um Exemplo de Definição de Comutadores*

Subsistemas IBM MQ diferentes possuem requisitos de segurança diferentes, que podem ser implementados usando diferentes perfis do comutador.

Quatro subsistemas IBM MQ foram definidos:

- MQP1 (um sistema de produção)
- MQP2 (um sistema de produção)
- MQD1 (um sistema de desenvolvimento)
- MQT1 (um sistema de teste)

Todos os quatro gerenciadores de filas são membros do grupo de filas compartilhadas QS01. Todas as classes do IBM MQ RACF foram definidas e ativadas.

Esses subsistemas possuem requisitos de segurança diferentes:

- Os sistemas de produção requerem que a verificação de segurança completa do IBM MQ esteja ativa no nível do grupo de filas compartilhadas em ambos os sistemas.

  Isso é feito especificando o perfil a seguir:

  ```
  RDEFINE MQADMIN QS01.NO.QMGR.CHECKS
  ```

  Isso configura a verificação de nível do grupo de filas compartilhadas para todos os gerenciadores de filas no grupo de filas compartilhadas. Não é necessário definir quaisquer outros perfis do comutador para os gerenciadores de filas de produção porque você deseja verificar tudo para esses sistemas.
- O gerenciador de filas de teste MQT1 também requer verificação de segurança integral. No entanto, como você pode desejar mudar isso posteriormente, a segurança pode ser definida no nível do gerenciador de filas para que seja possível mudar as configurações de segurança para esse gerenciador de filas sem afetar os outros membros do grupo de filas compartilhadas.

  Isso é feito definindo o perfil NO.QSG.CHECKS para MQT1 conforme a seguir:

  ```
  RDEFINE MQADMIN MQT1.NO.QSG.CHECKS
  ```
- O gerenciador de filas de desenvolvimento MQD1 possui requisitos de segurança diferentes do restante do grupo de filas compartilhadas. Ele requer apenas segurança de conexão e da fila para estar ativo.

  Isso é feito definindo um perfil `MQD1.YES.QMGR.CHECKS` para esse gerenciador de filas e, em seguida, definindo os perfis a seguir para desativar a verificação de segurança para os recursos que não precisam ser verificados:

  ```
  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
  ```

Quando o gerenciador de filas está ativo, é possível exibir as configurações de segurança atuais emitindo o comando DISPLAY SECURITY MQSC.

Também é possível alterar as configurações do comutador quando o gerenciador de filas está em execução, definindo ou excluindo o perfil do comutador apropriado na classe MQADMIN. Para tornar as mudanças nas configurações do comutador ativas, você deve emitir o comando REFRESH SECURITY para a classe MQADMIN.

Consulte “Atualizando a segurança do gerenciador de filas no z/OS” na página 251 para obter mais detalhes sobre o uso dos comandos DISPLAY SECURITY e REFRESH SECURITY.

z/OS Perfis usados para controlar o acesso a recursos do IBM MQ

Deve-se definir perfis do RACF para controlar o acesso a recursos do IBM MQ, além dos perfis do comutador que possam ter sido definidos. Esta coleção de tópicos contém informações sobre os perfis do RACF para os diferentes tipos de recursos do IBM MQ.

Se você não tiver um perfil de recurso definido para uma determinada verificação de segurança, e um usuário emitir uma solicitação que implicaria fazer essa verificação, o IBM MQ nega o acesso. Você não precisa definir perfis para tipos de segurança que se relacionam a quaisquer comutadores de segurança que você desativou.

z/OS *Perfis para Segurança de Conexão*

Se a segurança de conexão estiver ativa, deve-se definir perfis na classe MQCONN e permitir o acesso de grupos ou IDs de usuário necessários a esses perfis, de modo que possam se conectar ao IBM MQ.

Para permitir que uma conexão seja feita, deve-se conceder aos usuários do RACF acesso READ para o perfil apropriado. (Se não existir nenhum perfil de nível do gerenciador de filas e seu gerenciador de filas for um membro de um grupo de filas compartilhadas, as verificações poderão ser feitas com relação aos perfis de nível do grupo de filas compartilhadas, se a segurança estiver configurada para fazer isso.)

Um perfil de conexão qualificado com um nome do gerenciador de filas controla o acesso a um gerenciador de filas específico e os usuários que recebem acesso a esse perfil podem se conectar a esse gerenciador de filas. Um perfil de conexão qualificado com o nome do grupo de filas compartilhadas controla o acesso a todos os gerenciadores de filas dentro do grupo de filas compartilhadas para esse tipo de conexão. Por exemplo, um usuário com acesso a `QS01.BATCH` pode usar uma conexão em lotes para qualquer gerenciador de filas no grupo de filas compartilhadas QS01 que não tenha um perfil de nível do gerenciador de filas definido.

Nota:

1. Para obter informações sobre os IDs de usuário verificados para diferentes solicitações de segurança, consulte “IDs de usuário para verificação de segurança no z/OS” na página 239.
2. As verificações de segurança no nível de recurso (RESLEVEL) também são feitas no tempo de conexão. Para obter detalhes, consulte a seção “O perfil de segurança RESLEVEL” na página 233.

A segurança do IBM MQ reconhece os tipos de conexão diferentes a seguir:

- Conexões em lotes (e do tipo lote), que incluem:
  - Tarefas em lote do z/OS
  - Aplicativos TSO
  - Conexões do USS
  - Procedimentos armazenados do Db2
- Conexões do CICS
- Conexões do IMS a partir das regiões de processamento de controle e requisição
- O inicializador de canais do IBM MQ

z/OS *Perfis de Segurança de Conexão para Conexões em Lotes*

Os perfis para verificação de conexões de tipo de lote são compostos pelo nome do gerenciador de filas ou do grupo de filas compartilhadas, seguido pela palavra *BATCH*. Conceda ao ID do usuário associado com o espaço de endereço de conexão o acesso READ para o perfil de conexão.

Os perfis para verificação de conexões em lotes e do tipo lote têm o formato:

```
hlq.BATCH
```

em que `hlq` pode ser o `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas). Se você estiver usando o gerenciador de filas e segurança no nível do grupo de filas compartilhadas, o IBM MQ verifica se há perfil prefixado pelo nome do gerenciador de filas. Se não

localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas. Se ele falhar em localizar qualquer um dos perfis, a solicitação de conexão falhará.

Para solicitações de conexão em lotes ou do tipo lote, você deve permitir que o ID do usuário associado com o espaço de endereço de conexão acesse o perfil de conexão. Por exemplo, o seguinte comando do RACF permite que os usuários no grupo CONNTQM1 se conectem ao TQM1 do gerenciador de filas esses IDs de usuário serão autorizados a usar qualquer conexão em lote ou conexão do tipo de lote.

```
RDEFINE MQCONN TQM1.BATCH UACC(NONE)
PERMIT TQM1.BATCH CLASS(MQCONN) ID(CONNTQM1) ACCESS(READ)
```

z/OS *Usando o **CHCKLOCL** em aplicativos de limite local*

CHCKLOCL se aplica somente a conexões que são feitas através de conexões em BATCH e não se aplica a conexões feitas a partir do CICS ou IMS. As conexões feitas por meio do inicializador de canais são controladas por **CHCKCLNT**.

Visão Geral

Se você deseja configurar seu gerenciador de filas do z/OS para delegar verificação de ID do usuário e senha para alguns, mas não todos, dos seus aplicativos de limite local, será necessário executar alguma configuração adicional.

O motivo para isso é que uma vez que **CHCKLOCL** (*REQUERIDO*) é configurada, os aplicativos em lote anteriores que usam a chamada API MQCONN não podem mais se conectar ao gerenciador de filas.

Somente para o z/OS, um mecanismo mais granular com base na segurança de conexão de um espaço de endereço pode ser usado para fazer downgrade da configuração global CHCKLOCL(REQUIRED) para CHCKLOCL(OPCIONAL) para IDs do usuário especificamente definidos. O mecanismo usado é descrito no texto a seguir, juntamente com um exemplo.

Para permitir mais granularidade no **CHCKLOCL** (*REQUIRED*) que apenas EVERYONE, modifique **CHCKLOCL** da mesma maneira que você modifica o nível de acesso do ID do usuário associado com o espaço de endereço de conexão com os perfis de conexão `hlq.batch` na classe MQCONN.

Se o ID do usuário do espaço de endereço tem apenas acesso READ, que é o mínimo necessário para ser capaz de se conectar a todos, a configuração **CHCKLOCL** se aplica conforme gravados.

Se o ID do usuário do espaço de endereço tem acesso UPDATE (ou superior), a configuração **CHCKLOCL** opera no modo *OPTIONAL*. Ou seja, não é necessário fornecer um ID do usuário e senha, mas se isso for feito o ID do usuário e a senha devem ser um par válido.

Segurança de conexão já configurada para seu gerenciador de filas do z/OS

Se você tiver a segurança de conexão configurada para seu gerenciador de filas do z/OS e você deseja que o **CHCKLOCL** (*REQUIRED*) se aplique aos aplicativos de limite local WAS e não sobre nenhuns outros, execute as etapas a seguir:

1. Inicie com **CHCKLOCL** (*OPTIONAL*) como sua configuração. Isso significa que qualquer ID de usuário e senhas que são fornecidos são verificados quanto à validade, mas não é obrigatório.
2. Liste todos os usuários que possuem acesso aos perfis de segurança de conexão emitindo o comando:

   ```
   RLIST MQCONN MQ23.BATCH AUTHUSER
   ```

   Este comando exibe, por exemplo:

   ```
   CLASS    NAME
   -----    ----
   MQCONN   MQ23.BATCH

   USER     ACCESS  ACCESS COUNT
   ----     ------  ------ -----
   ```

```
JOHNDOE  READ    000009
JDOE1    READ    000003
WASUSER  READ    000000
```

3. Para cada ID do usuário listado como tendo acesso READ, mude o acesso a

```
UPDATE:- PERMIT MQ23.BATCH CLASS(MQCONN) ID(JOHNDOE) ACCESS(UPDATE)
```

4. Atualize a configuração do IBM MQ para **CHCKLOCL** (*REQUIRED*).

   A combinação de acesso UPDATE ao MQ23.BATCH e a configuração atual significam que você está usando **CHCKLOCL** (*OPTIONAL*).

5. Agora, aplique o comportamento **CHCKLOCL** (*REQUIRED*) para um ID do usuário específico, por exemplo WASUSER, de modo que todas as conexões provenientes dessa região deverão fornecer um ID do usuário e uma senha.

   Faça isso invertendo as mudanças feitas anteriormente, emitindo o comando:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

A segurança de conexão não está configurada para o gerenciador de filas do z/OS

Nesta situação, deve-se:

1. Crie perfis de conexão para o hlq.BATCH na classe MQCONN emitindo o comando:

```
RDEFINE MQCONN MQ23.BATCH UACC(NONE)
```

2. Autorize todos os IDs do usuário que criar conexões em lote para o gerenciador de filas, para que eles tenham acesso UPDATE para este perfil. Fazer isso efetua bypass do requisito **CHCKLOCL** (*REQUIRED*) para o ID do usuário e a senha no momento da conexão.

   Faça isso emitindo o comando:

```
PERMIT MQ23.BATCH CLASS(MQCONN)ID(JOHNDOE) ACCESS(UPDATE)
```

   Eles incluem IDs do usuário:

   a. Usado para CSQUTIL, painéis ISPF e outras ferramentas de limite local.

   b. Associado conexões como em lote com o gerenciador de filas. Considere, por exemplo, os procedimentos armazenados do Advanced Message Security, do IBM Integration Bus, do Db2, usuários do USS e TSO e aplicativos Java

3. Exclua o perfil do comutador para o gerenciador de filas emitindo o comando:

```
hlq.NO.CONNECT.CHECKS
```

4. Agora, aplique o comportamento **CHCKLOCL** (*REQUIRED*) para um ID do usuário específico, por exemplo WASUSER, de modo que todas as conexões provenientes dessa região deverão fornecer um ID do usuário e uma senha.

   Faça isso invertendo as mudanças feitas anteriormente, emitindo o comando:

```
PERMIT MQ23.BATCH CLASS(MQCONN) ID(WASUSER) ACCESS(READ)
```

z/OS *Perfis de segurança de conexão para conexões do CICS*

Os perfis para verificar conexões do CICS são compostos do nome do gerenciador de filas ou do grupo de filas compartilhadas seguido pela palavra *CICS* . Conceda ao ID do usuário associado o acesso READ do espaço de endereço do CICS para o perfil de conexão.

Os perfis para verificação de conexões a partir de CICS têm o formato:

```
hlq.CICS
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas). Se você estiver usando o gerenciador de filas e segurança no nível do grupo de filas compartilhadas, o IBM MQ verifica se há perfil prefixado pelo nome do gerenciador de filas. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas. Se ele falhar em localizar qualquer um dos perfis, a solicitação de conexão falhará

Para solicitações de conexão pelo CICS, é necessário permitir somente o acesso do ID do usuário do espaço de endereço do CICS para o perfil de conexão.

Por exemplo, os comandos do RACF a seguir permitem que o ID do usuário do espaço de endereço do CICS KCBCICS se conecte ao gerenciador de filas TQM1:

```
RDEFINE MQCONN TQM1.CICS UACC(NONE)
PERMIT TQM1.CICS CLASS(MQCONN) ID(KCBCICS) ACCESS(READ)
```

z/OS *Perfis de segurança de conexão para conexões do IMS*

Os perfis para verificar conexões do IMS são compostos do nome do gerenciador de filas ou do grupo de filas compartilhadas seguido pela palavra *IMS* . Forneça o controle e acesso READ de IDs de usuário da região do IMS dependente para o perfil de conexão.

Os perfis para verificação de conexões a partir de IMS têm o formato:

```
hlq.IMS
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas). Se você estiver usando o gerenciador de filas e segurança no nível do grupo de filas compartilhadas, o IBM MQ verifica se há perfil prefixado pelo nome do gerenciador de filas. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas. Se ele falhar em localizar qualquer um dos perfis, a solicitação de conexão falhará

Para solicitações de conexão pelo IMS, permita o acesso ao perfil de conexão para o controle e IDs de usuário da região dependente do IMS.

Por exemplo, os seguintes comandos do RACF permitem:

- O ID de usuário da região do IMS, IMSREG, para se conectar ao gerenciador de filas TQM1.
- Os usuários no grupo BMPGRP enviem tarefas BMP.

```
RDEFINE MQCONN TQM1.IMS UACC(NONE)
PERMIT TQM1.IMS CLASS(MQCONN) ID(IMSREG,BMPGRP) ACCESS(READ)
```

z/OS *Perfis de Segurança de Conexão para o Inicializador de Canais*

Perfis para verificação de conexões do inicializador de canais são compostos pelo nome do gerenciador de filas ou do grupo de filas compartilhadas, seguido pela palavra *CHIN*. Conceda ao ID do usuário usado pelo espaço de endereço de tarefa iniciada do inicializador de canais o acesso READ para o perfil de conexão.

Os perfis para verificação de conexões do inicializador de canais têm o formato:

```
hlq.CHIN
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas). Se você estiver usando o gerenciador de filas e segurança no nível do grupo de filas compartilhadas, o IBM MQ verifica se há perfil prefixado pelo nome do gerenciador de filas. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas. Se ele falhar em localizar qualquer um dos perfis, a solicitação de conexão falhará

Para solicitações de conexão pelo inicializador de canais, defina o acesso ao perfil de conexão para o ID do usuário usado pelo espaço de endereço de tarefa iniciada do inicializador de canais.

Por exemplo, os seguintes comandos do RACF permitem que o espaço de endereço do inicializador de canais em execução com o ID do usuário DQCTRL se conecte ao TQM1 gerenciador de filas:

```
RDEFINE MQCONN TQM1.CHIN UACC(NONE)
PERMIT TQM1.CHIN CLASS(MQCONN) ID(DQCTRL) ACCESS(READ)
```

z/OS *Perfis para Segurança de Fila*

Se a segurança da fila estiver ativa, você deverá definir perfis nas classes apropriadas e permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis. Os perfis de segurança da fila são nomeados após o gerenciador de filas ou o grupo de filas compartilhadas e a fila a ser aberta.

Se a segurança da fila estiver ativa, você deverá:

- Definir perfis nas classes **MQQUEUE** ou **GMQQUEUE** se estiver usando perfis em maiúsculas.
- Definir perfis nas classes **MXQUEUE** ou **GMXQUEUE** se estiver usando perfis compostos por letras maiúsculas e minúsculas.
- Permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis, para que eles possam emitir solicitações de API do IBM MQ que usam filas.

Os perfis para a segurança da fila têm o formato:

```
hlq.queuename
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas) e `queuename` é o nome da fila que está sendo aberta, conforme especificado no descritor de objeto na chamada `MQOPEN` ou `MQPUT1`.

Um perfil prefixado pelo nome do gerenciador de filas controla o acesso a uma única fila nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o acesso a uma ou mais filas com esse nome de fila em todos os gerenciadores de filas no grupo de filas compartilhadas ou o acesso a uma fila compartilhada por qualquer gerenciador de filas no grupo. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para essa fila nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

Se você estiver usando filas compartilhadas, recomenda-se usar a segurança no nível do grupo de filas compartilhadas.

Para obter detalhes de como a segurança da fila opera quando o nome da fila é o de um alias ou de uma fila modelo z/OS, consulte “Considerações para Filas de Alias” na página 202 e “Considerações para Filas Modelo” na página 203 .

O acesso RACF necessário para abrir uma fila depende das opções MQOPEN ou MQPUT1 especificadas. Se mais de uma das opções MQOO_* e MQPMO_* estiverem codificadas, a verificação de segurança da fila é executada para a autoridade mais alta do RACF necessária.

Tabela 31. Níveis de Acesso para a Segurança da Fila Usando as Chamadas MQOPEN ou MQPUT1

Opção MQOPEN ou MQPUT1	**Nível de acesso do RACF requerido para hlq.queuename**
MQOO_BROWSE	READ
MQOO_INQUIRE	READ
MQOO_BIND_*	UPDATE
MQOO_INPUT_*	UPDATE
MQOO_OUTPUT ou MQPUT1	UPDATE
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	UPDATE
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	UPDATE
MQOO_SAVE_ALL_CONTEXT	UPDATE
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	UPDATE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	UPDATE
MQOO_SET	ALTER

Por exemplo, no Gerenciador de Filas QM77 do IBM MQ, todos os IDs de usuário no grupo PAYGRP do RACF devem ter acesso para obter mensagens ou colocar mensagens em todas as filas com nomes iniciados com 'PAY.'. É possível fazer isso usando estes comandos do RACF:

```
RDEFINE MQQUEUE QM77.PAY.** UACC(NONE)
PERMIT QM77.PAY.** CLASS(MQQUEUE) ID(PAYGRP) ACCESS(UPDATE)
```

Além disso, todos os IDs de usuário no grupo PAYGRP devem ter acesso para colocar mensagens em filas que não seguem a convenção de nomenclatura PAY. Por exemplo:

```
REQUEST_QUEUE_FOR_PAYROLL
SALARY.INCREASE.SERVER
REPLIES.FROM.SALARY.MODEL
```

É possível fazer isso definindo perfis para estas filas na classe GMQQUEUE e fornecendo acesso a essa classe conforme a seguir:

```
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)
```

Nota:

1. Se o nível de acesso do RACF que um aplicativo tem para um perfil de segurança da fila for mudado, as mudanças entrarão em vigor somente para qualquer manipulação de objetos nova obtida (ou seja, novos MQOPEN s) para essa fila. Essas manipulações já em existência no momento da mudança retêm seu acesso existente para a fila. Se for necessário que um aplicativo use seu nível de acesso alterado para a fila em vez de seu nível de acesso existente, ele deverá fechar e reabrir a fila para cada manipulação de objeto que requerer a mudança.
2. No exemplo, o nome do gerenciador de filas QM77 também pode ser o nome de um grupo de filas compartilhadas.

Outros tipos de verificações de segurança também podem ocorrer no momento em que a fila é aberta dependendo das opções de abertura especificadas e dos tipos de segurança que estão ativos.

z/OS Consulte também “Perfis para Segurança de Contexto” na página 218 e “Perfis para segurança de usuário alternativo” na página 216. Para ver uma tabela de resumo mostrando as opções abertas e a autorização de segurança necessária quando a fila, o contexto e a segurança de usuário alternativo estão todos ativos, consulte Tabela 36 na página 208.

Se você estiver usando publicação/assinatura, deverá fazer as considerações a seguir. Quando uma solicitação MQSUB é processada, uma verificação de segurança é executada para garantir que o ID do usuário que está fazendo a solicitação tenha o acesso necessário para colocar mensagens para a fila de destino do IBM MQ, assim como o acesso necessário para se inscrever no tópico do IBM MQ.

Tabela 32. Níveis de Acesso para Segurança da Fila Usando a Chamada MQSUB

Opção MQSUB	**Nível de acesso do RACF requerido para hlq.queuename**
MQSO_ALTER, MQSO_CREATE e MQSO_RESUME	UPDATE

Nota:

1. A `hlq.queuename` é a fila de destino para publicações. Quando essa é uma fila gerenciada, é necessário acesso à fila modelo apropriada a ser usada para a fila gerenciada e a fila dinâmica que são criadas.
2. É possível usar uma técnica como essa para a fila de destino fornecida em uma chamada API MQSUB se você desejar distinguir entre os usuários que fazem as assinaturas e os usuários que recuperam as publicações da fila de destino.

z/OS *Considerações para Filas de Alias*

Ao emitir uma chamada MQOPEN ou MQPUT1 para uma fila de alias, o IBM MQ faz uma verificação de recursos com relação ao nome da fila especificado no descritor de objetos (MQOD) na chamada. Ele não verifica se o usuário tem permissão para acessar o nome da fila de destino.

Por exemplo, uma fila de alias chamada PAYROLL.REQUEST resolve para uma fila de destino de PAY.REQUEST. Se a segurança da fila estiver ativa, só será necessária autorização para acessar a fila PAYROLL.REQUEST. Nenhuma verificação é feita para ver se você está autorizado a acessar a fila PAY.REQUEST.

z/OS *Usando Filas de Alias para Distinguir entre Solicitações MQGET e MQPUT*

O intervalo de chamadas MQI disponível em um nível de acesso pode causar um problema se você desejar restringir o acesso a uma fila para permitir apenas a chamada **MQPUT** ou apenas a chamada **MQGET**. Uma fila pode ser protegida definindo dois aliases que resolvem para essa fila: um que permita que os aplicativos obtenham mensagens da fila e um que permita que os aplicativos coloquem mensagens na fila.

O texto a seguir fornece um exemplo de como é possível definir suas filas para o 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)
```

Também se deve fazer as seguintes definições do 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)
```

Em seguida, assegure-se de que nenhum usuário tenha acesso à fila hlq.MUST_USE_ALIAS_TO_ACCESS e conceda aos usuários ou grupos apropriados o acesso para o alias. É possível fazer isso usando os seguintes comandos do 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)
```

Isso significa que o ID do usuário GETUSER e os IDs de usuário no grupo GETGRP só são permitidos obter mensagens em MUST_USE_ALIAS_TO_ACCESS por meio da fila de alias USE_THIS_ONE_FOR_GETS e o ID do usuário PUTUSER e os IDs de usuário no grupo PUTGRP só são permitidos colocar mensagens por meio da fila de alias USE_THIS_ONE_FOR_PUTS.

Nota:

1. Se você desejar usar uma técnica como essa, deverá informar seus desenvolvedores de aplicativos para que eles possam projetar seus programas apropriadamente.
2. É possível usar uma técnica como essa para a fila de destino que você fornecer em uma solicitação da API MQSUB se desejar distinguir entre os usuários que fazem as assinaturas e os usuários que 'obtêm' as publicações da fila de destino

z/OS *Considerações para Filas Modelo*

Para abrir uma fila modelo, você deve estar apto a abrir a própria fila modelo e a fila dinâmica para a qual ela resolve. Defina perfis genéricos do RACF para filas dinâmicas, incluindo filas dinâmicas usadas por utilitários do IBM MQ.

Quando você abre uma fila modelo, a segurança do IBM MQ faz duas verificações de segurança da fila:

1. Você está autorizado a acessar a fila modelo?
2. Você está autorizado a acessar a fila dinâmica para a qual a fila modelo resolve?

Se o nome da fila dinâmica contém um caractere de asterisco final (*), este * é substituído por uma sequência de caracteres gerada pelo IBM MQ para criar uma fila dinâmica com um nome exclusivo. Entretanto, como o nome inteiro, incluindo essa sequência gerada, é usado para verificar a autoridade, você deve definir perfis genéricos para essas filas.

Por exemplo, uma chamada MQOPEN usa um nome de fila modelo de CREDIT.CHECK.REPLY.MODEL e um nome de fila dinâmica de CREDIT.REPLY.* no gerenciador de filas (ou grupo de filas compartilhadas) MQSP.

Para fazer isso, deve-se emitir os seguintes comandos do RACF para definir os perfis de filas necessários:

```
RDEFINE MQQUEUE MQSP.CREDIT.CHECK.REPLY.MODEL
RDEFINE MQQUEUE MQSP.CREDIT.REPLY.**
```

Também se deve emitir os comandos PERMIT do RACF correspondentes para permitir o acesso do usuário a esses perfis.

Um nome de fila dinâmica típico criado por um MQOPEN é algo como CREDIT.REPLY.A346EF00367849A0. O valor exato do último qualificador é imprevisível; este é o motivo pelo qual você deve usar perfis genéricos para tais nomes de filas.

Vários utilitários do IBM MQ colocam mensagens em filas dinâmicas. É necessário definir perfis para os nomes de fila dinâmica a seguir e fornecer acesso UPDATE do RACF para os IDs de usuário relevantes (consulte “IDs de usuário para verificação de segurança no z/OS” na página 239 para obter os IDs de usuário corretos):

```
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)
```

Você também pode considerar definir um perfil para controlar o uso do nome da fila dinâmica usado por padrão nos membros de cópia de programação de aplicativos. Os copybooks fornecidos pelo IBM MQ contêm um *DynamicQName* padrão, que é CSQ.*. Isso permite que um perfil adequado do RACF seja estabelecido.

Nota: Não permita que os programadores de aplicativos especifiquem um único * para o nome da fila dinâmica. Se você fizer isso, deverá definir um hlq. * * na classe MQQUEUE e você teria que dar a ela acesso amplo. Isso significa que este perfil também pode ser usado para outras filas não dinâmicas que não possuem um perfil do RACF mais específico. Seus usuários poderiam, portanto, obter acesso a filas que você não deseja que eles acessem.

z/OS *Opções de Fechamento em Filas Dinâmicas Permanentes*

Se um aplicativo abrir uma fila dinâmica permanente que foi criada por outro aplicativo e, em seguida, tentar excluir essa fila com uma opção MQCLOSE, algumas verificações de segurança extras serão aplicadas quando a tentativa for feita.

Tabela 33. Níveis de Acesso para Opções de Fechamento em Filas Dinâmicas Permanentes

Opção MQCLOSE	**Nível de acesso do RACF requerido para hlq.queuename**
MQCO_DELETE	ALTER
MQCO_DELETE_PURGE	ALTER

z/OS *Segurança e Filas Remotas*

Quando uma mensagem é colocada em uma fila remota, a segurança da fila implementada pelo gerenciador de filas locais depende de como a fila remota está especificada ao ser aberta.

As regras a seguir são aplicadas:

1. Se a fila remota tiver sido definida no gerenciador de filas locais por meio do comando IBM MQ DEFINE QREMOTE, a fila verificada será o nome da fila remota. Por exemplo, se uma fila remota estiver definida no gerenciador de filas MQS1 conforme a seguir:

   ```
   DEFINE QREMOTE(BANK7.CREDIT.REFERENCE)
          RNAME(CREDIT.SCORING.REQUEST)
          RQMNAME(BNK7)
          XMITQ(BANK1.TO.BANK7)
   ```

   Neste caso, um perfil para BANK7.CREDIT.REFERENCE deverá ser definido na classe MQQUEUE.
2. Se o *ObjectQMgrName* para a solicitação não resolver para o gerenciador de filas locais, uma verificação de segurança será executada com relação ao nome do gerenciador de filas (remoto) resolvido, exceto no caso de uma fila de clusters em que a verificação é feita com relação ao nome da fila de clusters.

   Por exemplo, a fila de transmissão BANK1.TO.BANK7 está definida no gerenciador de filas MQS1. Uma solicitação MQPUT1 é então emitida no MQS1 especificando *ObjectName* como BANK1.INTERBANK.TRANSFERS e um *ObjectQMgrName* de BANK1.TO.BANK7. Neste caso, o usuário que executa a solicitação deve ter acesso ao BANK1.TO.BANK7.
3. Se você fizer uma solicitação MQPUT para uma fila e especificar *ObjectQMgrName* como o nome de um alias do gerenciador de filas local, apenas o nome da fila será verificado para segurança, não o do gerenciador de filas.

Quando a mensagem chega ao gerenciador de filas remotas, ela pode estar sujeita ao processamento de segurança adicional. Para obter informações adicionais, consulte "Segurança para o Sistema de Mensagens Remoto" na página 96.

z/OS *Segurança da Fila de Devoluções*

Considerações especiais se aplicam à fila de devoluções, uma vez que muitos usuários devem estar aptos a colocar mensagens nela, mas o acesso para recuperar mensagens deve ser rigorosamente restrito. É possível atingir isso aplicando diferentes autoridades do RACF para a fila de mensagens não entregues e uma fila de alias.

As mensagens não entregues podem ser colocadas em uma fila especial chamada de fila de devoluções. Se você tiver dados sensíveis que possivelmente poderiam acabar nessa fila, deverá considerar as implicações de segurança disso porque não deseja que usuários não autorizados recuperem esses dados.

Cada um dos seguintes deve ser permitido colocar mensagens na fila de devoluções:

- Programas de aplicativos.
- O espaço de endereço do inicializador de canais e quaisquer IDs de usuário do MCA. (Se o perfil RESLEVEL não estiver presente, ou estiver definido de forma que os IDs do usuário do canal são verificados, o ID do usuário do canal também precisa de autoridade para colocar mensagens na fila de mensagens não entregues.)
- CKTI, o inicializador de tarefas do CICS fornecido por CICS.
- CSQQTRMN, o monitor acionador IBM MQ-fornecido IMS

O único aplicativo que pode recuperar mensagens da fila de mensagens não entregues deve ser um aplicativo 'especial' que processa essas mensagens. No entanto, um problema surge se você fornecer a autoridade UPDATE aos aplicativos RACF para a fila de mensagens não entregues do MQPUT, pois eles podem, então, recuperar automaticamente as mensagens da fila usando chamadas MQGET. Não é possível desativar a fila de mensagens não entregues para operações get porque, se você fizer isso, nem mesmo os aplicativos 'especiais' poderão recuperar as mensagens.

Uma solução para esse problema é configurar um acesso de dois níveis para a fila de devoluções. CKTI, as transações do agente do canal de mensagens ou o espaço de endereço do inicializador de canais e os aplicativos 'especiais' têm acesso direto; outros aplicativos podem acessar a fila de mensagens não entregues somente por meio de uma fila de alias. Esse alias é definido para permitir que os aplicativos coloquem mensagens na fila de devoluções, mas não obtenham mensagens a partir dela.

Esta é maneira como isso pode funcionar:

1. Defina a fila de devoluções real com atributos PUT(ENABLED) e GET(ENABLED), conforme mostrado na amostra thlqual.SCSQPROC(CSQ4INYG).
2. Forneça a autoridade UPDATE do RACF à fila de mensagens não entregues para os seguintes IDs de usuário:
   - Os IDs de usuário sob os quais o CKTI e os MCAs ou espaço de endereço do inicializador de canais são executados.
   - Os IDs de usuário associados ao aplicativo de processamento de fila de mensagens não entregues 'especiais'.
3. Defina uma fila de alias que resolva para a fila de devoluções real, mas forneça estes atributos à fila de alias: PUT(ENABLED) e GET(DISABLED). Forneça um nome para a fila de alias com a mesma raiz que o nome da fila de mensagens não entregues, mas anexe os caracteres ".PUT" a essa raiz. Por exemplo, se o nome da fila de devoluções for hlq.DEAD.QUEUE, o nome da fila de alias será hlq.DEAD.QUEUE.PUT.
4. Para colocar uma mensagem na fila de devoluções, um aplicativo usa a fila de alias. Isto é o que seu aplicativo deve fazer:
   - Recuperar o nome da fila de devoluções real. Para fazer isso, ele abre o objeto de gerenciador de filas usando `MQOPEN` e, em seguida, emite um `MQINQ` para obter o nome da fila de devoluções.
   - Construa o nome da fila de alias anexando os 'caracteres .PUT' a este nome, neste caso, hlq.DEAD.QUEUE.PUT.
   - Abra a fila de alias, hlq.DEAD.QUEUE.PUT.
   - Coloque a mensagem na fila de devoluções real emitindo um `MQPUT` com relação à fila de alias.
5. Conceda a autoridade UPDATE do RACF ao ID do usuário associado ao aplicativo para o alias, mas nenhum acesso (autoridade NONE) para a fila de mensagens não entregues real. Isto significa que:
   - O aplicativo pode colocar mensagens na fila de devoluções usando a fila de alias.
   - O aplicativo não pode obter mensagens da fila de devoluções usando a fila de alias porque a fila de alias está desativada para operações de obtenção.

   O aplicativo não pode obter quaisquer mensagens da fila de mensagens não entregues real porque ele tem a autoridade correta do RACF.

O Tabela 34 na página 206 resume a autoridade do RACF necessária para os vários participantes nesta solução.

Tabela 34. Autoridade do RACF para a fila de mensagens não entregues e seu alias

IDs de usuário associados	**Fila de devoluções real (hlq.DEAD.QUEUE)**	**Fila de devoluções do alias (hlq.DEAD.QUEUE.PUT)**
MCA ou espaço de endereço do inicializador de canais e CKTI	ATUALIZAÇÃO	NONE
Aplicativo 'especial' (para processamento de fila de devoluções)	ATUALIZAÇÃO	NONE
IDs de usuário do aplicativo gravado pelo usuário	NONE	ATUALIZAÇÃO

Se você usar esse método, o aplicativo não poderá determinar o comprimento máximo da mensagem (MAXMSGL) da fila de devoluções. Isso ocorre porque o atributo MAXMSGL não pode ser recuperado de uma fila de alias. Portanto, seu aplicativo deve assumir que o comprimento máximo da mensagem é de 100 MB, o tamanho máximo que o IBM MQ for z/OS suporta. A fila de devoluções real também deve ser definida com um atributo MAXMSGL de 100 MB.

Nota: Os programas de aplicativos gravados pelo usuário normalmente não usam autoridade de usuário alternativo para colocar mensagens na fila de devoluções. Isso reduz o número de IDs de usuário que possuem acesso à fila de devoluções.

z/OS *Segurança da Fila do Sistema*

Deve-se configurar o acesso do RACF para permitir que determinados IDs do usuário acessem as filas do sistema específico.

Muitas das filas do sistema são acessadas pelas partes auxiliares do IBM MQ:

- O Utilitário CSQUTIL
- O utilitário de política de segurança da mensagem (CSQ0UTIL)
- Os painéis de operações e controle
- O espaço de endereço do inicializador de canais (incluindo o Daemon de Publicação/Assinatura Enfileirada)
- V 9.1.0 O servidor mqweb, usado pelo MQ Console e REST API.

Os IDs de usuário sob os quais esses executam devem receber acesso do RACF a essas filas, conforme mostrado em Tabela 35 na página 207.

Tabela 35. Acesso necessário às filas SYSTEM por IBM MQ

Fila de SYSTEM	CSQUTIL	CSQ0UTIL	servidor mqweb	Painéis de operações e controle	Inicializador de canais para enfileiramento distribuído
SYSTEM.ADMIN.CHANNEL.EVENT	-	-	-	-	ATUALIZAÇÃO
SYSTEM.ADMIN.COMMAND.QUEUE	-	-	ATUALIZAÇÃO	-	-
SYSTEM.BROKER.ADMIN.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.CONTROL.QUEUE	-	-	-	-	ALTER
SYSTEM.BROKER.DEFAULT.STREAM	-	-	-	-	ALTER
SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS	-	-	-	-	ATUALIZAÇÃO
SYSTEM.CHANNEL.INITQ	-	-	-	-	ATUALIZAÇÃO
SYSTEM.CHANNEL.SYNCQ	-	-	-	-	ATUALIZAÇÃO
SYSTEM.CLUSTER.COMMAND.QUEUE	-	-	-	-	ALTER
SYSTEM.CLUSTER.REPOSITORY.QUEUE	-	-	-	-	ATUALIZAÇÃO
SYSTEM.CLUSTER.TRANSMIT.QUEUE	-	-	-	-	ALTER
SYSTEM.COMMAND.INPUT	ATUALIZAÇÃO	-	-	ATUALIZAÇÃO	ATUALIZAÇÃO
SYSTEM.COMMAND.REPLY.*	-	-	-	-	ATUALIZAÇÃO
SYSTEM.COMMAND.REPLY.MODEL	ATUALIZAÇÃO	-	-	ATUALIZAÇÃO	ATUALIZAÇÃO
SYSTEM.CSQOREXX.*	-	-	-	ATUALIZAÇÃO	-

Tabela 35. Acesso necessário às filas SYSTEM por IBM MQ (continuação)					
Fila de SYSTEM	**CSQUTIL**	**CSQ0UTIL**	**servidor mqweb**	**Painéis de operações e controle**	**Inicializador de canais para enfileiramento distribuído**
SYSTEM.CSQUTIL.*	ATUALIZAÇÃO	-	-	-	-
SYSTEM.CSQXCMD.*	-	-	-	-	ATUALIZAÇÃO
SYSTEM.HIERARCHY.STATE	-	-	-	-	ATUALIZAÇÃO
SYSTEM.INTER.QMGR.CONTROL	-	-	-	-	ATUALIZAÇÃO
SYSTEM.INTER.QMGR.PUBS	-	-	-	-	ATUALIZAÇÃO
SYSTEM.INTER.QMGR.FANREQ	-	-	-	-	ATUALIZAÇÃO
SYSTEM.PROTECTION.ERROR.QUEUE	-	-	-	-	ATUALIZAÇÃO
SYSTEM.PROTECTION.POLICY.QUEUE	-	UPDATE “1” na página 208	-	-	READ
SYSTEM.QSG.CHANNEL.SYNCQ	-	-	-	-	ATUALIZAÇÃO
SYSTEM.QSG.TRANSMIT.QUEUE	-	-	-	-	ATUALIZAÇÃO
SYSTEM.REST.REPLY.QUEUE	-	-	ATUALIZAÇÃO	-	-
SYSTEM.BLUEMIX.REGISTRATION.QUEUE	-	-	-	-	ATUALIZAÇÃO

Notes:

1. O usuário do espaço de endereço do Advanced Message Security também requer acesso READ a essa fila.

z/OS *Referência Rápida do Acesso de Segurança de Recursos da API*

Um resumo das opções **MQOPEN**, **MQPUT1**, **MQSUB** e **MQCLOSE** e o acesso requerido pelos diferentes tipos de segurança do recurso.

Tabela 36. Opções MQOPEN, MQPUT1, MQSUB e MQCLOSE e a Autorização de Segurança Necessária. Os textos explicativos mostrados como este **(1)** referem-se às notas após esta tabela.				
	Nível de acesso mínimo necessário do RACF			
Classe do RACF:	**MXTOPIC**	**MQQUEUE ou MXQUEUE (1)**	**MQADMIN ou MXADMIN**	**MQADMIN ou MXADMIN**
Perfil do RACF:	**(15 ou 16)**	**(2)**	**(3)**	**(4)**
Opção MQOPEN				
MQOO_INQUIRE		READ **(5)**	Sem verificação	Sem verificação
MQOO_BROWSE		READ	Sem verificação	Sem verificação

Tabela 36. Opções MQOPEN, MQPUT1, MQSUB e MQCLOSE e a Autorização de Segurança Necessária. Os textos explicativos mostrados como este **(1)** referem-se às notas após esta tabela. *(continuação)*

	Nível de acesso mínimo necessário do RACF			
Classe do RACF:	**MXTOPIC**	**MQQUEUE ou MXQUEUE (1)**	**MQADMIN ou MXADMIN**	**MQADMIN ou MXADMIN**
Perfil do RACF:	**(15 ou 16)**	**(2)**	**(3)**	**(4)**
MQOO_INPUT_*		ATUALIZAÇÃO	Sem verificação	Sem verificação
MQOO_SAVE_ALL_CONTEXT **(6)**		ATUALIZAÇÃO	Sem verificação	Sem verificação
MQOO_OUTPUT (USAGE=NORMAL) **(7)**		ATUALIZAÇÃO	Sem verificação	Sem verificação
MQOO_PASS_IDENTITY_CONTEXT **(8)**		ATUALIZAÇÃO	READ	Sem verificação
MQOO_PASS_ALL_CONTEXT **(8) (9)**		ATUALIZAÇÃO	READ	Sem verificação
MQOO_SET_IDENTITY_CONTEXT **(8) (9)**		ATUALIZAÇÃO	ATUALIZAÇÃO	Sem verificação
MQOO_SET_ALL_CONTEXT **(8) (10)**		ATUALIZAÇÃO	CONTROLE	Sem verificação
MQOO_OUTPUT (USAGE (XMITQ) **(11)**		ATUALIZAÇÃO	CONTROLE	Sem verificação
MQOO_OUTPUT (objeto do tópico)	UPDATE **(16)**			
MQOO_OUTPUT (fila de alias para objeto do tópico)	UPDATE **(16)**	ATUALIZAÇÃO		
MQOO_SET		ALTER	Sem verificação	Sem verificação
MQOO_ALTERNATE_USER_AUTHORITY		**(12)**	**(12)**	ATUALIZAÇÃO
Opção MQPUT1				
Coloque em uma fila normal **(7)**		ATUALIZAÇÃO	Sem verificação	Sem verificação
MQPMO_PASS_IDENTITY_CONTEXT		ATUALIZAÇÃO	READ	Sem verificação
MQPMO_PASS_ALL_CONTEXT		ATUALIZAÇÃO	READ	Sem verificação
MQPMO_SET_IDENTITY_CONTEXT		ATUALIZAÇÃO	ATUALIZAÇÃO	Sem verificação
MQPMO_SET_ALL_CONTEXT		ATUALIZAÇÃO	CONTROLE	Sem verificação
MQOO_OUTPUT Coloque em uma fila de transmissão **(11)**		ATUALIZAÇÃO	CONTROLE	Sem verificação
MQOO_OUTPUT (objeto do tópico)	UPDATE **(16)**			

Tabela 36. Opções MQOPEN, MQPUT1, MQSUB e MQCLOSE e a Autorização de Segurança Necessária. Os textos explicativos mostrados como este **(1)** referem-se às notas após esta tabela. *(continuação)*

	Nível de acesso mínimo necessário do RACF			
Classe do RACF:	**MXTOPIC**	**MQQUEUE ou MXQUEUE (1)**	**MQADMIN ou MXADMIN**	**MQADMIN ou MXADMIN**
Perfil do RACF:	**(15 ou 16)**	**(2)**	**(3)**	**(4)**
MQOO_OUTPUT (fila de alias para objeto do tópico)	UPDATE **(16)**	ATUALIZAÇÃO		
MQPMO_ALTERNATE_USER_AUTHORITY		**(13)**	**(13)**	ATUALIZAÇÃO
Opção MQCLOSE				
MQCO_DELETE **(14)**		ALTER	Sem verificação	Sem verificação
MQCO_DELETE_PURGE **(14)**		ALTER	Sem verificação	Sem verificação
MQCO_REMOVE_SUB	ALTER **(15)**			
Opção MQSUB				
MQSO_CREATE	ALTER **(15)**	**(17)**	**(18)**	
MQSO_ALTER	ALTER **(15)**	**(17)**	**(18)**	
MQSO_RESUME	READ **(15)**	**(17)**	Sem verificação	
MQSO_ALTERNATE_USER_AUTHORITY				ATUALIZAÇÃO
MQSO_SET_IDENTITY_CONTEXT			**(18)**	

Nota:

1. Esta opção não está restrita a filas. Use a classe MQNLIST ou MXNLIST para listas de nomes e a classe MQPROC ou MXPROC para processos.
2. Use o perfil RACF: hlq.resourcename
3. Use o perfil RACF: hlq.CONTEXT.queuename
4. Usar o perfil RACF: hlq.ALTERNATE.USER. `alternateuserid`

   `alternateuserid` é o identificador do usuário que está especificado no campo *`AlternateUserId`* do descritor de objeto. Observe que até 12 caracteres do campo *`AlternateUserId`* são usados para esta verificação, diferentemente de outras verificações em que apenas os primeiros 8 caracteres de um identificador de usuário são usados.
5. Nenhuma verificação é feita ao abrir o gerenciador de filas para consultas.
6. MQOO_INPUT_* também deve ser especificado. Isso é válido para uma fila local, modelo ou de alias.
7. Esta verificação é feita para uma fila local ou modelo que possui um atributo da fila **Usage** de MQUS_NORMAL e também para uma fila de alias ou remota (que está definida para o gerenciador de filas conectado.) Se a fila for uma fila remota que é aberta especificando um *`ObjectQMgrName`* (não o nome do gerenciador de filas conectado) explicitamente, a verificação será executada com relação à fila com o mesmo nome que *`ObjectQMgrName`* (que deve ser uma fila local com um atributo da fila **Usage** de MQUS_TRANSMISSION).
8. MQOO_OUTPUT também deve ser especificado.
9. MQOO_PASS_IDENTITY_CONTEXT também é deduzido por esta opção.

10. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT e MQOO_SET_IDENTITY_CONTEXT também são deduzidos por esta opção.
11. Esta verificação é feita para uma fila local ou modelo que possui um atributo da fila **Usage** de MQUS_TRANSMISSION e está sendo aberta diretamente para saída. Ela não se aplicará se uma fila remota estiver sendo aberta.
12. Pelo menos um de MQOO_INQUIRE, MQOO_BROWSE, MQOO_INPUT_*, MQOO_OUTPUT ou MQOO_SET também deve ser especificado. A verificação executada é a mesma que aquela das outras opções especificadas.
13. A verificação executada é a mesma que aquela das outras opções especificadas.
14. Isto se aplica apenas a filas dinâmicas permanentes que foram abertas diretamente, ou seja, não abertas por meio de uma fila modelo. Nenhuma segurança é necessária para excluir uma fila dinâmica temporária.
15. Use o perfil RACF hlq.SUBSCRIBE.topicname.
16. Use o perfil RACF hlq.PUBLISH.topicname.
17. Se na solicitação MQSUB você especificou uma fila de destino para as publicações serem enviadas, uma verificação de segurança será executada com relação a essa fila para assegurar que tenha a autoridade de colocação para essa fila.
18. Se na solicitação MQSUB, com as opções MQSO_CREATE ou MQSO_ALTER especificadas, você desejar configurar qualquer um dos campos de contexto de identidade na estrutura MQSD, também será necessário especificar a opção MQSO_SET_IDENTITY_CONTEXT e também será necessária a autoridade apropriada para o perfil de contexto da fila de destino.

z/OS *Perfis para Segurança do Tópico*

Se a segurança do tópico estiver ativa, você deverá definir perfis nas classes apropriadas e permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis.

O conceito de segurança do tópico em uma árvore de tópicos é descrito em Segurança de Publicação/Assinatura.

Se a segurança do tópico estiver ativa, você deverá executar as ações a seguir:

- Defina os perfis nas classes **MXTOPIC** ou **GMXTOPIC**.
- Permita aos grupos ou IDs de usuário necessários o acesso a esses perfis, para que possam emitir solicitações de API do IBM MQ que usam tópicos.

Os perfis para a segurança do tópico têm o formato:

```
hlq.SUBSCRIBE.topicname
hlq.PUBLISH.topicname
```

em que

- `hlq` é `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas).
- `topicname` é o nome do nó de administração do tópico na árvore de tópicos, associado ao tópico que está sendo assinado por meio de uma chamada MQSUB, ou que está sendo publicado por meio de uma chamada MQOPEN.

Um perfil prefixado pelo nome do gerenciador de filas controla o acesso a um único tópico nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o acesso a um ou mais tópicos com esse nome de tópico em todos os gerenciadores de filas dentro do grupo de filas compartilhadas. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para esse tópico nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um

perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

Assinar

Para assinar um tópico, você precisa de acesso ao tópico que está tentando assinar e à fila de destino para as publicações.

Quando você emite uma solicitação MQSUB, as verificações de segurança a seguir ocorrem:

- Se você tiver o nível apropriado de acesso para assinar esse tópico e também se a fila de destino (se especificada) estiver aberta para saída
- Se você tem o nível apropriado de acesso a essa fila de destino

Tabela 37. Nível de Acesso Necessário para Segurança do Tópico a Ser Assinado

Opção MQSUB	**RACF acesso necessário para o perfil `hlq.SUBSCRIBE.topicname` na classe MXTOPIC**
MQSO_CREATE e MQSO_ALTER	ALTER
MQSO_RESUME	READ

Tabela 38. Autoridade adicional necessária para assinar usando uma fila de destino não gerenciada

Opção MQSUB	**RACF acesso necessário para o perfil `hlq.CONTEXT.queuename` na classe MQADMIN ou MXADMIN**
MQSO_CREATE, MQSO_ALTER e MQSO_RESUME	UPDATE
	RACF acesso necessário para `hlq.queuename` perfil na classe MQQUEUE ou MXQUEUE
MQSO_CREATE e MQSO_ALTER	UPDATE
	RACF acesso necessário para `hlq.ALTERNATE.USER.alternateuserid` perfil na classe MQADMIN ou MXADMIN
MQSO_ALTERNATE_USER_AUTHORITY	UPDATE

Considerações de Filas Gerenciadas para Assinaturas

Uma verificação de segurança é executada para ver se você tem permissão para assinar o tópico. No entanto, nenhuma das verificações de segurança são executadas quando a fila gerenciada é criada ou para determinar se você tem acesso para colocar mensagens nessa fila de destino.

Não é possível fechar ou excluir uma fila gerenciada.

As filas modelo usadas são: `SYSTEM.DURABLE.MODEL.QUEUE` e `SYSTEM.NDURABLE.MODEL.QUEUE`.

As filas gerenciadas criadas a partir dessas filas modelo estão no formato `SYSTEM.MANAGED.DURABLE.A346EF00367849A0` e `SYSTEM.MANAGED.NDURABLE.A346EF0036785EA0`, em que o último qualificador é imprevisível.

Não conceda a nenhum usuário o acesso a essas filas. As filas podem ser protegidas usando perfis genéricos no formato `SYSTEM.MANAGED.DURABLE.*` e `SYSTEM.MANAGED.NDURABLE.*` sem autoridades concedidas.

As mensagens podem ser recuperadas dessas filas usando a manipulação retornada na solicitação MQSUB.

Se você emitir explicitamente uma chamada MQCLOSE para uma assinatura com a opção MQCO_REMOVE_SUB especificada e não criou a assinatura que está sendo fechada nessa manipulação, uma verificação de segurança será executada no momento do encerramento para assegurar que você tenha a autoridade correta para executar a operação.

Tabela 39. Nível de Acesso Necessário para Perfis de Segurança do Tópico para Encerramento de uma Operação de Assinatura

Opção MQCLOSE	**RACF acesso necessário para o perfil `hlq.SUBSCRIBE.topicname` na classe MXTOPIC**
MQCO_REMOVE_SUB	ALTER

Publicar

Para publicar em um tópico, é necessário acesso ao tópico e, se você estiver usando filas de alias, também à fila de alias.

Tabela 40. Nível de acesso necessário para a segurança do tópico para publicação

Opção MQOPEN ou MQPUT1	**RACF acesso necessário para o perfil `hlq.PUBLISH.topicname` na classe MXTOPIC**
MQOO_OUTPUT ou MQPUT1	UPDATE

Tabela 41. Nível de acesso necessário para abrir uma fila de alias que é resolvida para um tópico

Opção MQOPEN ou MQPUT1	**RACF acesso necessário ao perfil `hlq.queuename` na classe MQQUEUE ou MXQUEUE para a fila de alias**
MQOO_OUTPUT ou MQPUT1	UPDATE

Para obter detalhes de como a segurança do tópico opera quando uma fila de alias que resolve para um nome de tópico é aberta para publicação, consulte “Considerações de Filas de Alias que Resolvem para Tópicos para uma Operação de Publicação” na página 213.

Ao considerar filas de alias usadas para filas de destino para restrições PUT ou GET, consulte “Considerações para Filas de Alias” na página 202.

Se o nível de acesso do RACF que um aplicativo tem para um perfil de segurança do tópico for mudado, as mudanças entrarão em vigor apenas para as novas manipulações de objetos obtidas (ou seja, um novo MQSUB ou MQOPEN) para esse tópico. Essas manipulações já em existência no momento da mudança retêm seu acesso existente para o tópico. Além disso, os assinantes existentes retêm seu acesso para quaisquer assinaturas que eles já tenham feito.

Considerações de Filas de Alias que Resolvem para Tópicos para uma Operação de Publicação

Ao emitir uma chamada MQOPEN ou MQPUT1 para uma fila de alias que resolve para um tópico, o IBM MQ faz duas verificações de recursos:

- A primeira com relação ao nome da fila de alias especificado no descritor de objetos (MQOD) na chamada MQOPEN ou MQPUT1.
- A segunda com relação ao tópico para o qual a fila de alias é resolvida

Deve-se estar ciente de que esse comportamento é diferente do comportamento obtido quando as filas de alias são resolvidas para outras filas. É necessário o acesso correto a ambos os perfis para que a ação de publicação continue.

Segurança do Tópico do Sistema

Os seguintes tópicos do sistema são acessados pelo espaço de endereço do inicializador de canais.

Os IDs do usuário sob os quais isso é executado devem receber acesso RACF a essas filas, conforme mostrado em Tabela 42 na página 214

Tabela 42. Acesso Necessário para os Tópicos de SYSTEM

Tópico de SYSTEM	**O perfil**	**Inicializador de canais para enfileiramento distribuído**
SYSTEM.BROKER.ADMIN.STREAM	hlq.PUBLISH.topicname	UPDATE
SYSTEM.BROKER.ADMIN.STREAM	hlq.SUBSCRIBE.topicname	ALTER

z/OS *Perfis para Processos*

Se a segurança do processo estiver ativa, você deverá definir perfis nas classes apropriadas e permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis.

Se a segurança do processo estiver ativa, você deverá:

- Definir perfis nas classes **MQPROC** ou **GMQPROC** se estiver usando perfis em maiúsculas.
- Definir perfis nas classes **MXPROC** ou **GMXPROC** se estiver usando perfis compostos por letras maiúsculas e minúsculas.
- Permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis, para que eles possam emitir solicitações da API do IBM MQ que usam processos.

Os perfis para processos têm o formato:

```
hlq.processname
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas), e `processname` é o nome do processo que está sendo aberto.

Um perfil prefixado pelo nome do gerenciador de filas controla o acesso a uma única definição de processo nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o acesso a uma ou mais definições de processo com esse nome em todos os gerenciadores de filas dentro do grupo de filas compartilhadas. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para essa definição de processo nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

A tabela a seguir mostra o acesso necessário para abrir um processo.

Tabela 43. Níveis de Acesso para Segurança do Processo

Opção MQOPEN	**O nível de acesso do RACF requerido para hlq.processname**
MQOO_INQUIRE	READ

Por exemplo, no gerenciador de filas MQS9, o grupo RACF INQVPRC deve estar apto a consultar (`MQINQ`) em todos os processos iniciados com a letra V. As definições do RACF para isso seriam:

```
RDEFINE MQPROC MQS9.V* UACC(NONE)
PERMIT MQS9.V* CLASS(MQPROC) ID(INQVPRC) ACCESS(READ)
```

A segurança de usuário alternativo também pode estar ativa, dependendo das opções de abertura especificadas quando um objeto de definição de processo é aberto.

z/OS *Perfis para Listas de Nomes*

Se a segurança da lista de nomes estiver ativa, você definirá perfis nas classes apropriadas e conceder aos grupos ou IDs de usuário necessários o acesso a esses perfis.

Se a segurança da lista de nomes estiver ativa, você deverá:

- Defina perfis nas classes **MQNLIST** ou **GMQNLIST** se estiver usando perfis em letra maiúscula.
- Defina perfis nas classes **MXNLIST** ou **GMXNLIST** se estiver usando perfis compostos por letras maiúsculas.
- Permita aos grupos ou IDs de usuário necessários o acesso a esses perfis.

Os perfis para listas de nomes têm o formato:

```
hlq.namelistname
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas) e `namelistname` é o nome da lista de nomes que está sendo aberta.

Um perfil prefixado pelo nome do gerenciador de filas controla o acesso a uma única lista de nomes nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o acesso a uma ou mais listas de nomes com esse nome em todos os gerenciadores de filas no grupo de filas compartilhadas. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para essa lista de nomes nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

A tabela a seguir mostra o acesso necessário para abrir uma lista de nomes.

Tabela 44. Níveis de Acesso para Segurança da Lista de Nomes

Opção MQOPEN	**O nível de acesso do RACF requerido para hlq.namelistname**
MQOO_INQUIRE	READ

Por exemplo, no gerenciador de filas (ou grupo de filas compartilhadas) PQM3, o grupo DEPT571 do RACF deverá ser capaz de consultar (`MQINQ`) nestas listas de nomes:

- Todas as listas de nomes que iniciam com "DEPT571".
- PRINTER/DESTINATIONS/DEPT571
- AGENCY/REQUEST/QUEUES
- WAREHOUSE.BROADCAST

As definições do RACF para fazer isto são:

```
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)
```

A segurança de usuário alternativo pode estar ativa, dependendo das opções especificadas quando um objeto de lista de nomes é aberto.

Segurança da Lista de Nomes do Sistema

Muitas das listas de nomes do sistema são acessadas pelas partes auxiliares do IBM MQ:

- O Utilitário CSQUTIL
- Os painéis de operações e controle
- O espaço de endereço do inicializador de canais (incluindo o Daemon de publicação/assinatura enfileirada)

Os IDs de usuário sob os quais eles são executados devem receber acesso RACF a essas listas de nomes, conforme mostrado em Tabela 45 na página 216

Tabela 45. Acesso necessário para as listas de nomes SYSTEM por IBM MQ

Lista de nomes de SYSTEM	CSQUTIL	Painéis de operações e controle	Inicializador de canais para enfileiramento distribuído
SYSTEM.QPUBSUB.QUEUE.NAMELIST	-	-	READ
SYSTEM.QPUBSUB.SUBPOINT.NAMELIST	-	-	READ

z/OS *Perfis para segurança de usuário alternativo*

Se a segurança de usuário alternativo estiver ativa, você deverá definir perfis nas classes apropriadas e permitir aos grupos ou IDs de usuário necessários o acesso a esses perfis.

Para obter mais informações sobre *AlternateUserId*, consulte AlternateUserID (MQCHAR12).

Se a segurança de usuário alternativo estiver ativa, você deverá:

- Definir perfis nas classes MQADMIN ou GMQADMIN se estiver usando perfis em maiúsculas.
- Definir perfis nas classes MXADMIN ou GMXADMIN se estiver usando perfis compostos por letras maiúsculas e minúsculas.

Permita aos grupos ou IDs de usuário necessários o acesso a esses perfis, para que possam usar as opções ALTERNATE_USER_AUTHORITY quando o objeto for aberto.

Perfis para segurança de usuário alternativo podem ser especificados no nível do subsistema ou no nível do grupo de filas compartilhadas e têm o formato a seguir:

```
hlq.ALTERNATE.USER.alternateuserid
```

Em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas) e `alternateuserid` é o valor do campo *AlternateUserId* no descritor de objeto.

Um perfil prefixado pelo nome do gerenciador de filas controla o uso de um ID de usuário alternativo nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla

o uso de um ID do usuário alternativo em todos os gerenciadores de filas dentro do grupo de filas compartilhadas. Esse ID do usuário alternativo pode ser usado em qualquer gerenciador de filas dentro do grupo de filas compartilhadas por um usuário que possui o acesso correto. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para esse ID do usuário alternativo nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

A tabela a seguir mostra o acesso ao especificar uma opção de usuário alternativo.

Tabela 46. Níveis de Acesso para Segurança de Usuário Alternativo

Opção MQOPEN, MQSUB ou MQPUT1	**Nível de acesso do RACF requerido**
MQOO_ALTERNATE_USER_AUTHORITY MQSO_ALTERNATE_USER_AUTHORITY MQPMO_ALTERNATE_USER_AUTHORITY	ATUALIZAÇÃO

Além de verificações de segurança de usuário alternativo, outras verificações de segurança para segurança de fila, processo, lista de nomes e contexto também podem ser feitas. O ID de usuário alternativo, se fornecido, é usado somente para verificações de segurança em fila, definição de processo ou recursos de lista de nomes. Para verificações de segurança de usuário alternativo e contexto, o ID do usuário que está solicitando a verificação é usado. Para obter detalhes sobre como os IDs de usuário são manipulados, consulte “IDs de usuário para verificação de segurança no z/OS” na página 239. Para uma tabela de resumo que mostra as opções de abertura e as verificações de segurança necessárias quando as seguranças de fila, de contexto e de usuário alternativo estão ativas, consulte a Tabela 36 na página 208.

Um perfil de usuário alternativo concede o acesso do ID do usuário solicitante para recursos associados ao ID do usuário especificado no ID de usuário alternativo. Por exemplo, o servidor de folha de pagamento em execução sob o ID do usuário PAYSERV no gerenciador de filas QMPY processa solicitações de IDs de usuário de equipe que iniciam com PS. Para que o trabalho executado pelo servidor de folha de pagamento seja efetuado sob o ID do usuário solicitante, a autoridade do usuário alternativo é usada. O servidor de folha de pagamento sabe qual ID de usuário especificar como o ID do usuário alternativo porque os programas solicitantes geram mensagens usando a opção Enviar mensagem MQPMO_DEFAULT_CONTEXT. Consulte “IDs de usuário para verificação de segurança no z/OS” na página 239 para obter mais detalhes sobre a partir de onde os IDs de usuário alternativos são obtidos.

As definições de exemplo do RACF a seguir permitem que o programa do servidor especifique os IDs de usuário alternativo que começam com os caracteres PS:

```
RDEFINE MQADMIN QMPY.ALTERNATE.USER.PS* UACC(NONE)
PERMIT QMPY.ALTERNATE.USER.PS* CLASS(MQADMIN) ID(PAYSERV) ACCESS(UPDATE)
```

Nota:

1. Os campos *AlternateUserId* no descritor de objeto e descritor de assinatura têm 12 bytes de comprimento. Todos os 12 bytes são usados nas verificações de perfil, mas apenas os primeiros 8 bytes são usados como o ID do usuário pelo IBM MQ. Se o truncamento do ID deste usuário não for desejável, os programas de aplicativo que estão fazendo a solicitação devem converter qualquer ID de usuário alternativo de 8 bytes em algo mais apropriado.
2. Se você especificar MQOO_ALTERNATE_USER_AUTHORITY, MQSO_ALTERNATE_USER_AUTHORITY, ou MQPMO_ALTERNATE_USER_AUTHORITY e não especificar um campo *AlternateUserId* no descritor de objeto, um ID de usuário em branco será usado. Para os propósitos da verificação de

segurança do usuário alternativo, o ID do usuário usado para o qualificador *AlternateUserId* é -BLANK-. Por exemplo `RDEF MQADMIN hlq.ALTERNATE.USER.-BLANK-`.

Se o usuário for permitido acessar esse perfil, todas as verificações adicionais serão feitas com um ID de usuário em branco. Para obter detalhes de IDs de usuário em branco, consulte "IDs de Usuário em Branco e Níveis de UACC" na página 248.

A administração de IDs de usuários alternativos é mais fácil se você tiver uma convenção de nomenclatura para IDs do usuário que permite usar perfis de usuário alternativo genéricos. Se não tiver, será possível usar o recurso RACF RACVARS. Para obter detalhes sobre como usar RACVARS, veja o *z/OSSecureWay Security Server RACF Security Administrator's Guide*.

Quando uma mensagem é colocada em uma fila que foi aberta com autoridade de usuário alternativo, e o contexto da mensagem foi gerado pelo gerenciador de filas, o campo MQMD_USER_IDENTIFIER é definido com o ID do usuário alternativo.

z/OS *Perfis para Segurança de Contexto*

O IBM MQ usa perfis para controlar o acesso às informações de contexto específicas para uma determinada mensagem. O contexto está contido no descritor de mensagens (MQMD).

Usando Perfis para Segurança de Contexto

Se a segurança do contexto estiver ativa, você deverá:

- Definir um perfil na classe **MQADMIN** se estiver usando perfis em maiúsculas.
- Definir um perfil na classe **MXADMIN** se estiver usando perfis compostos por letras maiúsculas e minúsculas.

O perfil é chamado `hlq.CONTEXT.queuename` ou `hlq.CONTEXT.topicname`, em que:

hlq
Pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas).

queuename
Pode ser o nome completo da fila para a qual deseja definir o perfil de contexto, ou um perfil genérico.

TOPICNAME
Pode ser o nome completo do tópico para o qual deseja definir o perfil de contexto ou um perfil genérico.

Um perfil prefixado pelo nome do gerenciador de filas e com ** especificado como o nome da fila ou do tópico, permite o controle para a segurança de contexto em todas as filas e tópicos pertencentes a esse gerenciador de filas Isso pode ser substituído em uma fila ou tópico individual definindo um perfil específico para o contexto nessa fila ou tópico.

Um perfil prefixado pelo nome do grupo de filas compartilhadas e com ** especificado como o nome da fila ou do tópico, permite o controle de contexto em todas as filas e tópicos pertencentes aos gerenciadores de filas no grupo de filas compartilhadas. Isso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para o contexto nesse gerenciador de filas, especificando um perfil prefixado pelo nome do gerenciador de filas. Ele também pode ser substituído em uma fila ou tópico individual especificando um perfil sufixado com o nome da fila ou tópico.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

Você deve conceder aos grupos ou IDs de usuário necessários o acesso a esse perfil. A tabela a seguir mostra o nível de acesso necessário, dependendo da especificação das opções de contexto quando a fila é aberta.

Tabela 47. Níveis de Acesso para Segurança de Contexto	
Opção MQOPEN ou MQPUT1	**RACF nível de acesso necessário para hlq.CONTEXT.queuename ou hlq.CONTEXT.topicname**
MQPMO_NO_CONTEXT	Nenhuma verificação de segurança do contexto
MQPMO_DEFAULT_CONTEXT	Nenhuma verificação de segurança do contexto
MQOO_SAVE_ALL_CONTEXT	Nenhuma verificação de segurança do contexto
MQOO_PASS_IDENTITY_CONTEXT MQPMO_PASS_IDENTITY_CONTEXT	READ
MQOO_PASS_ALL_CONTEXT MQPMO_PASS_ALL_CONTEXT	READ
MQOO_SET_IDENTITY_CONTEXT MQPMO_SET_IDENTITY_CONTEXT	UPDATE
MQOO_SET_ALL_CONTEXT MQPMO_SET_ALL_CONTEXT	CONTROL
MQOO_OUTPUT ou MQPUT1(USAGE(XMITQ))	CONTROL
Opção MQSUB	
MQSO_SET_IDENTITY_CONTEXT **(Nota 2)**	UPDATE

Nota:

1. Os IDs de usuário usados para enfileiramento distribuído requerem acesso CONTROL para `hlq.CONTEXT.queuename` para colocar mensagens na fila de destino. Consulte "IDs de Usuário Usados pelo Inicializador de Canais" na página 243 para obter informações sobre os IDs de usuário usados.
2. Se na solicitação MQSUB, com as opções MQSO_CREATE ou MQSO_ALTER especificadas, você desejar configurar qualquer um dos campos de contexto de identidade na estrutura MQSD, será necessário especificar a opção MQSO_SET_IDENTITY_CONTEXT. Também é necessária a autoridade apropriada para o perfil de contexto para a fila de destino.

Se você colocar comandos na fila de entrada de comandos do sistema, use a opção de colocação de mensagem do contexto padrão para associar o ID de usuário correto ao comando.

Por exemplo, o programa de utilitário CSQUTIL fornecido pelo IBM MQ pode ser usado para transferir e recarregar mensagens em filas. Quando as mensagens transferidas são restauradas para uma fila, o utilitário CSQUTIL usa a opção MQOO_SET_ALL_CONTEXT para retornar as mensagens para seu estado original. Além da segurança da fila requerida por essa opção de abertura, a autoridade de contexto também é requerida. Por exemplo, se essa autoridade for requerida pelo grupo BACKGRP no gerenciador de filas MQS1, isso seria definido por:

```
RDEFINE MQADMIN MQS1.CONTEXT.** UACC(NONE)
PERMIT MQS1.CONTEXT.** CLASS(MQADMIN) ID(BACKGRP) ACCESS(CONTROL)
```

Dependendo das opções especificadas e dos tipos de segurança executados, outros tipos de verificações de segurança também podem ocorrer quando a fila é aberta. Eles incluem segurança da fila (consulte "Perfis para Segurança de Fila" na página 200) e segurança de usuário alternativo (consulte "Perfis para segurança de usuário alternativo" na página 216). Para uma tabela de resumo que mostra as opções

de abertura e as verificações de segurança necessárias quando as seguranças de fila, de contexto e de usuário alternativo estão ativas, consulte a Tabela 36 na página 208.

Segurança de Contexto da Fila do Sistema

Muitas das filas do sistema são acessadas pelas partes auxiliares do IBM MQ, por exemplo, o espaço de endereço do inicializador de canais V 9.1.0 e o servidor mqweb usado pelo IBM MQ Console e REST API.

Os IDs de usuário sob os quais eles são executados devem receber acesso do RACF a essas filas, conforme mostrado na Tabela 48 na página 220.

Tabela 48. Acesso Necessário para as Filas de SYSTEM para Operações de Contexto

Fila de SYSTEM	**Inicializador de canais para enfileiramento distribuído**	**servidor 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 *Perfis para Segurança de Comando*

Para ativar a verificação de segurança para comandos, inclua perfis na classe MQCMDS. Os nomes do perfil são baseados nos comandos MQSC, mas controlam ambos os comandos, MQSC e PCF. Perfis podem ser aplicados a um gerenciador de filas ou grupo de filas compartilhadas.

Se desejar a verificação de segurança para comandos (portanto, você não definiu o perfil do comutador de segurança de comando hlq.NO.CMD.CHECKS) você deve incluir perfis para a classe MQCMDS.

Os mesmos perfis de segurança controlam os comandos MQSC e PCF. Os nomes dos perfis do RACF para a verificação de segurança de comando são baseados nos próprios nomes de comandos MQSC. Esses perfis têm o formato:

```
hlq.verb.pkw
```

Em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas), `verb` é a parte do verbo do nome do comando, por exemplo, ALTER, e `pkw` é o tipo de objeto, por exemplo, QLOCAL para uma fila local.

Portanto, o nome do perfil para o comando ALTER QLOCAL no subsistema CSQ1 é:

```
CSQ1.ALTER.QLOCAL
```

É possível usar perfis genéricos para proteger conjuntos de comandos para que você tenha menos perfis para manter e, portanto, menos listas de acesso. Considere criar um perfil genérico que se aplique a todos os comandos não protegidos por um perfil mais específico. Defina este perfil com UACC(NONE) e conceda acesso ALTER apenas para os grupos do RACF que contêm administradores. Em seguida, você pode criar um perfil genérico aplicável a todos os comandos DISPLAY e conceder acesso amplo a ele. Entre esses extremos, é possível identificar grupos de usuários que precisam de acesso a determinados conjuntos de comandos; neste caso, é possível criar perfis para esses conjuntos e conceder acesso aos grupos do RACF que representam essas classes do usuário. Evite fornecer acessos de usuários a

comandos que eles não requerem: Aplique o princípio de menos privilégio, para que os usuários tenham acesso somente aos comandos que são necessários para suas tarefas.

Um perfil prefixado pelo nome do gerenciador de filas controla o uso do comando nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o uso do comando em todos os gerenciadores de filas dentro do grupo de filas compartilhadas. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para esse comando nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

Configurando perfis de comandos no nível do gerenciador de filas, um usuário pode ser restringido de emitir comandos em um gerenciador de filas específico. Como alternativa, é possível definir um perfil para um grupo de filas compartilhadas para cada verbo de comando e todas as verificações de segurança são efetuadas em relação a esse perfil em vez de gerenciadores de filas individuais.

Se a segurança do subsistema e a segurança do grupo de filas compartilhadas estiverem ativas e um perfil local não for localizado, uma verificação de segurança do comando será executada para ver se o usuário tem acesso a um perfil do grupo de filas compartilhadas.

Se você usar o atributo CMDSCOPE para rotear um comando para outros gerenciadores de filas em um grupo de filas compartilhadas, a segurança será verificada em cada gerenciador de filas no qual o comando é executado, mas não necessariamente no gerenciador de filas no qual o comando é inserido.

O Tabela 49 na página 221 mostra para cada comando MQSC do IBM MQ os perfis necessários para a verificação da segurança de comando e o nível de acesso correspondente para cada perfil na classe MQCMDS.

Tabela 50 na página 226 mostra para cada comando PCF do IBM MQ os perfis necessários para a verificação da segurança de comando e o nível de acesso correspondente para cada perfil na classe de MQCMDS.

Tabela 49. Comandos MQSC, Perfis e seus Níveis de Acesso

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
ALTER AUTHINFO	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
ALTER BUFFPOOL	hlq.ALTER.BUFFPOOL	ALTER	Sem verificação	-
ALTER CFSTRUCT	hlq.ALTER.CFSTRUCT	ALTER	Sem verificação	-
ALTER CHANNEL	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
ALTER NAMELIST	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
ALTER PROCESS	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
ALTER PSID	hlq.ALTER.PSID	ALTER	Sem verificação	-
ALTER QALIAS	hlq.ALTER.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
ALTER QLOCAL	hlq.ALTER.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
ALTER QMGR	hlq.ALTER.QMGR	ALTER	Sem verificação	-
ALTER QMODEL	hlq.ALTER.QMODEL	ALTER	hlq.QUEUE.queue	ALTER

Tabela 49. Comandos MQSC, Perfis e seus Níveis de Acesso (continuação)

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
ALTER QREMOTE	hlq.ALTER.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
ALTER SECURITY	hlq.ALTER.SECURITY	ALTER	Sem verificação	-
ALTER SMDS	hlq.ALTER.SMDS	ALTER	Sem verificação	-
ALTER STGCLASS	hlq.ALTER.STGCLASS	ALTER	Sem verificação	-
ALTER SUB	hlq.ALTER.SUB	ALTER	Sem verificação	-
ALTER TOPIC	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
ALTER TRACE	hlq.ALTER.TRACE	ALTER	Sem verificação	-
LOG DE ARCHIVE	hlq.ARCHIVE.LOG	CONTROLE	Sem verificação	-
BACKUP CFSTRUCT	hlq.BACKUP.CFSTRUCT	CONTROLE	Sem verificação	-
CLEAR QLOCAL	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
CLEAR TOPICSTR “3” na página 226	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER
DEFINE AUTHINFO	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
DEFINE BUFFPOOL	hlq.DEFINE.BUFFPOOL	ALTER	Sem verificação	-
DEFINE CFSTRUCT	hlq.DEFINE.CFSTRUCT	ALTER	Sem verificação	-
DEFINE CHANNEL	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DEFINE LOG	hlq.DEFINE.LOG	ALTER	Sem verificação	-
DEFINE MAXSMSGS	hlq.DEFINE.MAXSMSGS	ALTER	Sem verificação	-
DEFINE NAMELIST	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DEFINE PROCESS	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DEFINE PSID	hlq.DEFINE.PSID	ALTER	Sem verificação	-
DEFINE QALIAS	hlq.DEFINE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QLOCAL	hlq.DEFINE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QMODEL	hlq.DEFINE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DEFINE QREMOTE	hlq.DEFINE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DEFINE STGCLASS	hlq.DEFINE.STGCLASS	ALTER	Sem verificação	-
DEFINE SUB	hlq.DEFINE.SUB	ALTER	Sem verificação	-
DEFINE TOPIC	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
DELETE AUTHINFO	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
DELETE BUFFPOOL	hlq.DELETE.BUFFPOOL	ALTER	Sem verificação	-
DELETE CFSTRUCT	hlq.DELETE.CFSTRUCT	ALTER	Sem verificação	-

Tabela 49. Comandos MQSC, Perfis e seus Níveis de Acesso (continuação)

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
DELETE CHANNEL	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
DELETE NAMELIST	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
DELETE PROCESS	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
DELETE PSID	hlq.DELETE.PSID	ALTER	Sem verificação	-
DELETE QALIAS	hlq.DELETE.QALIAS	ALTER	hlq.QUEUE.queue	ALTER
DELETE QLOCAL	hlq.DELETE.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
DELETE QMODEL	hlq.DELETE.QMODEL	ALTER	hlq.QUEUE.queue	ALTER
DELETE QREMOTE	hlq.DELETE.QREMOTE	ALTER	hlq.QUEUE.queue	ALTER
DELETE STGCLASS	hlq.DELETE.STGCLASS	ALTER	Sem verificação	-
DELETE SUB	hlq.DELETE.SUB	ALTER	Sem verificação	-
DELETE TOPIC	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
DISPLAY ARCHIVE “1” na página 225	hlq.DISPLAY.ARCHIVE	READ	Sem verificação	-
DISPLAY AUTHINFO	hlq.DISPLAY.AUTHINFO	READ	Sem verificação	-
DISPLAY CFSTATUS	hlq.DISPLAY.CFSTATUS	READ	Sem verificação	-
DISPLAY CFSTRUCT	hlq.DISPLAY.CFSTRUCT	READ	Sem verificação	-
DISPLAY CHANNEL	hlq.DISPLAY.CHANNEL	READ	Sem verificação	-
DISPLAY CHINIT	hlq.DISPLAY.CHINIT	READ	Sem verificação	-
DISPLAY CHLAUTH	hlq.DISPLAY.CHLAUTH	READ	Sem verificação	-
DISPLAY CHSTATUS	hlq.DISPLAY.CHSTATUS	READ	Sem verificação	-
EXIBIR CLUSQMGR	hlq.DISPLAY.CLUSQMGR	READ	Sem verificação	-
DISPLAY CMDSERV	hlq.DISPLAY.CMDSERV	READ	Sem verificação	-
DISPLAY CONN “1” na página 225	hlq.DISPLAY.CONN	READ	Sem verificação	-
DISPLAY GROUP	hlq.DISPLAY.GROUP	READ	Sem verificação	-
DISPLAY LOG “1” na página 225	hlq.DISPLAY.LOG	READ	Sem verificação	-
DISPLAY MAXSMSGS	hlq.DISPLAY.MAXSMSGS	READ	Sem verificação	-
DISPLAY NAMELIST	hlq.DISPLAY.NAMELIST	READ	Sem verificação	-
DISPLAY PROCESS	hlq.DISPLAY.PROCESS	READ	Sem verificação	-
DISPLAY PUBSUB	hlq.DISPLAY.PUBSUB	READ	Sem verificação	-
DISPLAY QALIAS	hlq.DISPLAY.QALIAS	READ	Sem verificação	-
DISPLAY QCLUSTER	hlq.DISPLAY.QCLUSTER	READ	Sem verificação	-

Tabela 49. Comandos MQSC, Perfis e seus Níveis de Acesso (continuação)

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
DISPLAY QLOCAL	hlq.DISPLAY.QLOCAL	READ	Sem verificação	-
DISPLAY QMGR	hlq.DISPLAY.QMGR	READ	Sem verificação	-
DISPLAY QMODEL	hlq.DISPLAY.QMODEL	READ	Sem verificação	-
DISPLAY QREMOTE	hlq.DISPLAY.QREMOTE	READ	Sem verificação	-
DISPLAY QSTATUS	hlq.DISPLAY.QSTATUS	READ	Sem verificação	-
DISPLAY QUEUE	hlq.DISPLAY.QUEUE	READ	Sem verificação	-
DISPLAY SBSTATUS	hlq.DISPLAY.SBSTATUS	READ	Sem verificação	-
DISPLAY SMDS	hlq.DISPLAY.SMDS	READ	Sem verificação	-
DISPLAY SMDSCONN	hlq.DISPLAY.SMDSCONN	READ	Sem verificação	-
DISPLAY SUB	hlq.DISPLAY.SUB	READ	Sem verificação	-
DISPLAY SECURITY	hlq.DISPLAY.SECURITY	READ	Sem verificação	-
DISPLAY STGCLASS	hlq.DISPLAY.STGCLASS	READ	Sem verificação	-
DISPLAY SYSTEM “1” na página 225	hlq.DISPLAY.SYSTEM	READ	Sem verificação	-
DISPLAY THREAD	hlq.DISPLAY.THREAD	READ	Sem verificação	-
DISPLAY TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	Sem verificação	-
DISPLAY TOPIC	hlq.DISPLAY.TOPIC	READ	Sem verificação	-
DISPLAY TPSTATUS	hlq.DISPLAY.TPSTATUS	READ	Sem verificação	-
DISPLAY TRACE	hlq.DISPLAY.TRACE	READ	Sem verificação	-
DISPLAY USAGE “1” na página 225	hlq.DISPLAY.USAGE	READ	Sem verificação	-
MOVE QLOCAL	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
PING CHANNEL	hlq.PING.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
RECOVER conjunto de dados de autoinicialização	hlq.RECOVER.BSDS	CONTROLE	Sem verificação	-
RECOVER CFSTRUCT	hlq.RECOVER.CFSTRUCT	CONTROLE	Sem verificação	-
REFRESH CLUSTER	hlq.REFRESH.CLUSTER	ALTER	Sem verificação	-
REFRESH QMGR	hlq.REFRESH.QMGR	ALTER	Sem verificação	-
REFRESH SECURITY	hlq.REFRESH.SECURITY	ALTER	Sem verificação	-
RESET CFSTRUCT	hlq.RESET.CFSTRUCT	CONTROLE	Sem verificação	-
RESET CHANNEL	hlq.RESET.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE

Tabela 49. Comandos MQSC, Perfis e seus Níveis de Acesso (continuação)

Comando:	Perfil de comando para MQCMDS	Nível de acesso para MQCMDS	Perfil de Recurso do Comando para MQADMIN ou MXADMIN	Nível de acesso para MQADMIN ou MXADMIN
RESET CLUSTER	hlq.RESET.CLUSTER	CONTROLE	Sem verificação	-
RESET QMGR	hlq.RESET.QMGR	CONTROLE	Sem verificação	-
RESET QSTATS	hlq.RESET.QSTATS	CONTROLE	hlq.QUEUE.queue	CONTROLE
RESET SMDS	hlq.RESET.SMDS	CONTROLE	Sem verificação	-
RESET TPIPE	hlq.RESET.TPIPE	CONTROLE	Sem verificação	-
RESOLVE CHANNEL	hlq.RESOLVE.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
RESOLVE INDOUBT	hlq.RESOLVE.INDOUBT	CONTROLE	Sem verificação	-
RESUME QMGR	hlq.RESUME.QMGR	CONTROLE	Sem verificação	-
RVERIFY SECURITY	hlq.RVERIFY.SECURITY	ALTER	Sem verificação	-
SET ARCHIVE	hlq.SET.ARCHIVE	CONTROLE	Sem verificação	-
SET CHLAUTH	hlq.SET.CHLAUTH	CONTROLE	Sem verificação	-
SET LOG	hlq.SET.LOG	CONTROLE	Sem verificação	-
SET SYSTEM	hlq.SET.SYSTEM	CONTROLE	Sem verificação	-
START CHANNEL	hlq.START.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
START CHINIT “4” na página 226	hlq.START.CHINIT	CONTROLE	Sem verificação	-
START CMDSERV	hlq.START.CMDSERV	CONTROLE	Sem verificação	-
START LISTENER	hlq.START.LISTENER	CONTROLE	Sem verificação	-
START QMGR	Nenhum “2” na página 226	-	-	-
START SMDSCONN	hlq.START.SMDSCONN	CONTROLE	Sem verificação	-
START TRACE	hlq.START.TRACE	CONTROLE	Sem verificação	-
STOP CHANNEL	hlq.STOP.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
STOP CHINIT	hlq.STOP.CHINIT	CONTROLE	Sem verificação	-
STOP CMDSERV	hlq.STOP.CMDSERV	CONTROLE	Sem verificação	-
STOP LISTENER	hlq.STOP.LISTENER	CONTROLE	Sem verificação	-
STOP QMGR	hlq.STOP.QMGR	CONTROLE	Sem verificação	-
STOP SMDSCONN	hlq.STOP.SMDSCONN	CONTROLE	Sem verificação	-
STOP TRACE	hlq.STOP.TRACE	CONTROLE	Sem verificação	-
SUSPEND QMGR	hlq.SUSPEND.QMGR	CONTROLE	Sem verificação	-

Notes:

1. Estes comandos podem ser emitidos internamente pelo gerenciador de filas; nenhuma autoridade é verificada nestes casos.

2. O IBM MQ não verifica a autoridade do usuário que emite o comando START QMGR. No entanto, é possível usar o RACF ou os recursos de segurança alternativos para controlar o acesso ao comando START xxxxMSTR que é emitido como resultado do comando START QMGR. Isso é feito controlando o acesso ao perfil de MVS.START.STC.xxxxMSTR na classe dos comandos do operador do RACF (OPERCMDS). Para obter detalhes deste procedimento, veja o *z/OS SecureWay Security Server RACF Security Administrator's Guide*. Se você usar esta técnica e um usuário não autorizado tentar iniciar o gerenciador de filas, ele finalizará com um código de razão igual a 00F30216.
3. O recurso **hlq.TOPIC.topic** refere-se ao objeto do tópico derivado do TOPICSTR. Para obter mais detalhes, consulte "Segurança de Publicação/Assinatura" na página 470
4. Nas liberações anteriores à IBM MQ for z/OS V6, a verificação de segurança era para o MVS.START.STC.CSQ1CHIN. No IBM MQ for z/OS V6 e posterior, o nome do recurso possui um qualificador JOBNAME adicional anexado a ele. Isto pode causar problemas ao iniciar o inicializador de canais.

   Para resolver o problema, substitua MVS.START.STC. *ssid* CHIN por um perfil para um recurso chamado MVS.START.STC. *ssid* CHIN **.*** ou MVS.START.STC *ssid* CHIN. *ssid* CHIN, em que *ssid* é o ID de subsistema para o gerenciador de filas. Isso requer a autoridade UPDATE do RACF. Para obter mais detalhes, consulte o z/OS documentação do produto para *Planejamento de operação, Comandos MVS, RACF Autoridades de acessos e nomes de recurso*.

   O START para o *ssid* MSTR não inclui o parâmetro JOBNAME=. Para consistência, talvez você deseje atualizar o perfil para MVS.START.STC.ssidMSTR para MVS.START.STC.ssidMSTR.*.

Tabela 50. Comandos PCF, Perfis e seus Níveis de Acesso

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
Efetuar Backup de Estrutura de CF	hlq.BACKUP.CFSTRUCT	CONTROLE	Sem verificação	-
Change Authentication Information Object	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Alterar Estrutura de CF	hlq.ALTER.CFSTRUCT	ALTER	Sem verificação	-
Alterar Canal	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Alterar Lista de Nomes	hlq.ALTER.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Processo de Mudança	hlq.ALTER.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Alterar a Fila	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Alterar Gerenciador de Filas	hlq.ALTER.QMGR	ALTER	Sem verificação	-
Change Security	hlq.ALTER.SECURITY	ALTER	Sem verificação	-
Alterar SMDS	hlq.ALTER.SMDS	ALTER	Sem verificação	-
Alterar classe de armazenamento	hlq.ALTER.STGCLASS	ALTER	Sem verificação	-
Change Subscription	hlq.ALTER.SUB	ALTER	Sem verificação	-
Alterar tópico	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Limpar Fila	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Limpar sequência de tópicos "1" na página 230	hlq.CLEAR.TOPICSTR	ALTER	hlq.TOPIC.topic	ALTER

Tabela 50. Comandos PCF, Perfis e seus Níveis de Acesso (continuação)

Comando:	Perfil de comando para MQCMDS	Nível de acesso para MQCMDS	Perfil de Recurso do Comando para MQADMIN ou MXADMIN	Nível de acesso para MQADMIN ou MXADMIN
Copy Authentication Information Object	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Copiar Estrutura de CF	hlq.DEFINE.CFSTRUCT	ALTER	Sem verificação	-
Copiar Canal	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Copiar Lista de Nomes	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Copiar processo	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Copiar Fila	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Copiar Assinatura	hlq.DEFINE.SUB	ALTER	Sem verificação	-
Copiar Classe de Armazenamento	hlq.DEFINE.STGCLASS	ALTER	Sem verificação	-
Copiar Tópico	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Criar Objeto de Informações sobre Autenticação	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Criar Estrutura de CF	hlq.DEFINE.CFSTRUCT	ALTER	Sem verificação	-
Criar Canal	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Criar Lista de Nomes	hlq.DEFINE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Criar processo	hlq.DEFINE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Criar fila	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Criar Classe de Armazenamento	hlq.DEFINE.STGCLASS	ALTER	Sem verificação	-
Criar assinatura	hlq.DEFINE.SUB	ALTER	Sem verificação	-
Criar tópico	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Delete Authentication Information Object	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Excluir Estrutura de CF	hlq.DELETE.CFSTRUCT	ALTER	Sem verificação	-
Excluir Canal	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Delete Namelist	hlq.DELETE.NAMELIST	ALTER	hlq.NAMELIST.namelist	ALTER
Excluir Processo	hlq.DELETE.PROCESS	ALTER	hlq.PROCESS.process	ALTER
Excluir fila	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Excluir classe de armazenamento	hlq.DELETE.STGCLASS	ALTER	Sem verificação	-
Excluir assinatura	hlq.DELETE.SUB	ALTER	Sem verificação	-
Excluir Tópico	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Consultar Archive	hlq.DISPLAY.ARCHIVE	READ	Sem verificação	-
Investigar Objeto de Informação de Autenticação	hlq.DISPLAY.AUTHINFO	READ	Sem verificação	-

Tabela 50. Comandos PCF, Perfis e seus Níveis de Acesso (continuação)

Comando:	Perfil de comando para MQCMDS	Nível de acesso para MQCMDS	Perfil de Recurso do Comando para MQADMIN ou MXADMIN	Nível de acesso para MQADMIN ou MXADMIN
Investigar Nomes de Objeto de Informações sobre Autenticação	hlq.DISPLAY.AUTHINFO	READ	Sem verificação	-
Consultar Estrutura de CF	hlq.DISPLAY.CFSTRUCT	READ	Sem verificação	-
Consultar Nomes de Estrutura de CF	hlq.DISPLAY.CFSTRUCT	READ	Sem verificação	-
Consultar Status da Estrutura de CF	hlq.DISPLAY.CFSTATUS	READ	Sem verificação	-
Consultar Canal	hlq.DISPLAY.CHANNEL	READ	Sem verificação	-
Solicitar Registros de Autenticação de Canal	hlq.DISPLAY.CHLAUTH	READ	Sem verificação	-
Inquire Channel Initiator	hlq.DISPLAY.CHINIT	READ	Sem verificação	-
Consultar Nomes de Canal	hlq.DISPLAY.CHANNEL	READ	Sem verificação	-
Consultar Status do Canal	hlq.DISPLAY.CHSTATUS	READ	Sem verificação	-
Consultar Gerenciador de Filas de Clusters	hlq.DISPLAY.CLUSQMGR	READ	Sem verificação	-
Consultar Conexão	hlq.DISPLAY.CONNPCF	READ	Sem verificação	-
Investigar Grupo	hlq.DISPLAY.GROUP	READ	Sem verificação	-
Pesquisar Log	hlq.DISPLAY.LOG	READ	Sem verificação	-
Consultar Lista de Nomes	hlq.DISPLAY.NAMELIST	READ	Sem verificação	-
Consultar Nomes da Lista de Nomes	hlq.DISPLAY.NAMELIST	READ	Sem verificação	-
Consultar Processo	hlq.DISPLAY.PROCESS	READ	Sem verificação	-
Consultar Nomes de Processo	hlq.DISPLAY.PROCESS	READ	Sem verificação	-
Investigar Status da Pub/Ass	hlq.DISPLAY.PUBSUB	READ	Sem verificação	-
Consultar Fila	hlq.DISPLAY.QUEUE	READ	Sem verificação	-
Consultar Gerenciador de Filas	hlq.DISPLAY.QMGR	READ	Sem verificação	-
Consultar Nomes de Fila	hlq.DISPLAY.QUEUE	READ	Sem verificação	-
Consultar Status da Fila	hlq.DISPLAY.QSTATUS	READ	Sem verificação	-
Consultar Segurança	hlq.DISPLAY.SECURITY	READ	Sem verificação	-
Consultar SMDS	hlq.DISPLAY.SMDS	READ	Sem verificação	-
Investigar SMDSCONN	hlq.DISPLAY.SMDSCONN	READ	Sem verificação	-

Tabela 50. Comandos PCF, Perfis e seus Níveis de Acesso (continuação)

Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
Consultar Classe de Armazenamento	hlq.DISPLAY.STGCLASS	READ	Sem verificação	-
Consultar Nomes de Classe de Armazenamento	hlq.DISPLAY.STGCLASS	READ	Sem verificação	-
Consultar Assinatura	hlq.INQUIRE.SUB	READ	Sem verificação	-
Inquire Subscription Status	hlq.INQUIRE.SBSTATUS	READ	Sem verificação	-
Consultar Sistema	hlq.DISPLAY.SYSTEM	READ	Sem verificação	-
Consultar Tópico	hlq.DISPLAY.TOPIC	READ	Sem verificação	-
Inquire Topic Names	hlq.DISPLAY.TOPIC	READ	Sem verificação	-
Inquire Topic Status	hlq.DISPLAY.TPSTATUS	READ	Sem verificação	-
Consultar Uso	hlq.DISPLAY.USAGE	READ	Sem verificação	-
Mover Fila	hlq.MOVE.QLOCAL	ALTER	hlq.QUEUE.from-queue hlq.QUEUE.to-queue	ALTER
Executar ping no Canal	hlq.PING.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Recuperar Estrutura	hlq.RECOVER.CFSTRUCT	CONTROLE	Sem verificação	-
Refresh Cluster	hlq.REFRESH.CLUSTER	ALTER	Sem verificação	-
Atualizar Gerenciador de Filas	hlq.REFRESH.QMGR	ALTER	Sem verificação	-
Atualizar segurança	hlq.REFRESH.SECURITY	ALTER	Sem verificação	-
Reconfigurar Estrutura de CF	hlq.RESET.CFSTRUCT	CONTROLE	Sem verificação	-
Redefinir Canal	hlq.RESET.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Reconfigurar Cluster	hlq.RESET.CLUSTER	CONTROLE	Sem verificação	-
Reconfigurar Gerenciador de Filas	hlq.RESET.QMGR	CONTROLE	Sem verificação	-
Reconfigurar as Estatísticas de Fila	hlq.RESET.QSTATS	CONTROLE	hlq.QUEUE.queue	CONTROLE
Reconfigurar SMDS	hlq.RESET.SMDS	CONTROLE	Sem verificação	-
Resolver Canal	hlq.RESOLVE.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Retomar Gerenciador de Filas	hlq.RESUME.QMGR	CONTROLE	Sem verificação	-
Retomar Cluster de Gerenciador de Filas	hlq.RESUME.QMGR	CONTROLE	Sem verificação	-
Reverificar segurança	hlq.RVERIFY.SECURITY	ALTER	Sem verificação	-
Definir Archive	hlq.SET.ARCHIVE	CONTROLE	Sem verificação	-
Configurar Registro de Autenticação de Canal	hlq.SET.CHLAUTH	CONTROLE	Sem verificação	-

Tabela 50. Comandos PCF, Perfis e seus Níveis de Acesso (continuação)				
Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
Configurar Log	hlq.SET.LOG	CONTROLE	Sem verificação	-
Set System	hlq.SET.SYSTEM	CONTROLE	Sem verificação	-
Iniciar o Canal	hlq.START.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Iniciar Iniciador de Canal	hlq.START.CHINIT	CONTROLE	Sem verificação	-
Iniciar Ouvinte de Canal	hlq.START.LISTENER	CONTROLE	Sem verificação	-
Iniciar Conexão de SMDS	hlq.START.SMDSCONN	CONTROLE	Sem verificação	-
Parar Canal	hlq.STOP.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Parar Inicializador de Canais	hlq.STOP.CHINIT	CONTROLE	Sem verificação	-
Parar Listener do Canal	hlq.STOP.LISTENER	CONTROLE	Sem verificação	-
Parar Conexão de SMDS	hlq.STOP.SMDSCONN	CONTROLE	Sem verificação	-
Suspender Gerenciador de Filas	hlq.SUSPEND.QMGR	CONTROLE	Sem verificação	-
Suspender Cluster de Gerenciador de Filas	hlq.SUSPEND.QMGR	CONTROLE	Sem verificação	-

Notes:

1. O recurso **`hlq.TOPIC.topic`** refere-se ao objeto do tópico derivado do TOPICSTR. Para obter mais detalhes, consulte "Segurança de Publicação/Assinatura" na página 470

V 9.1.0 Veja "IBM MQ Console - perfis de segurança de comando necessários" na página 230 para obter detalhes dos perfis PCF necessários do IBM MQ, ao usar o IBM MQ Console.

z/OS V 9.1.0 *IBM MQ Console - perfis de segurança de comando necessários*

As operações executadas no IBM MQ Console por um usuário na função `MQWebAdmin` ou `MQWebAdminRO` ocorrem sob o contexto de segurança do ID do usuário da tarefa iniciada do servidor mqweb. Se você deseja usar o IBM MQ Console, o ID do usuário da tarefa iniciada do servidor mqweb precisa de autorização para emitir determinados comandos PCF.

A Tabela 51 na página 230 mostra, para cada comando PCF do IBM MQ, os perfis de segurança de comando necessários e o nível de acesso correspondente para cada perfil na classe MQCMDS necessária para o IBM MQ Console.

Tabela 51. Comandos PCF, perfis e seus níveis de acesso do IBM MQ Console				
Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
Change Authentication Information Object	hlq.ALTER.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Alterar Canal	hlq.ALTER.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Alterar a Fila	hlq.ALTER.QUEUE	ALTER	hlq.QUEUE.queue	ALTER

Tabela 51. Comandos PCF, perfis e seus níveis de acesso do IBM MQ Console (continuação)

Comando:	Perfil de comando para MQCMDS	Nível de acesso para MQCMDS	Perfil de Recurso do Comando para MQADMIN ou MXADMIN	Nível de acesso para MQADMIN ou MXADMIN
Alterar Gerenciador de Filas	hlq.ALTER.QMGR	ALTER	Sem verificação	-
Alterar tópico	hlq.ALTER.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Limpar Fila	hlq.CLEAR.QLOCAL	ALTER	hlq.QUEUE.queue	ALTER
Criar Objeto de Informações sobre Autenticação	hlq.DEFINE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Criar Canal	hlq.DEFINE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Criar fila	hlq.DEFINE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Criar assinatura	hlq.DEFINE.SUB	ALTER	Sem verificação	-
Criar tópico	hlq.DEFINE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Delete Authentication Information Object	hlq.DELETE.AUTHINFO	ALTER	hlq.AUTHINFO.resourcename	ALTER
Excluir Canal	hlq.DELETE.CHANNEL	ALTER	hlq.CHANNEL.channel	ALTER
Excluir fila	hlq.DELETE.QUEUE	ALTER	hlq.QUEUE.queue	ALTER
Excluir assinatura	hlq.DELETE.SUB	ALTER	Sem verificação	-
Excluir Tópico	hlq.DELETE.TOPIC	ALTER	hlq.TOPIC.topic	ALTER
Investigar Objeto de Informação de Autenticação	hlq.DISPLAY.AUTHINFO	READ	Sem verificação	-
Investigar Nomes de Objeto de Informações sobre Autenticação	hlq.DISPLAY.AUTHINFO	READ	Sem verificação	-
Consultar Canal	hlq.DISPLAY.CHANNEL	READ	Sem verificação	-
Solicitar Registros de Autenticação de Canal	hlq.DISPLAY.CHLAUTH	READ	Sem verificação	-
Inquire Channel Initiator	hlq.DISPLAY.CHINIT	READ	Sem verificação	-
Consultar Nomes de Canal	hlq.DISPLAY.CHANNEL	READ	Sem verificação	-
Consultar Status do Canal	hlq.DISPLAY.CHSTATUS	READ	Sem verificação	-
Consultar Fila	hlq.DISPLAY.QUEUE	READ	Sem verificação	-
Consultar Gerenciador de Filas	hlq.DISPLAY.QMGR	READ	Sem verificação	-
Consultar Nomes de Fila	hlq.DISPLAY.QUEUE	READ	Sem verificação	-
Consultar Status da Fila	hlq.DISPLAY.QSTATUS	READ	Sem verificação	-
Consultar Assinatura	hlq.INQUIRE.SUB	READ	Sem verificação	-
Inquire Subscription Status	hlq.INQUIRE.SBSTATUS	READ	Sem verificação	-

Tabela 51. Comandos PCF, perfis e seus níveis de acesso do IBM MQ Console (continuação)				
Comando:	**Perfil de comando para MQCMDS**	**Nível de acesso para MQCMDS**	**Perfil de Recurso do Comando para MQADMIN ou MXADMIN**	**Nível de acesso para MQADMIN ou MXADMIN**
Consultar Tópico	hlq.DISPLAY.TOPIC	READ	Sem verificação	-
Inquire Topic Names	hlq.DISPLAY.TOPIC	READ	Sem verificação	-
Inquire Topic Status	hlq.DISPLAY.TPSTATUS	READ	Sem verificação	-
Executar ping no Canal	hlq.PING.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Refresh Cluster	hlq.REFRESH.CLUSTER	ALTER	Sem verificação	-
Atualizar segurança	hlq.REFRESH.SECURITY	ALTER	Sem verificação	-
Redefinir Canal	hlq.RESET.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Resolver Canal	hlq.RESOLVE.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Configurar Registro de Autenticação de Canal	hlq.SET.CHLAUTH	CONTROLE	Sem verificação	-
Iniciar o Canal	hlq.START.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE
Parar Canal	hlq.STOP.CHANNEL	CONTROLE	hlq.CHANNEL.channel	CONTROLE

z/OS *Perfis para segurança do recurso de comando*

Se você não tiver definido o perfil do comutador de segurança do recurso de comando, porque deseja a verificação de segurança para recursos associados com comandos, deverá incluir perfis de recurso para cada recurso na classe apropriada. Os mesmos perfis de segurança controlam os comandos MQSC e PCF.

Se você não tiver definido o perfil do comutador de segurança do recurso de comando, `hlq.NO.CMD.RESC.CHECKS`, porque deseja executar a verificação de segurança nos recursos associados com comandos, deverá:

- Incluir um perfil de recurso na classe **MQADMIN**, se estiver usando perfis em maiúsculas, para cada recurso.
- Incluir um perfil de recurso na classe **MXADMIN**, se estiver usando perfis compostos por letras maiúsculas e minúsculas para cada recurso.

Os mesmos perfis de segurança controlam os comandos MQSC e PCF.

Os perfis para verificação de segurança do recurso de comando têm o formato:

```
hlq.type.resourcename
```

em que `hlq` pode ser `qmgr-name` (nome do gerenciador de filas) ou `qsg-name` (nome do grupo de filas compartilhadas).

Um perfil prefixado pelo nome do gerenciador de filas controla o acesso aos recursos associados com comandos nesse gerenciador de filas. Um perfil prefixado pelo nome do grupo de filas compartilhadas controla o acesso aos recursos associados a comandos em todos os gerenciadores de filas no grupo de filas compartilhadas. Esse acesso pode ser substituído em um gerenciador de filas individual, definindo um perfil de nível do gerenciador de filas para esse recurso de comando nesse gerenciador de filas.

Se o seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ verificará um perfil prefixado pelo nome do gerenciador de filas primeiro. Se não localizar nenhum, ele procurará um perfil prefixado pelo nome do grupo de filas compartilhadas.

Por exemplo, o nome do perfil do RACF para verificação de segurança do recurso de comando com relação à fila modelo CREDIT.WORTHY no subsistema CSQ1 é:

```
CSQ1.QUEUE.CREDIT.WORTHY
```

Como os perfis para todos os tipos de recurso de comando são mantidos na classe MQADMIN, a parte "type" do nome do perfil é necessária no perfil para distinguir entre diferentes tipos de recursos que possuem o mesmo nome. A parte "type" do nome do perfil pode ser CHANNEL, QUEUE, TOPIC, PROCESS ou NAMELIST. Por exemplo, um usuário pode ser autorizado a definir hlq.QUEUE.PAYROLL.ONE, mas não autorizado a definir hlq.PROCESS.PAYROLL.ONE

Se o tipo de recurso for uma fila e o perfil for um perfil de nível do grupo de filas compartilhadas, ele controlará o acesso a uma ou mais filas locais dentro do grupo de filas compartilhadas ou o acesso a uma única fila compartilhada por meio de qualquer gerenciador de filas no grupo de filas compartilhadas.

z/OS Os comandos do MQSC, perfis e seus níveis de acesso mostram, para cada comando do MQSC IBM MQ, os perfis necessários para que a verificação de segurança de comando seja executada e o nível de acesso correspondente para cada perfil na classe MQCMDS.

z/OS Os comandos do PCF, perfis e seus níveis de acesso mostram para cada comando do PCF do IBM MQ os perfis necessários para que a verificação de segurança de comando seja executada e o nível de acesso correspondente para cada perfil na classe MQCMDS.

z/OS *Verificação de Segurança do Recurso de Comando para Filas de Alias e Filas Remotas*
As filas de alias e as filas remotas fornecem via indireta para uma outra fila. Pontos adicionais se aplicam quando você considere a verificação de segurança para essas filas.

Filas de Alias

Quando você define uma fila de alias, as verificações de segurança do recurso de comando são executadas apenas com relação ao nome da fila de alias, não com relação ao nome da fila de destino para a qual o alias resolve.

As filas de alias podem resolver para as filas local e remota. Se você não desejar permitir que os usuários acessem determinadas filas locais ou remotas, deverá executar ambos os procedimentos a seguir:

1. Não permita aos usuários o acesso a essas filas locais e remotas.
2. Restrinja a capacidade de os usuários definirem aliases para essas filas. Ou seja, evite que eles tenham a capacidade de emitir comandos DEFINE QALIAS e ALTER QALIAS.

Filas Remotas

Quando você define uma fila remota, as verificações de segurança do recurso de comando são executadas apenas com relação ao nome da fila remota. Nenhuma verificação é executada com relação aos nomes das filas especificadas nos atributos RNAME ou XMITQ na definição de objeto de fila remota.

z/OS O perfil de segurança RESLEVEL

É possível definir um perfil especial na classe MQADMIN ou MXADMIN para controlar o número de IDs de usuário verificados para a segurança do recurso da API. Esse perfil é chamado de perfil RESLEVEL. Como este perfil afeta a segurança do recurso da API depende de como você acessa o IBM MQ.

Quando um aplicativo tenta se conectar ao IBM MQ, IBM MQ verifica o acesso que o ID do usuário associado à conexão tem para um perfil na classe MQADMIN ou MXADMIN, chamado:

```
hlq.RESLEVEL
```

Em que `hlq` pode ser `ssid` (ID do subsistema) ou `qsg` (ID do grupo de filas compartilhadas).

Os IDs de usuário associados a cada tipo de conexão são:

- O ID do usuário da tarefa conectada para conexões em batch;
- O ID do usuário do espaço de endereço do CICS para conexões do CICS
- O ID do usuário do espaço de endereço da região do IMS para conexões do IMS
- O ID do usuário do espaço de endereçamento do iniciador do canal das conexões do iniciador do canal.

Atenção: RESLEVEL é uma opção muito poderosa; ela pode causar o bypass de todas as verificações de segurança do recurso para uma conexão específica.

Se você não tiver um perfil RESLEVEL definido, deverá tomar cuidado para que nenhum outro perfil na classe MQADMIN corresponda a hlq.RESLEVEL. Por exemplo, se você tiver um perfil em MQADMIN chamado hlq. * * e nenhum perfil hlq.RESLEVEL , cuidado com as consequências do hlq. * * porque é usado para a verificação RESLEVEL.

Defina um perfil hlq.RESLEVEL e configure o UACC para NONE, em vez de não ter nenhum perfil RESLEVEL. Tenha o mínimo possível de usuários ou grupos na lista de acesso. Para obter detalhes sobre como auditar o acesso de RESLEVEL, consulte "Considerações de auditoria no z/OS" na página 260.

Se estiver usando somente a segurança no nível do gerenciador de filas, o IBM MQ executa verificações RESLEVEL com relação ao perfil `qmgr-name.RESLEVEL`. Se você estiver usando a segurança no nível do grupo de compartilhamento de filas apenas, o IBM MQ executa verificações RESLEVEL em relação ao Perfil `doqsg-name.RESLEVEL` . Se você estiver usando uma combinação de segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, o IBM MQ primeiro verificará a existência de um perfil RESLEVEL no nível do gerenciador de filas. Se não localizar um, ele verificará se há um perfil RESLEVEL no nível do grupo de filas compartilhadas.

Se ele não puder localizar um perfil RESLEVEL, o IBM MQ permite a verificação do ID do job e da tarefa (ou usuário alternativo) para um CICS ou uma conexão do IMS. Para uma conexão em lote, o IBM MQ permite a verificação do ID de usuário da tarefa (ou alternativo). Para o inicializador de canais, o IBM MQ permite a verificação do ID do usuário do canal e o ID do usuário do MCA (ou alternativo).

Se houver um perfil RESLEVEL, o nível de verificação dependerá do ambiente e do nível de acesso para o perfil.

Lembre-se de que se seu gerenciador de filas for um membro de um grupo de filas compartilhadas e você não definir esse perfil no nível do gerenciador de filas, poderá haver um definido no nível do grupo de filas compartilhadas que afetará o nível de verificação. Para ativar a verificação de dois IDs de usuário, defina um perfil RESLEVEL (prefixado com o nome do gerenciador de filas do nome do grupo de filas compartilhadas) com um UACC(NONE) e certifique-se de que os usuários relevantes não tenham acesso concedido com relação a esse perfil.

Ao considerar o acesso que o ID do usuário do inicializador de canais tem para o RESLEVEL, lembre-se de que a conexão estabelecida pelo inicializador de canais também é a conexão usada pelos canais. Uma configuração que causa bypass de todas as verificações de segurança do recurso para o ID do usuário do inicializador de canais efetua bypass efetivamente das verificações de segurança para todos os canais. Se o acesso do ID do usuário do inicializador de canais para o RESLEVEL for diferente de NONE, apenas um ID do usuário (para um nível de acesso READ ou UPDATE) ou nenhum ID do usuário (para um nível de acesso CONTROL ou ALTER) será verificado quanto ao acesso. Se você conceder ao ID do usuário do inicializador de canais um nível de acesso diferente de NONE para o RESLEVEL, certifique-se de que entender o efeito dessa definição sobre as verificações de segurança realizadas para canais.

O uso do perfil RESLEVEL significa que registros de auditoria de segurança normais não são tomados. Por exemplo, se você colocar UAUDIT em um usuário, o acesso ao perfil hlq.RESLEVEL em MQADMIN não será auditorado.

Se você usar a opção RACF WARNING no perfil hlq.RESLEVEL, nenhuma mensagem de aviso do RACF será produzida para perfis na classe RESLEVEL.

A verificação de segurança para mensagens de relatório como CODs é controlada pelo perfil RESLEVEL associado ao aplicativo de origem. Por exemplo, se o ID do usuário de uma tarefa em lote tiver autoridade

CONTROL ou ALTER para um perfil RESLEVEL, então será efetuado bypass de toda a verificação de recursos executada pela tarefa em lote, incluindo a verificação de segurança de mensagens de relatório.

Se você alterar o perfil RESLEVEL, os usuários deverão desconectar e conectar novamente antes que a mudança ocorra. (Isso inclui parar e reiniciar o inicializador de canais se o acesso que o ID do usuário do espaço de endereço de enfileiramento distribuído tiver para o perfil RESLEVEL for alterado.)

Para desativar a auditoria de RESLEVEL use o parâmetro do sistema RESAUDIT.

z/OS *RESLEVEL e Conexões em Lote*

Por padrão, quando um recurso do IBM MQ está sendo acessado por meio de conexões em lotes e conexões de tipo de lote, o usuário deve estar autorizado a acessar esse recurso para a operação específica. É possível efetuar bypass da verificação de segurança configurando uma definição RESLEVEL apropriada.

Se o usuário é verificado ou não, isso é baseado no ID do usuário usado no tempo de conexão, o mesmo ID do usuário usado para a verificação de conexão.

Por exemplo, é possível configurar o RESLEVEL de modo que quando um usuário confiável acessar determinados recursos por meio de uma conexão em lotes, nenhuma verificação de segurança do recurso da API será feita; mas quando um usuário não confiável tentar acessar os mesmos recursos, as verificações de segurança serão executadas normalmente. Você deve configurar a verificação de RESLEVEL para efetuar bypass das verificações de segurança do recurso da API apenas quando confiar suficientemente no usuário e nos programas executados por esse usuário.

A tabela a seguir mostra as verificações feitas para as conexões em lotes.

Tabela 52. Verificações feitas em diferentes níveis de acesso do RACF para conexões em lotes

Nível de Acesso do RACF	**Nível de verificação**
NONE	Verificações de recursos executadas
READ	Verificações de recursos executadas
ATUALIZAÇÃO	Verificações de recursos executadas
CONTROLE	Nenhuma verificação.
ALTER	Nenhuma verificação.

z/OS *RESLEVEL e Funções do Sistema*

O aplicativo de RESLEVEL para os painéis de operações e controle e para o CSQUTIL.

Os painéis de operações e controle e o utilitário CSQUTIL são aplicativos do tipo lote que fazem solicitações ao servidor de comandos do gerenciador de filas e, portanto, estão sujeitos às considerações descritas em “RESLEVEL e Conexões em Lote” na página 235. É possível usar RESLEVEL para ignorar a verificação de segurança para as filas SYSTEM.COMMAND.INPUT e SYSTEM.COMMAND.REPLY.MODEL que eles usam, mas não para as filas dinâmicas SYSTEM.CSQXCMD.*. SYSTEM.CSQOREXX.* e SYSTEM.CSQUTIL.*.

O servidor de comandos é uma parte integrante do gerenciador de filas e, portanto, não possui conexão ou verificação de RESLEVEL associada a ele. Para manter a segurança, portanto, o servidor de comandos deve confirmar se o ID do usuário do aplicativo de solicitação possui autoridade para abrir a fila que está sendo usada para respostas. Para os painéis de operações e controle, esta é SYSTEM.CSQOREXX.*. Para CSQUTIL, esta é SYSTEM.CSQUTIL.*. Os usuários devem estar autorizados a usar essas filas, conforme descrito em “Segurança da Fila do Sistema” na página 207, além de qualquer autorização de RESLEVEL concedida a eles.

Para outros aplicativos que usam o servidor de comandos, é a fila que eles nomeiam como sua fila de resposta. Esses outros aplicativos podem enganar o servidor de comandos ao colocar mensagens em filas desautorizadas, passando (no contexto da mensagem) um ID de usuário mais confiável que o seu

próprio para o servidor de comandos. Para evitar isso, use um perfil CONTEXT para proteger o contexto de identidade das mensagens colocadas em SYSTEM.COMMAND.INPUT.

z/OS *RESLEVEL e conexões do CICS*

Por padrão, quando uma verificação de segurança do recurso da API é feita em uma conexão do CICS, dois IDs de usuário são verificados. É possível alterar quais IDs de usuário são verificados configurando um perfil RESLEVEL.

O primeiro ID de usuário verificado é o do espaço de endereço do CICS. Esse é o ID do usuário no cartão de tarefa da tarefa do CICS ou o ID do usuário designado à tarefa iniciada do CICS pela classe STARTED do z/OS ou pela tabela de procedimentos iniciados. (Ele não é o CICS DFLTUSER.)

O segundo ID do usuário verificado é o ID do usuário associado à transação do CICS.

Se um desses IDs de usuário não tiver acesso ao recurso, a solicitação falhará com um código de conclusão de MQRC_NOT_AUTHORIZED. O ID do usuário do espaço de endereço do CICS e o ID do usuário da pessoa que está executando a transação do CICS deve ter acesso ao recurso no nível correto.

Como o RESLEVEL Pode Afetar as Verificações Feitas

Dependendo de como você configura seu perfil RESLEVEL, é possível alterar quais IDs de usuário são verificados quando o acesso a um recurso é solicitado. Veja Tabela 53 na página 236 para obter mais informações.

Os IDs de usuário verificados dependem da ID do usuário usado no momento da conexão, ou seja, o ID do usuário do espaço de endereço do CICS. Este controle permite ignorar a verificação de segurança do recurso da API para as solicitações do IBM MQ que chegam de um sistema (por exemplo, um sistema de teste, TESTCICS,) mas implementá-las para outro (por exemplo, um sistema de produção, PRODCICS).

Nota: Se você configurar seu ID do usuário do espaço de endereço do CICS com o atributo "trusted" na classe STARTED ou a tabela ICHRIN03 da tabela de procedimentos iniciados do RACF, isso substitui qualquer verificação de ID do usuário para o espaço de endereço do CICS estabelecido pelo perfil RESLEVEL para o seu gerenciador de filas (ou seja, o gerenciador de filas não desempenha as verificações de segurança para o espaço de endereço do CICS). Para obter mais informações, veja o *CICS Transaction Server for z/OS V3.2 RACF Security Guide*.

A tabela a seguir mostra as verificações feitas para conexões do CICS.

Tabela 53. Verificações feitas em diferentes níveis de acesso do RACF para conexões do CICS

Nível de Acesso do RACF	**Nível de verificação**
NONE	O IBM MQ verifica o ID do usuário do espaço de endereço do CICS e o ID do usuário da transação.
READ	O IBM MQ verifica somente o ID do usuário do espaço de endereço do CICS.
ATUALIZAÇÃO	Se a transação for definida para CICS com RESSEC(YES), o IBM MQ verificará o ID do usuário do espaço de endereço do CICS e o ID do usuário da transação.
ATUALIZAÇÃO	Se a transação for definida para CICS com RESSEC(NO), o IBM MQ verificará somente o ID do usuário do espaço de endereço do CICS.
CONTROL ou ALTER	O IBM MQ não verifica nenhum ID do usuário.

z/OS *RESLEVEL e conexões do IMS*

Por padrão, quando uma verificação de segurança do recurso da API é feita para uma conexão do IMS, dois IDs de usuário são verificados. É possível alterar quais IDs de usuário são verificados configurando um perfil RESLEVEL.

Por padrão, quando uma verificação de segurança do recurso da API é feita para uma conexão do IMS, dois IDs de usuário são verificados para ver se o acesso é permitido ao recurso.

O primeiro ID do usuário verificado será aquele do espaço de endereço da região do IMS. Isso é obtido a partir do campo USER do cartão de tarefa ou o ID do usuário designado à região da classe STARTED do z/OS ou pela tabela de procedimentos iniciados (SPT).

O segundo ID do usuário verificado é associado ao trabalho sendo feito na região dependente. Ele é determinado de acordo com o tipo da região dependente, conforme mostrado em Como o segundo ID do usuário será determinado para a conexão do IMS(tm).

Se o primeiro ou o segundo ID do usuário do IMS não tiver acesso ao recurso, a solicitação falhará com um código de conclusão de MQRC_NOT_AUTHORIZED.

A configuração dos perfis RESLEVEL do IBM MQ não pode alterar o ID do usuário sob o qual as transações do IMS são planejadas a partir do programa do monitor acionador CSQQTRMN do MQ-IMS fornecido IBM. Esse ID do usuário é o PSBNAME desse monitor acionador, que por padrão é CSQQTRMN.

Como o RESLEVEL Pode Afetar as Verificações Feitas

Dependendo de como você configura seu perfil RESLEVEL, é possível alterar quais IDs de usuário são verificados quando o acesso a um recurso é solicitado. As verificações possíveis são:

- Verifique o ID do usuário do espaço de endereço da região do IMS e o segundo ID do usuário ou ID de usuário alternativo.
- Verifique somente o ID do usuário do espaço de endereço da região do IMS.
- Não verificar nenhum ID do usuário.

A tabela a seguir mostra as verificações feitas para conexões do IMS.

Tabela 54. Verificações feitas em diferentes níveis de acesso do RACF para conexões do IMS

Nível de Acesso do RACF	**Nível de verificação**
NONE	Verifique o ID do usuário do espaço de endereço do IMS e o segundo ID do usuário do IMS ou o ID de usuário alternativo.
READ	Verifique o ID do usuário do espaço de endereço do IMS.
ATUALIZAÇÃO	Verifique o ID do usuário do espaço de endereço do IMS.
CONTROLE	Nenhuma verificação.
ALTER	Nenhuma verificação.

z/OS *RESLEVEL e a Conexão do Inicializador de Canais*

Por padrão, quando uma verificação de segurança do recurso da API é feita pelo inicializador de canais, dois IDs de usuário são verificados. É possível alterar quais IDs de usuário são verificados configurando um perfil RESLEVEL.

Por padrão, quando uma verificação de segurança do recurso da API é feita pelo inicializador de canais, dois IDs de usuário são verificados para ver se o acesso é permitido ao recurso.

Os IDs de usuário verificados podem ser aquele especificado pelo atributo do canal MCAUSER, aquele recebido da rede, aquele do espaço de endereço do inicializador de canais ou o ID de usuário alternativo para o descritor de mensagens. Quais IDs de usuário são verificados depende do protocolo de comunicação que você está usando e da configuração do atributo do canal PUTAUT. Veja “IDs de Usuário Usados pelo Inicializador de Canais” na página 243 para obter mais informações.

Se um desses IDs de usuário não tiver acesso ao recurso, a solicitação falhará com um código de conclusão de MQRC_NOT_AUTHORIZED.

Como o RESLEVEL Pode Afetar as Verificações Feitas

Dependendo de como você configura seu perfil RESLEVEL, é possível alterar quais IDs de usuário são verificados quando o acesso a um recurso é solicitado e quantos são verificados.

A tabela a seguir mostra as verificações feitas para a conexão do inicializador de canais e para todos os canais desde que usem essa conexão.

Tabela 55. As verificações feitas em diferentes níveis de acesso do RACF para conexões do inicializador de canais

Nível de Acesso do RACF	**Nível de verificação**
NONE	Verificar dois IDs de usuário.
READ	Verificar um ID do usuário.
ATUALIZAÇÃO	Verificar um ID do usuário.
CONTROLE	Nenhuma verificação.
ALTER	Nenhuma verificação.
Nota: Consulte "IDs de Usuário Usados pelo Inicializador de Canais" na página 243 para uma definição dos IDs de usuário verificados	

z/OS *RESLEVEL e o Enfileiramento Intragrupo*

Por padrão, quando uma verificação de segurança do recurso da API é feita pelo agente de enfileiramento intragrupos, dois IDs de usuário são verificados para ver se o acesso é permitido ao recurso. É possível mudar quais IDs de usuário são verificados configurando um perfil RESLEVEL.

Os IDs de usuário verificados podem ser o ID do usuário determinado pelo atributo IGQUSER do gerenciador de filas de recebimento, o ID do usuário do gerenciador de filas dentro do grupo de filas compartilhadas que coloca a mensagem no SYSTEM.QSG.TRANSMIT.QUEUE ou o ID do usuário alternativo especificado no campo *UserIdentifier* do descritor de mensagens da mensagem. Consulte o "IDs de Usuário Usados pelo Agente de Enfileiramento Intragrupo" na página 247 para obter mais informações.

Como o agente de enfileiramento intragrupo é uma tarefa interna do gerenciador de filas, ele não emite uma solicitação de conexão explícita e é executado sob o ID do usuário do gerenciador de filas. O agente de enfileiramento intragrupo inicia na inicialização do gerenciador de filas. Durante a inicialização do agente de enfileiramento intragrupo, o IBM MQ verifica o acesso que o ID do usuário associado com o gerenciador de filas tem para um perfil na classe MQADMIN, chamado:

```
hlq.RESLEVEL
```

Essa verificação é sempre executada a menos que o comutador hlq.NO.SUBSYS.SECURITY tenha sido configurado.

Se não houver nenhum perfil RESLEVEL, o IBM MQ permite verificar se há dois IDs de usuário. Se houver um perfil RESLEVEL, o nível de verificação dependerá do nível de acesso concedido ao ID do usuário do gerenciador de filas para o perfil. As verificações feitas em diferentes níveis de acesso do RACF(r) para o agente de enfileiramento intragrupo mostram as verificações feitas para o agente de enfileiramento intragrupo.

Tabela 56. Verificações feitas em diferentes níveis de acesso do RACF para o agente de enfileiramento intragrupo

Nível de Acesso do RACF	**Nível de verificação**
NONE	Verificar dois IDs de usuário.
READ	Verificar um ID do usuário.

Tabela 56. Verificações feitas em diferentes níveis de acesso do RACF para o agente de enfileiramento intragrupo (continuação)	
Nível de Acesso do RACF	**Nível de verificação**
ATUALIZAÇÃO	Verificar um ID do usuário.
CONTROLE	Nenhuma verificação.
ALTER	Nenhuma verificação.
Nota: Consulte "IDs de Usuário Usados pelo Agente de Enfileiramento Intragrupo" na página 247 para uma definição dos IDs de usuário verificados	

Se as permissões concedidas ao perfil RESLEVEL para o ID do usuário do gerenciador de filas forem alteradas, o agente de enfileiramento intragrupo deverá ser interrompido e reiniciado para captar as novas permissões. Como não existe uma maneira de parar e reiniciar independentemente o agente de enfileiramento intragrupo, o gerenciador de filas deve ser interrompido e reiniciado para realizar isso.

z/OS *RESLEVEL e os IDs de Usuário Verificados*

Exemplo de configuração de um perfil RESLEVEL e concessão de acesso a ele.

ID do usuário que verifica o nome do perfil para conexões em lotes por meio de IDs do usuário verificados com relação ao nome do perfil para canais de conexão do servidor do LU 6.2 e TCP/IP mostram como RESLEVEL afeta quais IDs de usuário são verificados para diferentes solicitações do MQI.

Por exemplo, você possui um gerenciador de filas chamado QM66 com os requisitos a seguir:

- O usuário WS21B deve ser isento da segurança do recurso.
- A tarefa iniciada WXNCICS do CICS em execução sob o ID do usuário do espaço de endereço CICSWXN deve executar verificação de recursos completos somente para transações definidas com RESSEC(YES).

Para definir o perfil RESLEVEL apropriado, emita o seguinte comando RACF:

```
RDEFINE MQADMIN QM66.RESLEVEL UACC(NONE)
```

Em seguida, conceda aos usuários o acesso a esse perfil, usando os comandos a seguir:

```
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(WS21B) ACCESS(CONTROL)
PERMIT QM66.RESLEVEL CLASS(MQADMIN) ID(CICSWXN) ACCESS(UPDATE)
```

Se você fizer essas mudanças enquanto os IDs de usuário estiverem conectados ao gerenciador de filas QM66, os usuários deverão desconectar e conectar novamente antes que a mudança ocorra.

Se a segurança do subsistema não estiver ativa quando um usuário conectar-se mas, enquanto esse usuário ainda estiver conectado, a segurança do recurso tornar-se ativa, a verificação de segurança do recurso integral será aplicada ao usuário. O usuário deve reconectar-se para obter o processamento de RESLEVEL correto.

z/OS IDs de usuário para verificação de segurança no z/OS

O IBM MQ inicia as verificações de segurança com base em IDs do usuário associados a usuários, terminais, aplicativos e outros recursos. Essa coleção de tópicos lista quais IDs de usuário são usados para cada tipo de verificação de segurança.

z/OS *IDs de Usuário para Segurança da Conexão*

O ID do usuário usado para a segurança de conexão depende do tipo de conexão.

Tipo de conexão	Conteúdo do ID do usuário
Conexão em lotes	O ID do usuário da tarefa de conexão. Por exemplo: • O ID do usuário TSO • O ID do usuário designado a uma tarefa em lote pelo parâmetro JCL USER • O ID do usuário designado a uma tarefa iniciada pela classe STARTED ou pela tabela de procedimentos iniciados
CICS Conexão	O ID do usuário do espaço de endereço do CICS.
IMS Conexão	O ID do usuário do espaço de endereço da região do IMS.
Conexão do inicializador de canais	O ID do usuário do espaço de endereço do inicializador de canais.

z/OS *IDs de usuário para segurança de comando e do recurso de comando*

O ID do usuário usado para segurança de comando ou segurança do recurso de comando depende a partir de onde o comando é emitido.

Emitido a partir de...	Conteúdo do ID do usuário
CSQINP1, CSQINP2 ou CSQINPT	Nenhuma verificação é feita.
Fila de entrada de comandos do sistema	O ID do usuário localizado no *UserIdentifier* do descritor de mensagens da mensagem que contém o comando. Se a mensagem não contiver um *UserIdentifier*, um ID de usuário em branco é transmitido ao gerenciador de segurança.
Console	O ID do usuário conectado ao console. Se o console não estiver conectado, o ID de usuário padrão configurado pelo parâmetro do sistema CMDUSER em CSQ6SYSP. Para emitir os comandos a partir de um console, o console deverá ter o atributo SYS AUTHORITY do z/OS.
Console do SDSF/TSO	ID do usuário do TSO ou da tarefa.
Painéis de operações e controle	ID do usuário do TSO. Caso pretenda usar os painéis de operações e controle, você deve ter a autoridade apropriada para emitir os comandos correspondentes às ações escolhidas. Além disso, deve-se ter acesso READ a todos os perfis hlq.DISPLAY. de *objeto* na classe MQCMDS, pois os painéis usam os vários comandos DISPLAY para reunir as informações que eles apresentam.
MGCRE	Se MGCRE for usado com UTOKEN, o ID do usuário será UTOKEN. Se MGCRE for emitido sem o UTOKEN, o ID do usuário de TSO ou da tarefa será usado.
CSQ0UTIL	ID do usuário da tarefa.
CSQUTIL	ID do usuário da tarefa.
CSQINPX	ID do usuário do espaço de endereço do inicializador de canais.

z/OS *IDs de Usuário para Segurança do Recurso (MQOPEN, MQSUB e MQPUT1)*

Estas informações mostram o conteúdo dos IDs de usuário para os IDs de usuário normal e alternativo para cada tipo de conexão. O número de verificações é definido pelo perfil RESLEVEL. O ID do usuário verificado é aquele usado para chamadas **MQOPEN**, **MQSUB** ou **MQPUT1**.

Nota: Todos os campos de ID do usuário são verificados exatamente como eles são recebidos. Não ocorrem conversões e, por exemplo, três campos de ID do usuário contendo "Bob", "BOB" e "bob" não são equivalentes.

z/OS *IDs de Usuário Verificados para Conexões em Lotes*

O ID do usuário verificado para uma conexão em lote depende de como a tarefa é executada e se um ID de usuário alternativo foi especificado.

Tabela 57. Verificação de ID do Usuário com Relação ao Nome do Perfil para Conexões em Lotes

ID de usuário alternativo especificado na abertura?	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
Não	-	CARGO	CARGO
Sim	CARGO	CARGO	ALT

Chave:

ALT
ID de usuário alternativo.

CARGO

- O ID do usuário de uma conexão do TSO ou USS.
- O ID do usuário designado a uma tarefa em lote.
- O ID do usuário designado a uma tarefa iniciada pela classe STARTED ou pela tabela de procedimentos iniciados.
- O ID do usuário associado ao procedimento armazenado do Db2 em execução

Uma tarefa em lote está executando um MQPUT1 para uma fila chamada Q1 com RESLEVEL configurado para READ e verificação de ID de usuário alternativo desligada.

Verificações feitas em diferentes níveis de acesso RACF(r) para conexões em lote e Verificação de ID do usuário contra nome do perfil para conexões em lote mostram que o ID do usuário da tarefa é verificado com relação ao perfil hlq.Q1.

z/OS *IDs de usuário verificados para conexões do CICS*

Os IDs de usuário verificados para as conexões do CICS dependem de se uma ou duas verificações serão realizadas, e se um ID de usuário alternativo é especificado.

Tabela 58. A verificação de ID do usuário com relação ao nome do perfil para IDs do usuário do tipo CICS

ID de usuário alternativo especificado na abertura?	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
Não, 1 verificação	-	ADS	ADS
Não, 2 verificações	-	ADS+TXN	ADS+TXN
Sim, 1 verificação	ADS	ADS	ADS
Sim, 2 verificações	ADS+TXN	ADS+TXN	ADS+ALT

Chave:

ALT
ID do usuário alternativo

ADS
O ID do usuário associado à tarefa em lote do CICS ou, se CICS estiver sendo executado como uma tarefa iniciada por meio da classe STARTED ou pela tabela de procedimentos iniciados.

TXN
O ID do usuário associado à transação do CICS. Este é normalmente o ID do usuário do usuário do terminal que iniciou a transação. Ele pode ser o CICS DFLTUSER, um terminal de segurança PRESET ou um usuário conectado manualmente.

Determine os IDs de usuário verificados para as condições a seguir:

- O nível de acesso do RACF para o perfil RESLEVEL, para um ID do usuário do espaço de endereço do CICS, está configurado como NONE.
- Uma chamada MQOPEN é feita com relação a uma fila com MQOO_OUTPUT e MQOO_PASS_IDENTITY_CONTEXT.

Primeiro, consulte quantos IDs de usuário do CICS são verificadas com base no acesso do ID do usuário do espaço de endereço do CICS ao perfil RESLEVEL. No Tabela 53 na página 236 no tópico "RESLEVEL e conexões do CICS" na página 236, dois IDs de usuário são verificados se o perfil RESLEVEL estiver configurado como NONE. Depois, a partir de Tabela 58 na página 241, estas verificações são realizadas:

- O perfil hlq.ALTERNATE.USER.userid não é verificado.
- O perfil hlq.CONTEXT.queuename é verificado com o ID do usuário do espaço de endereço do CICS e o ID do usuário da transação do CICS.
- O perfil hlq.resourcename é verificado com o ID do usuário do espaço de endereço do CICS e o ID do usuário da transação do CICS.

Isso significa que quatro verificações de segurança são feitas para essa chamada MQOPEN.

z/OS *IDs de usuário verificados para conexões do IMS*

Os IDs de usuário verificados para as conexões do IMS dependem de se uma ou duas verificações serão executadas, e se um ID de usuário alternativo será especificado. Se um segundo ID do usuário será verificado, isso depende do tipo de região dependente e de quais IDs de usuário estão disponíveis.

Tabela 59. A verificação de ID do usuário com relação ao nome do perfil para IDs do usuário do tipo IMS

ID de usuário alternativo especificado na abertura?	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
Não, 1 verificação	-	REG	REG
Não, 2 verificações	-	REG+SEC	REG+SEC
Sim, 1 verificação	REG	REG	REG
Sim, 2 verificações	REG+SEC	REG+SEC	REG+ALT

Chave:

ALT
ID de usuário alternativo.

REG
O ID do usuário normalmente é configurado por meio da classe STARTED ou da tabela de procedimentos iniciada ou, se IMS estiver executando, a partir de uma tarefa enviada, pelo parâmetro USER JCL.

SEC
O segundo ID do usuário é associado ao trabalho sendo feito na região dependente. Ele é determinado de acordo com a Tabela 60 na página 243.

Tabela 60. Como o segundo ID do usuário é determinado para a conexão do IMS	
Tipos de região dependente	**Hierarquia para determinar o segundo ID do usuário**
• BMP acionado por mensagem e GET UNIQUE bem-sucedido emitido. • IFP e GET UNIQUE emitidos. • MPP.	O ID do usuário associado à transação IMS se o usuário estiver conectado. O nome LTERM se disponível. PSBNAME.
• BMP acionado por mensagem e GET UNIQUE bem-sucedido não emitido. • BMP não acionado por mensagem. • IFP e GET UNIQUE não emitidos.	O ID do usuário associado ao espaço de endereço da região dependente do IMS se não forem todos espaços em branco ou zeros. PSBNAME.

z/OS *IDs de Usuário Usados pelo Inicializador de Canais*

Esta coleção de tópicos descreve os IDs de usuário usados e verificados para recebimento de canais e para solicitações de cliente MQI emitidas por meio de canais de conexão do servidor. As informações são fornecidas para TCP/IP e para LU6.2

É possível usar o parâmetro PUTAUT da definição de canal de recebimento para determinar o tipo de verificação de segurança usado. Para obter a verificação de segurança consistente por toda a sua rede do IBM MQ, é possível usar as opções ONLYMCA e ALTMCA.

É possível usar o comando DISPLAY CHSTATUS para determinar o identificador de usuários usado pelo MCA.

z/OS *Recebendo Canais Usando TCP/IP*

Os IDs de usuário verificados dependem da opção PUTAUT do canal e se uma ou duas verificações serão executadas.

Tabela 61. IDs de Usuário Verificados com Relação ao Nome do Perfil para Canais TCP/IP			
Opção PUTAUT especificada no canal do receptor ou do solicitante	**Perfil hlq.ALTERNATE.USER.userid**	**Perfil hlq.CONTEXT.queuename**	**Perfil hlq.resourcename**
DEF, 1 verificar	-	CHL	CHL
DEF, 2 verificações	-	CHL + MCA	CHL + MCA
CTX, 1 verificação	CHL	CHL	CHL
CTX, 2 verificações	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 verificação	-	MCA	MCA
ONLYMCA, 2 verificações	-	MCA	MCA
ALTMCA, 1 verificação	MCA	MCA	MCA
ALTMCA, 2 verificações	MCA	MCA	MCA + ALT

Chave:

MCA (ID do usuário do MCA)
O ID do usuário especificado para o atributo do canal MCAUSER no receptor; se em branco, o ID do usuário do espaço de endereço do inicializador de canais do lado do receptor ou do solicitante será usado.

CHL (ID do usuário do canal)
Em TCP/IP, a segurança não é suportada pelo sistema de comunicação para o canal. Se a Segurança da Camada de Transporte (TLS) estiver sendo usada e um certificado digital foi transmitido do parceiro, o ID do usuário associado a esse certificado (se instalado) ou o ID do usuário associado a um filtro correspondente localizado usando o RACF Certificate Name Filtragem (CNF) será usado. Se nenhum ID do usuário associado for localizado ou se o TLS não estiver sendo usado, o ID do usuário do espaço de endereço do inicializador de canais da extremidade do receptor ou solicitante será usado como o ID do usuário do canal em canais definidos com o parâmetro PUTAUT configurado como DEF ou CTX.

Nota: O uso do filtro do nome do certificado (CNF) do RACF permite atribuir o mesmo ID do usuário a vários usuários remotos do RACF, por exemplo, a todos os usuários na mesma unidade organizacional, que, naturalmente, teriam a mesma autoridade de segurança. Isso significa que o servidor não precisa ter uma cópia do certificado de cada usuário remoto possível em todo o mundo e simplifica bastante o gerenciamento e distribuição de certificado.

Se o parâmetro PUTAUT for configurado para ONLYMCA ou ALTMCA para o canal, o ID do usuário do canal será ignorado e o ID do usuário do MCA do receptor ou solicitante será usado. Isso também se aplica aos canais TCP/IP usando TLS.

ALT (ID de usuário alternativo)
O ID do usuário a partir das informações de contexto (ou seja, o campo *UserIdentifier*) no descritor de mensagens da mensagem. Esse ID do usuário é movido para o campo *AlternateUserID* no descritor de objeto antes de uma chamada **MQOPEN** ou **MQPUT1** ser emitida para a fila de destino.

z/OS *Recebendo Canais Usando LU 6.2*
Os IDs de usuário verificados dependem da opção PUTAUT do canal e se uma ou duas verificações serão executadas.

Tabela 62. IDs de Usuário Verificados com Relação ao Nome do Perfil para Canais LU 6.2

Opção PUTAUT especificada no canal do receptor ou do solicitante	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
DEF, 1 verificar	-	CHL	CHL
DEF, 2 verificações	-	CHL + MCA	CHL + MCA
CTX, 1 verificação	CHL	CHL	CHL
CTX, 2 verificações	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 verificação	-	MCA	MCA
ONLYMCA, 2 verificações	-	MCA	MCA
ALTMCA, 1 verificação	MCA	MCA	MCA
ALTMCA, 2 verificações	MCA	MCA	MCA + ALT

Chave:

MCA (ID do usuário do MCA)
O ID do usuário especificado para o atributo do canal MCAUSER no receptor; se em branco, o ID do usuário do espaço de endereço do inicializador de canais do lado do receptor ou do solicitante será usado.

CHL (ID do usuário do canal)

Canais solicitante-servidor
Se o canal for iniciado a partir do solicitante, não haverá oportunidade de receber um ID do usuário de rede (o ID do usuário do canal).

Se o parâmetro PUTAUT for configurado para DEF ou CTX no canal do solicitante, o ID do usuário do canal será aquele do espaço de endereço do inicializador de canais do solicitante porque nenhum ID do usuário é recebido da rede.

Se o parâmetro PUTAUT for configurado para ONLYMCA ou ALTMCA, o ID do usuário do canal será ignorado e o ID do usuário do MCA do solicitante será usado.

Outros tipos de canal
Se o parâmetro PUTAUT for configurado para DEF ou CTX no canal do receptor ou do solicitante, o ID do usuário do canal será o ID do usuário recebido do sistema de comunicações quando o canal for iniciado.

- Se o canal de envio estiver no z/OS, o ID do usuário do canal recebido é o ID do usuário do espaço de endereço do inicializador de canais do emissor.
- Se o canal de envio estiver em uma plataforma diferente (por exemplo, AIX), o ID do usuário do canal recebido será geralmente fornecido pelo parâmetro USERID da definição de canal.

Se o ID do usuário recebido estiver em branco ou nenhum ID do usuário for recebido, um ID do usuário do canal em branco será usado.

ALT (ID de usuário alternativo)
O ID do usuário a partir das informações de contexto (ou seja, o campo *UserIdentifier*) no descritor de mensagens da mensagem. Esse ID do usuário é movido para o campo *AlternateUserID* no descritor de objeto antes de uma chamada MQOPEN ou MQPUT1 ser emitida para a fila de destino.

z/OS *Solicitações de MQI do Cliente*

Vários IDs de usuário podem ser usados, dependendo de quais IDs de usuário e variáveis de ambiente foram configurados. Esses IDs de usuário são verificados com relação a vários perfis, dependendo da opção PUTAUT usada e se um ID de usuário alternativo é especificado.

Esta seção descreve os IDs de usuário verificados para solicitações de cliente MQI emitidas por meio de canais de conexão do servidor para TCP/IP e LU 6.2. O ID do usuário do MCA e o ID do usuário do canal são como nos canais TCP/IP e LU 6.2 descritos nas seções anteriores.

Para canais de conexão do servidor, o ID do usuário recebido do cliente será usado se o atributo MCAUSER estiver em branco.

Veja “Controle de acesso para clientes” na página 98 para obter mais informações.

Para solicitações **MQOPEN**, **MQSUB** e **MQPUT1** do cliente, use as regras a seguir para determinar o perfil que será verificado:

- Se a solicitação especifica a autoridade de usuário alternativo, uma verificação é feita com relação ao perfil *hlq*.ALTERNATE.USER. *userid*.
- Se a solicitação especifica a autoridade de contexto, uma verificação é feita com relação ao perfil *hlq*.CONTEXT. *queuename*.
- Para todas as solicitações **MQOPEN**, **MQSUB** e **MQPUT1**, uma verificação é feita com relação ao perfil *hlq.resourcename*.

Quando você tiver determinado quais perfis serão verificados, use a tabela a seguir para determinar quais IDs de usuário serão verificados com relação a esses perfis.

Tabela 63. IDs de Usuário Verificados com Relação ao Nome do Perfil para Canais de Conexão do Servidor LU 6.2 e TCP/IP

Opção PUTAUT especificada no canal de conexão do servidor	ID de usuário alternativo especificado na abertura?	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
DEF, 1 verificar	NÃO	-	CHL	CHL
DEF, 1 verificar	Sim	CHL	CHL	CHL
DEF, 2 verificações	NÃO	-	CHL + MCA	CHL + MCA
DEF, 2 verificações	Sim	CHL + MCA	CHL + MCA	CHL + ALT
ONLYMCA, 1 verificação	NÃO	-	MCA	MCA
ONLYMCA, 1 verificação	Sim	MCA	MCA	MCA
ONLYMCA, 2 verificações	NÃO	-	MCA	MCA
ONLYMCA, 2 verificações	Sim	MCA	MCA	MCA + ALT

Chave:

MCA (ID do usuário do MCA)
O ID do usuário especificado para o atributo do canal MCAUSER na conexão do servidor; se em branco, o ID do usuário do espaço de endereço do inicializador de canais é utilizado.

CHL (ID do usuário do canal)
Em TCP/IP, a segurança não é suportada pelo sistema de comunicação para o canal. Se a Segurança da Camada de Transporte (TLS) estiver sendo usada e um certificado digital foi transmitido do parceiro, o ID do usuário associado a esse certificado (se instalado) ou o ID do usuário associado a um filtro correspondente localizado usando o RACF Certificate Name Filtragem (CNF) será usado. Se nenhum ID do usuário associado for localizado ou se o TLS não estiver sendo usado, o ID do usuário do espaço de endereço do inicializador de canais será usado como o ID do usuário do canal em canais definidos com o parâmetro PUTAUT configurado para DEF ou CTX.

Nota: O uso do filtro do nome do certificado (CNF) do RACF permite atribuir o mesmo ID do usuário a vários usuários remotos do RACF, por exemplo, a todos os usuários na mesma unidade organizacional, que, naturalmente, teriam a mesma autoridade de segurança. Isso significa que o servidor não precisa ter uma cópia do certificado de cada usuário remoto possível em todo o mundo e simplifica bastante o gerenciamento e distribuição de certificado.

Se o parâmetro PUTAUT for configurado para ONLYMCA ou ALTMCA para o canal, o ID do usuário do canal será ignorado e o ID do usuário do MCA do canal de conexão do servidor será usado. Isso também se aplica aos canais TCP/IP usando TLS.

ALT (ID de usuário alternativo)
O ID do usuário a partir das informações de contexto (ou seja, o campo *UserIdentifier*) no descritor de mensagens da mensagem. Esse ID de usuário é movido para o campo *AlternateUserID* no descritor de objeto ou assinatura antes de uma chamada **MQOPEN**, **MQSUB** ou **MQPUT1** ser emitida em nome do aplicativo cliente.

z/OS *Exemplo de Inicializador de Canais*

Um exemplo de como IDs de usuário são verificados com relação aos perfis do RACF.

Um usuário executa uma operação **MQPUT1** para uma fila no gerenciador de filas QM01 que resolve para uma fila chamada QB no gerenciador de filas QM02. A mensagem é enviada em um canal TCP/IP chamado QM01.TO.QM02. RESLEVEL é configurado para NONE e a abertura é executada com o ID de usuário alternativo e a verificação de contexto. A definição de canal receptor possui PUTAUT(CTX) e o ID do usuário do MCA está configurado. Quais IDs de usuário são usados no canal de recebimento para colocar a mensagem na fila QB?

Resposta:O Tabela 55 na página 238 mostra que dois IDs de usuário são verificados porque RESLEVEL é configurado como NONE.

A Tabela 61 na página 243 mostra que, com PUTAUT configurado para CTX e 2 verificações, os IDs de usuário a seguir são verificados:

- O ID do usuário do inicializador de canais e o ID do usuário MCAUSER são verificados com relação ao perfil hlq.ALTERNATE.USER.userid.
- O ID do usuário do inicializador de canais e o ID do usuário MCAUSER são verificados com relação ao perfil hlq.CONTEXT.queuename.
- O ID do usuário do inicializador de canais e o ID de usuário alternativo especificados no descritor de mensagens (MQMD) são verificados com relação ao perfil hlq.Q2.

z/OS *IDs de Usuário Usados pelo Agente de Enfileiramento Intragrupo*

Os IDs de usuário que são verificados quando o agente de enfileiramento intragrupo abre filas de destino são determinados pelos valores dos atributos do valores IGQAUT e IGQUSER.

Os IDs de usuário possíveis são:

ID do usuário de enfileiramento intragrupo (IGQ)
O ID do usuário determinado pelo atributo IGQUSER do gerenciador de filas de recebimento. Se configurado para espaços em branco, o ID do usuário do gerenciador de filas de recebimento será usado. No entanto, como o gerenciador de filas de recebimento tem autoridade para acessar todas as filas definidas para ele, as verificações de segurança não são executadas para o ID do usuário do gerenciador de filas de recebimento. Nesse caso:

- Se apenas um ID do usuário será verificado e o ID do usuário for aquele do gerenciador de filas de recebimento, nenhuma verificação de segurança ocorrerá. Isso pode ocorrer quando IGQAUT é configurado para ONLYIGQ ou ALTIGQ
- Se dois IDs de usuário serão verificados e um dos IDs de usuário for aquele do gerenciador de filas de recebimento, as verificações de segurança ocorrerão apenas para o outro ID do usuário. Isso pode ocorrer quando IGQAUT é configurado como DEF, CTX ou ALTIGQ.
- Se dois IDs de usuário serão verificados e ambos os IDs de usuário forem aquele do gerenciador de filas de recebimento, nenhuma verificação de segurança ocorrerá. Isso pode ocorrer quando IGQAUT é configurado como ONLYIGQ

ID do usuário do gerenciador de filas de envio (SND)
O ID do usuário do gerenciador de filas dentro do grupo de filas compartilhadas que coloca a mensagem no SYSTEM.QSG.TRANSMIT.QUEUE.

ID do usuário alternativo (ALT)
O ID do usuário especificado no campo *UserIdentifier* no descritor de mensagens da mensagem.

Tabela 64. IDs de Usuário Verificados com Relação ao Nome do Perfil para Enfileiramento Intragrupo

Opção IGQAUT especificada no gerenciador de filas de recebimento	Perfil hlq.ALTERNATE.USER.userid	Perfil hlq.CONTEXT.queuename	Perfil hlq.resourcename
DEF, 1 verificar	-	SND	SND
DEF, 2 verificações	-	SND +IGQ	SND +IGQ
CTX, 1 verificação	SND	SND	SND
CTX, 2 verificações	SND + IGQ	SND +IGQ	SND + ALT
ONLYIGQ, 1 verificação	-	IGQ	IGQ
ONLYIGQ, 2 verificações	-	IGQ	IGQ
ALTIGQ, 1 verificação	-	IGQ	IGQ
ALTIGQ, 2 verificações	IGQ	IGQ	IGQ + ALT

Chave:

ALT
ID de usuário alternativo.

IGQ
ID do usuário IGQ.

SND
ID do usuário do gerenciador de filas de envio.

z/OS *IDs de Usuário em Branco e Níveis de UACC*

Se um ID do usuário em branco ocorrer, um RACF usuário indefinido efetuará sign on. Não conceda acesso muito abrangente para o usuário indefinido.

IDs de usuário em branco podem existir quando um usuário está manipulando mensagens usando o contexto ou segurança de usuário alternativo ou quando um ID do usuário em branco é transmitido para o IBM MQ. Por exemplo, um ID do usuário em branco é usado quando uma mensagem é gravada na fila de entrada de comandos do sistema sem contexto.

Nota: Um ID do usuário " * " (ou seja, um caractere asterisco seguido por sete espaços) é tratado como um ID do usuário indefinido.

O IBM MQ transmite o ID do usuário em branco para o RACF e um usuário indefinido do RACF está conectado. Todas as verificações de segurança usam o universal access (UACC) para o perfil relevante. Dependendo de como você configurou seus níveis de acesso, o UACC pode conceder ao usuário indefinido um acesso muito abrangente.

Por exemplo, se o comando do RACF for emitido a partir do TSO:

```
RDEFINE MQQUEUE Q.AVAILABLE.TO.EVERYONE UACC(UPDATE)
```

você define um perfil que permite que os dois IDs definidos pelo usuário do z/OS (que não foram colocadas na lista de acesso) e o ID do usuário indefinido do RACF para colocar as mensagens e obter as mensagens dessa fila.

Para proteger contra IDs de usuário em branco, você deve planejar seus níveis de acesso com cuidado e limitar o número de pessoas que podem usar a segurança do contexto e de usuário alternativo. Deve-se evitar que pessoas usando o ID do usuário indefinido do RACF obtenham acesso a recursos que eles não devem acessar. Entretanto, ao mesmo tempo, você deve permitir o acesso para pessoas com IDs de usuário diferentes. Para fazer isso, é possível especificar um ID do usuário de asterisco (*) em um comando PERMIT do RACF, fornecendo acesso aos recursos para todos os IDs de usuário definidos. Portanto, todos os IDs de usuário indefinidos (tais como " * ") têm acesso negado. Por exemplo, esses comandos do RACF evitam que o ID do usuário indefinido do RACF obtenha acesso a fila para colocar ou obter mensagens:

```
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 IDs do usuário do z/OS e Multi-Factor Authentication (MFA)

O IBM Multi-Factor Authentication for z/OS permite que os administradores de segurança do z/OS aprimorem a autenticação SAF, que requer que os usuários identificados usem autenticação de diversos fatores (por exemplo, uma senha e um token criptográfico) para efetuar sign on em um sistema z/OS. O IBM MFA também fornece suporte para as tecnologias de geração de senha descartável baseada em tempo, como RSA SecureId.

De um modo geral, o IBM MQ não está ciente de como os usuários "efetuaram logon" nos sistemas CICS ou em lote que estão levando o IBM MQ a funcionar, a credencial do ID do usuário que efetuou logon é associada à tarefa ou ao espaço de endereço do z/OS e o IBM MQ usa isso para verificar a autorização para recursos. Os IDs de usuários ativados para MFA podem ser usados para autorização a recursos do IBM MQ e autenticação por meio de passtickets usados com as pontes CICS e IMS.

Importante: Considerações especiais se aplicam, no entanto, ao usar aplicativos, como o IBM MQ Explorer, que passa um ID do usuário e as credenciais de senha em uma chamada API MQCONNX com a opção *MQCSP_AUTH_USER_ID_AND_PWD*. O IBM MQ não tem o recurso para passar uma credencial adicional nessa solicitação de API.

Limitações e potenciais soluções alternativas são descritas no texto a seguir.

IBM MQ Explorer

O IBM MQ Explorer não pode ser usado para efetuar logon em um sistema z/OS com um ID do usuário para o qual o MFA está ativado porque não há nenhum recurso para passar um segundo fator de autenticação do IBM MQ Explorer para o z/OS.

Além disso, há dois mecanismos diferentes usados pelo IBM MQ Explorer para reutilizar um ID do usuário e uma credencial de senha, que precisam de atenção especial quando senhas descartáveis estão em vigor:

1. O IBM MQ Explorer tem a capacidade de armazenar senhas em um formato ofuscado na máquina local para login em um momento posterior. Esse recurso deve ser desativado tendo um prompt de explorador para uma senha toda vez que uma conexão é feita para o gerenciador de filas do z/OS.

   Para fazer isto, utilize o seguinte procedimento:

   a. Selecione **Gerenciadores de filas**.
   b. Na lista exibida, escolha o gerenciador de filas que você requer e clique com o botão direito nesse gerenciador de filas.
   c. Selecione **Detalhes da conexão** na lista de menu que aparece.
   d. Selecione **Propriedades** na próxima lista de menu e escolha a guia **ID do usuário**.

      Assegure-se de selecionar o botão de opções **prompt para senha**.
2. Várias operações no IBM MQ Explorer, como procurar mensagens em filas, testar assinaturas e assim por diante, iniciam um novo encadeamento que autentica para o IBM MQ usando a credencial usada

pela primeira vez no logon. Como a credencial de senha não pode ser reutilizada, não é possível usar essas operações.

Há duas soluções alternativas possíveis no nível de configuração de MFA para estes problemas:

- Use a exclusão do ID do aplicativo do MFA para excluir as tarefas do IBM MQ do processamento de MFA por completo.

  Para fazer isso, emita os comandos a seguir:

  1. `RDEFINE MFADEF MFABYPASS.USERID.chinuser`

     em que *chinuser* é o ID do usuário de nível de espaço de endereço do inicializador de canais (associado com o inicializador de canais por meio da classe STC)

  2. `PERMIT MFABYPASS.USERID.chinuser CLASS MFADEF ACCESS(READ) ID(explorer user)`

  Para obter mais informações sobre essa abordagem, consulte Ignorando o IBM MFA para aplicativos.
- Use o suporte de Fora da banda no MFA, que foi introduzido com o IBM MFA 1.2. Com essa abordagem, você pré-autentica para o servidor da web IBM MFA e, além do seu ID do usuário e senha, especifica a autenticação adicional, conforme determinado por meio da política. O servidor IBM MFA gera uma credencial de token de cache que você então especifica no diálogo de autenticação do IBM MQ Explorer. O administrador de segurança pode permitir que essa credencial seja reproduzida por um período de tempo razoável, permitindo o uso normal do IBM MQ Explorer.

Para obter mais informações sobre esta abordagem, consulte Introdução ao IBM MFA.

z/OS IBM MQ for z/OS gerenciamento da segurança

IBM MQ usa uma tabela em armazenamento para conter informações relacionadas a cada usuário e aos pedidos de acesso feitos por cada usuário. Para gerenciar esta tabela de maneira eficiente e para reduzir o número de pedidos feitos a partir do IBM MQ para o gerenciador de segurança externa (ESM), um número de controles estão disponíveis.

Estes controles estão disponíveis através de ambas as operações e os painéis de controle e os comandos do IBM MQ.

z/OS *Nova Verificação do ID de Usuário*

Se a definição RACF de um usuário que estiver usando os recursos do IBM MQ tiver sido mudada, por exemplo, conectando o usuário a um novo grupo, será possível dizer ao gerenciador de filas para efetuar sign on desse usuário novamente na próxima vez que ele tentar acessar um recurso do IBM MQ. É possível fazer isso usando o comando RVERIFY SECURITY do IBM MQ.

- O usuário HX0804 está obtendo e colocando mensagens nas filas PAYROLL no gerenciador de filas PRD1. Entretanto, o HX0804 agora requer acesso a algumas das filas PENSION no mesmo gerenciador de filas (PRD1).
- O administrador de segurança de dados conecta o usuário HX0804 ao grupo RACF que permite acesso às filas PENSION.
- Para que HX0804 possa acessar as filas PENSION imediatamente (isto é, sem encerrar o gerenciador de filas PRD1 ou aguardar que HX0804 atinja o tempo limite), deve-se usar o comando do IBM MQ:

```
RVERIFY SECURITY(HX0804)
```

Nota: Se você desligar o tempo limite do ID do usuário por longos períodos de tempo (dias ou até semanas) enquanto o gerenciador de filas está em execução, deverá lembrar-se de executar o comando RVERIFY SECURITY para quaisquer usuários que tenham sido revogados ou excluídos nesse tempo.

z/OS *Tempos Limites do ID do Usuário*

É possível fazer o IBM MQ efetuar sign off de um usuário de um gerenciador de filas após um período de inatividade.

Quando um usuário acessa um recurso do IBM MQ, o gerenciador de filas tenta conectar este usuário ao gerenciador de filas (se a segurança do subsistema estiver ativa). Isso significa que o usuário é autenticado no ESM. Este usuário permanece conectado ao IBM MQ até que o gerenciador de filas seja encerrado ou até que o ID do usuário atinja *tempo limite* (a autenticação prescreve) ou seja verificado novamente (reautenticado).

Quando um usuário atinge o tempo limite, o ID do usuário *efetua sign off* no gerenciador de filas e quaisquer informações relacionadas à segurança retidas para esse usuário são descartadas. O sign on e o sign off do usuário no gerenciador de filas não é aparente para o programa de aplicativo ou para o usuário.

Os usuários são elegíveis para tempo limite quando eles não usaram qualquer recurso do IBM MQ por uma quantidade predeterminada de tempo. Esse período de tempo é configurado pelo comando MQSC ALTER SECURITY.

Dois valores podem ser especificados no comando ALTER SECURITY:

TIMEOUT
O período de tempo em minutos que um ID do usuário não usado e seus recursos associados podem permanecer dentro do gerenciador de filas do IBM MQ.

INTERVALO
O período de tempo em minutos entre as verificações para os IDs de usuário e seus recursos associados, para determinar se o *TIMEOUT* expirou.

Por exemplo, se o valor de *TIMEOUT* for 30 e o valor de *INTERVAL* for 10, a cada 10 minutos o IBM MQ verificará os IDs do usuário e seus recursos associados para determinar se algum não foi usado por 30 minutos. Se um ID do usuário com tempo limite esgotado for encontrado, ele será cancelado do gerenciador de filas. Se quaisquer informações do recurso com tempo limite atingido associadas a IDs de usuário sem tempo limite atingido forem localizadas, essas informações do recurso serão descartadas. Se você não desejar que os IDs de usuário atinjam o tempo limite, configure o valor de *INTERVAL* para zero. Entretanto, se o valor de *INTERVAL* for zero, o armazenamento ocupado por IDs de usuário e seus recursos associados não será liberado até que você emita um comando **REFRESH SECURITY** ou **RVERIFY SECURITY**.

Ajustar esse valor é importante se você tiver vários usuários únicos. Se você configurar valores pequenos de intervalo e tempo limite, os recursos que não forem mais necessários serão liberados.

Nota: Se você usar valores para *INTERVAL* ou *TIMEOUT* diferentes dos padrões, deverá inserir novamente o comando a cada inicialização do gerenciador de filas. É possível fazer isso automaticamente colocando o comando **ALTER SECURITY** no conjunto de dados CSQINP1 para esse gerenciador de filas.

z/OS *Atualizando a segurança do gerenciador de filas no z/OS*

O IBM MQ for z/OS armazena dados do RACF em cache para melhorar o desempenho. Quando você altera determinadas classes de segurança, deve atualizar essas informações armazenadas em cache. Atualize a segurança com pouca frequência por motivos de desempenho. Também é possível escolher atualizar apenas as informações de segurança TLS.

Quando uma fila é aberta pela primeira vez (ou pela primeira vez desde uma atualização de segurança), o IBM MQ executa uma verificação do RACF para obter os direitos de acesso do usuário e coloca essas informações no cache. Os dados em cache incluem IDs de usuário e recursos nos quais a verificação de segurança foi executada. Se a fila for aberta novamente pelo mesmo usuário, a presença dos dados em cache significa que o IBM MQ não terá de emitir verificações do RACF, o que irá melhorar o desempenho. A ação de uma atualização de segurança é descartar quaisquer informações de segurança em cache e, portanto, forçar o IBM MQ a fazer uma nova verificação com relação ao RACF. Sempre que incluir, mudar ou excluir um perfil de recurso do RACF que é mantida no MQADMIN, MXADMIN, MQPROC, MXPROC, MQQUEUE, MXQUEUE, MQNLIST, MXNLIST ou na classe MXTOPIC, deve-se informar os gerenciadores de filas que usam essa classe para atualizar as informações de segurança que elas contêm. Para fazer isso, emita os comandos a seguir:

- O comando SETROPTS RACLIST(classname) REFRESH do RACF para atualizar no nível do RACF.
- O comando IBM MQ REFRESH SECURITY para atualizar as informações de segurança mantidas pelo gerenciador de filas. Esse comando precisa ser emitido pelo gerenciador de filas que acessa os perfis que foram alterados. Se você tiver um grupo de filas compartilhadas, será possível usar o atributo de escopo de comando para direcionar o comando para todos os gerenciadores de filas no grupo.

  Nota: Se tiver conectado um novo usuário a um grupo existente, será necessário executar o comando IBM MQ RVERIFY SECURITY(userid). O comando REFRESH SECURITY(*) não deixa o gerenciador de filas conectar esse usuário novamente na próxima vez que ele tentar acessar um recurso IBM MQ.

Se você estiver usando perfis genéricos em qualquer uma das classes do IBM MQ, também deve-se emitir atualização normais dos comandos do RACF se você mudar, adicionar ou excluir quaisquer perfis genéricos. Por exemplo, SETROPTS GENERIC(classname) REFRESH.

No entanto, se um perfil de recurso RACF for incluído, alterado ou excluído, e o recurso para o qual ele se aplica ainda não tiver sido acessado (portanto, nenhuma informação está armazenada em cache), o IBM MQ usa as novas informações RACF sem que um comando REFRESH SECURITY seja emitido.

Se a auditoria do RACF estiver ativada, (por exemplo, usando o comando RALTER AUDIT(access-attempt (audit_access_level)) do RACF), nenhum armazenamento em cache ocorre, e, portanto, o IBM MQ irá se referir diretamente ao espaço para dados do RACF para cada verificação. As mudanças são portanto captadas imediatamente e REFRESH SECURITY não é necessário para acessar as mudanças. É possível confirmar se a auditoria do RACF está ligada usando o comando RLIST do RACF. Por exemplo, você poderia emitir o comando

```
RLIST MQQUEUE (qmgr.SYSTEM.COMMAND.INPUT) GEN
```

e receber os resultados

```
CLASS      NAME
-----      ----
MQQUEUE    QP*.SYSTEM.COMMAND.*.** (G)
    AUDITING
    --------
    FAILURES(READ)
```

Isso indica que a auditoria está ligada. Para obter mais informações, consulte o *z/OSSecurity Server RACF Auditor's Guide* e o *z/OS Security Server RACF Command Language Reference*.

A Figura 17 na página 253 resume as situações em que as informações de segurança são armazenadas em cache e em que as informações em cache são usadas.

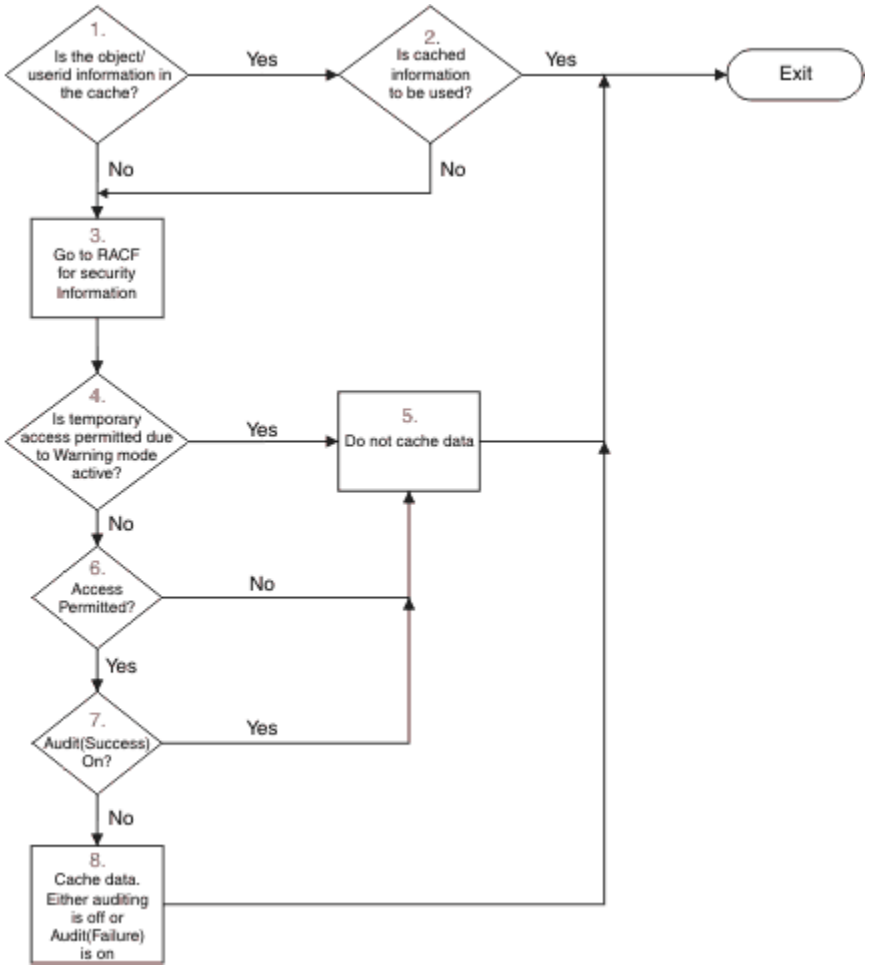


Figura 17. Fluxo Lógico para a segurança do IBM MQ em cache

Se você mudar suas configurações de segurança incluindo ou excluindo perfis do comutador nas classes MQADMIN ou MXADMIN, use um destes comandos para captar essas mudanças dinamicamente:

```
REFRESH SECURITY(*)
REFRESH SECURITY(MQADMIN)
REFRESH SECURITY(MXADMIN)
```

Isso significa que é possível ativar novos tipos de segurança ou desativá-los sem ter que reiniciar o gerenciador de filas.

Por motivos de desempenho, essas são as únicas classes afetadas pelo comando REFRESH SECURITY. Você não precisará usar REFRESH SECURITY se mudar um perfil nas classes MQCONN ou MQCMDS.

Nota: Uma atualização das classes MQADMIN ou MXADMIN não será necessária se um perfil de segurança RESLEVEL for mudado.

Por motivos de desempenho, use REFRESH SECURITY com menor frequência possível, idealmente em horários de menor atividade. É possível minimizar o número de atualizações de segurança conectando os usuários aos grupos RACF que já estão na lista de acesso para os perfis do IBM MQ, em vez de colocar usuários individuais na lista de acesso. Desta maneira, você altera o usuário em vez do perfil de recurso. Também é possível executar RVERIFY SECURITY para o usuário apropriado em vez de atualizar a segurança.

Como um exemplo de REFRESH SECURITY, suponha que você defina os novos perfis para proteger o acesso a filas que iniciam com INSURANCE.LIFE no gerenciador de filas PRMQ. Você usa estes comandos do RACF:

```
RDEFINE MQQUEUE PRMQ.INSURANCE.LIFE.** UACC(NONE)
PERMIT PRMQ.INSURANCE.LIFE.** ID(LIFEGRP) ACCESS(UPDATE)
```

Deve-se emitir o comando a seguir para informar ao RACF para atualizar as informações de segurança que ele mantém, por exemplo:

```
SETROPTS RACLIST(MQQUEUE) REFRESH
```

Como esses perfis são genéricos, deve-se informar ao RACF para atualizar os perfis genéricos para MQQUEUE. Por exemplo:

```
SETROPTS GENERIC(MQQUEUE) REFRESH
```

Em seguida, deve-se usar este comando para informar ao gerenciador PRMQ que os perfis de fila foram mudados:

```
REFRESH SECURITY(MQQUEUE)
```

Atualizando a segurança SSL/TLS

Para atualizar a visualização em cache do repositório de chaves TLS, emita o comando REFRESH SECURITY com a opção TYPE(SSL). Isso permite atualizar algumas de suas configurações do TLS sem precisar reiniciar o inicializador de canais.

z/OS *Exibindo o Status de Segurança*

Para exibir o status dos comutadores de segurança e outros controles de segurança, emita o comando MQSC DISPLAY SECURITY.

A figura a seguir mostra a saída típica do comando 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
```

Figura 18. Saída Típica do Comando DISPLAY SECURITY

O exemplo mostra que o gerenciador de filas que respondeu ao comando possui o subsistema, o comando, o usuário alternativo, o processo, a lista de nomes e a segurança da fila ativos no nível do gerenciador de filas, mas não no nível do grupo de filas compartilhadas. A segurança de conexão, recurso de comando e contexto não estão ativas. Também mostra que os tempos limites de ID do usuário estão ativos e que, a cada 12 minutos, o gerenciador de filas verifica os IDs de usuário que não foram usados nesse gerenciador de filas durante 54 minutos e os remove.

Nota: Esse comando mostra o status de segurança atual. Ele não necessariamente reflete o status atual dos perfis do comutador definidas para o RACF ou o status das classes do RACF. Por exemplo, os perfis do comutador podem ter sido alterados desde a última reinicialização desse gerenciador de filas ou comando REFRESH SECURITY.

z/OS Tarefas de instalação de segurança para o z/OS

Após a instalação e customização do IBM MQ, autorize os procedimentos de tarefa iniciada para RACF, autorize o acesso a vários recursos e configure as definições do RACF. Opcionalmente, configure seu sistema para TLS.

Quando o IBM MQ for instalado e customizado pela primeira vez, deve-se executar estas tarefas relacionadas à segurança:

1. Configure o conjunto de dados do IBM MQ e a segurança do sistema por:
   - Autorizando o procedimento de tarefa iniciada xxxxMSTR do gerenciador de filas e o procedimento de tarefa iniciada xxxxCHIN do enfileiramento distribuído para executar no RACF.
   - Autorizando o acesso aos conjuntos de dados do gerenciador de filas.
   - Autorizando o acesso a recursos para os IDs de usuário que usarão o gerenciador de filas e os programas utilitários.
   - Autorizando o acesso para os gerenciadores de filas que usarão as estruturas de lista do recurso de acoplamento.
   - Autorizando o acesso para os gerenciadores de filas que usarão o Db2.
2. Configure as definições do RACF para a segurança do IBM MQ.
3. Se você desejar usar Segurança da Camada de Transporte (TLS), prepare seu sistema para usar certificados e chaves.

z/OS *Configurando a segurança do conjunto de dados do IBM MQ for z/OS*

Existem vários tipos de usuário do IBM MQ. Use o RACF para controlar seu acesso aos conjuntos de dados do sistema.

Os usuários possíveis de conjuntos de dados do IBM MQ incluem as entidades a seguir:

- O próprio gerenciador de filas.
- O Inicializador de Canais
- Administradores do IBM MQ, que precisam criar conjuntos de dados do IBM MQ, executar programas utilitários e tarefas semelhantes.
- Os programadores de aplicativos que precisam usar os copybooks fornecidos pelo IBM MQ, incluir conjuntos de dados, macros e recursos semelhantes.
- Aplicativos envolvendo um ou mais destes:
  - Tarefas em Lote
  - Usuários do TSO
  - Regiões do CICS
  - Regiões do IMS
- Conjuntos de dados CSQOUTX e CSQSNAP
- Filas dinâmicas SYSTEM.CSQXCMD.*

Para todos estes usuários potenciais, proteja os conjuntos de dados do IBM MQ com o RACF.

Também deve-se controlar o acesso a todas os seus conjuntos de dados 'CSQINP'.

z/OS *Autorização do RACF de procedimentos de tarefa iniciada*

Alguns conjuntos de dados do IBM MQ são para uso exclusivo do gerenciador de filas. Se você protege os seus conjuntos de dados do IBM MQ usando o RACF, também deve-se autorizar o procedimento

de tarefa iniciada xxxxMSTR do gerenciador de filas e o procedimento de tarefa iniciada xxxxCHIN do enfileiramento distribuído, usando o RACF. Para fazer isso, use a classe STARTED. Como alternativa, é possível usar a tabela de procedimentos iniciados (ICHRIN03), mas deve-se executar um IPL no sistema z/OS para que as mudanças entrem em vigor.

Para obter mais informações, veja o *z/OS Security Server RACF: Guia do Programador de sistema*.

O ID do usuário do RACF identificado deve ter o acesso necessário para os conjuntos de dados no procedimento de tarefa iniciada. Por exemplo, se você associar um procedimento da tarefa iniciada do gerenciador de filas chamado CSQ1MSTR com o ID do usuário do RACF QMGRCSQ1, o ID do usuário QMGRCSQ1 deve ter acesso aos recursos do z/OS acessados pelo gerenciador de filas CSQ1.

Além disso, o conteúdo do campo GROUP no ID do usuário do gerenciador de filas deve ser igual ao conteúdo do campo GROUP no perfil STARTED para esse gerenciador de filas. Se o conteúdo em cada campo GROUP não corresponder, o ID do usuário apropriado será impedido de entrar no sistema. Esta situação faz com que o IBM MQ execute com um ID do usuário indefinido e, consequentemente, feche devido a uma violação de segurança.

Os IDs do usuário do RACF associados aos procedimentos de tarefa iniciada do gerenciador de filas e do inicializador de canais não devem ter o conjunto de atributos TRUSTED.

z/OS *Autorizando o Acesso aos Conjuntos de Dados*

Os conjuntos de dados do IBM MQ devem ser protegidos para que nenhum usuário não autorizado possa executar uma instância do gerenciador de filas ou obter acesso a qualquer dado do gerenciador de filas. Para fazer isso, use a proteção normal do conjunto de dados do z/OS RACF.

Tabela 65 na página 256 resume o acesso do RACF que o procedimento da tarefa iniciada do gerenciador de filas deve ter para os diferentes conjuntos de dados.

Tabela 65. acesso do RACF aos conjuntos de dados associados a um gerenciador de filas

Acesso do RACF	**Conjuntos de dados**
READ	• `thlqual.SCSQAUTH` e `thlqual.SCSQANLx` (em que x é a letra do idioma para o seu idioma nacional) • Os conjuntos de dados referidos por CSQINP1, CSQINP2 e CSQXLIB no procedimento de tarefa iniciada do gerenciador de filas. • Conjuntos de dados do SMDS pertencentes a outros gerenciadores de filas no grupo • Log, BSDS e conjuntos de dados de log de archive para outros gerenciadores de filas no grupo
ATUALIZAÇÃO	• Todos os conjuntos de páginas e conjuntos de dados do log e do BSDS. • Conjuntos de dados SMDS pertencentes a um gerenciador de filas
ALTER	• Todos os conjuntos de dados de log de archive.

Tabela 66 na página 257 resume o acesso do RACF que o procedimento de tarefa iniciada para enfileiramento distribuído deve ter para os diferentes conjuntos de dados.

Tabela 66. acesso do RACF aos conjuntos de dados associados com enfileiramento distribuído	
Acesso do RACF	**Conjuntos de dados**
READ	• thlqual.SCSQAUTH, thlqual.SCSQANLx (em que x é a letra de idioma para seu idioma nacional) e thlqual.SCSQMVR1. • Conjuntos de dados da biblioteca LE. • Os conjuntos de dados referidos por CSQXLIB e CSQINPX no procedimento de tarefa iniciada pelo iniciador de canal..
ATUALIZAÇÃO	• Conjuntos de dados CSQOUTX e CSQSNAP

Para obter mais informações, consulte o *z/OS Security Server RACF Security Administrator's Guide*.

V 9.1.4 z/OS *Criptografando conjuntos de dados*

Os conjuntos de dados do IBM MQ podem ser criptografados com a criptografia do conjunto de dados do z/OS, de forma que os dados sejam protegidos ou por motivos de regulamentação.

É possível proteger todos os conjuntos de páginas, o log ativo, o log de archive e os conjuntos de dados de autoinicialização (BSDS) com a criptografia do conjunto de dados do z/OS.

Atenção: Não é possível proteger conjuntos de dados de mensagens compartilhadas (SMDS) com a criptografia do conjunto de dados do z/OS pelo IBM MQ for z/OS 9.1.3 ou anterior.

Consulte a seção Confidencialidade para dados em repouso no IBM MQ for z/OS com criptografia do conjunto de dados. para obter informações adicionais.

z/OS *Configurando a segurança do recurso do IBM MQ for z/OS*

Existem vários tipos de usuário do IBM MQ. Use o RACF para controlar o acesso aos recursos do IBM MQ.

Os usuários possíveis dos recursos do IBM MQ, como filas e canais incluem as seguintes entidades:

- O próprio gerenciador de filas.
- O Inicializador de Canais
- Administradores do IBM MQ, que precisam criar conjuntos de dados do IBM MQ, executar programas utilitários e tarefas semelhantes
- Os programadores de aplicativos que precisam usar os copybooks fornecidos pelo IBM MQ, incluir conjuntos de dados, macros e recursos semelhantes.
- Aplicativos envolvendo um ou mais destes:
  - Tarefas em Lote
  - Usuários do TSO
  - Regiões do CICS
  - Regiões do IMS
- Conjuntos de dados CSQOUTX e CSQSNAP
- Filas dinâmicas SYSTEM.CSQXCMD.*

Para todos estes usuários potenciais, proteja os recursos do IBM MQ com o RACF. Em particular, observe que o inicializador de canais precisa de acesso a vários recursos, conforme descrito em “Considerações sobre segurança para o inicializador de canais no z/OS” na página 264, portanto, o ID do usuário sob o qual ele é executado deve estar autorizado a acessar esses recursos.

Se você estiver usando um grupo de filas compartilhadas, o gerenciador de filas poderá emitir vários comandos internamente, portanto, o ID do usuário que ele usa deve estar autorizado a emitir tais comandos. Os comandos são:

- DEFINE, ALTER e DELETE para cada objeto que possui QSGDISP(GROUP)

- START e STOP CHANNEL para cada canal usado com CHLDISP(SHARED)

z/OS *Configurando seu sistema z/OS para usar TLS*

Use este tópico como exemplo de como configurar o IBM MQ for z/OS com a Segurança da Camada de Transporte (TLS) usando comandos RACF.

Caso deseje usar TLS para segurança de canal, há várias tarefas que precisam ser executadas no sistema. (Para obter detalhes sobre como usar os comandos do RACF para certificados e repositórios de chaves (conjuntos de chaves), veja Trabalhando com TLS no z/OS .)

1. Crie um conjunto de chaves em RACF para reter todas as chaves e certificados para seu sistema, usando o comando RACDCERT do RACF. Por exemplo:

   ```
   RACDCERT ID(CHINUSER) ADDRING(QM1RING)
   ```

   O ID deve ser o ID do usuário do espaço de endereço do inicializador de canal ou o ID do usuário que possuirá o conjunto de chaves, se ele deve ser um conjunto de chaves compartilhado.

2. Crie um certificado digital para cada gerenciador de filas, usando o comando RACDCERT do RACF.

   O rótulo do certificado deve ser o valor do atributo IBM MQ **CERTLABL** , se ele estiver configurado, ou o padrão `ibmWebSphereMQ` com o nome do gerenciador de filas ou grupo de filas compartilhadas anexado. Consulte Rótulos de certificado digital para obter detalhes. Neste exemplo, é `ibmWebSphereMQQM1`.

   Por exemplo:

   ```
   RACDCERT ID(USERID) GENCERT
   SUBJECTSDN(CN('username') O('IBM') OU('departmentname') C('England'))
   WITHLABEL('ibmWebSphereMQQM1')
   ```

3. Conecte o certificado no RACF para o conjunto de chaves, usando o comando RACDCERT do RACF. Por exemplo:

   ```
   RACDCERT CONNECT(ID(USERID) LABEL('ibmWebSphereMQQM1') RING(QM1RING))
   CONNECT ID(CHINUSER)
   ```

   Também é necessário conectar quaisquer certificados de assinante relevantes (de uma autoridade de certificação) para o conjunto de chaves. Isto é, todas as autoridades de certificação para o certificado TLS desse gerenciador de filas e todas as autoridades de certificação para todos os certificados TLS com os quais esse gerenciador de filas se comunica. Por exemplo:

   ```
   RACDCERT ID(CHINUSER)
   CONNECT(CERTAUTH LABEL('My CA') RING(QM1RING) USAGE(CERTAUTH))
   ```

4. Em cada um de seus gerenciadores de filas, use o comando ALTER QMGR do IBM MQ para especificar o repositório de chaves para o qual o gerenciador de filas precisa apontar. Por exemplo, se o conjunto de chaves for possuído pelo espaço de endereço do inicializador de canal:

   ```
   ALTER QMGR SSLKEYR(QM1RING)
   ```

ou se você estiver usando um conjunto de chaves compartilhado:

```
ALTER QMGR SSLKEYR(userid/QM1RING)
```

em que *userid* é o ID do usuário que possui o conjunto de chaves compartilhado.

5. As CRLs (listas de revogação de certificado) permitem que as autoridades de certificação revoguem certificados que não podem mais ser confiáveis. As CRLs são armazenadas em servidores LDAP. Para acessar essa lista no servidor LDAP, primeiro é necessário criar um objeto AUTHINFO do AUTHTYPE CRLLDAP, usando o comando DEFINE AUTHINFO do IBM MQ. Por exemplo:

```
DEFINE AUTHINFO(LDAP1)
AUTHTYPE(CRLLDAP)
CONNAME(ldap.server(389))
LDAPUSER('')
LDAPPWD('')
```

Neste exemplo, a lista de revogação de certificado é armazenada em uma área pública do servidor LDAP, portanto, os campos LDAPUSER e LDAPPWD não são necessários.

Em seguida, coloque seu objeto AUTHINFO em uma lista de nomes, usando o comando DEFINE NAMELIST do IBM MQ. Por exemplo:

```
DEFINE NAMELIST(LDAPNL) NAMES(LDAP1)
```

Por último, associe a lista de nomes com cada gerenciador de filas, usando o comando ALTER QMGR do IBM MQ. Por exemplo:

```
ALTER QMGR SSLCRLNL(LDAPNL)
```

6. Configure seu gerenciador de filas para executar chamadas TLS, usando o comando ALTER QMGR do IBM MQ. Isso define subtarefas do servidor que manipulam apenas chamadas SSL, o que deixa os dispatchers normais continuarem o processamento normalmente sem serem afetados por quaisquer chamadas SSL. Você deve ter pelo menos duas dessas subtarefas. Por exemplo:

```
ALTER QMGR SSLTASKS(8)
```

Essa mudança só entra em vigor quando o inicializador de canais é reiniciado.

7. Especifique a especificação de criptografia a ser usada para cada canal, usando o comando DEFINE CHANNEL ou ALTER CHANNEL do IBM MQ. Por exemplo:

```
ALTER CHANNEL(LDAPCHL)
CHLTYPE(SDR)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

Ambas as extremidades do canal devem especificar a mesma especificação de código.

z/OS Gerenciando registros de autenticação de canal em um QSG

Os registros de autenticação de canal se aplicam ao gerenciador de filas no qual eles são criados, eles não são compartilhados em todo o grupo de filas compartilhadas (QSG). Portanto, se todos os gerenciadores de filas no grupo de compartilhamento de fila devem ter as mesmas regras, algum gerenciamento precisa ser realizado para manter todas as regras consistentes.

1. Sempre inclua a opção `CMDSCOPE(*)` para todos os comandos `SET CHLAUTH`. Isso enviará o comando para todos os gerenciadores de filas em execução no grupo de filas compartilhadas
2. Use o comando `DISPLAY CHLAUTH` com a opção `CMDSCOPE(*)` e, em seguida, analisar as respostas para ver se os registros são os mesmos de todos os gerenciadores de filas. Quando uma inconsistência é localizada, um comando `SET CHLAUTH` pode ser emitido contendo a mesma regra com `CMDSCOPE(*)` ou `CMDSCOPE(`*qmgr-name*`)`
3. Inclua um membro na concatenação CSQINP2 do gerenciador de filas (consulte Comandos de inicialização para obter detalhes) que possui o conjunto completo de regras. Elas serão lidas como parte do processo de inicialização do gerenciador de filas. Se o comando `SET CHLAUTH` usar `ACTION(ADD)`, a regra será apenas incluída se ela não existir. Usar o `ACTION(REPLACE)` substituirá uma regra existente se ela já existir ou a incluirá se ela não existir. O mesmo membro poderia, então, ser colocado na concatenação CSQINP2 de todos os gerenciadores de filas no grupo de filas compartilhadas.
4. Use o utilitário CSQUTIL (consulte Emitindo comandos para IBM MQ (COMMAND) para obter detalhes) para extrair as regras de um gerenciador de filas usando as opções `MAKEDEF` ou `MAKEREP`. Em seguida, reproduza a saída usando CSQUTIL para o gerenciador de filas de destino.

Conceitos relacionados

Registros de Autenticação de Canal

Para exercer um controle mais preciso sobre o acesso concedido à conexão de sistemas em um nível de canal, é possível usar registros de autenticação de canal.

z/OS Considerações de auditoria no z/OS

Os controles de auditoria normais do RACF estão disponíveis para realizar uma auditoria de segurança de um gerenciador de filas. O IBM MQ não reúne quaisquer estatísticas de segurança sozinho. As únicas estatísticas são aqueles que podem ser criadas por auditoria.

A auditoria do RACF pode ser baseada em:

- IDs de Usuário
- Classes de recurso
- Perfis

Para obter mais detalhes, veja o *z/OS Security Server RACF Auditor's Guide*.

Nota: A auditoria degrada o desempenho; quando mais auditoria você implementa, mais desempenho é degradado. Essa também é uma consideração para uso da opção WARNING do RACF.

z/OS *RESLEVEL de Auditoria*

Use o parâmetro do sistema RESAUDIT para controlar a produção de registros de auditoria de RESLEVEL. Registros de auditoria GENERAL do RACF são produzidos.

Produza registros de auditoria de RESLEVEL configurando o parâmetro do sistema RESAUDIT para YES. Se o parâmetro RESAUDIT for configurado para NO, os registros de auditoria não serão produzidos. Para obter mais detalhes sobre a configuração desse parâmetro, consulte Usando CSQ6SYSP.

Se RESAUDIT estiver configurado YES, nenhum registro de auditoria normal do RACF serão tomados quando a verificação RESLEVEL for feita para ver qual acesso um ID do usuário do espaço de endereço tem para o perfil hlq.RESLEVEL. Em vez disso, o IBM MQ solicita que o RACF crie um registro de auditoria GENERAL (número do evento 27). Essas verificações são executadas apenas de saída no tempo de conexão, portanto, o custo de desempenho é mínimo.

É possível relatar os registros de auditoria gerais do IBM MQ usando o relator do RACF (RACFRW). É possível usar os comandos RACFRW a seguir para relatar o acesso RESLEVEL:

```
RACFRW
SELECT PROCESS
EVENT GENERAL
LIST
END
```

Um relatório de amostra do RACFRW, excluindo os campos *Date*, *Time*e *SYSID* , é mostrado em Figura 19 na página 261

```
       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
```

Figura 19. Saída de Amostra de RACFRW Mostrando Registros de Auditoria Gerais de RESLEVEL

Ao verificar os dados LOGSTR nessa saída de amostra, é possível ver que o usuário WS21B do TSO tem acesso de CONTROL para o QM66.RESLEVEL. Isso significa que é efetuado bypass de todas as verificações de segurança do recurso quando o usuário WS21B acessa recursos QM66.

Para obter mais informações sobre o uso de RACFRW, consulte o *Guia do auditor do servidor de segurança do z/OSRACF*.

z/OS Customizando a Segurança

Se desejar mudar como a segurança do IBM MQ opera, deve-se fazer isso por meio da saída de SAF (ICHRFR00) ou saídas em seu gerenciador de segurança externa.

Para saber mais sobre as saídas do RACF, consulte o manual *z/OS Referência de macro RACROUTE do servidor de segurança* .

Nota: Como o IBM MQ otimiza as chamadas para o ESM, as solicitações de RACROUTE podem não ser feitas, por exemplo, a cada abertura para uma fila específica por um determinado usuário.

z/OS Mensagens de violação de segurança no z/OS

Uma violação de segurança é indicada pelo código de retorno MQRC_NOT_AUTHORIZED em um programa de aplicativo ou por uma mensagem no log da tarefa.

Um código de retorno de MQRC_NOT_AUTHORIZED pode ser retornado a um programa de aplicativo pelos motivos a seguir:

- Um usuário não é permitido conectar-se ao gerenciador de filas. Neste caso, você obtém uma mensagem ICH408I no log Batch/TSO, CICS ou log da tarefa do IMS.
- Uma conexão do usuário com o gerenciador de filas falhou porque, por exemplo, o ID do usuário da tarefa não é válido ou apropriado ou o ID do usuário da tarefa ou ID do usuário alternativo não é válido. Um ou mais desses IDs de usuário podem não ser válidos porque foram revogados ou excluídos. Neste

caso, você obtém uma mensagem ICHxxxx e possivelmente uma mensagem IRRxxxx no log da tarefa do gerenciador de filas que fornece o motivo para a falha da conexão. Por exemplo:

```
ICH408I USER(NOTDFND ) GROUP(        ) NAME(???                 )
  LOGON/JOB INITIATION - USER AT TERMINAL          NOT RACF-DEFINED
IRR012I  VERIFICATION FAILED. USER PROFILE NOT FOUND
```

- Um usuário alternativo foi solicitado, mas o ID do usuário da tarefa não possui acesso ao ID do usuário alternativo. Para essa falha, você obtém uma mensagem de violação no log da tarefa do gerenciador de filas relevante.
- Uma opção de contexto foi usada ou é deduzida abrindo uma fila de transmissão para saída, mas o ID do usuário da tarefa ou, onde aplicável, o ID do usuário da tarefa ou alternativo não possui acesso à opção de contexto. Neste caso, uma mensagem de violação é colocada no log da tarefa do gerenciador de filas relevante.
- Um usuário não autorizado tentou acessar um objeto de gerenciador de filas protegido, por exemplo, uma fila. Neste caso, uma mensagem ICH408I para a violação é colocada no log da tarefa do gerenciador de filas relevante. Essa violação pode ser devido à tarefa ou, quando aplicável, ao ID do usuário da tarefa ou alternativo.

As mensagens de violação para a segurança de comando e a segurança do recurso de comando também podem ser localizadas no log da tarefa do gerenciador de filas.

Se a mensagem de violação ICH408I mostrar o nome da tarefa do gerenciador de filas em vez de um ID do usuário, este é normalmente o resultado da especificação de um ID do usuário alternativo em branco. Por exemplo:

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          INSUFFICIENT ACCESS AUTHORITY
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

É possível descobrir quem tem permissão para usar IDs de usuário alternativos em branco verificando a lista de acesso do perfil MQADMIN hlq.ALTERNATE.USER.-BLANK-.

Uma mensagem de violação ICH408I também pode ser gerada por:

- Um comando sendo enviado para a fila de entrada de comando do sistema sem contexto. Os programas gravados pelo usuário que gravam na fila de entrada de comando do sistema sempre devem usar uma opção de contexto. Para obter informações adicionais, consulte “Perfis para Segurança de Contexto” na página 218.
- Quando a tarefa acessando o recurso do IBM MQ não tem um ID do usuário associado a ele ou quando um adaptador do IBM MQ não pode extrair o ID do usuário do ambiente do adaptador.

As mensagens de violação também podem ser emitidas se você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas. Talvez você receba mensagens indicando que nenhum perfil foi encontrado no nível do gerenciador de filas, mas ainda receba acesso devido a um perfil de nível do grupo de filas compartilhadas.

```
ICH408I JOB(MQS1MSTR) STEP(MQS1MSTR)
          MQS1.PAYROLL.REQUEST CL(MQQUEUE)
          PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
          ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

z/OS O que Fazer se o Acesso For Permitido ou Desaprovado Incorretamente

Além das etapas detalhadas no *z/OS Security Server RACF Security Administrator's Guide*, use esta lista de verificação se o acesso a um recurso parece estar controlado incorretamente.

- Os perfis do comutador estão configurados corretamente?
  - O RACF está ativo?
  - As classes do IBM MQ RACF estão instaladas e ativas?

    Use o comando do RACF, SETROPTS LIST, para verificar isso.
  - Use o comando DISPLAY SECURITY IBM MQ para exibir o status do comutador atual do gerenciador de filas.
  - Verifique os perfis do comutador na classe MQADMIN.

    Use os comandos SEARCH e RLIST do RACF para isso.
  - Verifique novamente os perfis do comutador do RACF emitindo o comando REFRESH SECURITY(MQADMIN) do IBM MQ.
- O perfil de recurso do RACF foi mudado? Por exemplo, o acesso universal no perfil foi alterado ou a lista de acesso do perfil foi alterada?
  - O perfil é genérico?

    Se for, emita o comando SETROPTS GENERIC(classname) REFRESH do RACF.
  - Você atualizou a segurança neste gerenciador de filas?

    Se necessário, emita o comando SETROPTS RACLIST(classname) REFRESH do RACF.

    Se necessário, emita o comando IBM MQ REFRESH SECURITY(*).
- A definição de usuário do RACF foi mudada? Por exemplo, o usuário foi conectado a um novo grupo ou a autoridade de acesso de usuário foi revogada?
  - Você verificou novamente o usuário emitindo o comando RVERIFY SECURITY(userid) do IBM MQ?
- Está sendo efetuado bypass das verificações em razão do RESLEVEL?
  - Verifique o acesso do ID do usuário de conexão para o perfil RESLEVEL. Use os registros de auditoria do RACF para determinar para o qual o RESLEVEL está configurado.
  - Para canais, lembre-se de que o nível de acesso que o ID do usuário do inicializador de canais tem para o RESLEVEL é herdado por todos os canais, portanto, um nível de acesso, como ALTER, que causa bypass de todas as verificações faz com que seja efetuado bypass de verificações de segurança para todos os canais.
  - Se você estiver executando a partir do CICS, verifique a configuração de RESSEC da transação.
  - Se o RESLEVEL tiver sido alterado enquanto um usuário estiver conectado, será necessário desconectar e reconectar para que a nova configuração RESLEVEL entre em vigor.
- Você está utilizando grupos de filas compartilhadas?
  - Se você estiver usando a segurança no nível do grupo de filas compartilhadas e do gerenciador de filas, verifique se você definiu todos os perfis corretos. Se o perfil do gerenciador de filas não estiver definido, uma mensagem será enviada ao log informando que o perfil não foi localizado.
  - Você usou uma combinação de configurações do comutador que não é válida de modo que a verificação de segurança integral foi configurada como ligada?
  - Você precisa definir os comutadores de segurança para substituir algumas das configurações do grupo de filas compartilhadas para seu gerenciador de filas?
  - O perfil de nível do gerenciador de filas está tendo precedência sobre um perfil de nível do grupo de filas compartilhadas?

z/OS Considerações sobre segurança para o inicializador de canais no z/OS

Se você estiver usando a segurança do recurso em um ambiente de enfileiramento distribuído, o espaço de endereço do inicializador de canais precisa de acesso apropriado para vários recursos do IBM MQ. É possível usar o Integrated Cryptographic Support Facility (ICSF) para iniciar o algoritmo de proteção de senha.

Usando a segurança do recurso

Se você estiver usando a segurança do recurso, considere os pontos a seguir se estiver usando enfileiramento distribuído:

Filas do sistema
O espaço de endereço do inicializador de canais precisa do acesso UPDATE RACF às filas do sistema listadas em "Segurança da Fila do Sistema" na página 207 e para todas as filas de destino do usuário e a fila de mensagens não entregues (mas consulte "Segurança da Fila de Devoluções" na página 205).

Filas de transmissão
O espaço de endereço do inicializador de canais precisa de acesso ALTER para todas as filas de transmissão do usuário.

Segurança de contexto
O ID do usuário do canal (e o ID do usuário do MCA se um foi especificado) precisa de acesso CONTROL do RACF para os perfis hlq.CONTEXT.queuename na classe MQADMIN. Dependendo do perfil RESLEVEL, o ID do usuário do canal pode também precisar de acesso CONTROL para esses perfis.

Todos os canais precisam de acesso CONTROL para o perfil de fila de devoluções MQADMIN hlq.CONTEXT . Todos os canais (iniciando ou respondendo) podem gerar relatórios e, consequentemente, eles precisam de acesso CONTROL para o perfil hlq.CONTEXT.reply-q.

Os canais SENDER, CLUSSDR e SERVER precisam de acesso CONTROL para os perfis hlq.CONTEXT.xmit-queue-name, uma vez que mensagens podem ser colocadas na fila de transmissão para ativar o canal para terminar progressivamente.

Nota: Se o ID do usuário do canal, ou um grupo de RACF ao qual o ID do usuário do canal será conectado, tem acesso CONTROL ou ALTER para o hlq.RESLEVEL, então não há verificações de recurso para o inicializador de canais ou qualquer um de seus canais.

Consulte "Perfis para Segurança de Contexto" na página 218 "RESLEVEL e a Conexão do Inicializador de Canais" na página 237 e "IDs de usuário para verificação de segurança no z/OS" na página 239 para obter informações adicionais.

CSQINPX
Se você estiver usando o conjunto de dados de entrada CSQINPX, o inicializador de canais também precisará de acesso READ para o CSQINPX e acesso UPDATE para o conjunto de dados CSQOUTX e filas dinâmicas SYSTEM.CSQXCMD.*.

Segurança de Conexão
As solicitações de conexão do espaço de endereço do inicializador de canais usam um tipo de conexão CHIN, para o qual a segurança de acesso apropriada deve ser configurada; consulte "Perfis de Segurança de Conexão para o Inicializador de Canais" na página 199.

Conjuntos de dados
O espaço de endereço do inicializador de canais precisa de acesso apropriado para conjuntos de dados do gerenciador de filas; consulte "Autorizando o Acesso aos Conjuntos de Dados" na página 256.

Comandos
Os comandos de enfileiramento distribuído (por exemplo, DEFINE CHANNEL, START CHINIT, START LISTENER e outros comandos do canal) devem ter a segurança de comando apropriada configurada; consulte a Tabela 49 na página 221.

Se você estiver usando um grupo de filas compartilhadas, o inicializador de canais poderá emitir vários comandos internamente, portanto, o ID do usuário que ele usar deverá estar autorizado a emitir tais comandos. Esses comandos são START e STOP CHANNEL para cada canal usado com CHLDISP(SHARED).

Se o PSMODE do gerenciador de filas não for DISABLED, o inicializador de canais deverá ter acesso READ para o comando DISPLAY PUBSUB.

Segurança de canal

Os canais, particularmente receptores e conexões do servidor, precisam de segurança apropriada para serem configurados; consulte "IDs de usuário para verificação de segurança no z/OS" na página 239 para obter informações adicionais.

Também é possível usar o protocolo Segurança da Camada de Transporte (TLS) para fornecer segurança em canais. Veja "Protocolos de segurança TLS no IBM MQ" na página 24 para obter mais informações sobre como usar o TLS com o IBM MQ.

Consulte também "Controle de acesso para clientes" na página 98 para obter informações sobre a segurança da conexão do servidor.

IDs de Usuário

Os IDs de usuário descritos em "IDs de Usuário Usados pelo Inicializador de Canais" na página 243 e "IDs de Usuário Usados pelo Agente de Enfileiramento Intragrupo" na página 247 precisam do acesso a seguir:

- Acesso UPDATE do RACF às filas de destino apropriado e a fila de mensagens não entregues
- Acesso CONTROL RACF ao perfil `hlq.CONTEXT.queuename` se a verificação de contexto é executada no receptor
- Acesso apropriado para os perfis hlq.ALTERNATE.USER.userid que eles podem precisar usar.
- Para clientes, o acesso apropriado do RACF aos recursos a serem usados.

segurança de APPC

Configure a segurança do APPC se você estiver usando o protocolo de transmissão LU 6.2. (Use a classe APPCLU do RACF por exemplo.) Para obter informações sobre a configuração de segurança para APPC, consulte os manuais a seguir:

- *z/OS V1R2.0 Planejamento de MVS: Gerenciamento APPC*
- *Guia de configuração APPC de Multiplataforma*, uma publicação IBM Redbooks

As transmissões de saída usam a opção APPC "SECURITY(SAME)". Como resultado, o ID do usuário do espaço de endereço do inicializador de canais e seu perfil padrão (RACF GROUP) fluem através da rede para o receptor com um indicador de que o ID do usuário já foi verificado (ALREADYV).

Se o lado de recebimento também é z/OS, o ID do usuário e perfil são verificados por APPC e o ID do usuário é apresentado ao canal receptor e usado como o ID do usuário do canal.

Em um ambiente no qual o gerenciador de filas está usando o APPC para se comunicar com outro gerenciador de filas no mesmo ou em outro sistema z/OS, é preciso garantir que o:

- A definição VTAM para a LU de comunicação especifica SETACPT(ALREADYV)
- Há um perfil APPCLU do RACF para a conexão entre LUs que especifica CONVSEC(ALREADYV)

Alterando Definições de Segurança

Se o nível de acesso do RACF que o ID do usuário do canal ou ID do usuário MCA tem para uma fila de destino for mudado, esta mudança entrará em vigor somente para novas manipulações de objeto (ou seja, novos `MQOPEN` s) para a fila de destino. As vezes em que os MCAs abrem e fecham as filas são variáveis; se um canal já estiver em execução quando uma mudança de acesso for feita, o MCA poderá continuar a colocar mensagens na fila de destino usando o acesso de segurança existente dos IDs de usuário em vez do acesso de segurança atualizado. Parar e reiniciar os canais para impingir o nível de acesso atualizado evita esse cenário.

Reinício automático
Se você estiver usando o z/OS Automatic Restart Manager (ARM) para reiniciar o inicializador de canais, o ID do usuário associado ao espaço de endereço XCFAS deve estar autorizado a emitir o comando START CHINIT do IBM MQ.

Usando o Integrated Cryptographic Service Facility (ICSF)

O inicializador de canais poderá usar o ICSF para gerar um número aleatório ao criar um valor inicial do algoritmo de proteção de senha para ofuscar as senhas que fluem por meio de canais de cliente, se o TLS não estiver sendo usado. O processo de gerar um número aleatório é chamado *entropia*.

Se você tiver o recurso z/OS instalado, mas não tiver iniciado o ICSF, você verá a mensagem CSQX213E e o inicializador de canais usará STCK para entropia.

A mensagem CSQX213E avisa que o algoritmo de proteção de senha não é tão seguro quanto poderia ser. No entanto, é possível continuar seu processo; não há outro impacto no tempo de execução.

Se você não tiver o recurso z/OS instalado, o inicializador de canais usará STCK automaticamente.

Notes:

1. Usar ICSF para entropia gera mais sequências aleatórias do que usar STCK.
2. Se você iniciar ICSF deve-se reiniciar o inicializador de canais.
3. ICSF é necessário para alguns CipherSpecs. Se você tentar usar um desses CipherSpecs e você não tiver o ICSF instalado, você receberá uma mensagem CSQX629E.

z/OS Segurança em clusters de gerenciadores de filas no z/OS

Considerações de segurança para os clusters são as mesmas para gerenciadores de filas e canais que não estão em cluster. O inicializador de canais precisa de acesso para algumas filas do sistema adicionais e alguns comandos adicionais precisam de um conjunto de segurança apropriado.

É possível usar o ID do usuário do MCA, registros de autenticação de canal, TLS e saídas de segurança para autenticar canais do cluster (como com canais convencionais). Os registros de autenticação de canal ou saída de segurança relacionados ao canal do receptor de clusters devem verificar se o gerenciador de filas remotas é permitido o acesso a filas de cluster do gerenciador de filas do servidor. É possível começar a usar o suporte de cluster IBM MQ sem mudar sua segurança da fila de acesso existente. Deve-se, no entanto, permitir que outros gerenciadores de filas no cluster gravem no SYSTEM.CLUSTER.COMMAND.QUEUE se eles forem unir o cluster.

O suporte de cluster do IBM MQ não fornece um mecanismo para limitar um membro de um cluster para somente a função do cliente. Como resultado, você deve ter certeza de confiar em quaisquer gerenciadores de filas que sejam permitidos no cluster. Se algum gerenciador de filas no cluster criar uma fila com um nome específico, ele poderá receber mensagens para essa fila, independentemente se o aplicativo que coloca mensagens nessa fila deseja isso ou não.

Para restringir a associação de um cluster, tome a mesma ação que você tomaria para evitar que gerenciadores de filas se conectem a canais receptores. É possível restringir a associação de um cluster usando registros de autenticação de canal ou gravando um programa de saída de segurança no canal receptor. Também é possível gravar um programa de saída para evitar que gerenciadores de filas não autorizados gravem no SYSTEM.CLUSTER.COMMAND.QUEUE.

Nota: Não é aconselhável permitir que aplicativos abram o SYSTEM.CLUSTER.TRANSMIT.QUEUE diretamente. Também não é aconselhável permitir que um aplicativo abra qualquer outra fila de transmissão diretamente.

Se você estiver usando a segurança do recurso, considere os seguintes pontos além das considerações contidas em “Considerações sobre segurança para o inicializador de canais no z/OS” na página 264:

Filas do sistema
O inicializador de canais precisa do acesso ALTER do RACF às seguintes filas do sistema:

- SYSTEM.CLUSTER.COMMAND QUEUE

- SYSTEM.CLUSTER.TRANSMIT.QUEUE.

e acesso UPDATE para SYSTEM.CLUSTER.REPOSITORY.QUEUE

Também precisa de acesso READ para quaisquer listas de nomes usadas para armazenamento em cluster.

Comandos

Configure a segurança de comando apropriada (conforme descrito em Tabela 49 na página 221) para os comandos de suporte de cluster (REFRESH e RESET CLUSTER, SUSPEND e RESUME QMGR).

z/OS Considerações de segurança para usar o IBM MQ com o CICS

Todas as versões do CICS suportadas pelo IBM MQ 9.0.0 e mais recente usam a versão fornecida pelo CICS do adaptador e ponte.

Para obter detalhes de considerações de segurança, veja:

- Segurança do adaptador CICS/IBM MQ.
- Segurança da ponte CICS/IBM MQ.

z/OS Considerações de segurança para usar o IBM MQ com o IMS

Use este tópico para planejar seus requisitos de segurança ao usar o IBM MQ com o IMS.

Usando a Classe OPERCMDS

Se você estiver usando o RACF para proteger recursos na classe OPERCMDS, assegure que o ID do usuário associado a seu espaço de endereço do gerenciador de filas do IBM MQ possui autoridade para emitir o comando MODIFY para qualquer sistema IMS para o qual ele pode se conectar.

Considerações de segurança para a Ponte do IMS

Há quatro aspectos que devem ser considerados ao decidir seus requisitos de segurança para a Ponte do IMS, estes são:

- Qual autorização de segurança é necessária para conectar o IBM MQ ao IMS
- Quanta verificação de segurança é executada nos aplicativos que utilizam a ponte para acessar o IMS
- Quais recursos do IMS esses aplicativos têm permissão para usar
- Qual autoridade deve ser usada para mensagens que são colocadas e obtidas pela ponte

Ao definir seus requisitos de segurança para a Ponte do IMS, deve-se considerar o seguinte:

- As mensagens que passam pela ponte podem ter se originado de aplicativos em plataformas que não oferecem recursos de segurança forte
- As mensagens que passam pela ponte podem ter se originado de aplicativos que não são controlados pela mesma empresa ou organização

z/OS *Considerações de segurança para se conectar ao IMS*

Conceda ao ID do usuário do espaço de endereço do gerenciador de filas do IBM MQ acesso ao grupo de OTMA.

A Ponte do IMS é um cliente OTMA. A conexão com o IMS opera sob o ID do usuário do espaço de endereço do gerenciador de filas do IBM MQ. Isto é normalmente definido como um membro do grupo de tarefas iniciadas. Esse ID do usuário deve receber acesso para o grupo OTMA (a menos que a configuração /SECURE OTMA seja NONE).

Para fazer isso, defina o perfil a seguir na classe FACILITY:

```
IMSXCF.xcfgname.mqxcfmname
```

Em que `xcfgname` é o nome do grupo XCF e `mqxcfmname` é o nome do membro XCF do IBM MQ.

Deve-se fornecer seu ID do usuário do gerenciador de filas do IBM MQ acesso de leitura a este perfil.

Nota:

1. Se as autoridades na classe FACILITY forem mudadas, deve-se emitir o comando SETROPTS RACLIST(FACILITY) REFRESH do RACF para ativar as mudanças.
2. Se o perfil hlq.NO.SUBSYS.SECURITY existir na classe MQADMIN, nenhum ID do usuário será passado para IMS e a conexão falhará a menos que a configuração /SECURE OTMA seja NONE.

z/OS *Controle de acesso ao aplicativo para a Ponte do IMS*

Defina um perfil do RACF na classe FACILITY para cada sistema IMS. Conceda um nível apropriado de acesso para o ID do usuário do gerenciador de filas do IBM MQ.

Para cada sistema IMS que a Ponte do IMS se conectar, será possível definir o seguinte perfil do RACF na classe FACILITY para determinar quanto de verificação de segurança será executada para cada mensagem transmitida para o sistema IMS.

```
IMSXCF.xcfgname.imsxcfmname
```

Em que `xcfgname` é o nome do grupo XCF e `imsxcfmname` é o nome do membro XCF para o IMS. (É necessário definir um perfil separado para cada sistema IMS.)

O nível de acesso permitido para o ID do usuário do gerenciador de filas do IBM MQ neste perfil será retornado ao IBM MQ quando a Ponte do IMS se conectar ao IMS e indica o nível de segurança que é necessário em transações subsequentes. Para transações subsequentes, o IBM MQ solicita os serviços apropriados a partir do RACF e, onde o ID do usuário estiver autorizado, transmite a mensagem para o IMS.

O OTMA não suporta o comando /SIGN do IMS; no entanto, o IBM MQ permite definir a verificação de acesso para cada mensagem para ativar a implementação do nível necessário de controle.

As informações de nível de acesso a seguir podem ser retornadas:

NONE ou NO PROFILE FOUND
Estes valores indicam que a segurança máxima é necessária, ou seja, a autenticação é necessária para cada transação. Uma verificação é feita para verificar se o ID do usuário especificado no campo *UserIdentifier* da estrutura MQMD e a senha ou PassTicket no campo *Authenticator* da estrutura MQIIH são conhecidos para o RACF e são uma combinação válida. Um UTOKEN é criado com uma senha ou PassTicket e transmitido ao IMS; o UTOKEN não é armazenado em cache.

Nota: Se o perfil hlq.NO.SUBSYS.SECURITY existir na classe MQADMIN, esse nível de segurança substituirá o que estiver definido no perfil.

READ
Este valor indica que a mesma autenticação deve ser executada igualmente para `NONE` sob as circunstâncias a seguir:

- Na primeira vez que um ID do usuário específico é encontrado
- Quando o ID do usuário tiver sido encontrado antes, mas o UTOKEN em cache não foi criado com uma senha ou PassTicket

O IBM MQ solicita um UTOKEN se necessário e transmite-o para o IMS.

Nota: Se uma solicitação para verificar novamente tiver aplicada, todas as informações em cache serão perdidas e um UTOKEN será solicitado na primeira vez que cada ID do usuário for encontrado posteriormente.

ATUALIZAÇÃO
Uma verificação é feita que o ID do usuário no campo *UserIdentifier* da estrutura MQMD é conhecido para RACF.

Um UTOKEN é construído e transmitido para o IMS; o UTOKEN é armazenado em cache.

CONTROL/ALTER
Estes valores indicam que nenhum UTOKEN de segurança precisa ser fornecido para quaisquer IDs do usuário para esse sistema IMS. (Você provavelmente usará esta opção apenas para sistemas de desenvolvimento e teste.)

Atenção: Observe que o ID do usuário contido no campo *UserIdentifier* da estrutura MQMD ainda será transmitido para o **CONTROL/ALTER**.

Nota:

1. Esse acesso é definido quando o IBM MQ se conecta ao IMS e permanece pela duração da conexão. Para alterar o nível de segurança, o acesso ao perfil de segurança deve ser alterado e, em seguida, a ponte interrompida e reiniciada (por exemplo, parando e reiniciando o OTMA).
2. Se as autoridades na classe FACILITY forem mudadas, deve-se emitir o comando SETROPTS RACLIST(FACILITY) REFRESH do RACF para ativar as mudanças.
3. É possível usar uma senha ou um PassTicket, mas deve-se lembrar de que a ponte do IMS não criptografa dados. Para obter informações sobre o uso de PassTickets, consulte "Usando PassTickets do RACF no cabeçalho do IMS" na página 270.
4. Alguns desses resultados podem ser afetados pelas configurações de segurança no IMS, usando o comando /SECURE OTMA.
5. As informações de UTOKEN em cache são mantidas pela duração definida pelos parâmetros INTERVAL e TIMEOUT do comando ALTER SECURITY do IBM MQ.
6. A opção WARNING do RACF não tem efeito no perfil IMS XCF.xcfgname.imsxcfmname. Seu uso não afeta o nível de acesso concedido e nenhuma mensagem WARNING do RACF é produzida.

z/OS *Verificação de segurança no IMS*

As mensagens que passam pela ponte contêm informações de segurança. As verificações de segurança feitas dependem da configuração do comando /SECURE OTMA do IMS.

Cada mensagem do IBM MQ que passa pela ponte contém as informações de segurança a seguir:

- Um ID do usuário contido no campo *UserIdentifier* da estrutura MQMD
- O escopo de segurança contido no campo *SecurityScope* da estrutura MQIIH (se a estrutura MQIIH estiver presente)
- Um UTOKEN (a menos que o subsistema IBM MQ tenha acesso CONTROL ou ALTER para o perfil relevante do `IMSXCF.xcfgname.imsxcfmname`)

As verificações de segurança feitas dependem da configuração do comando /SECURE OTMA do IMS, conforme a seguir:

/SECURE OTMA NONE
Não são feitas verificações de segurança para a transação.

/SECURE OTMA CHECK
O campo *UserIdentifier* da estrutura MQMD é transmitido ao IMS para verificação de autoridade de transação ou comando.

Um ACEE (Acessador Environment Element) é construído na região de controle do IMS.

/SECURE OTMA FULL
O campo *UserIdentifier* da estrutura MQMD é transmitido ao IMS para verificação de autoridade de transação ou comando.

Um ACEE é construído na região dependente do IMS, bem como a região de controle do IMS.

/SECURE OTMA PROFILE
O campo *UserIdentifier* da estrutura MQMD é passado para o IMS para verificação de autorização de transação ou comando

O campo *SecurityScope* da estrutura MQIIH é usado para determinar a possibilidade criar um ACEE na região dependente do IMS, bem como na região de controle.

Nota:

1. Se você mudar as autoridades na classe TIMS ou CIMS ou as classes GIMS ou DIMS de grupo associado, deve-se emitir os comandos a seguir do IMS para ativar as mudanças:
   - /MODIFICAR PREPARAÇÃO RACF
   - /MODIFY COMMIT
2. Se você não usar /SECURE OTMA PROFILE, qualquer valor especificado no campo *SecurityScope* da estrutura MQIIH será ignorado.

z/OS *Verificação de segurança feita pela Ponte do IMS*

Diferentes autoridades são usadas dependendo da ação sendo executada.

Quando a ponte coloca ou obtém uma mensagem, as autoridades a seguir são usadas:

Obtendo uma mensagem da fila de pontes
Nenhuma verificação de segurança é executada.

Colocando uma exceção ou uma mensagem de relatório COA
Usa a autoridade do ID do usuário no campo *UserIdentifier* da estrutura MQMD.

Colocando uma mensagem de resposta
Usa a autoridade do ID do usuário no campo *UserIdentifier* da estrutura MQMD da mensagem original.

Colocando uma mensagem na fila de devoluções
Nenhuma verificação de segurança é executada.

Nota:

1. Se os perfis de classe do IBM MQ forem alterados, deve-se emitir o comando REFRESH SECURITY(*) do IBM MQ para ativar as mudanças.
2. Se você alterar a autoridade de um usuário, deverá emitir o comando RVERIFY SECURITY do MQSC para ativar a mudança.

z/OS *Usando PassTickets do RACF no cabeçalho do IMS*

É possível usar um PassTicket no lugar de uma senha no cabeçalho do IMS.

Se desejar usar um PassTicket em vez de uma senha no cabeçalho (MQIIH) do IMS, especifique o nome do aplicativo com o qual o PassTicket é validado no atributo PASSTKTA da definição de STGCLASS da fila de ponte do IMS para o qual a mensagem deve ser roteada.

Se o valor de PASSTKTA for deixado em branco, você deverá providenciar que um PassTicket seja gerado. O nome do aplicativo neste caso deve estar no formato MVSxxxx, em que xxxx é o SMFID do sistema z/OS no qual o gerenciador de filas de destino é executado.

Um PassTicket é construído a partir de um ID do usuário, do nome do aplicativo de destino e de uma chave secreta. É um valor de 8 bytes contendo caracteres alfabéticos maiúsculos e numéricos. Ele pode ser usado apenas uma vez e é válido para um período de 20 minutos. Se um PassTicket é gerado por um sistema RACF local, o RACF verifica somente que o perfil exista e não que o usuário tem autoridade com relação ao perfil. Se PassTicket foi gerado em um sistema remoto, o RACF valida o acesso do ID do usuário ao perfil. Para obter informações integrais sobre PassTickets, veja o *z/OS SecureWay Security Server RACF Security Administrator's Guide*.

Os PassTickets no cabeçalhos do IMS são fornecidos para RACF pelo IBM MQ, não IMS.

z/OS z/OS Migrando um Gerenciador de Filas para Segurança Composta por Letras Maiúsculas e Minúsculas

Siga estas etapas para migrar um gerenciador de filas para a segurança composto por letras maiúsculas e minúsculas. Revise o nível do produto de segurança que você está usando e ative as novas classes de monitor de segurança externa IBM MQ. Execute o comando **REFRESH SECURITY** para ativar os perfis compostos por letras maiúsculas e minúsculas.

Antes de começar

1. Assegure-se de que todas as classes do monitor de segurança externa do IBM MQ estejam ativadas.
2. Certifique-se de que o gerenciador de filas esteja iniciado.

Sobre esta tarefa

Siga estas etapas para converter um gerenciador de filas em segurança composta por letras maiúsculas e minúsculas.

Procedimento

1. Copie todos os níveis de acesso e perfis existentes das classes maiúsculas para o composto por letras maiúsculas e minúsculas equivalente da classe de monitor de segurança externa.
   a) MQADMIN para MXADMIN.
   b) MQPROC para MXPROC.
   c) MQNLIST para MXNLIST.
   d) MQQUEUE para MXQUEUE.
2. Altere o valor do atributo SCYCASE para MIXED.

```
ALTER QMGR SCYCASE(MIXED)
```

3. Ative seus perfis de segurança existentes.

```
REFRESH SECURITY(*) TYPE(CLASSES)
```

4. Teste se os seus perfis de segurança estão funcionando corretamente.

Como proceder a seguir

Revise suas definições de objeto e crie novos perfis compostos por letras maiúsculas e minúsculas conforme apropriado, usando **REFRESH SECURITY** conforme necessário para ativar os perfis.

Configurando a Segurança do IBM MQ MQI client

Deve-se considerar a segurança do IBM MQ MQI client, para que os aplicativos clientes não tenham acesso sem restrição aos recursos no servidor.

Ao executar um aplicativo cliente, não execute o aplicativo usando um ID do usuário que tenha mais direitos de acesso do que necessário; por exemplo, um usuário no grupo mqm ou até mesmo o usuário mqm em si.

Ao executar um aplicativo como um usuário com direitos de acesso em excesso, você corre o risco de o aplicativo acessar e alterar as partes do gerenciador de filas, seja por acaso ou intencionalmente.

Existem dois aspectos de segurança entre um aplicativo cliente e seu servidor do gerenciador de filas: autenticação e controle de acesso.

- A autenticação pode ser usada para assegurar que o aplicativo cliente, em execução como um usuário específico, é quem eles dizem que são. Ao usar autenticação é possível evitar que um invasor ganhe acesso ao seu gerenciador de filas personificando um de seus aplicativos.

  No IBM MQ 8.0, a autenticação é fornecida por uma das duas opções:

  – O recurso de autenticação de conexão.

    Para obter mais informações sobre autenticação de conexão, consulte “Autenticação de conexão” na página 67.

  – Usando autenticação mútua dentro do TLS.

    Para obter informações adicionais sobre TLS, veja “Trabalhando com SSL/TLS” na página 276.

- O controle de acesso pode ser usado para conceder ou remover direitos de acesso para um usuário ou grupo específico de usuários. Ao executar um aplicativo cliente com um usuário especificamente criado (ou usuário em um grupo específico), é possível usar controles de acesso para assegurar que o aplicativo não possa acessar partes de seu gerenciador de filas que ele não deve.

  Ao configurar o controle de acesso, deve-se considerar as regras de autenticação de canal e o campo MCAUSER em um canal. Ambos os recursos têm a capacidade de mudar o ID do usuário que está sendo usado para verificar os direitos de controle de acesso.

  Para obter informações adicionais sobre controle de acesso, consulte o “Autorizando o acesso aos objetos” na página 353.

Se você configurou um aplicativo cliente para se conectar a um canal específico com um ID restrito, mas o canal tem um ID de administrador configurado em seu campo MCAUSER, então, considerando que o aplicativo cliente se conecte com sucesso, o ID de administrador é usado para verificações do controle de acesso. Portanto, o aplicativo cliente terá direitos de acesso completos ao seu gerenciador de filas.

Para obter mais informações sobre o atributo MCAUSER, consulte “Mapeando um ID de usuário cliente para um ID do usuário MCAUSER” na página 391.

As regras de autenticação de canal também podem ser usadas como um método para controlar o acesso a um gerenciador de filas, configurando regras e os critérios específicos para uma conexão para ser aceito.

Para obter mais informações sobre as regras de autenticação de canal, consulte: “Registros de Autenticação de Canal” na página 49.

Especificando que Apenas CipherSpecs Certificados por FIPS São Usados no Tempo de Execução no Cliente de MQI

Crie seus repositórios de chaves usando software compatível com FIPS e, em seguida, especifique que o canal deve usar CipherSpecs certificados por FIPS.

Para serem compatíveis com FIPS no tempo de execução, os repositórios de chaves devem ter sido criados e gerenciados apenas com o uso de software compatível com FIPS, como runmqakm com a opção -fips.

É possível especificar que um canal TLS deve usar somente CipherSpecs certificados por FIPS de três maneiras, listadas por ordem de precedência:

1. Configure o campo FipsRequired na estrutura MQSCO como MQSSL_FIPS_YES.
2. Configure a variável de ambiente MQSSLFIPS como YES.
3. Configure o atributo SSLFipsRequired no arquivo de configuração do cliente como YES.

Por padrão, CipherSpecs certificados por FIPS não são obrigatórios.

Estes valores possuem o mesmo significado que os valores de parâmetro equivalentes em ALTER QMGR SSLFIPS (consulte ALTER QMGR). Se atualmente o processo do cliente não tiver conexões TLS ativas e um valor FipsRequired for especificado validamente em SSL MQCONNX, todas as conexões TLS subsequentes associadas a esse processo deverão usar somente CipherSpecs associados a esse valor.

Isso se aplica até que esta e todas as outras conexões TLS sejam interrompidas, em cujo estágio um MQCONNX subsequente pode fornecer um novo valor para FipsRequired.

Se o hardware de criptografia estiver presente, os módulos de criptografia usados pelo IBM MQ poderão ser configurados para ser aqueles módulos fornecidos pelo produto de hardware e eles poderão ser certificados por FIPS em um nível específico. Os módulos configuráveis, e se eles são certificados por FIPS, dependem do produto de hardware em uso.

Onde for possível, se CipherSpecs apenas FIPS forem configurados, o cliente de MQI rejeitará conexões que especifiquem um CipherSpec não FIPS com MQRC_SSL_INITIALIZATION_ERROR. O IBM MQ não garante rejeitar todas essas conexões e é sua responsabilidade determinar se sua configuração do IBM MQ está com o padrão FIPS.

Conceitos relacionados

“Federal Information Processing Standards (FIPS) para UNIX, Linux, and Windows” na página 33
Quando a criptografia é necessária em um canal SSL/TLS em sistemas Windows, UNIX and Linux, o IBM MQ usa um pacote de criptografia chamado IBM Crypto for C (ICC). Nas plataformas Windows, UNIX and Linux, o software ICC passou no Federal Information Processing Standards (FIPS) Cryptomodule Validation Program do US National Institute of Standards and Technology, no nível 140-2.

Sub-rotina SSL do Arquivo de Configuração do Cliente

Referências relacionadas

FipsRequired (MQLONG)

MQSSLFIPS

AIX Executando os aplicativos cliente TLS com múltiplas instalações do GSKit V8.0 no AIX

Os aplicativos cliente TLS em AIX podem experimentar MQRC_CHANNEL_CONFIG_ERROR e erro AMQ6175 ao executar em sistemas AIX com múltiplas instalações do GSKit V8.0.

Ao executar aplicativos cliente em um sistema AIX com múltiplas instalações do GSKit V8.0, as chamadas de conexão do cliente podem retornar MQRC_CHANNEL_CONFIG_ERROR ao usar TLS. O /var/mqm/errors registra erro de registro AMQ6175 e AMQ9220 para o aplicativo cliente com falha, por exemplo:

```
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 ------------------------------------------------------
```

Uma causa comum desse erro é que a configuração da variável de ambiente LIBPATH ou LD_LIBRARY_PATH fez com que o cliente IBM MQ carregasse um conjunto misto de bibliotecas de duas instalações do GSKit V8.0 diferentes. Executar um aplicativo cliente do IBM MQ em um ambiente do Db2 pode causar este erro.

Para evitar este erro, inclua os diretórios da biblioteca do IBM MQ na frente do caminho da biblioteca para que as bibliotecas do IBM MQ tenham precedência. Isso pode ser alcançado usando o comando **setmqenv** com o parâmetro **-k**, por exemplo:

```
. /usr/mqm/bin/setmqenv -s -k
```

Para obter informações adicionais sobre o uso do comando **setmqenv**, consulte o setmqenv (configurar o ambiente IBM MQ)

IBM i Configurando as comunicações para SSL ou TLS no IBM i

As comunicações seguras que usam os protocolos de segurança criptográfica SSL ou TLS envolvem a configuração dos canais de comunicação e o gerenciamento de certificados digitais que serão usados para autenticação.

Para configurar sua instalação de SSL ou TLS, você deve definir seus canais para usar SSL ou TLS. Você deve também criar e gerenciar seus certificados digitais. Em alguns sistemas operacionais, é possível executar os testes com certificados autoassinados. No entanto, no IBM i, deve-se usar certificados pessoais assinados por uma CA local.

Para obter informações completas sobre a criação e o gerenciamento de certificados, consulte “Trabalhando com SSL/TLS no IBM i” na página 276.

Esta coleção de tópicos apresenta algumas das tarefas envolvidas na configuração de comunicações SSL ou TLS e fornece orientação passo a passo para concluir essas tarefas

Você talvez também deseje testar as autenticações de cliente SSL ou TLS, que são partes opcionais dos protocolos SSL e TLS. Durante o handshake de SSL ou TLS, o cliente SSL ou TLS sempre obtém e valida um certificado digital do servidor. Com a implementação do IBM MQ , o servidor SSL ou TLS sempre solicita um certificado do cliente.

No IBM i, o cliente SSL ou TLS enviará um certificado somente se tiver um com o rótulo no formato correto do IBM MQ:

- Para um gerenciador de filas, `ibmwebspheremq`, seguido pelo nome de seu gerenciador de filas, mudado para minúsculas. Por exemplo, para `QM1`, `ibmwebspheremqqm1`.
- Para um IBM MQ C Client para IBM i, `ibmwebspheremq` seguido por seu logon ID do usuário alterado para minúscula, por exemplo `ibmwebspheremqmyuserid`.

O IBM MQ usa o prefixo `ibmwebspheremq` em um rótulo para evitar confusão com certificados de outros produtos. Assegure-se de especificar o rótulo inteiro do certificado em minúsculas.

O servidor SSL ou TLS sempre valida o certificado de cliente se um for enviado. Se o cliente SSL ou TLS não enviar um certificado, a autenticação falhará somente se a extremidade do canal que age como o servidor SSL ou TLS estiver definida com o parâmetro SSLCAUTH configurado como REQUIRED ou um valor de parâmetro SSLPEER configurado. Para obter mais informações, consulte Conectando dois gerenciadores de filas usando SSL ou TLS.

ULW Configurando comunicações para SSL ou TLS no UNIX, Linux ou Windows

As comunicações seguras que usam os protocolos de segurança criptográfica SSL ou TLS envolvem a configuração dos canais de comunicação e o gerenciamento de certificados digitais que serão usados para autenticação.

Para configurar sua instalação de SSL ou TLS, você deve definir seus canais para usar SSL ou TLS. Você deve também criar e gerenciar seus certificados digitais. Nos sistemas UNIX, Linux e Windows, é possível executar os testes com certificados autoassinados.

Atenção: Não é possível usar uma combinação de certificados assinados por Curva elíptica e certificados assinados por RSA nos gerenciadores de filas que você deseja associar juntos usando canais ativados para TLS.

Os gerenciadores de filas que usam canais ativados para TLS devem usar todos os certificados assinados por RSA ou todos os certificados assinados pela EC, não uma mistura de ambos.

Veja “Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45 para obter mais informações.

Certificados autoassinados não podem ser revogados, isso poderia permitir que um invasor copiasse uma identidade após o comprometimento de uma chave privada. CAs podem revogar um certificado comprometido, evitando seu uso adicional. O uso de certificados assinados por CA são, portanto, mais seguros em um ambiente de produção, embora certificados autoassinados sejam mais convenientes em um sistema de teste.

Para obter informações completas sobre a criação e o gerenciamento de certificados, consulte “Trabalhando com SSL/TLS no UNIX, Linux, and Windows” na página 288.

Esta coleção de tópicos apresenta algumas das tarefas envolvidas na configuração de comunicações SSL, e fornece orientação passo a passo para concluir essas tarefas.

Você também pode querer testar a autenticação de cliente SSL ou TLS, que são uma parte opcional dos protocolos. Durante o handshake de SSL ou TLS, o cliente SSL ou TLS sempre obtém e valida um certificado digital do servidor. Com a implementação do IBM MQ , o servidor SSL ou TLS sempre solicita um certificado do cliente.

No UNIX, Linux, and Windows, o cliente SSL ou TLS só enviará um certificado se ele tiver um rotulado no formato correto do IBM MQ:

- Para um gerenciador de filas, o formato é `ibmwebspheremq`, seguido pelo nome de seu gerenciador de filas mudado para minúsculas. Por exemplo, para `QM1`, `ibmwebspheremqqm1`
- Para um cliente IBM MQ, `ibmwebspheremq` seguido por seu ID do usuário de logon mudado para minúsculas, por exemplo, `ibmwebspheremqmyuserid`.

O IBM MQ usa o prefixo `ibmwebspheremq` em um rótulo para evitar confusão com certificados de outros produtos. Assegure-se de especificar o rótulo inteiro do certificado em minúsculas.

O servidor SSL ou TLS sempre valida o certificado de cliente se um for enviado. Se o cliente não enviar um certificado, a autenticação falhará somente se a extremidade do canal que age como o servidor SSL ou TLS estiver definida com o parâmetro SSLCAUTH configurado como REQUIRED ou um valor de parâmetro SSLPEER configurado. Para obter mais informações, consulte Conectando dois gerenciadores de filas usando SSL ou TLS.

z/OS Configurando as comunicações para SSL ou TLS no z/OS

As comunicações seguras que usam os protocolos de segurança criptográfica SSL ou TLS envolvem a configuração dos canais de comunicação e o gerenciamento de certificados digitais que serão usados para autenticação.

Para configurar sua instalação de SSL ou TLS, você deve definir seus canais para usar SSL ou TLS. Você deve também criar e gerenciar seus certificados digitais. No z/OS, é possível executar os testes com

certificados autoassinados ou com certificados pessoais assinados por uma autoridade de certificação (CA) local.

Certificados autoassinados não podem ser revogados, isso poderia permitir que um invasor copiasse uma identidade após o comprometimento de uma chave privada. CAs podem revogar um certificado comprometido, evitando seu uso adicional. O uso de certificados assinados por CA são, portanto, mais seguros em um ambiente de produção, embora certificados autoassinados sejam mais convenientes em um sistema de teste.

Para obter informações completas sobre a criação e o gerenciamento de certificados, consulte "Trabalhando com SSL/TLS no z/OS" na página 321.

Esta coleção de tópicos apresenta algumas das tarefas envolvidas na configuração de comunicações SSL ou TLS e fornece orientação passo a passo para concluir essas tarefas.

Você também pode querer testar a autenticação de cliente SSL ou TLS, que são uma parte opcional dos protocolos. Durante o handshake de SSL ou TLS, o cliente SSL ou TLS sempre obtém e valida um certificado digital do servidor. Com a implementação do IBM MQ , o servidor SSL ou TLS sempre solicita um certificado do cliente.

No z/OS, o cliente SSL ou TLS enviará um certificado somente se tiver um dos certificados a seguir:

- para um canal compartilhado apenas, um certificado com um rótulo no formato `ibmWebSphereMQ`, seguido pelo nome de seu grupo de filas compartilhadas, por exemplo, `ibmWebSphereMQQSG1`
- Um certificado com um rótulo no formato `ibmWebSphereMQ`, seguido pelo nome de seu gerenciador de filas, por exemplo, `ibmWebSphereMQQM1`
- Um certificado padrão (que pode ser o certificado `ibmWebSphereMQ`).

Se o canal for compartilhado, ele tentará primeiro localizar um certificado para o grupo de filas compartilhadas. Se ele não localizar um certificado para um grupo de filas compartilhadas, ele tentará localizar um certificado para o gerenciador de filas.

No z/OS, o IBM MQ usa o prefixo `ibmWebSphereMQ` em um rótulo para evitar confusão com certificados para outros produtos.

O servidor SSL ou TLS sempre valida o certificado de cliente se um for enviado. Se o cliente SSL ou TLS não enviar um certificado, a autenticação falhará somente se a extremidade do canal que age como o servidor SSL ou TLS estiver definida com o parâmetro SSLCAUTH configurado como REQUIRED ou um valor de parâmetro SSLPEER configurado. Para obter mais informações, consulte Conectando dois gerenciadores de filas usando SSL ou TLS.

Trabalhando com SSL/TLS

Estes tópicos fornecem instruções para executar tarefas únicas relacionadas ao uso do TLS com o IBM MQ.

Muitos deles são usados como etapas nas tarefas de alto nível descritos nas seguintes seções:

- "Identificando e autenticando usuários" na página 333
- "Autorizando o acesso aos objetos" na página 353
- "Confidencialidade das mensagens" na página 423
- "Integridade de dados de mensagens" na página 462
- "Mantendo Clusters Seguros" na página 463

IBM i Trabalhando com SSL/TLS no IBM i

Esta coleção de tópicos fornece instruções para tarefas individuais que trabalham com a Segurança da Camada de Transporte (TLS) no IBM MQ for IBM i.

Para o IBM i, o suporte ao TLS é integral para o sistema operacional. Assegure-se de que instalou os pré-requisitos listados na Requisitos de hardware e software no IBM i.

No IBM i, gerencie chaves e certificados digitais com a ferramenta DCM (Digital Certificate Manager).

Acessando DCM

Siga estas instruções para acessar a interface do DCM.

Sobre esta tarefa

Execute as etapas a seguir em um navegador da web que suporte quadros.

Procedimento

1. Vá para `http:// machine.domain:2001` ou `https:// machine.domain:2010`, em que *machine* é o nome do seu computador.
2. Digite um perfil do usuário e uma senha válidos quando solicitado.

   Assegure-se de que seu perfil do usuário tenha as autoridades especiais *ALLOBJ e *SECADM para permitir a criação de novos armazenamentos de certificados. Se você não possuir as autoridades especiais, poderá gerenciar apenas os certificados pessoais ou visualizar as assinaturas de objeto dos objetos que estão autorizados. Se você tiver autorização para usar um aplicativo de assinatura de objeto, também poderá assinar objetos a partir do DCM.
3. Na página Configurações da Internet, clique em **Digital Certificate Manager**.

   A página Digital Certificate Manager é exibida.

Atribuindo um certificado a um gerenciador de filas no IBM i

Use o DCM para designar um certificado a um gerenciador de filas.

Use o gerenciamento de certificado digital tradicional do IBM i para designar um certificado a um gerenciador de filas. Isso significa que é possível especificar que um gerenciador de filas use um armazenamento de certificados do sistema, e que o gerenciador de filas seja registrado para ser usado como um aplicativo com o Digital Certificate Manager. Para fazer isso, mude o valor do atributo **SSLKEYR** do gerenciador de filas para *SYSTEM.

Quando o parâmetro **SSLKEYR** é alterado para *SYSTEM, IBM MQ registra o gerenciador de fila como um aplicativo do servidor com um rótulo de aplicativo exclusivo de QIBM_WEBSPHERE_MQ_QMGRNAME e um rótulo com uma descrição de Qmgrname (WMQ). Observe que os atributos **CERTLABL** do canal não são usados se você usar o armazenamento de certificados *SYSTEM. O gerenciador de filas aparecerá como um aplicativo do servidor no Digital Certificate Manager e será possível atribuir a este aplicativo qualquer servidor ou certificado de cliente no armazenamento do sistema.

Como o gerenciador de filas é registrado como um aplicativo, recursos avançados do DCM tais como a definição das listas de confiança da CA poderão ser executadas.

Se o parâmetro **SSLKEYR** for alterado para um valor diferente de *SYSTEM, IBM MQ removerá o registro do gerenciador de filas como um aplicativo com Digital Certificate Manager. Se um gerenciador de filas for excluído, o registro também será removido do DCM. Um usuário com autoridade *SECADM suficiente também pode incluir ou remover manualmente os aplicativos do DCM.

Configurando um repositório de chaves no IBM i

Um repositório de chaves deve ser configurado em ambas as extremidades da conexão. Os armazenamentos de certificados padrão podem ser usados ou é possível criar seus próprios.

Uma conexão TLS requer um *repositório de chaves* em cada extremidade da conexão. Cada gerenciador de filas e IBM MQ MQI client devem ter acesso a um repositório de chaves. Se você deseja acessar o repositório de chaves usando um nome de arquivo e senha (ou seja, não usando a opção *SYSTEM) assegure que o perfil do usuário QMQM possua as seguintes autoridades:

- Autoridade de execução para o diretório que contém o repositório de chaves
- Autoridade de leitura para o arquivo que contém o repositório de chaves

Consulte a “O repositório de chaves SSL/TLS” na página 25 para obter mais informações. Observe que os atributos **CERTLABL** do canal não serão usados se você usar o armazenamento de certificados *SYSTEM..

No IBM i, os certificados digitais são armazenados em um armazenamento de certificados que é gerenciado com o DCM. Esses certificados digitais possuem rótulos que associam um certificado a um gerenciador de filas ou um IBM MQ MQI client. O TLS usa os certificados para propósitos de autenticação.

O rótulo é o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou o ID de logon do usuário do IBM MQ MQI client anexado, todo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.

O nome armazenamento de certificados do gerenciador de filas ou IBM MQ MQI client é composto de um caminho e nome de raiz. O caminho padrão é `/QIBM/UserData/ICSS/Cert/Server/` e o nome de raiz padrão é `Default`. No IBM i, o armazenamento de certificados padrão, `/QIBM/UserData/ICSS/Cert/Server/Default.kdb`, também é conhecido como `*SYSTEM` Como opção, é possível definir o seu próprio caminho e nome de raiz.

Se você definir seu próprio caminho ou nome de arquivo, configure as permissões para que o arquivo controle rigorosamente o acesso a ele.

"Alterando o local do repositório de chaves de um gerenciador de filas no IBM i" na página 279 traz informações sobre como especificar o nome do armazenamento de certificados. Você pode especificar o nome do armazenamento de certificados antes ou depois de criar o armazenamento de certificados.

Nota: As operações que você pode executar com o DCM podem ser limitadas pela autoridade do seu perfil de usuário. Por exemplo, as autoridades *ALLOBJ e *SECADM são necessárias para criar um certificado de CA.

Criando um armazenamento de certificados no IBM i
Se não desejar usar o armazenamento de certificados padrão, siga este procedimento para criar seu próprio.

Sobre esta tarefa

Crie um novo armazenamento de certificados somente se você não desejar usar o certificado padrão de armazenamento do IBM i.

Para especificar que o armazenamento de certificados do sistema IBM i deve ser usado, altere o valor do atributo SSLKEYR do gerenciador de filas para *SYSTEM. Esse valor indica que o gerenciador de filas usa o armazenamento de certificados do sistema e que o gerenciador de filas está registrado para ser usado como um aplicativo com o Digital Certificate Manager (DCM).

Procedimento

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277
2. No painel de navegação, clique em **Criar um Novo Armazenamento de Certificados**.
   A página Criar Novo Armazenamento de Certificados é exibida no quadro de tarefas.
3. No quadro de tarefas, selecione **Outro Armazenamento de Certificados do Sistema** e clique em **Continuar**.
   A página Criar um Certificado no Novo Armazenamento de Certificados é exibida no quadro de tarefas.
4. Selecione **Não - Não criar um certificado no armazenamento de certificados** e clique em **Continuar**.
   A página Nome e Senha do Armazenamento de Certificados é exibida no quadro de tarefas.
5. No campo **Caminho e nome de arquivo do armazenamento de certificados**, digite um caminho e nome de arquivo IFS, por exemplo `/QIBM/UserData/mqm/qmgrs/qm1/key.kdb`
6. Digite uma senha no campo **Senha** e digite-a novamente no campo **Confirmar Senha**. Clique em **Continuar**.
   Anote a senha (que faz distinção entre maiúsculas e minúsculas) porque ela será necessária quando você armazenar a chave do repositório em arquivo stash.
7. Para sair do DCM, feche a janela do navegador.

Como proceder a seguir

Quando você tiver criado o armazenamento de certificados usando o DCM, assegure-se de armazenar a senha em arquivo stash, conforme descrito em “Armazenar em arquivo stash a senha do armazenamento de certificados em sistemas IBM i” na página 279.

Tarefas relacionadas

“Importando um certificado em um repositório de chaves no IBM i” na página 284
Siga este procedimento para importar um certificado.

Armazenar em arquivo stash a senha do armazenamento de certificados em sistemas IBM i

Armazenar em arquivo stash a senha de armazenamento de certificados usando comandos CL.

As instruções a seguir se aplicam a armazenar em arquivo stash a senha de armazenamento de certificados no IBM i para um gerenciador de filas. Como alternativa, para um IBM MQ MQI client, se você não estiver usando o armazenamento de certificados *SYSTEM (ou seja, o ambiente MQSSLKEYR estiver configurado para um valor diferente de *SYSTEM) siga o procedimento descrito na seção “Armazenar em arquivo stash a senha de armazenamento de certificados” na página 287 de “Utilitário do cliente SSL (amqrsslc) do IBM MQ para IBM i” na página 286..

Se você tiver especificado que o armazenamento de certificados *SYSTEM deve ser usado (ao alterar o valor do atributo SSLKEYR do gerenciador de filas para *SYSTEM) não se deve seguir estas etapas.

Ao criar o armazenamento de certificados usando o DCM, use os seguintes comandos para proteger a senha:

```
STRMQM MQMNAME('queue_manager_name')
CHGMQM MQMNAME('queue_manager_name') SSLKEYRPWD('password')
```

A senha faz distinção entre maiúsculas e minúsculas. Ela deve ser inserida entre aspas simples exatamente como você a inseriu na etapa 6 em “Criando um armazenamento de certificados no IBM i” na página 278.

Nota: Se você não estiver usando o armazenamento de certificados do sistema padrão e não armazenar a senha em arquivo stash, as tentativas para iniciar os canais TLS falharão porque eles não podem obter a senha necessária para acessar o armazenamento de certificados.

Localizando o repositório de chaves para um gerenciador de filas no IBM i

Use este procedimento para obter o local do armazenamento de certificados do gerenciador de filas.

Procedimento

1. Exiba os atributos de seu gerenciador de filas, usando o seguinte comando:

   ```
   DSPMQM MQMNAME('queue manager name')
   ```

2. Examine a saída do comando para o nome do caminho e de raiz do armazenamento de certificados.

   Por exemplo: `/QIBM/UserData/ICSS/Cert/Server/Default`, em que `/QIBM/UserData/ICSS/Cert/Server` é o caminho e `Default` é o nome derivado.

Alterando o local do repositório de chaves de um gerenciador de filas no IBM i

Altere o local do armazenamento de certificados do gerenciador de filas usando CHGMQM ou ALTER QMGR.

Procedimento

Use o comando CHGMQM ou o comando ALTER QMGR MQSC para configurar o atributo de repositório de chaves do gerenciador de filas.

a) Usando CHGMQM: `CHGMQM MQMNAME('qm1') SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

b) Usando ALTER QMGR: `ALTER QMGR SSLKEYR('/QIBM/UserData/ICSS/Cert/Server/MyKey')`

Em qualquer um dos casos, o armazenamento de certificados tem o nome completo do arquivo: `/QIBM/UserData/ICSS/Cert/Server/MyKey.kdb`

Como proceder a seguir

Ao alterar o local de um armazenamento de certificados do gerenciador de filas, os certificados não serão transferidos a partir do local antigo. Se os certificados de CA pré-instalados ao criar o armazenamento de certificados forem insuficientes, você deverá preencher o novo armazenamento de certificados com certificados, conforme descrito em "Importando um certificado em um repositório de chaves no IBM i" na página 284. Também é necessário proteger a senha para o novo local, conforme descrito em "Armazenar em arquivo stash a senha do armazenamento de certificados em sistemas IBM i" na página 279.

Criando uma autoridade de certificação e certificado para testes no IBM i

Use este procedimento para criar um certificado de CA local para assinar solicitações de certificados e para criar e instalar o certificado de CA.

Antes de começar

As instruções deste tópico supõem que não existe uma autoridade de certificação (CA) local. Se existir uma CA local, acesse "Solicitando um certificado do servidor no IBM i" na página 281.

Sobre esta tarefa

Os certificados de CA fornecidos ao instalar o TLS são assinados pela CA emitente. No IBM i, é possível gerar uma autoridade de certificação local que pode assinar certificados do servidor para testar comunicações TLS em seu sistema. Siga estas etapas em um navegador da web para criar um certificado de CA local:

Procedimento

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
2. No painel de navegação, clique em **Criar uma Autoridade de Certificados**.

   A página Criar uma Autoridade de Certificação é exibida no quadro de tarefas.
3. Digite uma senha no campo **Senha de Armazenamento de Certificados** e digite-a novamente no campo **Confirmar Senha**.
4. Digite um nome no campo **Nome da Autoridade de Certificação (CA)**, por exemplo, `Autoridade de certificação de teste TLS`.
5. Digite valores apropriados nos campos **Nome Comum** e **Organização** e selecione um país. Para os campos opcionais restantes, digite os valores que você precisa.
6. Digite um período de validade para o CA local no campo **Período de Validade**.

   O valor padrão é 1095 dias.
7. Clique em **Continuar**.

   O CA é criado e o DCM criará um armazenamento de certificados e um certificado de CA para o CA local.
8. Clique em **Instalar Certificado**.

   A caixa de diálogo Gerenciador de Download é exibida.
9. Digite o nome do caminho completo para o arquivo temporário no qual deseja armazenar o certificado de CA e clique em **Salvar**.
10. Quando o download estiver concluído, clique em **Abrir**.

    A janela Certificado é exibida.
11. Clique em **Instalar Certificado**.

    O Assistente de Importação de Certificado é exibido.
12. Clique em **Avançar**.

13. Selecione **Selecionar o armazenamento de certificados automaticamente com base no tipo de certificado** e clique em **Avançar**.
14. Clique em **Concluir**.

    Uma janela de confirmação é exibida.
15. Clique em **OK**.
16. Na janela Certificado, clique em **OK**.
17. Clique em **Continuar**.

    A página Política de Autoridade de Certificação é exibida no quadro de tarefas.
18. No campo **Permitir a criação de certificados de usuários**, selecione **Sim**.
19. No campo **Período de Validade**, digite o período de validade dos certificados que são emitidos pela sua CA local.

    O valor padrão é 365 dias.
20. Clique em **Continuar**.

    A página Criar um Certificado no Novo Armazenamento de Certificados é exibida no quadro de tarefas.
21. Verifique se nenhum dos aplicativos está selecionado.
22. Clique em **Continuar** para concluir a configuração da CA local.

Solicitando um certificado do servidor no IBM i

Os certificados digitais são protegidos contra personificação, certificando que uma chave pública pertence a uma entidade especificada. Um novo certificado do servidor pode ser solicitado a partir de uma autoridade de certificação usando o Digital Certificate Manager (DCM).

Sobre esta tarefa

Execute as seguintes etapas em um navegador da web:

Procedimento

1. Acesse a interface DCM, conforme descrito em “Acessando DCM” na página 277.
2. No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**.

   A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.
3. Selecione o armazenamento de certificados que deseja usar e clique em **Continuar**.
4. Opcional: Se você tiver selecionado ***SYSTEM** na etapa 3, insira a senha de armazenamento do sistema e clique em **Continuar**.
5. Opcional: Se você tiver selecionado **Outro armazenamento de certificados do sistema** na etapa 3, no campo **Caminho e nome do arquivo do armazenamento de certificados**, digite o caminho e nome de arquivo IFS configurado durante a criação do armazenamento de certificados. Além disso, digite uma senha no campo **Senha do armazenamento de certificados**. Em seguida, clique em **Continuar**
6. No painel de navegação, clique em **Criar Certificado**.
7. No quadro de tarefas, selecione o botão de opção **Certificado do servidor ou do cliente** e clique em **Continuar**.

   A página Selecionar uma Autoridade de Certificação (CA) é exibida no quadro de tarefas.
8. Se você possuir uma CA local na sua estação de trabalho, escolha a CA local ou uma CA comercial para assinar o certificado. Selecione o botão de opção para a CA desejada e clique em **Continuar**.

   A página Criar um Certificado é exibida no quadro de tarefas.
9. Opcional: Para um gerenciador de filas, no campo **Rótulo do certificado** insira o rótulo certificado.

   O rótulo é o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.

   Por exemplo, para o gerenciador de filas QM1, digite `ibmwebspheremqqm1` para usar o valor padrão.

10. Opcional: Para um IBM MQ MQI client, no campo **Certificado do rótulo**, digite `ibmwebspheremq` seguido por seu ID do usuário de logon em letras minúsculas.
    Por exemplo, digite `ibmwebspheremqmyuserID`
11. Digite valores apropriados nos campos **Nome Comum** e **Organização** e selecione um país. Para os campos opcionais restantes, digite os valores que você precisa.

Resultados

Se você selecionou uma CA comercial para assinar o certificado, o DCM criará um pedido de certificado no formato PEM (Privacy-Enhanced Mail). Encaminhe o pedido para a CA escolhida.

Se você selecionou a CA local para assinar o certificado, o DCM informará que o certificado foi criado no armazenamento de certificados e poderá ser usado.

Solicitando um certificado do servidor para IBM Key Manager no IBM i

Siga este procedimento para criar um certificado assinado por sua autoridade de certificação (CA) local ou para aplicar um certificado do servidor assinado por uma CA comercial para importação para o utilitário IBM Key Management (iKeyman).

Sobre esta tarefa

Um certificado de usuário deve ser usado quando o Digital Certificate Manager (DCM) servir como o gerenciador de certificado para o IBM MQ em várias plataformas. Para certificados pessoais distribuídos para outras plataformas e para importação para o utilitário iKeyman, execute as seguintes etapas em um navegador da web:

Procedimento

1. Acesse a interface DCM, conforme descrito em “Acessando DCM” na página 277.
2. Na área de janela de **navegação**, clique em **Criar Certificado**.
   A página **Criar Certificado** é exibida no quadro de tarefas.
3. No painel **Criar Certificado**, selecione o botão de opções **Certificado de Usuário** e clique em **Continuar**.
   A página **Criar Certificado de Usuário** é exibida.
4. No painel **Criar Certificado de Usuário**, preencha os campos obrigatórios de Informações de Certificado para **Nome da organização**, **Estado** ou **município**, **País** ou **região**. Opcionalmente, coloque valores nos campos **Unidade de Organização** e **Localidade** ou **cidade**. Clique em **Continuar**.
   O **Nome comum** é configurado automaticamente para o ID do usuário com o qual você efetuou logon no sistema iSeries.
5. No próximo painel **Criar Certificado de Usuário**, clique em **Instalar Certificado** e clique em **Continuar**.
   É exibida uma mensagem indicando: `Seu certificado pessoal foi instalado. É necessário manter uma cópia de backup desse certificado.`
6. Clique em **OK**.
7. Dependendo do navegador da Internet usado para acessar o DCM, execute as seguintes etapas:
   a) Para o Microsoft Edge escolha: **Ferramentas>Opções da Internet>Guia Conteúdo>botão Certificados>Guia Pessoal>**. Selecione o certificado e clique em **Exportar**.
   b) Para Mozilla Firefox escolha: **Ferramentas>Opções>Avançado>guia Criptografia>botão Visualizar certificados>guia Seus certificados>**. Selecione o certificado e clique em **Backup**. Selecione o caminho e o nome do arquivo e clique em **OK**.
8. Transfira o certificado exportado para o sistema remoto usando FTP no formato binário.
9. Inclua o certificado exportado da etapa 7 no utilitário iKeyman no banco de dados de chaves.
   a) Se o certificado foi salvo usando Microsoft Edge, use as instruções descritas em Importando a partir de um arquivo Microsoft `.pfx` .

b) Se o certificado tiver sido salvo usando o Mozilla Firefox, use as instruções descritas em Importando um Certificado Pessoal para um Repositório de Chaves.

Durante a importação, assegure que o nome do rótulo certificado pessoal e o certificado de assinante são mudados para o que o IBM MQ está esperando. O rótulo deve ser o valor do atributo do IBM MQ **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas anexado, todo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.

Incluindo certificados de servidor em um repositório de chaves no IBM i

Siga este procedimento para incluir um certificado solicitado no repositório de chaves.

Sobre esta tarefa

Depois que a CA enviar um novo certificado do servidor, inclua-o ao armazenamento de certificados a partir do qual o pedido foi gerado. Se a CA enviar o certificado como parte de uma mensagem de e-mail, copie o certificado em um arquivo separado.

Nota:

- Não será necessário executar esse procedimento se o certificado do servidor for assinado pela sua CA local.
- Antes de importar um certificado do servidor no formato PKCS #12 para o DCM, é necessário primeiramente importar o certificado de CA correspondente.

Use o seguinte procedimento para receber um certificado do servidor para o armazenamento de certificados do gerenciador de filas:

Procedimento

1. Acesse a interface DCM, conforme descrito em “Acessando DCM” na página 277.
2. Na categoria de tarefa **Gerenciar Certificados** no painel de navegação, clique em **Importar Certificado**.

   A página Importar Certificado é exibida no quadro de tarefas.
3. Selecione o botão de opção para o seu tipo de certificado e clique em **Continuar**.

   A página Servidor de Importação ou Certificado do Cliente, ou a página Importar Certificado CA (Autoridade de Certificação) é exibida no quadro de tarefas.
4. No campo **Importar Arquivo**, digite o nome do arquivo do certificado que deseja importar e clique em **Continuar**.

   O DCM determina automaticamente o formato do arquivo.
5. Se o certificado for um certificado **Servidor ou cliente**, digite a senha no quadro de tarefas e clique em **Continuar**.

   O DCM informará que o certificado foi importado.

Exportando um certificado de um repositório de chaves no IBM i

Exportar um certificado exporta as chaves pública e privada. Esta ação deve ser tomada com extremo cuidado, pois passar uma chave privada comprometeria completamente a sua segurança.

Antes de começar

Quando você compartilha um certificado do usuário com outro usuário, você troca chaves públicas. Este processo é descrito na **Tarefa 5. Compartilhando Certificados** no Guia de Início Rápido para AMS no UNIX. Quando você exporta um certificado conforme descrito aqui, você exporta as chaves pública e privada. Esta ação deve ser tomada com extremo cuidado, pois passar uma chave privada comprometeria completamente a sua segurança.

Sobre esta tarefa

Execute as seguintes etapas no computador do qual você deseja exportar o certificado:

Procedimento

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
2. No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**.

   A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.
3. Selecione o armazenamento de certificados que deseja usar e clique em **Continuar**.
4. Opcional: Se você tiver selecionado ***SYSTEM** na etapa 3, insira a senha de armazenamento do sistema e clique em **Continuar**.
5. Opcional: Se você tiver selecionado **Outro Armazenamento de Certificados do Sistema** na etapa 3, no campo **Caminho e Nome de Arquivo do Armazenamento de Certificados**, digite o caminho e o nome de arquivo do IFS configurados durante a criação do armazenamento de certificados e digite uma senha no campo **Senha de Armazenamento do Certificado**. Em seguida, clique em **Continuar**
6. Na categoria de tarefa **Gerenciar Certificados**, no painel de navegação, clique em **Exportar Certificado**.

   A página Exportar um Certificado é exibida no quadro de tarefas.
7. Selecione o botão de opção para o seu tipo de certificado e clique em **Continuar**.

   A página Servidor de Exportação ou Certificado do Cliente ou a página Exportar Certificado da Autoridade de Certificação (CA) é exibida no quadro de tarefas.
8. Selecione o certificado que deseja exportar.
9. Selecione o botão de opção para especificar se deseja exportar o certificado para um arquivo ou diretamente para outro armazenamento de certificados.
10. Se você selecionou exportar um certificado de servidor ou cliente para um arquivo, forneça as seguintes informações:
    - O caminho e o nome do arquivo do local onde deseja armazenar o certificado exportado.
    - Para um certificado pessoal, a senha que é usada para criptografar o certificado exportado e o release de destino. Para certificados de CA, não é necessário especificar a senha.
11. Se você selecionou exportar um certificado diretamente para outro armazenamento de certificados, especifique o armazenamento de certificados de destino e a senha.
12. Clique em **Continuar**.

Importando um certificado em um repositório de chaves no IBM i

Siga este procedimento para importar um certificado.

Antes de começar

Antes de importar um certificado pessoal no formato PKCS #12 para o DCM, é necessário primeiramente importar o certificado de CA correspondente.

Sobre esta tarefa

Execute estas etapas na máquina para a qual deseja importar o certificado.

Procedimento

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
2. No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**.

   A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.
3. Selecione o armazenamento de certificados que deseja usar e clique em **Continuar**.
4. Opcional: Se você tiver selecionado ***SYSTEM** na etapa 3, insira a senha de armazenamento do sistema e clique em **Continuar**.
5. Opcional: Se você tiver selecionado **Outro Armazenamento de Certificados do Sistema** na etapa 3, no campo **Caminho e Nome de Arquivo do Armazenamento de Certificados**, digite o caminho e o

nome de arquivo do IFS configurados durante a criação do armazenamento de certificados e digite uma senha no campo **Senha de Armazenamento do Certificado**. Em seguida, clique em **Continuar**

6. Na categoria de tarefa **Gerenciar Certificados** no painel de navegação, clique em **Importar Certificado**.

   A página Importar Certificado é exibida no quadro de tarefas.

7. Selecione o botão de opção para o seu tipo de certificado e clique em **Continuar**.

   A página Servidor de Importação ou Certificado do Cliente ou a página Importar Certificado da Autoridade de Certificação (CA) é exibida no quadro de tarefas.

8. No campo **Importar Arquivo**, digite o nome do arquivo do certificado que deseja importar e clique em **Continuar**.

   O DCM determina automaticamente o formato do arquivo.

9. Se o certificado for um certificado **Servidor ou cliente**, digite a senha no quadro de tarefas e clique em **Continuar**. O DCM informará que o certificado foi importado.

Removendo certificados no IBM i

Use este procedimento para remover certificados pessoais.

Procedimento

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
2. No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**.

   A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.

3. Selecione a caixa de opção **Outro Armazenamento de Certificados do Sistema** e clique em **Continuar**.

   A página Armazenamento de Certificados e Senha é exibida.

4. No campo **Caminho e Nome de Arquivo do Armazenamento de Certificados**, digite o caminho e o nome de arquivo do IFS configurados durante a criação do armazenamento de certificados.
5. Digite uma senha no campo **Senha do Armazenamento de Certificados**. Clique em **Continuar**.

   A página Armazenamento de Certificados Atual é exibida no quadro de tarefas.

6. Na categoria de tarefas **Gerenciar Certificados** no painel de navegação, clique em **Excluir Certificado**.

   A página Confirmar Exclusão de Certificado é exibida no quadro de tarefas.

7. Selecione o certificado que deseja excluir. Clique em **Excluir (Delete)**.
8. Clique em **Sim** para confirmar que deseja excluir o certificado. Caso contrário, clique em **Não**.

   O DCM o informará se o certificado tiver sido excluído.

*Usando o armazenamento de certificados *SYSTEM para autenticação unidirecional no IBM i*

Siga estas instruções para configurar a autenticação unilateral.

Antes de começar

- Crie um gerenciador de filas, canais e filas de transmissão.
- Crie um certificado de servidor ou cliente no gerenciador de filas do servidor.
- Transfira o certificado de autoridade de certificação para o gerenciador de filas do cliente e importo-o no repositório de chaves.
- Inicie um listener nos gerenciadores de filas do servidor e do cliente.

Sobre esta tarefa

Para usar a autenticação unidirecional, usando um computador executando IBM i como o servidor TLS, configure o parâmetro SSL Key Repository (SSLKEYR) para *SYSTEM. Esta configuração registra

o gerenciador de filas do IBM MQ como um aplicativo. É possível então designar um certificado ao gerenciador de filas para ativar uma autenticação unilateral.

Também é possível usar keystores privadas para implementar a autenticação unilateral criando um certificado simulado para o gerenciador de filas do cliente no repositório de chaves.

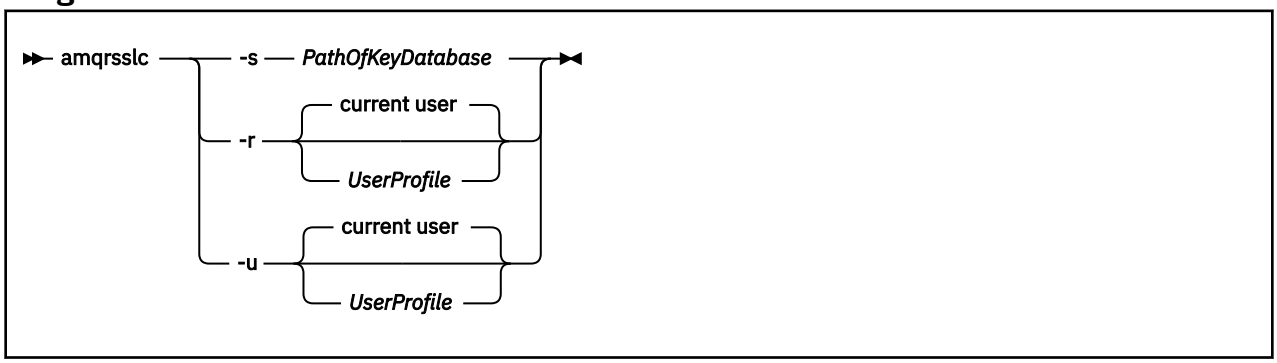
Procedimento

1. Execute as seguintes etapas nos gerenciadores de filas do servidor e do cliente:
   a) Altere o gerenciador de filas para configurar o parâmetro SSLKEYR, emitindo o comando `CHGMQM MQMNAME(SSL) SSLKEYR(*SYSTEM)`.
   b) Armazene em arquivo stash a senha do repositório de chaves padrão, emitindo o comando `CHGMQM MQMNAME(SSL) SSLKEYRPWD('xxxxxxx')`.
      A senha deve estar entre aspas simples.
   c) Altere os canais para que tenham o CipherSpec correto no parâmetro SSLCIPHER.
   d) Atualize a segurança TLS emitindo o comando `RFRMQMAUT QMNAME(QMGRNAME) TYPE(*SSL)`.
2. Designe o certificado ao gerenciador de filas do servidor usando o DCM, conforme a seguir:
   a) Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
   b) No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**.
      A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.
   c) Selecione o armazenamento de certificados *SYSTEM e clique em **Continuar**.
   d) No painel esquerdo, expanda **Gerenciar Aplicativos**.
   e) Selecione a definição **Visualização do aplicativo** para verificar se o gerenciador de filas foi registrado como um aplicativo.
      `SSL (WMQ)` está listado na tabela.
   f) Selecione **Atualizar Designação de Certificado**.
   g) Selecione **Servidor** e clique em **Continuar**.
   h) Selecione QMGRNAME (WMQ) e clique em **Atualizar Designação de Certificado**.
   i) Selecione o certificado e clique em **Designar Novo Certificado**. Uma janela é aberta indicando que o certificado foi designado ao aplicativo.

Utilitário do cliente SSL (amqrsslc) do IBM MQ para IBM i

O utilitário do cliente SSL (amqrsslc) do IBM MQ para o IBM i é usado pelo IBM MQ MQI client nos sistemas IBM i para registrar ou cancelar registro do perfil do usuário cliente ou armazenar em arquivo stash a senha de armazenamento de certificados. O utilitário pode somente ser executado por um usuário com um perfil com a autoridade especial *ALLOBJ ou um membro do QMQMADM que tem opções de criar ou excluir registros de aplicativos no Digital Certificate Manager (DCM).

Diagrama de sintaxe



Registre o perfil do usuário do cliente

Se o IBM MQ MQI client estiver usando o armazenamento de certificados *SYSTEM, você deverá registrar o perfil do usuário cliente (usuário de logon) para uso como um aplicativo com Digital Certificate Manager (DCM).

Se você desejar registrar o perfil do usuário do cliente, execute o programa **amqrsslc** com a opção `-r` com o *UserProfile*. O perfil do usuário usado ao chamar **amqrsslc** deve ter autoridade *USE. Fornecer o *UserProfile* com a opção `-r` registra o *UserProfile* como um aplicativo do servidor com um rótulo do aplicativo exclusivo de QIBM_WEBSPHERE_MQ_*UserProfile* e um rótulo com uma descrição do *UserProfile* (WMQ). Esse aplicativo do servidor, em seguida, é exibido no DCM e é possível atribuir a este aplicativo qualquer servidor ou certificado cliente no armazenamento do sistema.

Nota: Se um perfil do usuário não for especificado com a opção `-r`, então, o perfil do usuário do usuário que estiver executando a ferramenta **amqrsslc** será registrado.

O código a seguir usa o **amqrsslc** para registrar um perfil do usuário. No primeiro exemplo, o perfil de usuário especificado está registrado; no segundo é o perfil do usuário com login efetuado:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-r' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-r')
```

Cancelar o registro do perfil do usuário do cliente

Para cancelar o registro do perfil do cliente, execute o programa **amqrsslc** com a opção `-u` com *UserProfile*. O perfil do usuário usado ao chamar **amqrsslc** deve ter autoridade *USE. Fornecer o *UserProfile* com a opção `-u` cancela o registro do *UserProfile* com o rótulo QIBM_WEBSPHERE_MQ_*UserProfile* do DCM.

Nota: Se um perfil do usuário não for especificado com a opção `-u`, o perfil do usuário do usuário que estiver executando o **amqrsslc** ferramenta terá o registro cancelado.

O código a seguir usa **amqrsslc** para cancelar o registro de um perfil do usuário. No primeiro exemplo, o perfil de usuário especificado não está registrado; no segundo é o perfil do usuário com login efetuado:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-u' UserProfile)
CALL PGM(QMQM/AMQRSSLC) PARM('-u')
```

Armazenar em arquivo stash a senha de armazenamento de certificados

Se o IBM MQ MQI client não estiver usando o armazenamento de certificados *SYSTEM e usar outro armazenamento de certificados (ou seja, MQSSLKEYR for configurado para um valor diferente de *SYSTEM), a senha do banco de dados de chaves deverá ser armazenada em arquivo stash. Use a opção `-s` para armazenar em arquivo stash a senha do banco de dados de chaves.

No código a seguir, o nome completo do arquivo do armazenamento de certificados é `/Path/Of/KeyDatabase/MyKey.kdb`:

```
CALL PGM(QMQM/AMQRSSLC) PARM('-s' '/Path/Of/KeyDatabase/MyKey')
```

A execução deste código resulta em um pedido para a senha desse banco de dados de chaves. Esta senha é armazenada em um arquivo stash com o mesmo nome de banco de dados de chaves com uma extensão .sth. Este arquivo é armazenado no mesmo caminho que o banco de dados de chaves. O exemplo de código gera um arquivo stash de `/Path/Of/KeyDatabase/MyKey.sth`. O QMQM é o proprietário do usuário e o QMQMADM o proprietário do grupo para este arquivo. O QMQM e QMQMADM têm permissão de leitura, de gravação e outros perfis têm apenas permissão de leitura.

Quando mudanças nos certificados ou no armazenamento de certificados tornam-se efetivas no IBM i

Ao alterar os certificados em um armazenamento de certificados, ou o local do armazenamento de certificados, as mudanças entrarão em vigor, dependendo do tipo de canal e de como o canal está sendo executado.

Mudanças nos certificados no armazenamento de certificados e no atributo de repositório de chaves entrarão em vigor nas seguintes situações:

- Quando um novo processo de canal único de saída executa um canal do TLS pela primeira vez.
- Quando um novo processo de canal único TCP/IP de entrada recebe pela primeira vez uma solicitação para iniciar um canal do TLS.
- Quando o comando MQSC REFRESH SECURITY TYPE(SSL) é emitido para atualizar o ambiente TLS do IBM MQ.
- Para processos do aplicativo cliente, quando a última conexão do TLS no processo é fechada. A próxima conexão do TLS escolhe as mudanças de certificado.
- Para canais que são executados como encadeamentos de um processo de conjunto de processo (amqrmppa), quando o processo de conjunto de processo é iniciado ou reiniciado e executa pela primeira vez um canal do TLS. Se o processo de conjunto de processo já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).
- Para canais que são executados como encadeamentos do inicializador de canal, quando o inicializador de canais é iniciado ou reiniciado e executa um canal do TLS pela primeira vez. Se o processo do inicializador de canais já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).
- Para canais que são executados como encadeamentos de um listener TCP/IP, quando o listener é iniciado ou reiniciado e recebe pela primeira vez uma solicitação para iniciar um canal do TLS. Se o listener já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).

Configurando hardware de criptografia no IBM i

Use este procedimento para configurar o Coprocessador Criptográfico no IBM i

Antes de começar

Verifique se o seu perfil de usuário possui autoridades especiais *ALLOBJ e *SECADM para que seja possível configurar o hardware do co-processador.

Procedimento

1. Acesse `http://`*`machine`*`.domain:2001` ou `https://`*`machine`*`.domain:2010`, em que *machine* é o nome do computador.

   Uma caixa de diálogo é exibida solicitando um nome de usuário e uma senha.
2. Digite um perfil válido do usuário e senha do IBM i.
3. Acesse Criptografia e siga os links apropriados para obter informações adicionais.

Como proceder a seguir

Para obter informações mais específicas sobre como configurar o Coprocessador Criptográfico 4767, veja Coprocessador Criptográfico 4767.

ULW Trabalhando com SSL/TLS no UNIX, Linux, and Windows

Em sistemas UNIX, Linux, and Windows, o suporte de Segurança da Camada de Transporte (TLS) é instalado com o IBM MQ.

Para obter informações mais detalhadas sobre as políticas de validação de certificado, consulte Validação do certificado e design da política de confiança.

ULW *Usando runmqckm, runmqakm e strmqikm para gerenciar certificados digitais*

Nos sistemas UNIX, Linux, and Windows, gerencie chaves e certificados digitais com a GUI do **strmqikm** (iKeyman) ou na linha de comandos usando **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

V 9.1.0

Atenção: Ambos os comandos, **runmqckm** e **strmqikm**, dependem do Java Runtime Environment (JRE) do IBM MQ. No IBM MQ 9.1, se o JRE não estiver instalado, você receberá a mensagem AMQ9183.

- Para sistemas **UNIX and Linux**:
  - Use o comando **strmqikm** (iKeyman) para iniciar a GUI iKeyman.
  - Use o comando **runmqckm** (iKeycmd) para executar tarefas com a interface da linha de comandos do iKeycmd.
  - Use o comando **runmqakm** (GSKCapiCmd) para executar tarefas com a interface da linha de comandos runmqakm. A sintaxe de comando para **runmqakm** é a mesma que a sintaxe para **runmqckm**.

    Se for preciso gerenciar certificados TLS de um modo compatível com FIPS, use o comando **runmqakm** no lugar dos comandos **runmqckm** ou **strmqikm**.

  Consulte Gerenciando chaves e certificados para uma descrição completa das interfaces da linha de comandos para os comandos **runmqckm** e **runmqakm**.

  Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS #11, observe que iKeycmd e iKeyman são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 32-bit bits são as únicas exceções, pois o iKeyman e iKeycmd são programas de 32-bit bits nessas plataformas.

  Consulte GSKit: PKCS#11 e IBM MQ modo de endereçamento do JRE para informações adicionais.

  Antes de executar o comando **strmqikm** para iniciar a GUI do iKeyman, assegure-se de estar trabalhando em uma máquina que esteja apta para executar o X Window System e faça o seguinte:
  - Defina a variável de ambiente DISPLAY, por exemplo:

    ```
    export DISPLAY=mypc:0
    ```
  - Verifique se a variável de ambiente PATH contém **/usr/bin** e **/bin**. Isso também é necessário para os comandos **runmqckm** e **runmqakm** Por exemplo:

    ```
    export PATH=$PATH:/usr/bin:/bin
    ```
- Para sistemas **Windows**:
  - Use o comando **strmqikm** para iniciar a GUI iKeyman.
  - Use o comando **runmqckm** para executar tarefas com a interface da linha de comandos do iKeycmd.

    Se for preciso gerenciar certificados TLS de um modo compatível com FIPS, use o comando **runmqakm** no lugar dos comandos **runmqckm** ou **strmqikm**.
  - Use o comando **runmqakm -keydb** com a opção *stashpw* ou *stash*.

Ao usar o comando **runmqakm -keydb** dessa maneira, para exemplo:

```
runmqakm -keydb -create -db key.kdb -pw secretpwd -stash
```

o arquivo resultante `.sth` não tem permissão de leitura ativada para o grupo `mqm`.

Somente o criador pode ler o arquivo. Depois de criar um arquivo stash utilizando o comando **runmqakm**, verifique as permissões de arquivo e conceda permissão para a conta de serviço em execução do gerenciador de filas ou para um grupo como o `mqm` local.

Para solicitar rastreio de TLS em sistemas UNIX, Linux ou Windows, veja strmqtrc.

Referências relacionadas

Comandos runmqckm e runmqakm

Esta seção descreve os comandos runmqckm e runmqakm de acordo com o objeto do comando.

ULW *Configurando um repositório de chaves no UNIX, Linux, and Windows*

É possível configurar um repositório de chaves usando a GUI **strmqikm** (iKeyman) ou a partir da linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

Sobre esta tarefa

Uma conexão TLS requer um *repositório de chaves* em cada extremidade da conexão. Cada gerenciador de filas do IBM MQ e IBM MQ MQI client deverá ter acesso a um repositório de chaves. Para obter informações adicionais, consulte "O repositório de chaves SSL/TLS" na página 25.

Em sistemas UNIX, Linux, and Windows, os certificados digitais são armazenados em um arquivo do banco de dados de chave que é gerenciado usando a interface com o usuário **strmqikm** ou usando os comandos **runmqckm** ou **runmqakm**. Esses certificados digitais têm rótulos. Um rótulo específico associa um certificado pessoal a um gerenciador de filas ou IBM MQ MQI client. O TLS usa esse certificado para propósitos de autenticação. Em sistemas UNIX, Linux, and Windows, o IBM MQ usa o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou IBM MQ MQI client ID de logon do usuário anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.

O nome do arquivo do banco de dados de chave contém um caminho e nome de raiz:

- Em sistemas UNIX and Linux, o caminho padrão para um Gerenciador de Filas (configurado quando você criou o Gerenciador de Filas) é `/var/mqm/qmgrs/`*`queue_manager_name`*`/ssl`.

  Em sistemas Windows, o caminho padrão é *`MQ_INSTALLATION_PATH`*`\Qmgrs\`*`queue_manager_name`*`\ssl`, em que *`MQ_INSTALLATION_PATH`* é o diretório no qual o IBM MQ é instalado. Por exemplo, `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl`.

  O nome de raiz padrão é `key`. Opcionalmente, é possível escolher seu próprio caminho e nome de raiz, mas a extensão deve ser `.kdb`.

  Se você escolher seu próprio caminho ou nome de arquivo, configure as permissões para que o arquivo controle rigorosamente o acesso a ele.
- Para um cliente IBM MQ não há caminho padrão ou nome de raiz. Controle rigorosamente o acesso a esse arquivo. A extensão deve ser `.kdb`.

Não crie os repositórios de chaves em um sistema de arquivos que não suporta bloqueios no nível de arquivos, por exemplo, o NFS versão 2 em sistemas Linux.

Consulte "Alterando o local do repositório de chaves de um gerenciador de filas no UNIX, Linux, and Windows" na página 295 para obter informações sobre a verificação e a especificação do nome do arquivo de banco de dados de chave. Você pode especificar o nome do arquivo de banco de dados de chave antes ou depois de criar o arquivo de banco de dados de chave.

O ID do usuário usado para executar os comandos **strmqikm** ou **runmqckm** precisa ter permissão de gravação no diretório no qual o arquivo de banco de dados de chaves é criado ou atualizado. Para

um gerenciador de filas que usa o diretório padrão `ssl`, o ID do usuário com o qual você executa **strmqikm** ou **runmqckm** precisa ser um membro do grupo mqm. Para um IBM MQ MQI client, ao executar **strmqikm** ou **runmqckm** com um ID do usuário diferente daquele no qual o cliente é executado, deve-se alterar as permissões do arquivo para permitir que o IBM MQ MQI client acesse o arquivo do banco de dados de chave no tempo de execução. Para obter mais informações, consulte "Acessando e protegendo seus arquivos do banco de dados de chaves no Windows" na página 292 ou "Acessando e Protegendo seus Arquivos do Banco de Dados de Chaves nos Sistemas UNIX and Linux" na página 293.

Em **strmqikm** ou **runmqckm** para IBM WebSphere MQ 7.0, novos bancos de dados de chaves são preenchidos automaticamente com um conjunto de certificados de autoridade de certificação (CA) pré-definidos. Em **strmqikm** ou **runmqckm** para IBM MQ 8.0, os bancos de dados de chaves não são preenchidos automaticamente, tornando a configuração inicial mais segura porque apenas os certificados de autoridade de certificação desejados são incluídos no arquivo do banco de dados de chaves.

Nota: Devido a essa mudança no comportamento do GSKit 8.0 que resulta em certificados de CA que não são mais incluídos automaticamente no repositório, deve-se incluir manualmente seus certificados de CA preferenciais. Essa mudança de comportamento fornece a você um controle mais granular sobre os certificados de CA usados. Consulte "Incluindo certificados de autoridade de certificação em um repositório de chaves vazio no UNIX, Linux, and Windows com o GSKit 8.0" na página 293.

Você cria o banco de dados de chaves usando a linha de comandos ou usando a interface com o usuário **strmqikm** (iKeyman).

Nota: Se deve-se gerenciar certificados TLS de uma maneira que esteja de acordo com FIPS, use o comando **runmqakm**. A interface com o usuário **strmqikm** não fornece uma opção compatível com FIPS.

Procedimento

Crie um banco de dados de chave usando a linha de comandos

1. Execute um dos comandos a seguir:
   - Usando o **runmqckm**:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Usando o **runmqakm**:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
     -stash -fips -strong
     ```

   em que:

   -db *filename*
   Especifica o nome completo do arquivo de um banco de dados de chaves do CMS e deve ter uma extensão de arquivo de `.kdb`.

   -pw *password*
   Especifica a senha para o banco de dados de chaves do CMS.

   -type *cms*
   Especifica o tipo de banco de dados. (Para o IBM MQ, ele deve ser `cms`.)

   -stash
   Salva a senha do banco de dados de chaves em um arquivo.

   -fips
   Especifica que o comando é executado no modo FIPS. Quando em modo FIPS, o componente ICC usa algoritmos que são validados para FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

   -strong
   Verifica se a senha inserida atende aos requisitos mínimos de força da senha. Os requisitos mínimos para uma senha são como a seguir:

- A senha deve ter no mínimo 14 caracteres.
- A senha deve conter no mínimo um caractere minúsculo, um caractere maiúsculo e um dígito ou caractere especial. Os caracteres especiais incluem o asterisco (*), o sinal de dólar ($), o sinal de número (#) e o sinal de percentual (%). Um espaço é classificado como um caractere especial.
- Cada caractere pode ocorrer no máximo de três vezes em uma senha.
- O máximo de dois caracteres consecutivos na senha podem ser idênticos.
- Todos os caracteres estão configurados no padrão para caracteres para impressão ASCII dentro do intervalo –. 0x20 - 0x7E.

Como alternativa, crie um banco de dados de chaves usando a interface com o usuário **strmqikm** (iKeyman).

2. Nos sistemas UNIX and Linux, efetue login como usuário raiz. Nos sistemas Windows, efetue login como Administrador ou como um membro do grupo MQM.
3. Inicie a interface com o usuário executando o comando **strmqikm**.
4. No menu **Arquivo do Banco de Dados de Chave**, clique em **Novo**.

   A janela Novo é aberta.
5. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
6. No campo **Nome do Arquivo**, digite um nome de arquivo.

   Este campo já contém o texto `key.kdb`. Se o seu nome de raiz for `key`, deixe este campo inalterado. Se você especificou um nome de raiz diferente, substitua `key` por seu nome de raiz. No entanto, a extensão `.kdb` não deve ser mudada.
7. No campo **Localização**, digite o caminho.

   Por exemplo:

   - Para um Gerenciador de Filas: `/var/mqm/qmgrs/QM1/ssl` (em sistemas UNIX and Linux) ou `C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl` (em sistemas Windows).

     O caminho deve corresponder ao valor do atributo **SSLKeyRepository** do gerenciador de filas.
   - Para um cliente IBM MQ: `/var/mqm/ssl` (em sistemas UNIX and Linux) ou `C:\mqm\ssl` (em sistemas Windows).
8. Clique em **OK**.

   A janela Prompt de Senha é aberta.
9. Digite a senha no campo **Senha** e digite-a novamente no campo **Confirmar Senha**.
10. Selecione a caixa de seleção **Stash the password to a file**.

    Nota: Se você não armazenar a senha em arquivo stash, as tentativas para iniciar os canais TLS falharão porque não será possível obter a senha necessária para acessar o arquivo do banco de dados de chave.
11. Clique em **OK**.

    A janela Certificados pessoais é aberta.
12. Configure as permissões de acesso conforme descrito em “Acessando e protegendo seus arquivos do banco de dados de chaves no Windows” na página 292 ou “Acessando e Protegendo seus Arquivos do Banco de Dados de Chaves nos Sistemas UNIX and Linux” na página 293.

Windows *Acessando e protegendo seus arquivos do banco de dados de chaves no Windows*

Os arquivos do banco de dados de chave podem não ter as permissões de acesso apropriadas. Você deve configurar o acesso apropriado a esses arquivos.

Configure o controle de acesso aos arquivos *key*`.kdb`, *key*`.sth`, *key*`.crl` e *key*`.rdb`, em que *chave* é o nome derivado de seu banco de dados de chave, para conceder autoridade a um conjunto restrito de usuários.

Considere conceder acesso da seguinte forma:

autoridade plena
BUILTIN\Administrators, NT AUTHORITY\SYSTEM e o usuário que criou os arquivos de banco de dados.

autoridade de leitura
Para um gerenciador de filas, apenas o grupo mqm local. Isto supõe que o MCA esteja em execução com um ID do usuário no grupo mqm.

Para um cliente, o ID do usuário com o qual o processo do cliente está sendo executado.

Linux UNIX *Acessando e Protegendo seus Arquivos do Banco de Dados de Chaves nos Sistemas UNIX and Linux*

Os arquivos do banco de dados de chave podem não ter as permissões de acesso apropriadas. Você deve configurar o acesso apropriado a esses arquivos.

Para um gerenciador de filas, configure permissões nos arquivos de banco de dados de chave para que os processos de gerenciador de filas e de canal possam lê-los quando necessário, mas outros usuários não possam ler ou modificá-los. Normalmente, o usuário mqm precisa de permissões de leitura. Se você tiver criado o arquivo do banco de dados de chave efetuando login como o usuário mqm, as permissões serão provavelmente suficientes; se você não era o usuário mqm, mas outro usuário nesse grupo, provavelmente precisará conceder permissões de leitura a outros usuários no grupo mqm.

De forma semelhante para um cliente, configure permissões nos arquivos de banco de dados de chave para que os processos de cliente possam lê-los quando necessário, mas outros usuários não possam ler ou modificá-los. Normalmente, o usuário sob o qual o processo do cliente é executado precisa de permissões de leitura. Se você tiver criado o arquivo do banco de dados de chave efetuando login como esse usuário, as permissões serão provavelmente suficientes; se você não era o usuário do processo de cliente, mas outro usuário nesse grupo, provavelmente precisará conceder permissões de leitura a outros usuários no grupo.

Configure as permissões nos arquivos *key*`.kdb`, *key*`.sth`, *key*`.crl` e *key*`.rdb`, em que *key* é o nome raiz de seu banco de dados de chaves, para leitura e gravação para o proprietário do arquivo, e para leitura para o grupo de usuários mqm ou cliente (-rw-r -----).

ULW *Incluindo certificados de autoridade de certificação em um repositório de chaves vazio no UNIX, Linux, and Windows com o GSKit 8.0*

Siga este procedimento para incluir um ou mais dos certificados de CA padrão em um repositório de chaves vazio com GSKit versão 8.

No GSKit 7.0, o comportamento ao criar um novo repositório de chaves foi incluir automaticamente um conjunto de certificados de autoridade de certificação padrão nas autoridades de certificação normalmente usadas. Para o GSKit versão 8, este comportamento foi mudado para que os certificados de CA não sejam mais automaticamente incluídos no repositório. Agora é exigido que o usuário inclua certificados de CA manualmente no repositório de chaves.

Usando o `strmqikm`

Execute as seguintes etapas na máquina na qual deseja incluir o certificado de CA:

1. Inicie a GUI usando o comando **`strmqikm`** (no UNIX, Linux, and Windows).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo de banco de dados de chave ao qual deseja adicionar o certificado, por exemplo `key.kdb`.
6. Clique em **Abrir**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do arquivo de banco de dados de chave é exibido no campo **Nome de Arquivo**.

8. No campo **Conteúdo do banco de dados de chave**, selecione **Certificados de Assinante**.
9. Clique em **Preencher**. A janela Incluir Certificado de CA é aberta.
10. Os certificados de CA que estão disponíveis para serem incluídos no repositório são exibidos em uma estrutura de árvore hierárquica. Selecione a entrada de nível superior para a organização em cujos certificados de CA você deseja confiar para visualizar a lista completa de certificados de CA válidos.
11. Selecione na lista os certificados de CA nos quais deseja confiar e clique em **OK**. Os certificados são incluídos no repositório de chaves.

Usando a linha de comandos

Use os comandos a seguir para listar e, em seguida, inclua certificados de autoridade de certificação usando o **runmqckm**:

- Emita o seguinte comando para listar os certificados de CA padrão junto com as organizações que os emitem:

```
runmqckm -cert -listsigners
```

- Emita o seguinte comando para incluir todos os certificados de CA para a organização especificada no campo *rótulo*:

```
runmqckm -cert -populate -db filename -pw password -label label
```

em que:

-db *filename*	é o nome do caminho completo do banco de dados de chaves.
-pw *password*	é a senha do banco de dados de chave.
-label *label*	é o rótulo anexado ao certificado.

Nota: Incluir um certificado de autoridade de certificação para um repositório de chaves resulta no IBM MQ confiando em todos os certificados pessoais assinados por esse certificado de autoridade de certificação. Considere cautelosamente em quais Autoridades de certificação você deseja confiar e inclua apenas o conjunto de certificados de CA necessários para autenticar seus clientes e gerenciadores. Não é recomendado incluir o conjunto completo de certificados de CA padrão, a menos que esse seja um requisito definitivo para sua política de segurança.

ULW *Localizando o repositório de chaves para um gerenciador de filas no UNIX, Linux, and Windows*

Use este procedimento para obter o local do arquivo do banco de dados de chave do gerenciador de filas

Procedimento

1. Exiba os atributos do seu gerenciador de filas, usando um dos seguintes comandos MQSC:

```
DISPLAY QMGR ALL
DISPLAY QMGR SSLKEYR
```

   Também é possível exibir os atributos do gerenciador de filas usando o IBM MQ Explorer ou comandos PCF.
2. Examine a saída do comando para o nome do caminho e de raiz do arquivo de banco de dados da chave.
   Por exemplo,
   a. no UNIX and Linux: `/var/mqm/qmgrs/QM1/ssl/key`, em que `/var/mqm/qmgrs/QM1/ssl` é o caminho e `key` e o nome derivado

b. no Windows: *MQ_INSTALLATION_PATH*\qmgrs\QM1\ssl\key, em que *MQ_INSTALLATION_PATH*\qmgrs\QM1\ssl é o caminho e key é o nome derivado. O *MQ_INSTALLATION_PATH* representa o diretório de alto nível no qual o IBM MQ está instalado.

ULW *Alterando o local do repositório de chaves de um gerenciador de filas no UNIX, Linux, and Windows*

É possível alterar o local do arquivo de banco de dados de chave do gerenciador de filas por vários meios, incluindo o comando MQSC ALTER QMGR.

É possível alterar o local do arquivo de banco de dados de chave do seu gerenciador de filas, ao usar o comando MQSC ALTER QMGR para configurar o atributo do repositório de chaves do seu gerenciador de filas. Por exemplo, no UNIX and Linux:

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

O arquivo de banco de dados chave tem o nome completo do arquivo: `/var/mqm/qmgrs/QM1/ssl/MyKey.kdb`

No Windows:

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey')
```

O arquivo de banco de dados chave tem o nome completo do arquivo: `C:\Program Files\IBM\MQ\Qmgrs\QM1\ssl\Mykey.kdb`

Atenção: Assegure-se de não incluir a extensão `.kdb` no nome do arquivo na palavra-chave SSLKEYR, já que o gerenciador de filas anexa esta extensão automaticamente.

Também é possível mudar os atributos do gerenciador de filas usando os comandos Explorer ou PCF do IBM MQ.

Ao alterar o local de um arquivo de banco de dados de chave do gerenciador de filas, os certificados não serão transferidos a partir do local antigo. Se o arquivo de banco de dados de chave que você está agora acessando for um novo arquivo de banco de dados de chave, você deverá preenchê-lo com os certificados pessoal e de autoridade de certificação de que precisa, conforme descrito em "Importando um certificado pessoal em um repositório de chaves no UNIX, Linux, and Windows" na página 310.

ULW *Localizando o repositório de chaves para um IBM MQ MQI client no UNIX, Linux, and Windows*

O local do repositório de chaves é fornecido pela variável MQSSLKEYR ou especificado na chamada MQCONNX.

Examine a variável de ambiente MQSSLKEYR para encontrar o local do arquivo de banco do dados de chave para seu IBM MQ MQI client. Por exemplo:

```
echo $MQSSLKEYR
```

Verifique também o aplicativo, porque o nome do arquivo do banco de dados de chave também poderá ser configurado em uma chamada MQCONNX, conforme descrito em "Especificando a o local do repositório de chaves para um IBM MQ MQI client no UNIX, Linux, and Windows" na página 295. O valor definido em uma chamada MQCONNX substitui o valor de MQSSLKEYR.

ULW *Especificando a o local do repositório de chaves para um IBM MQ MQI client no UNIX, Linux, and Windows*

Não há um repositório de chaves padrão para um IBM MQ MQI client. É possível especificar seu local em uma de duas maneiras. Certifique-se de que o arquivo do banco de dados de chaves somente possa ser acessado por usuários ou administradores pretendidos para evitar cópias não-autorizadas para outros sistemas.

É possível especificar o local do arquivo do banco de dados de chaves para o IBM MQ MQI client de duas maneiras:

- Configurar a variável de ambiente MQSSLKEYR. Por exemplo, no UNIX and Linux:

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  O arquivo de banco de dados de chave tem o nome completo de arquivo:

  ```
  /var/mqm/ssl/key.kdb
  ```

  No Windows:

  ```
  set MQSSLKEYR=C:\Program Files\IBM\MQ\ssl\key
  ```

  O arquivo de banco de dados de chave tem o nome completo de arquivo:

  ```
  C:\Program Files\IBM\MQ\ssl\key.kdb
  ```

  Nota: A extensão **.**kdb é uma parte obrigatória do nome do arquivo, mas não é incluída como parte do valor da variável de ambiente.
- Forneça o nome do caminho e de raiz do arquivo de banco de dados de chaves no campo *KeyRepository* da estrutura do MQSCO quando um aplicativo executar uma chamada MQCONNX. Para obter mais informações sobre a utilização da estrutura MQSCO em MQCONNX, consulte Visão geral para MQSCO.

ULW *Quando mudanças nos certificados ou no armazenamento de certificados tornam-se efetivas no UNIX, Linux, and Windows*

Ao alterar os certificados em um armazenamento de certificados, ou o local do armazenamento de certificados, as mudanças entrarão em vigor, dependendo do tipo de canal e de como o canal está sendo executado.

Mudanças nos certificados no arquivo do banco de dados de chave e no atributo de repositório de chaves entrarão em vigor nas seguintes situações:

- Quando um novo processo de canal único de saída executa um canal do TLS pela primeira vez.
- Quando um novo processo de canal único TCP/IP de entrada recebe pela primeira vez uma solicitação para iniciar um canal do TLS.
- Quando o comando MQSC REFRESH SECURITY TYPE(SSL) é emitido para atualizar o ambiente do TLS.
- Para processos do aplicativo cliente, quando a última conexão do TLS no processo é fechada. A próxima conexão do TLS selecionará as mudanças do certificado.
- Para canais que são executados como encadeamentos de um processo de conjunto de processo (amqrmppa), quando o processo de conjunto de processo é iniciado ou reiniciado e executa pela primeira vez um canal do TLS. Se o processo de conjunto de processo já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).
- Para canais que são executados como encadeamentos do inicializador de canal, quando o inicializador de canais é iniciado ou reiniciado e executa um canal do TLS pela primeira vez. Se o processo do inicializador de canais já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).
- Para canais que são executados como encadeamentos de um listener TCP/IP, quando o listener é iniciado ou reiniciado e recebe pela primeira vez uma solicitação para iniciar um canal do TLS. Se o listener já tiver executado um canal do TLS e você desejar que a mudança entre em vigor imediatamente, execute o comando MQSC REFRESH SECURITY TYPE(SSL).

Também é possível atualizar o ambiente do TLS do IBM MQ usando o IBM MQ Explorer ou comandos PCF.

ULW *Criando um certificado pessoal autoassinado no UNIX, Linux, and Windows*

É possível criar um certificado autoassinado usando a GUI (iKeyman) **strmqikm** ou a partir da linha de comandos usando **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

Nota: O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.

Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.

Para obter mais informações sobre o motivo pelo qual você pode desejar usar certificados autoassinados, consulte Usando certificados autoassinados para autenticação mútua de dois gerenciadores de filas.

Nem todos os certificados digitais podem ser usados com todos os CipherSpecs. Assegure-se de criar um certificado que seja compatível com os CipherSpecs que precisa usar. O IBM MQ suporta três tipos diferentes de CipherSpec. Para obter detalhes, consulte “Interoperabilidade da curva elíptica e do RSA de CipherSpecs” na página 46 no tópico “Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45.

Para usar o CipherSpecs do Tipo 1 (aqueles com nomes que começam com ECDHE_ECDSA_), deve-se usar o comando **runmqakm** para criar o certificado e deve-se especificar um parâmetro de algoritmo de assinatura ECDSA da Curva Elíptica; por exemplo **-sig_alg** EC_ecdsa_with_SHA384.

Consulte “Opções runmqckm e runmqakm em UNIX, Linux, and Windows” na página 535 para obter uma lista das opções disponíveis com o algoritmo hash **-sig_alg** ..

Se você estiver usando:

- A GUI, consulte “Usando a interface com o usuário strmqikm” na página 297
- A linha de comandos, consulte “Usando a linha de comandos” na página 298

ULW *Usando a interface com o usuário **strmqikm***

É possível criar um certificado pessoal usando a GUI **strmqikm** (iKeyman).

Sobre esta tarefa

O **strmqikm** não fornece uma opção compatível com FIPS. Se precisar gerenciar certificados TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Procedimento

Conclua as etapas a seguir para criar um certificado pessoal para o seu gerenciador de filas ou IBM MQ MQI client usando a interface gráfica com o usuário:

1. Inicie a GUI usando o comando **strmqikm**.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**.

   A janela **Abrir** é exibida.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo do banco de dados de chaves a partir do qual você quer gerar seu pedido; por exemplo, key.kdb.
6. Clique em **OK**.

   A janela **Prompt de senha** é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**.

   O nome do seu arquivo do banco de dados de chave é mostrado no campo **Nome do arquivo**.

8. No menu **Criar** clique em **Novo Certificado Auto-Assinado**. A janela Criar Novo Certificado Autoassinado é exibida.
9. No campo **Rótulo chave**, insira o rótulo certificado.

   O rótulo é o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou o ID do usuário de logon do IBM MQ MQI client anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.
10. Digite ou selecione um valor para qualquer campo no campo **Nome distinto** ou qualquer um dos campos **Nome alternativo do assunto**.
11. Para os campos restantes, aceite os valores padrão ou digite ou selecione novos valores.

    Para obter mais informações sobre Nomes Distintos, consulte “Nomes Distintos” na página 11.
12. Clique em **OK**.

    A lista **Certificados Pessoais** mostra o rótulo certificado pessoal auto-assinado que você criou.

Como proceder a seguir

Enviar uma solicitação de certificado para uma CA. Consulte “Recebendo certificados pessoais em um repositório de chaves no UNIX, Linux, and Windows” na página 304 para obter informações adicionais.

ULW *Usando a linha de comandos*

É possível criar um certificado pessoal na linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd). Se precisar gerenciar certificados SSL ou TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Procedimento

Crie um certificado pessoal autoassinado usando o comando **runmqckm** ou **runmqakm** (GSKCapiCmd).

- Usando o **runmqckm** no UNIX, Linux, and Windows:

```
runmqckm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days
 -sig_alg algorithm
```

  Em vez de `-dn` *distinguished_name*, é possível usar `-san_dnsname` *DNS_names*, `-san_emailaddr` *email_addresses* ou `-san_ipaddr` *IP_addresses*.

- Usando o **runmqakm**:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -fips -sig_alg algorithm
```

em que:

-db *filename*
Especifica o nome completo do arquivo de um banco de dados de chaves do CMS.

-pw *password*
Especifica a senha para o banco de dados de chaves do CMS.

-label *label*
Especifica o rótulo chave anexado ao certificado. O rótulo é o valor do atributo **CERTLABL**, se estiver configurado, ou o `ibmwebspheremq` padrão com o nome do gerenciador de filas ou o ID do usuário de logon IBM MQ MQI client anexado, tudo em letras minúsculas. Consulte “Rótulos de Certificados Digitais, Entendendo os Requisitos” na página 26 para obter detalhes.

-dn *distinguished_name*
Especifica o nome distinto X.500 colocado entre aspas duplas. Pelo menos um atributo é necessário. É possível fornecer diversos atributos OU e DC.

Nota: As ferramentas **runmqckm** e **runmqakm** se referem ao atributo de código de endereçamento postal como POSTALCODE, não PC. Sempre especifique POSTALCODE no parâmetro **-dn** ao usar esses comandos de gerenciamento de certificados para solicitar certificados com um código de endereçamento postal.

-size *key_size*
Especifica o tamanho da chave. Se você estiver usando o **runmqckm**, o valor poderá ser 512 ou 1024. Se estiver usando **runmqakm**, o valor pode ser 512, 1024 ou 2048.

x509version *version*
A versão do certificado X.509 a ser criado. O valor pode ser de 1, 2 ou 3. O padrão é 3.

-file *filename*
Especifica o nome do arquivo para a solicitação de certificado.

-expire *days*
O prazo de expiração em dias do certificado. O padrão é 365 dias para um certificado.

-fips
Especifica que o comando é executado no modo FIPS. Somente o componente FIPS ICC será usado e este componente deverá ser inicializado com sucesso no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqaqm** falhará.

-sig_alg
Para **runmqckm**, especifica o algoritmo de assinatura assimétrica usado para a criação do par de chaves da entrada. O valor pode ser 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. O valor padrão é SHA1WithRSA.

-sig_alg
Para o **runmqakm**, especifica o algoritmo hash usado durante a criação de uma solicitação de certificado. Este algoritmo hash é usado para criar a assinatura associada a solicitação de certificado criada recentemente. O valor pode ser md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 ou EC_ecdsa_with_SHA512. O valor padrão é SHA1WithRSA.

-san_dnsname *DNS_names*
Especifica uma lista de nomes DNS delimitada por vírgulas ou espaços para a entrada sendo criada.

-san_emailaddr *email_addresses*
Especifica uma lista de endereços de e-mail delimitada por vírgulas ou espaços para a entrada sendo criada.

-san_ipaddr *IP_addresses*
Especifica uma lista de endereços IP delimitada por vírgulas ou espaços para a entrada sendo criada.

Como proceder a seguir

Enviar uma solicitação de certificado para uma CA. Consulte “Recebendo certificados pessoais em um repositório de chaves no UNIX, Linux, and Windows” na página 304 para obter informações adicionais.

ULW *Solicitando um certificado pessoal no UNIX, Linux, and Windows*

É possível solicitar um certificado pessoal usando a GUI (iKeyman) **strmqikm** ou a partir da linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd). Se precisar gerenciar certificados SSL ou TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Sobre esta tarefa

É possível solicitar um certificado pessoal usando a GUI do **strmqikm** ou por meio da linha de comandos, desde que as contraprestações a seguir sejam cumpridas:

- O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.
- Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.
- Nem todos os certificados digitais podem ser usados com todos os CipherSpecs. Assegure-se de solicitar um certificado que seja compatível com os CipherSpecs que precisa usar. O IBM MQ suporta três tipos diferentes de CipherSpec. Para obter detalhes, consulte "Interoperabilidade da curva elíptica e do RSA de CipherSpecs" na página 46 no tópico "Certificados digitais e compatibilidade de CipherSpec no IBM MQ" na página 45.
- Para usar o Tipo 1 CipherSpecs (com nomes começando com ECDHE_ECDSA_), deve-se usar o comando **runmqakm** para solicitar o certificado e deve-se especificar um parâmetro de algoritmo de assinatura ECDSA de Curva Elíptica; por exemplo, **-sig_alg** EC_ecdsa_with_SHA384.

  Consulte "Opções runmqckm e runmqakm em UNIX, Linux, and Windows" na página 535 para obter uma lista das opções disponíveis com o algoritmo hash **-sig_alg** ..
- Apenas o comando **runmqakm** fornece uma opção compatível com FIPS.
- Se você estiver usando o hardware de criptografia, consulte "Solicitando um Certificado Pessoal para o Hardware PKCS #11" na página 319.

Se você estiver usando:

- A GUI, consulte "Usando a interface com o usuário strmqikm" na página 300
- A linha de comandos, consulte "Usando a linha de comandos" na página 301

ULW *Usando a interface com o usuário **strmqikm***

É possível solicitar um certificado pessoal usando a GUI (iKeyman) **strmqikm** ou a partir da linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd). Se precisar gerenciar certificados SSL ou TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Sobre esta tarefa

O **strmqikm** não fornece uma opção compatível com FIPS. Se precisar gerenciar certificados TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Procedimento

Conclua as etapas a seguir para se candidatar a um certificado pessoal usando a interface com o usuário iKeyman:

1. Inicie a interface com o usuário usando o comando **strmqikm**.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**.

   A janela **Abrir** é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.

5. Selecione o arquivo do banco de dados de chaves a partir do qual você quer gerar seu pedido; por exemplo, `key.kdb`.
6. Click **Open**.

   A janela **Prompt de senha** é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**.

   O nome do seu arquivo do banco de dados de chave é mostrado no campo **Nome do arquivo**.
8. No menu **Criar** clique em **Novo Pedido de Certificado**. A janela **Criar nova chave e solicitação de certificado** é aberta.
9. No campo **Rótulo chave**, insira o rótulo certificado.

   O rótulo é o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou o ID do usuário de logon do IBM MQ MQI client anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.
10. Digite ou selecione um valor para qualquer campo no campo **Nome distinto** ou qualquer um dos campos **Nome alternativo do assunto**. Para os campos restantes, seja aceito os valores padrão ou insira ou selecione novos valores.

    Para obter mais informações sobre Nomes Distintos, consulte “Nomes Distintos” na página 11.
11. No campo **Inserir o nome de um arquivo no qual armazenar a solicitação de certificado**, aceite o padrão `certreq.arm` ou insira um novo valor com um caminho completo.
12. Clique em **OK**.

    Uma janela de confirmação é exibida.
13. Clique em **OK**.

    A lista **Pedidos de Certificado Pessoal** mostra o rótulo do novo pedido de certificado pessoal que você criou. O pedido de certificado é armazenado no arquivo que você escolheu na etapa “11” na página 301.
14. Solicite o novo certificado pessoal enviando o arquivo para uma autoridade de certificação (CA) ou copiando o arquivo no formulário de solicitação no website para a CA.

ULW *Usando a linha de comandos*

É possível solicitar um certificado pessoal na linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd). Se precisar gerenciar certificados SSL ou TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Procedimento

Solicite um certificado pessoal usando o comando **runmqckm** ou **runmqakm** (GSKCapiCmd).

- Usando o **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
        -file filename -sig_alg algorithm
```

  Em vez de `-dn distinguished_name`, é possível usar `-san_dsname DNS_names`, `-san_emailaddr email_addresses` ou `-san_ipaddr IP_addresses`.

- Usando o **runmqakm**:

```
runmqakm -certreq -create -db filename -pw
password -label label
         -dn distinguished_name -size key_size
         -file filename -fips -sig_alg algorithm
```

em que:

-db ***filename***
Especifica o nome completo do arquivo de um banco de dados de chaves do CMS.

-pw ***password***
Especifica a senha para o banco de dados de chaves do CMS.

-label ***label***
Especifica o rótulo chave anexado ao certificado. O rótulo é o valor do atributo **CERTLABL**, se estiver configurado, ou o `ibmwebspheremq` padrão com o nome do gerenciador de filas ou o ID do usuário de logon IBM MQ MQI client anexado, tudo em letras minúsculas. Consulte "Rótulos de Certificados Digitais, Entendendo os Requisitos" na página 26 para obter detalhes.

-dn ***distinguished_name***
Especifica o nome distinto X.500 colocado entre aspas duplas. Pelo menos um atributo é necessário. É possível fornecer diversos atributos OU e DC.

Nota: As ferramentas **runmqckm** e **runmqakm** se referem ao atributo de código de endereçamento postal como POSTALCODE, não PC. Sempre especifique POSTALCODE no parâmetro **-dn** ao usar esses comandos de gerenciamento de certificados para solicitar certificados com um código de endereçamento postal.

-size ***key_size***
Especifica o tamanho da chave. Se você estiver usando o **runmqckm**, o valor poderá ser 512 ou 1024. Se estiver usando **runmqakm**, o valor pode ser 512, 1024 ou 2048.

-file ***filename***
Especifica o nome do arquivo para a solicitação de certificado.

-fips
Especifica que o comando é executado no modo FIPS. Quando em modo FIPS, o componente ICC usa algoritmos que são validados para FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

-sig_alg
Para **runmqckm**, especifica o algoritmo de assinatura assimétrica usado para a criação do par de chaves da entrada. O valor pode ser `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`. O valor padrão é `SHA1WithRSA`.

-sig_alg
Para o **runmqakm**, especifica o algoritmo hash usado durante a criação de uma solicitação de certificado. Este algoritmo hash é usado para criar a assinatura associada a solicitação de certificado criada recentemente. O valor pode ser `md5`, `MD5_WITH_RSA`, `MD5WithRSA`, `SHA_WITH_DSA`, `SHA_WITH_RSA`, `sha1`, `SHA1WithDSA`, `SHA1WithECDSA`, `SHA1WithRSA`, `sha224`, `SHA224_WITH_RSA`, `SHA224WithDSA`, `SHA224WithECDSA`, `SHA224WithRSA`, `sha256`, `SHA256_WITH_RSA`, `SHA256WithDSA`, `SHA256WithECDSA`, `SHA256WithRSA`, `SHA2WithRSA`, `sha384`, `SHA384_WITH_RSA`, `SHA384WithECDSA`, `SHA384WithRSA`, `sha512`, `SHA512_WITH_RSA`, `SHA512WithECDSA`, `SHA512WithRSA`, `SHAWithDSA`, `SHAWithRSA`, `EC_ecdsa_with_SHA1`, `EC_ecdsa_with_SHA224`, `EC_ecdsa_with_SHA256`, `EC_ecdsa_with_SHA384` ou `EC_ecdsa_with_SHA512`. O valor padrão é `SHA1WithRSA`.

-san_dnsname ***DNS_names***
Especifica uma lista de nomes DNS delimitada por vírgulas ou espaços para a entrada sendo criada.

-san_emailaddr ***email_addresses***
Especifica uma lista de endereços de e-mail delimitada por vírgulas ou espaços para a entrada sendo criada.

-san_ipaddr ***IP_addresses***
Especifica uma lista de endereços IP delimitada por vírgulas ou espaços para a entrada sendo criada.

Como proceder a seguir

Enviar uma solicitação de certificado para uma CA. Consulte “Recebendo certificados pessoais em um repositório de chaves no UNIX, Linux, and Windows” na página 304 para obter informações adicionais.

ULW *Renovando um certificado pessoal existente no UNIX, Linux, and Windows*

É possível renovar um certificado pessoal usando a GUI **strmqikm** (iKeyman) ou a partir da linha de comandos usando os comandos **runmqckm** (iKeycmd) ou **runmqakm** (GSKCapiCmd).

Sobre esta tarefa

Se você tiver um requisito para usar tamanhos maiores de chaves para certificados pessoais, não é possível renovar um certificado existente. Deve-se substituir sua chave existente seguindo as etapas descritas em “Solicitando um certificado pessoal no UNIX, Linux, and Windows” na página 300 para criar uma nova solicitação de certificado que usa os tamanhos chave necessários.

Um certificado pessoal possui uma data de expiração, após a qual o certificado não pode mais ser usado. Esta tarefa explica como renovar um certificado pessoal existente antes de ele expirar.

*Usando a interface com o usuário **strmqikm***

Sobre esta tarefa

O **strmqikm** não fornece uma opção compatível com FIPS. Se precisar gerenciar certificados TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**.

Procedimento

Conclua as etapas a seguir para inscrever-se em um certificado pessoal, usando a interface com o usuário **strmqikm**:

1. Inicie a interface com o usuário usando o comando **strmqikm** no UNIX, Linux, and Windows.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**.

   A janela **Abrir** é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo do banco de dados de chaves a partir do qual você quer gerar seu pedido; por exemplo, `key.kdb`.
6. Click **Open**.

   A janela **Prompt de senha** é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**.

   O nome do seu arquivo do banco de dados de chave é mostrado no campo **Nome do arquivo**.
8. Selecione **Certificados pessoais** a partir do menu suspenso de seleção e selecione o certificado que você deseja renovar a partir da lista.
9. Clique em **Recriar solicitação ...** .

   Uma janela é aberta para que você insira o nome do arquivo e as informações de local do arquivo.
10. No campo **file name** , aceite o padrão `certreq.arm`ou digite um novo valor, incluindo o caminho de arquivo completo.
11. Clique em **OK**. A solicitação de certificado é armazenada no arquivo selecionado na etapa “9” na página 303.
12. Solicite o novo certificado pessoal enviando o arquivo para uma autoridade de certificação (CA) ou copiando o arquivo no formulário de solicitação no website para a CA.

Procedimento

Use os comandos a seguir para solicitar um certificado pessoal usando o comando **runmqckm** ou o comando **runmqakm**:

- Usando o **runmqckm** em sistemas UNIX, Linux, and Windows:

```
runmqckm -certreq -recreate -db filename -pw
password -label label
-target filename
```

- Usando runmqakm:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
-target filename
```

em que:

-db *filename*
Especifica o nome completo do arquivo de um banco de dados de chaves do CMS.

-pw *password*
Especifica a senha para o banco de dados de chaves do CMS.

-target *filename*
Especifica o nome do arquivo para a solicitação de certificado.

Como proceder a seguir

Depois de ter recebido o certificado pessoal assinado da autoridade de certificação, será possível incluí-lo em seu banco de dados de chaves usando as etapas descritas em "Recebendo certificados pessoais em um repositório de chaves no UNIX, Linux, and Windows" na página 304.

ULW *Recebendo certificados pessoais em um repositório de chaves no UNIX, Linux, and Windows*

Use este procedimento para receber um certificado pessoal no arquivo de banco de dados de chave. O repositório de chaves deve ser o mesmo repositório em que foi criada a solicitação de certificado.

Depois que a CA enviar um novo certificado pessoal, inclua-o ao arquivo de banco de dados de chave a partir do qual o novo pedido de certificado foi gerado. Se a CA enviar o certificado como parte de uma mensagem de e-mail, copie o certificado em um arquivo separado.

Usando o strmqikm

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** não fornece uma opção compatível com FIPS.

Assegure-se de que o arquivo de certificado a ser importado possui permissões de gravação para o usuário atual, e, em seguida, use o procedimento a seguir para um gerenciador de filas ou um IBM MQ MQI client para receber um certificado pessoal no arquivo do banco de dados de chave:

1. Inicie a GUI usando o comando **strmqikm** (no Windows UNIX and Linux).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.

5. Selecione o arquivo de banco de dados de chave ao qual deseja adicionar o certificado, por exemplo `key.kdb`.
6. Clique em **Abrir** e, em seguida, clique em **OK**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do seu arquivo de banco de dados de chave é exibido no campo **Nome do Arquivo**. Selecione a visualização **Certificados Pessoais**.
8. Clique em **Receber**. A janela Receber Certificado de um Arquivo é aberta.
9. Digite o nome do arquivo do certificado para o novo certificado pessoal ou clique em **Procurar** para selecionar o nome e a localização.
10. Clique em **OK**. Se você já tiver um certificado pessoal no banco de dados de chave, uma janela será aberta perguntando se você deseja configurar a chave que está incluindo como a chave padrão no banco de dados.
11. Clique em **Sim** ou **Não**. A janela Inserir um Rótulo é aberta.
12. Clique em **OK**. O campo**Certificados Pessoais** mostra o rótulo do novo certificado pessoal que você incluiu.

Usando a linha de comandos

Para incluir um certificado pessoal em um arquivo de banco de dados de chaves, use um dos comandos a seguir:

- Usando o **runmqckm**:

```
runmqckm -cert -receive -file filename -db filename -pw password
         -format ascii
```

- Usando o **runmqakm**:

```
runmqakm -cert -receive -file filename -db filename -pw password -fips
```

em que:

-file *filename*
Especifica o nome completo do arquivo do certificado pessoal.

-db *filename*
Especifica o nome completo do arquivo de um banco de dados de chaves do CMS.

-pw *password*
Especifica a senha para o banco de dados de chaves do CMS.

-format *ascii*
Especifica o formato do certificado. O valor pode ser `ascii` para Base64-encoded ASCII ou `binary` para dados DER binários. O padrão é `ascii`.

-fips
Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

Se você estiver usando o hardware de criptografia, consulte o “Recebendo um certificado pessoal no hardware do PKCS #11” na página 319.

ULW *Extraindo um certificado de autoridade de certificação de um repositório de chaves no UNIX, Linux, and Windows*

Siga este procedimento para extrair um certificado de CA.

Usando o strmqikm

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** (iKeyman) não fornece uma opção compatível com FIPS.

Execute as seguintes etapas na máquina a partir da qual deseja extrair o certificado de CA:

1. Inicie a GUI usando o comando **strmqikm**.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo do banco de dados de chave a partir do qual você deseja extrair, por exemplo `key.kdb`.
6. Clique em **Abrir**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do seu arquivo de banco de dados de chave é exibido no campo **Nome do Arquivo**.
8. No campo **Conteúdo do banco de dados de chave**, selecione **Certificados do Signatário** e selecione o certificado que deseja extrair.
9. Clique em **Extrair**. A janela Extrair um Certificado para um Arquivo é aberta.
10. Selecione o **Tipo de Dados** do certificado, por exemplo **Dados ASCII codificados na Base64** para um arquivo com a extensão `.arm`.
11. Digite o nome do arquivo do certificado e a localização onde você quer armazenar o certificado, ou clique em **Procurar** para selecionar o nome e a localização.
12. Clique em **OK**. O certificado é gravado no arquivo que você especificou.

Usando a linha de comandos

Use os comandos a seguir para extrair um certificado de autoridade de certificação usando **runmqckm**:

- No UNIX, Linux, and Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

em que:

`-db` *filename*	é o nome qualificado do caminho de um banco de dados de chave CMS.
`-pw` *password*	é a senha do banco de dados de chave CMS.
`-label` *label*	é o rótulo anexado ao certificado.
`-target` *filename*	é o nome do arquivo de destino.
`-format` *ascii*	é o formato do certificado. O valor pode ser `ascii` para Base64-encoded ASCII ou `binary` para dados DER binários. O padrão é `ascii`.
`-fips`	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

ULW *Extraindo a parte pública de um certificado autoassinado de um repositório de chaves no UNIX, Linux, and Windows*

Siga este procedimento para extrair a parte pública de um certificado autoassinado.

Usando o strmqikm

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** (iKeyman) não fornece uma opção compatível com FIPS.

Execute as seguintes etapas na máquina a partir da qual você deseja extrair a parte pública de um certificado autoassinado:

1. Inicie a GUI usando o comando **strmqikm** (no UNIX, Linux, and Windows).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo de banco de dados da chave a partir do qual você deseja extrair o certificado, por exemplo, `key.kdb`.
6. Clique em **OK**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do seu arquivo de banco de dados de chave é exibido no campo **Nome do Arquivo**.
8. No campo **Conteúdo do Banco de Dados de Chaves**, selecione **Certificados Pessoais** e selecione o certificado.
9. Clique **Extrair Certificado**. A janela Extrair um Certificado para um Arquivo é aberta.
10. Selecione o **Tipo de Dados** do certificado, por exemplo **Dados ASCII codificados na Base64** para um arquivo com a extensão `.arm`.
11. Digite o nome do arquivo do certificado e a localização onde você quer armazenar o certificado, ou clique em **Procurar** para selecionar o nome e a localização.
12. Clique em **OK**. O certificado é gravado no arquivo que você especificou. Observe que ao extrair um certificado (em vez de exportar), apenas a parte pública do certificado é incluída, de modo que uma senha não seja necessária.

Usando a linha de comandos

Use os comandos a seguir para extrair a parte pública de um certificado autoassinado usando o **runmqckm** ou o **runmqakm**:

- No UNIX, Linux, and Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Usando runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

em que:

`-db` *filename*	é o nome qualificado do caminho de um banco de dados de chave CMS.
`-pw` *password*	é a senha do banco de dados de chave CMS.
`-label` *label*	é o rótulo anexado ao certificado.
`-target` *filename*	é o nome do arquivo de destino.
`-format` *ascii*	é o formato do certificado. O valor pode ser `ascii` para Base64-encoded ASCII ou `binary` para dados DER binários. O padrão é `ascii`.

`-fips`	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

ULW *Incluindo um certificado de autoridade de certificação ou a parte pública de um certificado autoassinado em um repositório de chaves no UNIX, Linux, and Windows*

Siga este procedimento para incluir um certificado de CA ou a parte pública de um certificado autoassinado no repositório de chaves.

Se o certificado que deseja incluir estiver em uma cadeia de certificados, será necessário incluir também todos os certificados que estão acima dele na cadeia. É necessário incluir os certificados em ordem estritamente decrescente iniciando da raiz, seguido pelo certificado de CA logo abaixo dela na cadeia, e assim por diante.

Onde as instruções a seguir se referirem a um certificado de CA, elas também se aplicarão à parte pública de um certificado autoassinado.

Nota: Deve-se assegurar que o certificado está em codificação em ASCII (UTF-8) ou binário (DER), porque o IBM GSKit (Global Secure Toolkit) não suporta certificados com outros tipos de codificação.

Usando o `strmqikm`

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** não fornece uma opção compatível com FIPS.

Execute as seguintes etapas na máquina na qual deseja incluir o certificado de CA:

1. Inicie a GUI usando o comando **strmqikm** (nos sistemas UNIX, Linux e Windows).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo de banco de dados de chave ao qual deseja adicionar o certificado, por exemplo `key.kdb`.
6. Clique em **OK**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do arquivo de banco de dados de chave é exibido no campo **Nome de Arquivo**.
8. No campo **Conteúdo do banco de dados de chave**, selecione **Certificados de Assinante**.
9. Clique em **Incluir**. A janela Incluir Certificado de CA de um Arquivo é aberta.
10. Digite o nome do arquivo do certificado e a localização em que está armazenado, ou clique em **Procurar** para selecionar o nome e a localização.
11. Clique em **OK**. A janela Inserir um Rótulo é aberta.
12. Na janela Digite um Rótulo, digite o nome do certificado.
13. Clique em **OK**. O certificado é incluído ao banco de dados de chave.

Usando a linha de comandos

Para incluir um certificado de autoridade de certificação em um banco de dados de chaves, use um dos comandos a seguir:

- Usando o **runmqckm**:

```
runmqckm -cert -add -db filename -pw password -label label
         -file filename -format ascii
```

- Usando o **runmqakm**:

```
runmqakm -cert -add -db filename -pw password -label label
         -file filename -format ascii -fips
```

em que:

-db *filename*
Especifica o nome completo do arquivo do banco de dados de chaves do CMS.

-pw *password*
Especifica a senha para o banco de dados de chaves do CMS.

-label *label*
Especifica o rótulo anexado ao certificado.

-file *filename*
Especifica o nome do arquivo que contém o certificado.

-format *ascii*
Especifica o formato do certificado. O valor pode ser `ascii` para Base64-encoded ASCII ou `binary` para dados DER binários. O padrão é `ascii`.

-fips
Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

ULW *Exportando um certificado pessoal de um repositório de chaves no UNIX, Linux, and Windows*

Siga este procedimento para exportar um certificado pessoal.

Usando o strmqikm

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** (iKeyman) não fornece uma opção compatível com FIPS.

Execute as seguintes etapas na máquina a partir da qual você deseja exportar o certificado pessoal:

1. Inicie a GUI usando o comando **strmqikm** (no Windows UNIX and Linux).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo do banco de dados de chaves a partir do qual você deseja exportar o certificado, por exemplo `key.kdb`.
6. Clique em **Abrir**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do seu arquivo de banco de dados de chave é exibido no campo **Nome do Arquivo**.
8. No campo **Conteúdo do banco de dados de chave**, selecione **Certificados Pessoais** e selecione o certificado que deseja exportar.
9. Clique em **Exportar/Importar**. A janela Exportar/Importar chave é aberta.
10. Selecione **Exportar Chave**.
11. Selecione o **Tipo de arquivo de chave** do certificado que deseja exportar, por exemplo **PKCS12**.
12. Digite o nome do arquivo e o local para o qual deseja exportar o certificado, ou clique em **Procurar** para selecionar o nome e o local.
13. Clique em **OK**. A janela Prompt de Senha é aberta. Observe que quando o certificado é exportado (em vez de extraído), ambas as partes pública e privada do certificado são incluídas. Eis o motivo

pelo qual o arquivo exportado é protegido por uma senha. Ao extrair um certificado, apenas a parte pública do certificado é incluída, de modo que uma senha não seja necessária.

14. Digite a senha no campo **Senha** e digite-a novamente no campo **Confirmar Senha**.
15. Clique em **OK**. O certificado é exportado para o arquivo que você especificou.

Usando a linha de comandos

Use os comandos a seguir para exportar um certificado pessoal usando **runmqckm**:

- No UNIX, Linux, and Windows:

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

em que:

-db *filename*	é o nome do caminho completo do banco de dados de chave CMS.
-fips	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.
-pw *password*	é a senha do banco de dados de chave CMS.
-label *label*	é o rótulo anexado ao certificado.
-type *cms*	é o tipo do banco de dados.
-target *filename*	é o nome do caminho completo do arquivo de destino.
-target_pw *password*	é a senha para criptografar o certificado.
-target_type *pkcs12*	é o tipo do certificado.

ULW *Importando um certificado pessoal em um repositório de chaves no UNIX, Linux, and Windows*

Siga este procedimento para importar um certificado pessoal

Antes de importar um certificado pessoal no formato PKCS #12 para o arquivo do banco de dados de chave, deve-se primeiramente incluir a cadeia válida completa da emissão de certificados de CA para o arquivo de banco de dados chave (consulte "Incluindo um certificado de autoridade de certificação ou a parte pública de um certificado autoassinado em um repositório de chaves no UNIX, Linux, and Windows" na página 308).

Os arquivos PKCS #12 devem ser considerados temporariamente e excluídos após o uso.

Usando o strmqikm

Se precisar gerenciar certificados TLS de uma maneira que seja compatível com FIPS, use o comando **runmqakm**. O **strmqikm** não fornece uma opção compatível com FIPS.

Execute as seguintes etapas na máquina para a qual deseja importar o certificado pessoal:

1. Inicie a GUI usando o comando **strmqikm**.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é exibida.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo de banco de dados de chave ao qual deseja adicionar o certificado, por exemplo key.kdb.

6. Click **Open**. A janela Prompt de Senha é exibida.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do arquivo de banco de dados de chave é exibido no campo **Nome de Arquivo**.
8. No campo **Conteúdo do banco de dados de chave**, selecione **Certificados Pessoais**.
9. Se houver certificados na visualização Certificados Pessoais, siga estas etapas:
   a. Clique em **Exportar/Importar**. A janela Exportar/Importar chave é exibida.
   b. Selecione **Importar Chave**.
10. Se não houver certificados na visualização Certificados Pessoais, clique em **Importar**.
11. Selecione **Tipo de Arquivo-chave** do certificado que deseja importar, por exemplo, PKCS12.
12. Digite o nome do arquivo do certificado e a localização em que está armazenado, ou clique em **Procurar** para selecionar o nome e a localização.
13. Clique em **OK**. A janela Prompt de Senha é exibida.
14. No campo **Senha**, digite a senha usada quando o certificado foi exportado.
15. Clique em **OK**. A janela Alterar Rótulos é exibida. É possível mudar os rótulos de certificados que estão sendo importados se, por exemplo, um certificado com o mesmo rótulo já existir no banco de dados de chave de destino. A alteração dos rótulos de certificado não possui efeito na validação da cadeia de certificados. Para associar o certificado com um gerenciador de filas particular ou IBM MQ MQI client, o IBM MQ usa o valor do atributo **CERTLABL**, se estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou ID de logon do usuário do IBM MQ MQI client anexado, tudo em minúscula. Consulte Rótulos de certificado digital para obter detalhes.
16. Para alterar um rótulo, selecione o rótulo necessário da lista **Selecionar um rótulo para alterar**. O rótulo é copiado no campo de entrada **Inserir um novo rótulo**. Substitua o texto do rótulo pelo texto do novo rótulo e clique em **Aplicar**.
17. O texto no campo de entrada **Inserir um novo rótulo** é copiado de volta no campo **Selecionar um rótulo para alterar**, substituindo o rótulo selecionado originalmente e, assim, designando um novo rótulo ao certificado correspondente.
18. Ao alterar todos os rótulo necessários, clique em **OK**. A janela Mudar rótulos é fechada e a janela original do IBM Key Management é reaberta com os campos **Certificados pessoais** e **Certificados de assinante** atualizados com os certificados rotulados corretamente.
19. O certificado é importado para o banco de dados de chave de destino.

Usando a linha de comandos

Para importar um certificado pessoal usando o **runmqckm**, use o comando a seguir:

- No UNIX, Linux, and Windows:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

em que:

`-file` *filename*	é o nome qualificado do arquivo que contém o certificado PKCS #12.
`-pw` *password*	é a senha do certificado PKCS #12.
`-type` *pkcs12*	é o tipo do arquivo.
`-target` *filename*	é o nome do banco de dados de chave CMS de destino.
`-target_pw` *password*	é a senha do banco de dados de chave CMS.
`-target_type` *cms*	é o tipo de banco de dados especificado por `-target`
`-label` *label*	é o rótulo certificado que será importado a partir do banco de dados de chave de origem.

`-new_label` *label*	é o rótulo que será atribuído ao certificado no banco de dados de destino. Se a opção `-new_label` for omitida, o padrão será usar a mesma opção `-label`.
`-fips`	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

O **runmqckm** não fornece um comando para mudar os rótulos certificados diretamente. Use as seguintes etapas para alterar um rótulo de certificado:

1. Exporte os certificados para um arquivo PKCS #12 usando o comando **-cert -export**. Especifique o rótulo certificado existente para a opção `-label`.
2. Remova a cópia existente do certificado do banco e dados de chave original usando o comando **-cert -delete**.
3. Importe o certificado de um arquivo PKCS #12 usando o comando **-cert -import**. Especifique o rótulo antigo para a opção `-label` e o novo rótulo necessário para a opção `-new_label`. O certificado será importado de volta para o banco de dados de chave com o rótulo necessário.

ULW *Importando um certificado pessoal a partir de um arquivo .pfx Microsoft*

Siga este procedimento para importar de um arquivo Microsoft.pfx no UNIX, Linux, and Windows.

Um arquivo .pfx pode conter dois certificados relacionados à mesma chave. Um certificado é um certificado pessoal ou de site (contendo ambas as chaves pública e privada). O outro é o certificado (signatário) de CA (contendo apenas uma chave pública). Esses certificados não podem coexistir no mesmo arquivo de banco de dados de chave CMS, portanto, apenas um deles poderá ser importado. Além disso, o "nome fácil" ou rótulo é anexado somente ao certificado de assinante.

O certificado pessoal é identificado por um UUID (Unique User Identifier) gerado pelo sistema. Esta seção mostra a importação de um certificado pessoal de um arquivo pfx ao rotulá-lo com o nome amigável anteriormente atribuído ao certificado (signatário) de CA. Os certificados (signatário) de CA já deverão ter sido incluídos no banco de dados de chave de destino. Observe que os arquivos PKCS#12 devem ser considerados temporariamente e excluídos depois do uso.

Siga essas etapas para importar um certificado pessoal de um banco de dados de chave pfx de origem:

1. Inicie a GUI usando o comando **strmqikm**. A janela do IBM Key Management é exibida.
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é exibida.
3. Selecione um tipo de banco de dados de chave de **PKCS12**.
4. **É recomendável fazer um backup do banco de dados pfx antes de executar esta etapa.** Selecione o banco de dados de chave pfx que deseja importar. Clique em **Abrir**. A janela Prompt de Senha é exibida.
5. Digite a senha do banco de dados de chave e clique em **OK**. A janela do IBM Key Management é exibida. A barra de títulos mostra o nome do arquivo do banco de dados de chave pfx selecionado, indicando que o arquivo está aberto e pronto para uso.
6. Selecione **Certificados do Signatário** na lista. O "nome fácil" do certificado necessário é exibido como um rótulo no painel Certificado de assinante.
7. Selecione a entrada do rótulo e clique em **Excluir** para remover o certificado do signatário. A janela de Confirmação é exibida.
8. Clique em **Sim**. O rótulo selecionado não é mais exibido no painel de Certificados do Signatário.
9. Repita as etapas 6, 7 e 8 para todos os certificados do signatário.
10. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é exibida.
11. Selecione o banco de dados CMS de chave de destino para o qual o arquivo pfx está sendo importado. Clique em **Abrir**. A janela Prompt de Senha é exibida.

12. Digite a senha do banco de dados de chave e clique em **OK**. A janela do IBM Key Management é exibida. A barra de título mostra o nome do arquivo de banco de dados de chave selecionado, indicando que o arquivo está aberto e pronto.
13. Selecione **Certificados Pessoais** na lista.
14. Se houver certificados na visualização Certificados Pessoais, siga estas etapas:
    a. Clique em **Exportar/Importar chave**. A janela Exportar/Importar chave é exibida.
    b. Selecione **Importar** a partir Escolher tipo de ação.
15. Se não houver certificados na visualização Certificados Pessoais, clique em **Importar**.
16. Selecione o arquivo PKCS12.
17. Insira o nome do arquivo pfx como usado na Etapa 4. Clique em **OK**. A janela Prompt de Senha é exibida.
18. Especifique a mesma senha especificada quando o certificado de signatário foi excluído. Clique em **OK**.
19. A janela Alterar Rótulos é exibida (devendo ter apenas um único certificado disponível para importar). O rótulo certificado deve ser um UUID com o formato `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.
20. Para alterar o rótulo, selecione o UUID no painel **Selecionar um rótulo para alterar:**. O rótulo será replicado no campo **Inserir novo rótulo:**. Substitua o texto do rótulo pelo texto do nome amigável que foi excluído na Etapa 7 e clique em **Aplicar**. O nome fácil deve ser o valor do atributo IBM MQ **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou IBM MQ MQI client ID de logon do usuário anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.
21. Clique em **OK**. A janela Mudar rótulos é agora removida e a janela original do IBM Key Management será reaberta com os painéis Certificados pessoais e Certificados de assinante atualizados com o certificado pessoal com o rótulo.
22. O certificado pessoal pfx será agora importado para o banco de dados de destino.

Não é possível mudar um rótulo certificado usando o **runmqckm** ou o **runmqakm**.

Usando a linha de comandos

Para importar um certificado pessoal usando **runmqckm** no UNIX, Linux, and Windows, use o seguinte comando:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -pfx
```

Para importar um certificado pessoal usando **runmqakm**, use o comando a seguir:

```
runmqakm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label -fips -pfx
```

em que:

`-file` *filename*	é o nome qualificado do arquivo que contém o certificado PKCS #12.
`-pw` *password*	é a senha do certificado PKCS #12.
`-type` *pkcs12*	é o tipo do arquivo.
`-target` *filename*	é o nome do banco de dados de chave CMS de destino.
`-target_pw` *password*	é a senha do banco de dados de chave CMS.
`-target_type` *cms*	é o tipo de banco de dados especificado por `-target`

`-label` *label*	é o rótulo certificado que será importado a partir do banco de dados de chave de origem.
`-new_label` *label*	é o rótulo que será atribuído ao certificado no banco de dados de destino. Se a opção `-new_label` for omitida, o padrão será usar a mesma opção `-label`.
`-fips`	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.
`-pfx`	indica o formato do arquivo PFX.

O **runmqckm** não fornece um comando para mudar os rótulos certificados diretamente. Use as seguintes etapas para alterar um rótulo de certificado:

1. Exporte os certificados para um arquivo PKCS #12 usando o comando **-cert -export**. Especifique o rótulo certificado existente para a opção `-label`.
2. Remova a cópia existente do certificado do banco e dados de chave original usando o comando **-cert -delete**.
3. Importe o certificado de um arquivo PKCS #12 usando o comando **-cert -import**. Especifique o rótulo antigo para a opção `-label` e o novo rótulo necessário para a opção `-new_label`. O certificado será importado de volta para o banco de dados de chave com o rótulo necessário.

ULW *Importando um certificado pessoal a partir de um arquivo PKCS #7*

As ferramentas **strmqikm** (iKeyman) e **runmqckm** (iKeycmd) não suportam os arquivos PKCS #7 (`.p7b`). Use a ferramenta **runmqckm** para importar certificados de um arquivo PKCS #7 no UNIX, Linux, and Windows.

Use o seguinte comando para incluir o certificado de CA a partir de um arquivo PKCS #7:

```
runmqckm -cert -add -db filename -pw password -type cms -file filename
-label label
```

`-db` *filename*	é o nome qualificado do arquivo do banco de dados de chave CMS.
`-pw` *password*	é a senha do banco de dados de chave.
`-type` *cms*	é o tipo do banco de dados de chave.
`-file` *filename*	é o nome do arquivo PKCS #7.
`-label` *label*	é o rótulo atribuído ao certificado no banco de dados de destino. O primeiro certificado recebe o rótulo fornecido. Todos os outros certificados, se estiverem presentes, serão identificados com o nome do assunto.

Use o seguinte comando para importar um certificado pessoal a partir de um arquivo PKCS #7:

```
runmqckm -cert -import -db filename -pw password -type pkcs7 -target filename
-target_pw password -target_type cms -label label -new_label label
```

`-db` *filename*	é o nome qualificado do arquivo que contém o certificado PKCS #7.
`-pw` *password*	é a senha do certificado PKCS #7.
`-type` *pkcs7*	é o tipo do arquivo.
`-target` *filename*	é o nome do banco de dados de chave de destino.
`-target_pw` *password*	é a senha do banco de dados de chave de destino.
`-target_type` *cms*	é o tipo de banco de dados especificado por `-target`

`-label label`	é o rótulo certificado que deve ser importado.
`-new_label label`	é o rótulo que será atribuído ao certificado no banco de dados de destino. Se a opção `-new_label` for omitida, o padrão é usar a mesma opção `-label`.

ULW *Excluindo um certificado de um repositório de chaves no UNIX, Linux, and Windows*

Use este procedimento para remover certificados pessoais ou de CA.

Usando o strmqikm

Se for necessário gerenciar certificados de TLS de um modo que seja compatível com o FIPS, você deverá usar o comando **runmqakm**. O **strmqikm** (iKeyman) não fornece uma opção compatível com FIPS.

1. Inicie a GUI usando o comando **strmqikm** (no UNIX, Linux, and Windows).
2. A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**. A janela Abrir é aberta.
3. Clique em **Tipo de banco de dados de chave** e selecione **CMS** (Certificate Management System).
4. Clique em **Procurar** para navegar até o diretório que contém os arquivos de banco de dados da chave.
5. Selecione o arquivo do banco de dados de chaves a partir do qual você deseja excluir o certificado, por exemplo `key.kdb`.
6. Clique em **Abrir**. A janela Prompt de Senha é aberta.
7. Digite a senha definida ao criar o banco de dados de chave e clique em **OK**. O nome do seu arquivo de banco de dados de chave é exibido no campo **Nome do Arquivo**.
8. Na lista suspensa, selecione **Certificados pessoais** ou **Certificados de assinante**
9. Selecione o certificado que deseja excluir.
10. Se você ainda não possuir uma cópia do certificado e deseja salvá-lo, clique em **Exportar/Importar** e exporte-o (consulte “Exportando um certificado pessoal de um repositório de chaves no UNIX, Linux, and Windows” na página 309).
11. Com o certificado selecionado, clique em **Excluir**. A janela Confirmar é aberta.
12. Clique em **Sim**. O campo **Certificados Pessoais** não mostrará mais o rótulo certificado que você excluiu.

Usando a linha de comandos

Use os comandos a seguir para excluir um certificado usando **runmqckm**:

- No UNIX, Linux, and Windows:

```
runmqckm -cert -delete -db filename -pw password -label label
```

em que:

`-db filename`	é o nome qualificado do arquivo de um banco de dados de chave CMS.
`-pw password`	é a senha do banco de dados de chave CMS.
`-label label`	é o rótulo anexado ao certificado pessoal.
`-fips`	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

ULW *Gerando senhas fortes para proteção do repositório de chaves no UNIX, Linux, and Windows*

É possível gerar senhas fortes para o repositório de chaves de proteção usando o comando **runmqakm** (GSKCapiCmd).

É possível usar o comando **runmqakm** com os parâmetros a seguir para gerar uma senha forte:

```
runmqakm -random -create -length 14 -strong -fips
```

Ao usar a senha gerada no parâmetro **-pw** dos comandos de administração de certificados subsequentes, sempre coloque aspas duplas ao redor da senha. Nos sistemas UNIX and Linux, também deve-se usar um caractere de barra invertida para escapar os caracteres a seguir se eles aparecerem na sequência de senha:

```
!  \  "  '
```

Ao inserir a senha em resposta a um prompt de **runmqckm**, **runmqakm** ou da GUI **strmqikm**, não é necessário colocar entre aspas ou escapar a senha. Não é necessário porque o shell do sistema operacional não afeta a entrada de dados nesses casos.

ULW *Configurando para o hardware de criptografia no UNIX, Linux, and Windows*

É possível configurar o hardware de criptografia para um gerenciador de filas ou cliente de várias maneiras.

É possível configurar o hardware de criptografia para um gerenciador de filas no UNIX, Linux, and Windows usando um dos métodos a seguir:

- Use o comando ALTER QMGR MQSC com o parâmetro SSLCRYP, conforme descrito em ALTER QMGR.
- Use o IBM MQ Explorer para configurar o hardware de criptografia nos seus sistemas UNIX, Linux ou Windows. Para obter mais informações, consulte a ajuda online.

É possível configurar o hardware de criptografia para um cliente do IBM MQ no UNIX, Linux, and Windows usando um dos métodos a seguir:

- Configure a variável de ambiente MQSSLCRYP. Os valores permitidos para MQSSLCRYP são os mesmos do parâmetro SSLCRYP, conforme descrito em ALTER QMGR.

  Se você usar a versão GSK_PKCS11 do parâmetro SSLCRYP, o rótulo do token PKCS #11 deverá corresponder ao rótulo com o qual seu hardware foi configurado.
- Configure o campo **CryptoHardware** da estrutura de opções de configuração de SSL, MQSCO, em uma chamada MQCONNX. Para obter mais informações, consulte Visão geral para MQSCO.

Se você configurou um hardware criptográfico que usa a interface PKCS #11 usando qualquer um desses métodos, será necessário armazenar o certificado pessoal para ser usado nos canais no arquivo de banco de dados de chave para o token de criptografia que você configurou. Isso é descrito no "Gerenciando certificados em hardware PKCS #11" na página 316.

ULW *Gerenciando certificados em hardware PKCS #11*

É possível gerenciar certificados digitais no hardware de criptografia que suporta a interface PKCS #11.

Sobre esta tarefa

Deve-se criar um banco de dados de chaves para preparar o ambiente do IBM MQ, mesmo se você não pretender armazenar certificados de autoridade de certificação (CA) nele, mas irá armazenar todos os certificados no seu hardware de criptografia. Um banco de dados de chaves é necessário para que o gerenciador de filas faça referência sem seu campo SSLKEYR ou para o aplicativo cliente fazer referência

na variável de ambiente MQSSLKEYR. Este banco de dados de chaves também é necessário se você estiver criando uma solicitação de certificado.

Você cria o banco de dados de chaves usando a linha de comandos ou usando a interface com o usuário **strmqikm** (iKeyman).

Procedimento

Crie um banco de dados de chave usando a linha de comandos

1. Execute um dos comandos a seguir:
   - Usando o **runmqckm**:

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Usando o **runmqakm**:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
     -stash -fips -strong
     ```

   em que:

   -db *filename*
   Especifica o nome completo do arquivo de um banco de dados de chaves do CMS e deve ter uma extensão de arquivo de `.kdb`.

   -pw *password*
   Especifica a senha para o banco de dados de chaves do CMS.

   -type *cms*
   Especifica o tipo de banco de dados. (Para o IBM MQ, ele deve ser `cms`.)

   -stash
   Salva a senha do banco de dados de chaves em um arquivo.

   -fips
   Especifica que o comando é executado no modo FIPS. Quando em modo FIPS, o componente ICC usa algoritmos que são validados para FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

   -strong
   Verifica se a senha inserida atende aos requisitos mínimos de força da senha. Os requisitos mínimos para uma senha são como a seguir:
   - A senha deve ter no mínimo 14 caracteres.
   - A senha deve conter no mínimo um caractere minúsculo, um caractere maiúsculo e um dígito ou caractere especial. Os caracteres especiais incluem o asterisco (*), o sinal de dólar ($), o sinal de número (#) e o sinal de percentual (%). Um espaço é classificado como um caractere especial.
   - Cada caractere pode ocorrer no máximo de três vezes em uma senha.
   - O máximo de dois caracteres consecutivos na senha podem ser idênticos.
   - Todos os caracteres estão configurados no padrão para caracteres para impressão ASCII dentro do intervalo –. 0x20 - 0x7E.

Como alternativa, crie um banco de dados de chaves usando a interface com o usuário **strmqikm** (iKeyman).

2. Nos sistemas UNIX and Linux, efetue login como usuário raiz. Nos sistemas Windows, efetue login como Administrador ou como um membro do grupo MQM.
3. Abra o arquivo de propriedades de segurança Java, `java.security`.
   - Nos sistemas UNIX and Linux o arquivo de propriedades de segurança Java está localizado no subdiretório `java/jre64/jre/lib/security` do diretório de instalação do IBM MQ.

- Nos sistemas Windows o arquivo de propriedades de segurança Java está localizado no subdiretório `java\jre\lib\security` do diretório de instalação do IBM MQ.

Se ele ainda não estiver presente no arquivo, você deverá incluir o provedor de segurança IBMPKCS11Impl. Por exemplo, incluindo a linha a seguir:

```
security.provider.12=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
```

4. Inicie a interface com o usuário executando o comando **strmqikm**.
5. Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.
6. Clique em **Tipo de banco de dados de chave** e selecione **PKCS11Direct**.
7. No campo **Nome do arquivo**, digite o nome do módulo para gerenciar o hardware de criptografia; por exemplo, `PKCS11_API.so`.

   Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.
8. No campo **Localização**, insira o caminho:
   - Nos sistemas UNIX and Linux, este pode ser `/usr/lib/pksc11`, por exemplo.
   - Nos sistemas Windows, é possível digitar o nome da biblioteca; por exemplo, `cryptoki`.

   Clique em **OK**. A janela Abrir Token Criptográfico é aberta.
9. Selecione o rótulo do token do dispositivo criptográfico que você deseja usar para armazenar os certificados.
10. No campo **Senha de Token de Criptografia**, digite a senha que você definiu ao configurar o hardware de criptografia.
11. Se o seu hardware de criptografia possuir o recurso para manter os certificados do signatário necessários para receber ou importar um certificado pessoal, limpe ambas as caixas de opções do banco de dados de chave secundários e continue a partir da etapa “15” na página 319.

    Se você requerer um banco de dados de chave CMS secundário para manter os certificados de assinante, selecione **Abrir arquivo existente do banco de dados de chave secundário** ou **Criar novo arquivo secundário do banco de dados de chave**.
12. No campo **Nome do Arquivo**, digite um nome de arquivo. Esse campo já contém o texto `key.kdb`. Se o seu nome de raiz for `key`, deixe esse campo inalterado Se você especificou um nome de raiz diferente, substitua `key` pelo seu nome de raiz. Não se deve mudar o sufixo `.kdb`.
13. No campo **Localização** digite o caminho, por exemplo:
    - Para um gerenciador de filas: `/var/mqm/qmgrs/QM1/ssl`
    - Para um IBM MQ MQI client: `/var/mqm/ssl`

    Clique em **OK**. A janela Prompt de Senha é aberta.
14. Insira uma senha.

    Se você selecionou **Abrir arquivo existente do banco de dados de chave secundário** na etapa “11” na página 318, digite uma senha no campo **Senha**.

    Se você selecionou **Criar novo arquivo do banco de dados de chave secundário** na etapa “11” na página 318; conclua as seguintes subetapas:

    a) Digite a senha no campo **Senha** e digite-a novamente no campo **Confirmar Senha**.

    b) Selecione **Criar um arquivo stash contendo a senha**. Observe que se você não armazenar a senha em arquivo stash, as tentativas para iniciar os canais TLS falharão porque não é possível obter a senha necessária para acessar o arquivo do banco de dados de chave.

    c) Clique em **OK**. Uma janela é aberta, confirmando que a senha está no arquivo `key.sth` (a menos que você tenha especificado um nome de raiz diferente).

15. Clique em **OK**. O quadro do conteúdo do banco de dados de Chave é exibido.

ULW *Solicitando um Certificado Pessoal para o Hardware PKCS #11*

Use este procedimento para um gerenciador de filas ou um IBM MQ MQI client para solicitar um certificado pessoal para o hardware de criptografia.

Sobre esta tarefa

Esta tarefa descreve como você usa a interface com o usuário **strmqikm** para solicitar um certificado pessoal. Se você estiver usando a interface da linha de comandos, consulte "Usando a linha de comandos" na página 301.

Nota: O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.

Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.

Procedimento

Para solicitar um certificado pessoal por meio da interface com o usuário **strmqikm** (iKeyman), conclua as etapas a seguir:

1. Conclua as etapas para trabalhar com o hardware de criptografia. Consulte o "Gerenciando certificados em hardware PKCS #11" na página 316.
2. No menu **Criar** clique em **Novo Pedido de Certificado**.

   A janela Criar Nova Chave e Pedido de Certificado é aberta.
3. No campo **Rótulo chave**, insira o rótulo certificado.

   O rótulo é o valor do atributo **CERTLABL**, se ele estiver configurado ou o padrão `ibmwebspheremq` com o nome do gerenciador de filas ou o ID do usuário de logon do IBM MQ MQI client anexado, tudo em minúsculas. Consulte Rótulos de certificado digital para obter detalhes.
4. Selecione o **Tamanho da chave** e o **Algoritmo de assinatura** requerido.
5. Insira os valores para **Nome comum** e **Organização** e selecione um **País**. Para os campos opcionais remanescentes, você pode tanto aceitar os valores padrão como digitar ou selecionar novos valores.

   Observe que é possível fornecer apenas um nome no campo **Unidade Organizacional**. Para obter informações adicionais sobre estes campos, consulte "Nomes Distintos" na página 11.
6. No campo **Inserir o nome de um arquivo no qual armazenar a solicitação de certificado**, aceite o padrão `certreq.arm` ou insira um novo valor com um caminho completo.
7. Clique em **OK**.

   A janela de confirmação é aberta.
8. Clique em **OK**.

   A lista **Pedidos de Certificado Pessoal** mostra o rótulo do novo pedido de certificado pessoal que você criou. O pedido de certificado é armazenado no arquivo que você escolheu na etapa "6" na página 319.
9. Solicite o novo certificado pessoal enviando o arquivo para uma autoridade de certificação (CA) ou copiando o arquivo no formulário de solicitação no website para a CA.

ULW *Recebendo um certificado pessoal no hardware do PKCS #11*

Use este procedimento para um gerenciador de filas ou um IBM MQ MQI client para receber um certificado pessoal para o seu hardware de criptografia.

Antes de começar

Inclua o certificado de autoridade de certificação da autoridade de certificação que assinou o certificado pessoal. Inclua-o no hardware de criptografia ou no banco de dados de chaves CMS secundário. Faça

isso antes de receber o certificado assinado no hardware de criptografia. Para incluir um certificado de autoridade de certificação em um conjunto de chaves, siga o procedimento descrito em "Incluindo um certificado de autoridade de certificação ou a parte pública de um certificado autoassinado em um repositório de chaves no UNIX, Linux, and Windows" na página 308.

Procedimento

- Para receber um certificado pessoal usando a interface com o usuário **strmqikm** (iKeyman), conclua as etapas a seguir:
  a) Conclua as etapas para trabalhar com o hardware de criptografia. Consulte o "Gerenciando certificados em hardware PKCS #11" na página 316.
  b) Clique em **Receive**. A janela Receber Certificado de um Arquivo é aberta.
  c) Digite o nome do arquivo do certificado para o novo certificado pessoal ou clique em **Procurar** para selecionar o nome e a localização.
  d) Clique em **OK**. Se você já tiver um certificado pessoal no banco de dados de chave de uma janela será aberta, perguntando se você deseja configurar a chave que está incluindo como a chave padrão no banco de dados.
  e) Clique em **Sim** ou **Não**. A janela Inserir um Rótulo é aberta.
  f) Clique em **OK**. A lista **Certificados Pessoais** mostra o rótulo do novo certificado pessoal que você incluiu. Este rótulo é formado ao incluir o token criptográfico antes do rótulo que você forneceu.
- Para receber um certificado pessoal usando o comando **runmqakm** (GSKCapiCmd), conclua as etapas a seguir:
  a) Abra uma janela de comandos configurada para seu ambiente.
  b) Receba o certificado pessoal usando o comando **runmqakm** (GSKCapiCmd):

```
runmqakm -cert -receive -file filename -crypto module_name
         -tokenlabel hardware_token -pw hardware_password
         -format cert_format -fips
         -secondaryDB filename -secondaryDBpw password
```

  em que:

  -file *filename*
  Especifica o nome completo do arquivo que contém o certificado pessoal.

  -crypto *module_name*
  Especifica o nome completo da biblioteca do PKCS #11 fornecida com o hardware de criptografia.

  -tokenlabel *hardware_token*
  Especifica o rótulo do token do dispositivo criptográfico do PKCS #11.

  -pw *hardware_password*
  Especifica a senha para acesso ao hardware de criptografia.

  -format *cert_format*
  Especifica o formato do certificado. O valor pode ser `ascii` para ASCII codificado na Base64 ou `binary` para dados DER binários. O padrão é ASCII.

  -fips
  Especifica que o comando é executado no modo FIPS. Quando em modo FIPS, o componente ICC usa algoritmos que são validados para FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.

  -secondaryDB *filename*
  Especifica o nome completo do arquivo do banco de dados de chaves do CMS.

  -secondaryDBpw *password*
  Especifica a senha para o banco de dados de chaves do CMS.

MQ Appliance Trabalhando com SSL/TLS no IBM MQ Appliance

O IBM MQ Appliance tem suporte a Segurança da Camada de Transporte (TLS).

O IBM MQ Appliance possui comandos distintos para o gerenciamento de certificados. Para obter informações detalhadas sobre gerenciamento de certificado, consulte a documentação do IBM MQ Appliance, Gerenciamento de certificado de TLS

z/OS Trabalhando com SSL/TLS no z/OS

Estas informações descrevem como configurar e trabalhar com a Segurança da Camada de Transporte (TLS) no z/OS.

Cada tópico inclui exemplos para executar cada tarefa usando o RACF. Você pode executar tarefas similares usando os outros gerenciadores de segurança externos.

No z/OS, também se deve configurar o número de subtarefas do servidor que cada gerenciador de filas usa para processar chamadas do TLS, conforme descrito em “Configurando o parâmetro SSLTASKS no z/OS” na página 322.

O suporte do TLS do z/OS é integral para o sistema operacional e é conhecido como *SSL do sistema*. O SSL do sistema faz parte do elemento do elemento base dos serviços criptográficos do z/OS. Os membros da base dos serviços criptográficos são instalados no *pdsname*. conjunto de dados particionados (PDS) SIEALNKE . Ao instalar o SSL do Sistema, verifique se você escolheu as opções apropriadas para fornecer o CipherSpecs que você precisa.

z/OS *Requisitos adicionais de ID do usuário para TLS no z/OS*

Estas informações descrevem os requisitos adicionais que seu ID do usuário precisa para configurar e trabalhar com TLS no z/OS.

Assegure-se de que tenha todas as atualizações apropriadas de High Impact or Pervasive (HIPER) no sistema.

Assegure-se de que tenha configurado os seguintes pré-requisitos:

- O ID do usuário *ssidCHIN* esteja definido corretamente em RACF e que o ID do usuário *ssidCHIN* tenha acesso READ para os perfis a seguir:
  - IRR.DIGTCERT.LIST
  - IRR.DIGTCERT.LISTRING

  Essas variáveis são definidas na classe FACILITY do RACF.
- O ID do usuário *ssidCHIN* é o proprietário do conjunto de chave.
- O certificado pessoal do gerenciador de filas, se criado pelo comando RACDCERT, é criado com um ID do usuário de tipo de certificado que também é o mesmo que o ID do usuário *ssidCHIN*.
- O inicializador de canais é reciclado ou o comando **REFRESH SECURITY TYPE(SSL)** é emitido, para selecionar as mudanças feitas no conjunto de chaves.
- O procedimento de inicializador de canais do IBM MQ tem acesso a biblioteca de tempo de execução do SSL do Sistema *pdsname*.SIEALNKE por meio da lista de links, LPA ou uma instrução DD STEPLIB. Essa biblioteca deve ser autorizada pelo APF.
- O ID do usuário com cuja autoridade o inicializador de canais está sendo executado esteja configurado para usar o UNIX System Services (USS), conforme descrito na documentação de planejamento do z/OS UNIX System Services.

  Os usuários que não desejam que o inicializador de canais chame o UNIX System Services usando o UID convidado/padrão e o segmento OMVS precisam apenas do modelo de um novo segmento OMVS baseado no segmento padrão, já que o inicializador de canais não requer permissões especiais, e não é executado dentro do UNIX como um superusuário.

z/OS *Configurando o parâmetro SSLTASKS no z/OS*

Use o comando ALTER QMGR para configurar o número de subtarefas do servidor para processar chamadas TLS

Para usar canais TLS, assegure-se de que haja no mínimo duas subtarefas de servidor ao configurar o parâmetro SSLTASKS, usando o comando ALTER QMGR. Por exemplo:

```
ALTER QMGR SSLTASKS(5)
```

Para evitar problemas com alocação de armazenamento, não configure o atributo SSLTASKS para um valor maior que oito em um ambiente no qual não há verificação de CRL (lista de revogação de certificado).

Se a verificação de CRL for usada, um SSLTASK é mantido pelo canal em questão durante essa verificação. Isso poderia ser um tempo decorrido significativo enquanto o servidor LDAP relevante é contatado, porque cada SSLTASK é um bloco de controle de tarefa do z/OS.

Deve-se reiniciar o inicializador de canais se mudar o valor do atributo SSLTASKS.

z/OS *Configurando um repositório de chaves no z/OS*

Configure um repositório de chaves em ambas as extremidades da conexão. Associe cada repositório de chaves a seu gerenciador de filas.

Uma conexão TLS requer um *repositório de chaves* em cada extremidade da conexão. Cada gerenciador de filas deve ter acesso a um repositório de chaves. Use o parâmetro SSLKEYR no comando ALTER QMGR para associar um repositório de chaves com um gerenciador de filas. Consulte o “O repositório de chaves SSL/TLS” na página 25 para obter mais informações.

No z/OS, os certificados digitais são armazenados em um *conjunto de chaves* que é gerenciado pelo ESM (gerenciador de segurança externa). Esses certificados digitais possui rótulos que associa o certificado a um gerenciador de filas. O TLS usa esses certificados para propósitos de autenticação. Todos os exemplos a seguir usam os comandos do RACF. Os comandos equivalentes existem para outros programas ESM.

No z/OS, o IBM MQ usa o valor do atributo **CERTLABL**, se ele estiver configurado ou o `ibmWebSphereMQ` padrão com o nome do gerenciador de filas anexado. Consulte Rótulos de certificado digital para obter detalhes.

O nome do repositório de chaves de um gerenciador de filas é o nome de um conjunto de chaves em seu banco de dados do RACF. Você pode especificar o nome do anel de chaves antes ou depois de criar o anel de chaves.

Use o seguinte procedimento para criar um novo anel de chaves para um gerenciador de filas:

1. Assegure-se de que você tenha a autoridade apropriada para emitir o comando RACDCERT (consulte a *SecureWay Security Server do RACF Referência de linguagem de comando* para obter mais detalhes).
2. Emita o seguinte comando:

   ```
   RACDCERT ID( userid1 ) ADDRING( ring-name )
   ```

   em que:

   - *userid1* é o ID do usuário do espaço de endereço do inicializador de canal, ou o ID do usuário que possuirá o anel de chaves (se o anel de chaves for compartilhado).
   - *ring-name* é o nome que você quer dar ao seu anel de chaves. O comprimento deste nome pode ser de até 237 caracteres. Esse nome faz distinção entre maiúsculas e minúsculas. Especifique *ring-name* em caracteres maiúsculos para evitar problemas.

z/OS *Disponibilizando certificados CA para um gerenciador de filas no z/OS*

Depois de ter criado o conjunto de chaves, conecte a ele quaisquer certificados CA relevantes.

Se você tem o certificado de CA em um conjunto de dados, deve-se primeiro incluir o certificado no banco de dados RACF usando o comando a seguir:

```
RACDCERT ID( userid1 ) ADD( input-data-set-name ) WITHLABEL( 'My CA' )
```

Em seguida, para conectar um certificado de autoridade de certificação para My CA ao seu anel de chaves, use o comando a seguir:

```
RACDCERT ID(userid1)
CONNECT(CERTAUTH LABEL('My CA') RING(ring-name) USAGE(CERTAUTH))
```

em que *userid1* é o ID do usuário do inicializador de canal ou o proprietário de um anel de chaves compartilhado.

Para obter mais informações sobre certificados CA, consulte “Certificados Digitais” na página 9.

z/OS *Localizando o repositório de chaves para um gerenciador de filas no z/OS*

Use este procedimento para obter o local do conjunto de chaves do gerenciador de filas.

1. Exiba os atributos do seu gerenciador de filas, usando um dos seguintes comandos MQSC:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

2. Examine a saída do comando para a localização do anel de chaves.

z/OS *Especificando o local do repositório de chaves para um gerenciador de filas no z/OS*

Para especificar o local do anel de chave do gerenciador de filas, utilize o comando ALTER QMGR MQSC para configurar o atributo do repositório de chaves do gerenciador de filas.

Por exemplo:

```
ALTER QMGR SSLKEYR(CSQ1RING)
```

se o anel de chave for possuído pelo espaço de endereço do inicializador de canal, ou:

```
ALTER QMGR SSLKEYR(userid1/CSQ1RING)
```

se este for um anel de chave compartilhada, em que*userid1* é o ID do usuário que possui o anel de chave.

z/OS *Fornecendo ao inicializador de canais os direitos de acesso corretos no z/OS*

O inicializador de canais (CHINIT) precisa de acesso ao repositório de chaves e a determinados perfis de segurança.

Concedendo o Acesso CHINIT para Ler o Repositório de Chaves

Se o repositório de chaves é de propriedade do ID do usuário do CHINIT, esse ID do usuário precisa de acesso de leitura ao perfil IRR.DIGTCERT.LISTRING na classe FACILITY e atualizar o acesso de outra forma. Conceda acesso usando o comando PERMIT com ACCESS(UPDATE) ou ACCESS(READ), conforme apropriado:

```
PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID( userid ) ACCESS(UPDATE)
```

em que *userid* é o ID do usuário do espaço de endereço do inicializador de canal.

Concedendo o Acesso de Leitura CHINIT aos Perfis CSF* Apropriados

Para obter suporte de hardware fornecido por meio do Integrated Cryptographic Service Facility (ICSF) a ser usado, assegure que o ID do usuário do CHINIT possui acesso de leitura aos perfis CSF* apropriados na classe CSFSERV usando o comando a seguir:

```
PERMIT csf-resource CLASS(CSFSERV) ID( userid ) ACCESS(READ)
```

em que *csf-resource* é o nome do perfil CSF* e *userid* é o ID do usuário do espaço de endereço do inicializador de canais.

Repita esse comando para cada um dos perfis CSF* a seguir:

- CSFDSG
- CSFDSV
- CSFPKD
- CSFPKE
- CSFPKI

O seu ID de usuário CHINIT também pode precisar de acesso de leitura para outros perfis de CSF*. Por exemplo, se você estiver usando a Especificação de Código ECDHE_RSA_AES_256_GCM_SHA384, o seu ID de usuário CHINIT também precisará de acesso de leitura para os perfis de CSF* a seguir:

- CSF1DVK
- CSF1GAV
- CSF1GKP
- CSF1SKE
- CSF1TRC
- CSF1TRD

Para obter mais informações, consulte Requisitos de recurso RACF CSFSERV.

Se as suas chaves do certificado são armazenadas no ICSF e a sua instalação tiver estabelecido controle de acesso sobre as chaves armazenadas no ICSF, assegure-se de que o ID do usuário do CHINIT possui acesso de leitura ao perfil na classe CSFKEYS usando o comando a seguir:

```
PERMIT IRR.DIGTCERT. userid.* CLASS(CSFKEYS) ID( userid ) ACCESS(READ)
```

em que *userid* é o ID do usuário do espaço de endereço do inicializador de canal.

Usando o Integrated Cryptographic Service Facility (ICSF)

O inicializador de canais poderá usar o ICSF para gerar um número aleatório ao criar um valor inicial do algoritmo de proteção de senha para ofuscar as senhas que fluem por meio de canais de cliente, se o TLS não estiver sendo usado.

Para obter informações adicionais, consulte “Usando o Integrated Cryptographic Service Facility (ICSF)” na página 266

z/OS *Quando as mudanças nos certificados ou no repositório de chaves tornam-se efetivas no z/OS*

As mudanças tornam-se efetivas quando o inicializador de canais é iniciado ou o repositório é atualizado.

Especificamente, as mudanças nos certificados no conjunto de chaves e no atributo de repositório de chaves tornam-se efetivas em uma das seguintes ocasiões:

- Quando o inicializador de canais é iniciado ou reiniciado.

- Quando o comando REFRESH SECURITY TYPE(SSL) é emitido para atualizar o conteúdo do repositório de chaves.

z/OS *Criando um certificado pessoal autoassinado no z/OS*

Siga este procedimento para um certificado pessoal autoassinado.

1. Gere um certificado e um par de chaves pública e privada utilizando o seguinte comando:

```
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. Conecte o certificado a seu anel de chaves utilizando o seguinte comando:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

em que:

- *userid1* é o ID do usuário do espaço de endereço do inicializador de canal ou do proprietário do anel de chave compartilhada.
- *userid2* é o ID do usuário associado ao certificado e deve ser o ID do usuário do espaço de endereço do inicializador de canais.

  userid1 e *userid2* podem ser o mesmo ID.
- *ring-name* é o nome que você deu ao anel de chaves em “Configurando um repositório de chaves no z/OS” na página 322.
- *label-name* deverá ser o valor do atributo IBM MQ **CERTLABL**, se ele estiver configurado ou o padrão `ibmWebSphereMQ` com o nome do gerenciador de filas anexado. Consulte Rótulos de certificado digital para obter detalhes.

z/OS *Solicitando um certificado pessoal no z/OS*

Aplicar para um certificado pessoal usando o RACF.

Para solicitar um certificado pessoal, use o RACF conforme a seguir:

1. Crie um certificado pessoal autoassinado, como em “Criando um certificado pessoal autoassinado no z/OS” na página 325. Este certificado fornece ao pedido os valores de atributo para o Nome Distinto.
2. Crie um pedido de certificado codificado em Base64 PKCS #10 gravado em um conjunto de dados, utilizando o seguinte comando:

```
RACDCERT ID(userid2) GENREQ(LABEL(' label_name ')) DSN(' output_data_set_name ')
```

   em que

   - *userid2* é o ID do usuário associado ao certificado e deve ser o ID do usuário do espaço de endereço do inicializador de canais
   - *label_name* é o rótulo usado ao criar o certificado autoassinado

   Consulte “Rótulos de Certificados Digitais, Entendendo os Requisitos” na página 26 para obter detalhes.
3. Envie o conjunto de dados a uma Autoridade de certificação (CA) para solicitar um novo certificado pessoal.

4. Quando o certificado assinado for retornado para você pela Autoridade de certificação, inclua o certificado de volta para o banco de dados do RACF usando o rótulo original, conforme descrito em “Incluindo certificados pessoais em um repositório de chaves no z/OS” na página 326.

z/OS *Criando um certificado pessoal assinado do RACF*

O RACF pode funcionar como uma autoridade de certificação e emitir seu próprio certificado de autoridade de certificação.

Esta seção usa o termo *certificado de assinante* para denotar um certificado de autoridade de certificação emitido pelo RACF.

A chave privada para o certificado de assinante deve estar no banco de dados do RACF antes de executar o procedimento a seguir:

1. Use o comando para a seguir gerar um certificado pessoal assinado pelo RACF, usando o certificado de assinante contido em seu banco de dados do 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. Conecte o certificado a seu anel de chaves utilizando o seguinte comando:

```
RACDCERT ID(userid1)
CONNECT(ID(userid2) LABEL('label-name') RING(ring-name) USAGE(PERSONAL))
```

em que:

- *userid1* é o ID do usuário do espaço de endereço do inicializador de canal ou do proprietário do anel de chave compartilhada.
- *userid2* é o ID do usuário associado ao certificado e deve ser o ID do usuário do espaço de endereço do inicializador de canais.

  userid1 e *userid2* podem ser o mesmo ID.
- *ring-name* é o nome que você deu ao anel de chaves em “Configurando um repositório de chaves no z/OS” na página 322.
- *label-name* deve ser o valor do atributo IBM MQ **CERTLABL**, se estiver configurado, ou o padrão `ibmWebSphereMQ` com o nome do gerenciador de filas ou do grupo de filas compartilhadas anexado. Consulte Rótulos de certificado digital para obter detalhes.
- *signer-label* é o rótulo de seu próprio certificado de assinante.

z/OS *Incluindo certificados pessoais em um repositório de chaves no z/OS*

Use este procedimento para incluir ou importar um certificado pessoal para um conjunto de chaves.

Depois que a autoridade de certificação enviar a você um novo certificado pessoal, inclua-o no conjunto de chaves, usando o procedimento a seguir:

1. Inclua o certificado ao banco de dados do RACF usando o comando a seguir:

```
RACDCERT ID( userid2 ) ADD( input-data-set-name ) WITHLABEL(' label-name ')
```

2. Conecte o certificado a seu anel de chaves utilizando o seguinte comando:

```
RACDCERT ID( userid1 )
CONNECT(ID( userid2 ) LABEL(' label-name ') RING( ring-name ) USAGE(PERSONAL))
```

em que:

- *userid1* é o ID do usuário do espaço de endereço do inicializador de canal ou do proprietário do anel de chave compartilhada.
- *userid2* é o ID do usuário associado ao certificado e deve ser o ID do usuário do espaço de endereço do inicializador de canais.
- *ring-name* é o nome que você deu ao anel de chaves em "Configurando um repositório de chaves no z/OS" na página 322.
- *input-data-set-name* é o nome do conjunto de dados que contém o certificado assinado pela CA. O conjunto de dados deve ser catalogado e não deve ser um PDS ou um membro de um PDS. O formato de registro(RECFM) esperado pelo RACDCERT é VB. O RACDCERT aloca dinamicamente e abre o conjunto de dados, e lê o certificado a partir dele como dados binários.
- *label-name* é o nome do rótulo que foi utilizado ao criar o pedido original. Ele deve ser o valor do atributo IBM MQ **CERTLABL** , se ele estiver configurado, ou o padrão `ibmWebSphereMQ` com o nome do gerenciador de filas ou grupo de filas compartilhadas anexado. Consulte Rótulos de certificado digital para obter detalhes.

z/OS *Exportando um certificado pessoal de um repositório de chaves no z/OS*

Exporte o certificado usando o comando RACDCERT.

No sistema a partir do qual você deseja exportar o certificado, use o seguinte comando:

```
RACDCERT ID(userid2) EXPORT(LABEL('label-name'))
DSN(output-data-set-name) FORMAT(CERTB64)
```

em que:

- *userid2* é o ID do usuário no qual o certificado foi incluído no anel de chaves.
- *label-name* é o rótulo certificado que você quer extrair.
- *output-data-set-name* é o conjunto de dados em que o certificado é colocado.
- CERTB64 é um certificado X.509 codificado DER, que está em formato Base64. Você pode escolher um formato alternativo, por exemplo:

  CERTDER
  certificado X.509 codificado DER em formato binário

  PKCS12B64
  Certificado PKCS #12 em formato Base64

  PKCS12DER
  Certificado PKCS #12 em formato binário

z/OS *Excluindo um certificado pessoal de um repositório de chaves no z/OS*

Exclua um certificado pessoal usando o comando RACDCERT.

Antes de excluir um certificado pessoal, você pode querer salvar uma cópia dele. Para copiar seu certificado pessoal para um conjunto de dados antes de excluí-lo, siga o procedimento em "Exportando um certificado pessoal de um repositório de chaves no z/OS" na página 327. Em seguida, utilize o seguinte comando para excluir seu certificado pessoal:

```
RACDCERT ID( userid2 ) DELETE(LABEL(' label-name '))
```

em que:

- *userid2* é o ID do usuário no qual o certificado foi incluído no anel de chaves.

- *label-name* é o nome do certificado que você quer excluir.

z/OS *Renomeando um certificado pessoal em um repositório de chaves no z/OS*

Renomeie um certificado usando o comando RACDCERT.

Se você não quiser que um certificado com um rótulo específico seja encontrado, mas não quer excluí-lo, você pode renomeá-lo temporariamente utilizando o seguinte comando:

```
RACDCERT ID( userid2 ) LABEL(' label-name ') NEWLABEL(' new-label-name ')
```

em que:

- *userid2* é o ID do usuário no qual o certificado foi incluído no anel de chaves.
- *label-name* é o nome do certificado que você quer renomear.
- *new-label-name* é o novo nome do certificado.

Isso pode ser útil ao testar a autenticação de cliente TLS.

z/OS *Associando um ID do usuário a um certificado digital no z/OS*

O IBM MQ pode usar um ID do usuário associado a um certificado do RACF como um ID do usuário do canal. Associe um ID do usuário a um certificado instalando-o sob esse ID do usuário, ou usando um Filtro do Nome do Certificado.

O método descrito neste tópico é uma alternativa para o método de plataforma independente para associar um ID do usuário com um certificado digital, que usa os registros de autenticação de canal. Para obter mais informações sobre os registros de autenticação de canal, consulte “Registros de Autenticação de Canal” na página 49.

Quando uma entidade em uma extremidade de um canal TLS recebe um certificado de uma conexão remota, a entidade pergunta ao RACF se há um ID do usuário associado àquele certificado. A entidade utiliza aquele ID do usuário como o ID do usuário do canal. Se não houver um ID do usuário associado ao certificado, a entidade utilizará o ID do usuário sob o qual o iniciador de canal está sendo executado.

Associe um ID do usuário a um certificado em uma das seguintes maneiras:

- Instale esse certificado no banco de dados do RACF sob o ID do usuário com o qual você deseja associá-lo, conforme descrito em “Incluindo certificados pessoais em um repositório de chaves no z/OS” na página 326.
- Utilize um CNF (Certificate Name Filter) para mapear o Nome Distinto do sujeito ou do emissor do certificado para o ID do usuário, conforme descrito em “Configurando um filtro de nome de certificado no z/OS” na página 328.

z/OS *Configurando um filtro de nome de certificado no z/OS*

Use o comando RACDCERT para definir um filtro de nome de certificado (CNF), que mapeie um Nome Distinto para um ID do usuário.

Execute as seguintes etapas para configurar um CNF.

1. Ative funções do CNF usando o comando a seguir. Você precisa ter autoridade de atualização na classe DIGTNMAP para fazer isso.

   ```
   SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
   ```

2. Defina o CNF. Por exemplo:

   ```
   RACDCERT ID(USER1) MAP WITHLABEL('filter1') TRUST
   SDNFILTER('O=IBM.C=UK') IDNFILTER('O=ExampleCA.L=Internet')
   ```

   em que USER1 é o ID do usuário a ser usado quando:

- O DN do assunto tem como Organização `IBM` e um País UK.
- O DN do emissor tem como Organização `ExampleCA` e como Localidade `Internet`.

3. Atualize os mapeamentos do CNF:

```
SETROPTS RACLIST(DIGTNMAP) REFRESH
```

Nota:

1. Se o certificado real estiver armazenado no banco de dados do RACF, o ID do usuário sob o qual ele está instalado é usado em preferência ao ID do usuário associado a qualquer CNF. Se o certificado não estiver armazenado no banco de dados do RACF, o ID do usuário associado com o CNF de correspondência mais específico será usado. Correspondências de DN de sujeito são consideradas mais específicas do que correspondências de DN do emissor.
2. Alterações para CNFs não se aplicam até que você atualize os mapeamentos de CNF.
3. Um DN somente corresponde ao filtro de DN em um CNF se o filtro de DN for idêntico à *porção menos significante* do DN. A porção menos significante do DN compreende os atributos que são geralmente listados na extremidade mais à direita do DN, mas que aparecem no início do certificado.

   Por exemplo, considere SDNFILTER `'O=IBM.C=UK'`. Um DN de sujeito `'CN=QM1.O=IBM.C=UK'` corresponde àquele filtro, mas um DN de sujeito `'CN=QM1.O=IBM.L=Hursley.C=UK'` não corresponde àquele filtro.

   A parte menos significativa de alguns certificados pode conter campos que não correspondem ao filtro de DN. Considere excluir estes certificados especificando um padrão de DN no padrão SSLPEER no comando DEFINE CHANNEL.
4. Se o CNF de correspondência mais específico for definido para o RACF como NOTRUST, a entidade usará o ID do usuário sob o qual o iniciador de canal estiver sendo executado.
5. O RACF usa o caractere `'.'` como um separador O IBM MQ usa uma vírgula ou um ponto e vírgula.

Você pode definir CNFs para assegurar que a entidade nunca configure o ID do usuário do canal como o padrão, que é o ID do usuário sob o qual o iniciador de canal está sendo executado. Para cada certificado de CA no anel de chaves associado à entidade, defina um CNF com um IDNFILTER que corresponda exatamente ao DN de sujeito do certificado de CA. Isso assegura que todos os certificados que a entidade possa utilizar correspondam a no mínimo um destes CNFs. Isso porque tais certificados devem ser conectados ao anel de chaves associado à entidade, ou devem ser emitidos por uma CA para a qual um certificado for conectado ao anel de chaves associado à entidade.

Consulte a *SecureWay Security Server RACF Security Administrator's Guide* para obter mais informações sobre os comandos usados para manipular CNFs.

z/OS *Definindo um canal emissor e uma fila de transmissão no QMA no z/OS*

Use os comandos **DEFINE CHANNEL** e **DEFINE QLOCAL** para configurar os objetos necessários.

Procedimento

No QMA, emita comandos como o seguinte exemplo:

```
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)
```

Resultados

Um canal emissor, TO.QMB, e uma fila de transmissão, QMB, são criados.

z/OS *Definindo um canal receptor no QMB no z/OS*

Use o comando **DEFINE CHANNEL** para configurar o objeto necessário.

Procedimento

No QMB, emita um comando como o seguinte exemplo:

```
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')
```

Resultados

Um canal receptor, TO.QMB, é criado.

z/OS *Iniciando o canal emissor no QMA no z/OS*

Se necessário, inicie um programa listener e atualize a segurança. Em seguida, inicie o canal usando o comando **START CHANNEL**.

Procedimento

1. Opcional: Se ainda não tiver iniciado um programa listener no QMB, faça isso.

   O programa listener atende aos pedidos de rede que chegam e inicia o canal receptor quando for necessário. Para obter informações sobre como iniciar um listener, consulte Iniciando um Listener do Canal.
2. Opcional: Se algum canal SSL/TLS tiver sido executado anteriormente, emita o comando REFRESH SECURITY TYPE(SSL)

   Isso garante que todas as alterações feitas no repositório de chaves estejam disponíveis.
3. Inicie o canal no QMA usando o comando START CHANNEL(TO.QMB).

Resultados

O canal emissor é iniciado.

z/OS *Trocando certificados autoassinados no z/OS*

Troque os certificados extraídos anteriormente. Se você usar FTP, use o formato correto.

Procedimento

Transfira a parte da CA do certificado do QM1 para o sistema do QM2 e vice-versa, por exemplo, por FTP.

Se você transferir os certificados usando FTP, deverá fazê-lo no formato correto.

Transfira os seguintes tipos de certificados em formato *binário*:

- X.509 codificado DER binário
- PKCS #7 (certificados CA)
- PKCS #12 (certificados pessoais)

Transfira os seguintes tipos de certificados no formato ASCII:

- PEM (privacy-enhanced mail)
- X.509 codificado Base64

z/OS *Definindo um canal emissor e uma fila de transmissão no QM1 no z/OS*

Use os comandos **DEFINE CHANNEL** e **DEFINE QLOCAL** para configurar os objetos necessários.

Procedimento

No QM1, emita comandos como o seguinte exemplo:

```
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)
```

Os CipherSpecs em cada extremidade do canal devem ser iguais.

Somente o parâmetro SSLCIPH será obrigatório se você desejar que o canal use TLS. Consulte “CipherSpecs e CipherSuites no IBM MQ” na página 40 para obter informações sobre os valores permitidos para o parâmetro SSLCIPH.

Resultados

Um canal emissor, QM1.TO.QM2, e uma fila de transmissão, QM2, são criados.

z/OS *Definindo um canal receptor no QM2 no z/OS*

Use o comando **DEFINE CHANNEL** para configurar o objeto necessário.

Procedimento

No QM2, emita um comando como o seguinte exemplo:

```
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')
```

O canal deve ter o mesmo nome que o canal emissor definido em “Definindo um canal emissor e uma fila de transmissão no QM1 no z/OS” na página 330 e usar o mesmo CipherSpec.

z/OS *Iniciando o canal emissor no QM1 no z/OS*

Se necessário, inicie um programa listener e atualize a segurança. Em seguida, inicie o canal usando o comando **START CHANNEL**.

Procedimento

1. Opcional: Se ainda não tiver iniciado um programa listener no QM2, faça isso.

   O programa listener atende aos pedidos de rede que chegam e inicia o canal receptor quando for necessário. Para obter informações sobre como iniciar um listener, consulte Iniciando um ouvinte de canal
2. Opcional: Se quaisquer canais SSL/TLS tiverem sido executados anteriormente, emita o comando REFRESH SECURITY TYPE(SSL).

   Isso garante que todas as alterações feitas no repositório de chaves estejam disponíveis.
3. Em QM1, inicie o canal usando o comando `START CHANNEL(QM1.TO.QM2)`.

Resultados

O canal emissor é iniciado.

z/OS *Atualizando o ambiente de SSL ou TLS no z/OS*

Atualize o ambiente TLS no gerenciador de filas QMA usando o comando **REFRESH SECURITY**.

Procedimento

No QMA, digite o seguinte comando:

```
REFRESH SECURITY TYPE(SSL)
```

Isso garante que todas as alterações feitas no repositório de chaves estejam disponíveis.

z/OS *Permitindo conexões anônimas em um canal receptor no z/OS*

Use o comando **ALTER CHANNEL** para fazer a autenticação de cliente SSL ou TLS opcional.

Procedimento

No QMB, digite o seguinte comando:

```
ALTER CHANNEL(TO.QMB) CHLTYPE(RCVR) SSLCAUTH(OPTIONAL)
```

z/OS *Iniciando o canal emissor no QM1 no z/OS*

Se necessário, inicie o inicializador de canais, inicie um programa listener e atualize a segurança. Em seguida, inicie o canal usando o comando **START CHANNEL**.

Procedimento

1. Opcional: Se ainda não tiver iniciado o inicializador de canais, faça isso.
2. Opcional: Se ainda não tiver iniciado um programa listener no QM2, faça isso.

   O programa listener atende aos pedidos de rede que chegam e inicia o canal receptor quando for necessário. Para obter informações sobre como iniciar um listener, consulte Iniciando um ouvinte de canal
3. Opcional: Se o inicializador de canais já estava em execução ou quaisquer canais SSL/TLS já tinham sido executados anteriormente, emita o comando REFRESH SECURITY TYPE(SSL).

   Isso garante que todas as alterações feitas no repositório de chaves estejam disponíveis.
4. Em QM1, inicie o canal usando o comando START CHANNEL(QM1.TO.QM2).

Resultados

O canal emissor é iniciado.

z/OS *Iniciando o canal emissor no QMA no z/OS*

Se necessário, inicie o inicializador de canais, inicie um programa listener e atualize a segurança. Em seguida, inicie o canal usando o comando **START CHANNEL**.

Procedimento

1. Opcional: Se ainda não tiver iniciado o inicializador de canais, faça isso.
2. Opcional: Se ainda não tiver iniciado um programa listener no QMB, faça isso.

   O programa listener atende aos pedidos de rede que chegam e inicia o canal receptor quando for necessário. Para obter informações sobre como iniciar um listener, consulte Iniciando um Listener do Canal.
3. Opcional: Se o inicializador de canais já estava em execução ou se quaisquer canais SSL/TLS já tinham sido executados anteriormente, emita o comando REFRESH SECURITY TYPE(SSL).

   Isso garante que todas as alterações feitas no repositório de chaves estejam disponíveis.
4. Inicie o canal no QMA usando o comando START CHANNEL(TO.QMB).

Resultados

O canal emissor é iniciado.

z/OS *Modificando o comprimento da chave de curva elíptica no z/OS*

O modo como você modifica a variável de ambiente GSK_CLIENT_ECURVE_LIST, para configurar a lista de curvas elípticas ou grupos suportados que são especificados pelo cliente, como uma sequência formada por um ou mais valores de 4 caracteres em ordem de preferência de uso.

Importante: Deve-se aplicar a correção no z/OS APAR OA61783 para permitir que determinadas curvas elípticas sejam efetivadas pelo sistema operacional ao usar conexões negociadas TLS 1.0, TLS 1.1 e / ou TLS 1.2 .

É possível configurar esta variável de ambiente TLS na inicialização do inicializador de canais, usando a instrução DD CEEOPTS:

```
CEEOPTS DD DSN=<dataset-name>,DISP=SHR
```

No conjunto de dados referenciado acima, especifique a lista que você deseja usar, por exemplo:

```
ENVAR("GSK_CLIENT_ECURVE_LIST=002300240025")
```

Importante: Não use esta declaração CEEOPTS com dados in-stream, pois isso evita que a variável de ambiente seja configurada para todas as tarefas TLS que usam essa instrução.

Assegure-se de referenciar um conjunto de dados sequenciais, ou membro do conjunto de dados particionados, para permitir que isso funcione ao usar um valor SSLTASKS maior que um.

Também é possível usar o equivalente analógico do servidor de GSK_CLIENT_ECURVE_LIST, que é GSK_SERVER_ALLOWED_KEX_ECURVES Consulte Limitando curvas elípticas de troca de chave para obter mais informações.

Além disso, consulte a Tabela 5 em Definições de conjunto de cifras para obter uma lista de curva elíptica de 4 caracteres válida e especificações de grupos suportados.

A especificação padrão é `00210023002400250019`. Se o TLS V1.3 estiver ativado, `0029 (x25519)` será anexado ao final da lista padrão.

Identificando e autenticando usuários

É possível identificar e autenticar usuários usando certificados X.509, a estrutura MQCSP ou em diversos tipos de programas de saída de usuário.

Usando certificados X.509

É possível identificar e autenticar usuários usando certificados x.509 com o comando **CHLAUTH** e o parâmetro **SSLPEER**. O parâmetro **SSLPEER** especifica um filtro a ser usado para comparar com o Nome distinto do assunto do certificado do gerenciador de filas ou cliente peer na outra extremidade do canal.

Para obter mais informações sobre como usar o comando **CHLAUTH** e o parâmetro **SSLPEER** , consulte SET CHLAUTH

Usando a estrutura MQCSP

É possível especificar a estrutura de parâmetros de segurança de conexão do MQCSP em uma chamada MQCONNX; essa estrutura contém um ID do usuário e senha. Se necessário, é possível mudar o MQCSP em uma saída de segurança.

Nota: O gerenciador de autoridade de objeto (OAM) não usa a senha. No entanto, o OAM faz algum trabalho limitado com o ID do usuário, que pode ser considerado uma forma comum de autenticação. Essas verificações param você adotar outro ID do usuário, se você usar esses parâmetros em seus aplicativos.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas apropriadamente, consulte "Proteção de senha do MQCSP" na página 30.

Implementando identificação e autenticação em saídas de segurança

O principal objetivo da saída de segurança é permitir que o MCA de cada extremidade de um canal autentique o seu parceiro. Em cada extremidade de um canal de mensagens, e na extremidade do

servidor de um canal MQI, um MCA geralmente age em lugar do gerenciador de filas ao qual está conectado. Na extremidade do cliente de um canal do MQI, um MCA geralmente age em nome do usuário do aplicativo cliente do IBM MQ. Nesta situação, a autenticação mútua realmente ocorre entre dois gerenciadores de filas ou entre um gerenciador de filas e o usuário de um aplicativo do IBM MQ MQI client.

A saída de segurança fornecida (a saída de canal SSPI) ilustra como a autenticação mútua pode ser implementada trocando-se os tokens de autenticação que são gerados e, em seguida, verificados por um servidor de autenticação confiável, como o Kerberos. Para obter mais detalhes, consulte "O programa de saída do canal SSPI no Windows" na página 154.

A autenticação mútua pode ser implementa também pela tecnologia PKI (Public Key Infrastructure). Cada saída de segurança gera alguns dados aleatórios, assina-os utilizando a tecla privativa do gerenciador ou usuário de fila que está representando e envia os dados assinados a seu parceiro em uma mensagem de segurança. A saída de segurança do parceiro executa a autenticação verificando a assinatura digital com a tecla privativa do gerenciador ou usuário da fila. Antes de trocar as assinaturas digitais, as saídas de segurança podem ter que concordar o algoritmo para gerar uma compilação de mensagem, se existir mais de um algoritmo disponível para uso.

Quando uma saída de segurança envia os dados assinados a seu parceiro, também precisa enviar algum meio de identificar o gerenciador ou usuário da fila que está representando. Pode ser um Nome Distinto ou mesmo um certificado digital. Se for enviado um certificado digital, a saída de segurança do parceiro poderá validar o certificado, operando pela cadeia de certificados do certificado CA raiz. Isto garante a propriedade da tecla pública utilizada para verificar a assinatura digital.

A saída de segurança do parceiro poderá validar um certificado digital somente se tiver acesso a um repositório de chaves que contenha os certificados restantes na cadeia de certificados. Se um certificado digital do gerenciador ou usuário de fila não for enviado, deverá haver um disponível no repositório de chaves ao qual a saída de segurança do parceiro tenha acesso. A saída de segurança do parceiro não poderá verificar a assinatura digital a menos que encontre a tecla pública do assinante.

A Segurança da Camada de Transporte (TLS) usa técnicas PKI como as que acabaram de ser descritas. Para obter mais informações sobre como o TLS executa a autenticação, veja "Conceitos de TLS (Transport Layer Security)" na página 15.

Se o suporte do servidor de autenticação ou PKI não estiver disponível, poderão ser utilizadas outras técnicas. Uma técnica comum, que pode ser implementada em saídas de segurança, utiliza um algoritmo de chave simétrico.

Uma das saídas de segurança, saída A, gera um número aleatório e o envia em uma mensagem de segurança para sua saída de segurança parceira, a saída B. A saída B criptografa o número usando sua cópia de uma chave que é conhecida apenas pelas duas saídas de segurança. A saída B envia o número criptografado para a saída A em uma mensagem de segurança com um segundo número aleatório que a saída B gerou. A saída A verifica se o primeiro número aleatório foi criptografado corretamente, criptografa o segundo número aleatório utilizando sua cópia da chave e envia o número criptografado à saída B em uma mensagem de segurança. A saída B verifica então se o segundo número foi criptografado corretamente. Durante essa troca, se nenhuma saída de segurança estiver satisfeita com a autenticidade da outra, poderá instruir o MCA a fechar o canal.

Uma vantagem desta técnica é que nenhuma chave ou senha é enviada para a conexão de comunicações durante a troca. Uma desvantagem é que não fornece uma solução para o problema de como distribuir a chave compartilhada de forma segura. Uma solução para esse problema está descrita em "Implementando confidencialidade em programas de saída do usuário" na página 452. Uma técnica semelhante é utilizada no SNA para a autenticação mútua de duas LUs quando elas se ligam para formar uma sessão. A técnica está descrita no "Autenticação em nível de sessão" na página 118.

Todas as técnicas anteriores de autenticação mútua podem ser adaptadas para fornecer autenticação unilateral.

Implementando a identificação e autenticação em saídas de mensagem

Quando um aplicativo põe uma mensagem em uma fila, o campo *UserIdentifier* no descritor da mensagem contém um ID do usuário associado ao aplicativo. Porém, não há dados presentes para serem utilizados para autenticar o ID do usuário. Esses dados podem ser incluídos por uma saída de mensagem na extremidade de envio de um canal e verificados por uma saída de mensagem na extremidade receptora do canal. Os dados de autenticação podem ser uma senha criptografada ou uma assinatura digital, por exemplo.

Este serviço pode ser mais efetivo se implementado no nível do aplicativo. O requisito básico é que o usuário do aplicativo que recebe a mensagem seja capaz de identificar e autenticar o usuário do aplicativo que enviou a mensagem. É, portanto, natural considerar a implementação desse serviço no nível do aplicativo. Para obter informações adicionais, consulte "Mapeamento de identidade na saída de API e saída cruzada da API" na página 340.

Implementando identificação e autenticação na saída de API e saída cruzada da API

No nível de uma mensagem individual, identificação e autenticação é um serviço que envolve dois usuários, o emissor e o receptor da mensagem. O requisito básico é que o usuário do aplicativo que recebe a mensagem seja capaz de identificar e autenticar o usuário do aplicativo que enviou a mensagem. Observe que este requisito serve para autenticação de uma via, não de duas vias.

Dependendo de como seja implementado, os usuários e seus aplicativos podem precisar fazer interface, ou mesmo interagir, com o serviço. Além disso, quando e como o serviço será utilizado pode depender de onde os usuários e seus aplicativos estão localizados, e da natureza dos próprios aplicativos. É, portanto, natural considerar a implementação do serviço ao nível do aplicativo, ao invés de ao nível do link.

Se você considerar a implementação deste serviço ao nível do link, você pode precisar resolver questões tais como as seguintes:

- Em um canal de mensagens, como aplicar o serviço apenas às mensagens que precisam?
- Como habilitar usuários e seus aplicativos a fazer interface, ou interagir, com o serviço, se isso é um requisito?
- Em uma situação de multisalto, em que uma mensagem é enviada em mais de um canal de mensagens a caminho de seu destino, onde você chamará os componentes do serviço?

Aqui estão alguns exemplos de como o serviço de identificação e autenticação pode ser implementado no nível do aplicativo. O termo *saída API* significa tanto uma saída API, quanto uma saída cruzada da API.

- Quando um aplicativo coloca uma mensagem em uma fila, uma saída API pode adquirir um token de autenticação de um servidor de autenticação confiável, como Kerberos. A saída API pode incluir este token nos dados do aplicativo na mensagem. Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode pedir ao servidor de autenticação que autentique o emissor verificando o token.
- Quando um aplicativo põe uma mensagem em uma fila, uma saída API pode anexar os seguintes itens aos dados do aplicativo na mensagem:
  - O certificado digital do emissor
  - A assinatura digital do emissor

  Se diferentes algoritmos para gerar uma compilação da mensagem estiverem disponíveis para utilização, a saída API pode incluir o nome do algoritmo que ela utilizou.

  Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode executar as seguintes verificações:

  - A saída API pode validar o certificado digital verificando toda a cadeia de certificados até o certificado de CA raiz. Para fazer isto a saída da API deve ter acesso ao repositório de chaves que contém os certificados restantes na cadeia de certificados. Esta verificação proporciona garantia de

que o emissor, identificado pelo Nome Distinto, seja o proprietário genuíno da chave pública contida no certificado.

– A saída API pode verificar a assinatura digital utilizando a chave pública contida no certificado. Essa verificação autentica o emissor.

O Nome Distinto do emissor pode ser enviado, ao invés do certificado digital inteiro. Neste caso, o repositório de chaves deve conter o certificado do emissor, de modo que a segunda saída API possa encontrar a chave pública do emissor. Outra possibilidade é enviar todos os certificados na cadeia de certificados.

- Quando um aplicativo põe uma mensagem em uma fila, o campo *UserIdentifier* no descritor da mensagem contém um ID do usuário associado ao aplicativo. O ID do usuário pode ser utilizado para identificar o emissor. Para ativar a autenticação, uma saída API pode anexar alguns dados, tal com uma senha criptografada, aos dados do aplicativo na mensagem. Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode autenticar o ID do usuário utilizando os dados que seguiram com a mensagem.

  Esta técnica pode ser considerada suficiente para mensagens que se originem em um ambiente controlado e confiável, e em circunstâncias em que um servidor de autenticação confiável ou suporte PKI não estejam disponíveis.

Método de autenticação conectável (PAM)

Linux UNIX

O PAM agora é comum em plataformas UNIX and Linux e fornece um mecanismo geral que oculta os detalhes de autenticação do usuário dos serviços.

Regras de autenticação diferentes podem ser usadas para diferentes serviços configurando as regras sem qualquer mudança necessária para os próprios serviços.

Consulte “Usando o Pluggable Authentication Method (PAM)” na página 353 para obter informações adicionais.

Usuários Privilegiados

Um usuário privilegiado é aquele que tem total autoridade administrativa para o IBM MQ.

Além dos usuários listados na tabela a seguir, há alguns objetos e autorizações para os quais muito cuidado deve ser tomado ao conceder acesso, para assegurar a integridade e a segurança do gerenciador de filas. Um exame detalhado extra deve ser aplicado ao conceder qualquer uma das autorizações a seguir:

- Quaisquer autorizações para objetos SYSTEM
- Autorizações de administração para criar, alterar e excluir objetos.

  z/OS No z/OS, essa autorização é a segurança de comando e a autoridade de segurança do recurso de comando para emitir comandos DEFINE, ALTER e DELETE.

  Multi Em todas as outras plataformas, essas autorizações são autorizações de administração, como `+crt`, `+chg` e `+dlt`.
- Autorização de administração para limpar filas.

  z/OS No z/OS, essa autorização é a segurança de comando e a autoridade de segurança do recurso de comando para emitir comandos CLEAR.

  Multi Em todas as outras plataformas, essa autorização é `+clr`.
- Autorizações de administração para parar canais, restaurar ou confirmar mensagens.

z/OS No z/OS, essa autorização é a segurança de comando e a autoridade de segurança do recurso de comando para emitir comandos, como RESET CHANNEL, START CHANNEL e STOP CHANNEL.

Multi Em todas as outras plataformas, essas autorizações são `+ctrl` e `+ctrlx`.

- Autorização do MQI de usuário alternativo que permite que os aplicativos escalem privilégios para verificações de autorização.

  z/OS No z/OS, essa autorização é qualquer autoridade concedida aos perfis de segurança de usuário alternativo.

  Multi Em todas as outras plataformas, essa autorização é `+altusr`.
- Autorizações de contexto que permitem que os aplicativos mudem o contexto de segurança de mensagens.

  z/OS No z/OS, essa autorização é qualquer autoridade concedida aos perfis de segurança de contexto.

  Multi Em todas as outras plataformas, essas autorizações são `+setall` e `+setid`.

Como um principal geral, os aplicativos de sistema de mensagens devem ter concedidos somente autorizações básicas de MQI para as filas ou os tópicos que são necessários. Os canais de MCA que são executados sob um MCAUSER não privilegiado e certos outros tipos especiais de aplicativos, como manipuladores de filas de mensagens não entregues, podem requerer autorizações adicionais não normalmente concedidas a aplicativos para operar corretamente.

Tabela 67. Usuários privilegiados por plataforma

Plataforma	**Usuários Privilegiados**
Sistemas Windows	• SISTEMA • Membros do grupo mqm • Membros do grupo Administradores
Sistemas UNIX and Linux	• Membros do grupo mqm
IBM i IBM i Sistemas IBM i	• Os perfis qmqm e qmqmadm • Todos os membros do grupo qmqmadm • Qualquer usuário definido com a configuração *ALLOBJ
z/OS	O ID do usuário no qual o inicializador de canais, gerenciador de filas e espaços de endereço de segurança de mensagem avançada estão em execução. Esses IDs de usuário não têm automaticamente autoridades administrativas integrais para o IBM MQ, mas são considerados privilegiados devido ao nível de acesso que é normalmente concedido a esses IDs de usuário.

Identificando e autenticando usuários usando a estrutura MQCSP

É possível especificar a estrutura de parâmetros de segurança de conexão do MQCSP em uma chamada MQCONNX.

A estrutura de parâmetros de segurança de conexão do MQCSP contém um ID do usuário e senha, que o serviço de autorização pode usar para identificar e autenticar o usuário.

É possível alterar o MQCSP em uma saída de segurança.

Aviso: Em alguns casos, a senha em uma estrutura MQCSP para um aplicativo cliente será enviada através de uma rede em texto simples. Para assegurar que as senhas do aplicativo cliente sejam protegidas apropriadamente, consulte “Proteção de senha do MQCSP” na página 30.

Relacionamento entre as configurações MQCSP e AdoptCTX

O IBM MQ sempre autentica as credenciais passadas por meio da estrutura MQCSP, a menos que o recurso de autenticação de conexão não esteja ativado. Uma vez que as credenciais foram autenticadas com sucesso, o IBM MQ tenta adotar o ID do usuário para verificações de autorização futuras, a menos que ADOPTCTX não esteja ativado.

O IBM MQ tem um limite no comprimento de IDs de usuário que ele pode usar para verificações de autorização. Esses limites são detalhados em “IDs de Usuário” na página 83. Ao adotar um ID do usuário passado por meio da estrutura MQCSP, o IBM MQ se comporta de forma diferente, dependendo de outras opções de configuração:

- Ao usar a autenticação de conexão LDAP, o IBM MQ recupera o valor do campo configurado em SHORTUSR do registro LDAP do usuário desse usuário e adota esse ID do usuário.

  Por exemplo, se SHORTUSR for configurado como `'CN'` e um registro LDAP listar um usuário como `'CN=Test,SN=MQ,O=IBM,C=UK'`, o ID do usuário `Test` será usado
- Ao usar a autenticação de conexão de S.O. ou a autenticação de PAM, se ADOPTCTX for YES, o ID do usuário transmitido por meio da estrutura MQCSP será truncado para atender o limite de ID de usuário de 12 caracteres de IBM MQ quando adotado como o contexto de conexão...

  Se **ChlAuthEarlyAdopt** estiver ativado, o truncamento acontecerá após as credenciais do usuário terem sido autenticadas.

  Se **ChlAuthEarlyAdopt** não estiver ativado, o truncamento acontecerá antes da adoção. No Windows, se o usuário for fornecido no formato `user@domain`, isso significará que o truncamento pode resultar em uma especificação de domínio que não é válida quando o usuário tiver menos de 12 caracteres.

  Por exemplo, se um usuário `` `ibmmq@windowsdomain` `` for fornecido por meio do MQCSP, ele será truncado para `` `ibmmq@window` `` neste cenário.. Isso resulta no seguinte erro:

  ```
  AMQ8074W: a autorização falhou porque o SID 'SID' não corresponde à entidade 'ibmmq@window'
  ```

  Nessa base, se você passar um ID do usuário com mais de 12 caracteres, como um ID do usuário do domínio Windows no formato `user@domain`, por meio do MQCSP, deverá configurar **ChlAuthEarlyAdopt**=*Y* no arquivo qm.ini para evitar esse erro.

  Como alternativa, use ADOPTCTX (NO) na configuração CONNAUTH AUTHINFO e use uma abordagem alternativa, como uma regra CHLAUTH USERMAP, uma saída de segurança ou a configuração MCAUSER do objeto do canal para configurar o ID do usuário para o canal.

Implementando identificação e autenticação em saídas de segurança

É possível usar uma saída de segurança para implementar a autenticação unilateral ou mútua.

O principal objetivo da saída de segurança é permitir que o MCA de cada extremidade de um canal autentique o seu parceiro. Em cada extremidade de um canal de mensagens, e na extremidade do servidor de um canal MQI, um MCA geralmente age em lugar do gerenciador de filas ao qual está conectado. Na extremidade do cliente de um canal do MQI, um MCA geralmente age em nome do usuário do aplicativo do IBM MQ MQI client. Nesta situação, a autenticação mútua realmente ocorre entre dois gerenciadores de filas ou entre um gerenciador de filas e o usuário de um aplicativo do IBM MQ MQI client.

A saída de segurança fornecida (a saída de canal SSPI) ilustra como a autenticação mútua pode ser implementada trocando-se os tokens de autenticação que são gerados e, em seguida, verificados por um servidor de autenticação confiável, como o Kerberos. Para obter mais detalhes, consulte “O programa de saída do canal SSPI no Windows” na página 154.

A autenticação mútua pode ser implementa também pela tecnologia PKI (Public Key Infrastructure). Cada saída de segurança gera alguns dados aleatórios, assina-os utilizando a tecla privativa do gerenciador ou usuário de fila que está representando e envia os dados assinados a seu parceiro em uma mensagem de segurança. A saída de segurança do parceiro executa a autenticação verificando a assinatura digital com a tecla privativa do gerenciador ou usuário da fila. Antes de trocar as assinaturas digitais, as saídas de segurança podem ter que concordar o algoritmo para gerar uma compilação de mensagem, se existir mais de um algoritmo disponível para uso.

Quando uma saída de segurança envia os dados assinados a seu parceiro, também precisa enviar algum meio de identificar o gerenciador ou usuário da fila que está representando. Pode ser um Nome Distinto ou mesmo um certificado digital. Se for enviado um certificado digital, a saída de segurança do parceiro poderá validar o certificado, operando pela cadeia de certificados do certificado CA raiz. Isto garante a propriedade da tecla pública utilizada para verificar a assinatura digital.

A saída de segurança do parceiro poderá validar um certificado digital somente se tiver acesso a um repositório de chaves que contenha os certificados restantes na cadeia de certificados. Se um certificado digital do gerenciador ou usuário de fila não for enviado, deverá haver um disponível no repositório de chaves ao qual a saída de segurança do parceiro tenha acesso. A saída de segurança do parceiro não poderá verificar a assinatura digital a menos que encontre a tecla pública do assinante.

A Segurança da Camada de Transporte (TLS) usa técnicas PKI como as que acabaram de ser descritas. Para obter mais informações sobre como o SSL realiza a autenticação, consulte “Conceitos de TLS (Transport Layer Security)” na página 15.

Se o suporte do servidor de autenticação ou PKI não estiver disponível, poderão ser utilizadas outras técnicas. Uma técnica comum, que pode ser implementada em saídas de segurança, utiliza um algoritmo de chave simétrico.

Uma das saídas de segurança, saída A, gera um número aleatório e o envia em uma mensagem de segurança para sua saída de segurança parceira, a saída B. A saída B criptografa o número usando sua cópia de uma chave que é conhecida apenas pelas duas saídas de segurança. A saída B envia o número criptografado para a saída A em uma mensagem de segurança com um segundo número aleatório que a saída B gerou. A saída A verifica se o primeiro número aleatório foi criptografado corretamente, criptografa o segundo número aleatório utilizando sua cópia da chave e envia o número criptografado à saída B em uma mensagem de segurança. A saída B verifica então se o segundo número foi criptografado corretamente. Durante essa troca, se nenhuma saída de segurança estiver satisfeita com a autenticidade da outra, poderá instruir o MCA a fechar o canal.

Uma vantagem desta técnica é que nenhuma chave ou senha é enviada para a conexão de comunicações durante a troca. Uma desvantagem é que não fornece uma solução para o problema de como distribuir a chave compartilhada de forma segura. Uma solução para esse problema está descrita em “Implementando confidencialidade em programas de saída do usuário” na página 452. Uma técnica semelhante é utilizada no SNA para a autenticação mútua de duas LUs quando elas se ligam para formar uma sessão. A técnica está descrita no “Autenticação em nível de sessão” na página 118.

Todas as técnicas anteriores de autenticação mútua podem ser adaptadas para fornecer autenticação unilateral.

Mapeamento de identidade em saídas de mensagem

É possível usar saídas de mensagens para processar informações para autenticar um ID do usuário, mas pode ser melhor implementar a autenticação no nível do aplicativo.

Quando um aplicativo põe uma mensagem em uma fila, o campo *UserIdentifier* no descritor da mensagem contém um ID do usuário associado ao aplicativo. Porém, não há dados presentes para serem utilizados para autenticar o ID do usuário. Esses dados podem ser incluídos por uma saída de mensagem na extremidade de envio de um canal e verificados por uma saída de mensagem na extremidade receptora do canal. Os dados de autenticação podem ser uma senha criptografada ou uma assinatura digital, por exemplo.

Este serviço pode ser mais efetivo se implementado no nível do aplicativo. O requisito básico é que o usuário do aplicativo que recebe a mensagem seja capaz de identificar e autenticar o usuário do aplicativo

que enviou a mensagem. É, portanto, natural considerar a implementação desse serviço no nível do aplicativo. Para obter mais informações, consulte “Mapeamento de identidade na saída de API e saída cruzada da API” na página 340.

Mapeamento de identidade na saída de API e saída cruzada da API

Um aplicativo que recebe uma mensagem deve ser capaz de identificar e autenticar o usuário do aplicativo que enviou a mensagem. Esse serviço é geralmente melhor implementado no nível do aplicativo. Saídas de API podem implementar o serviço de várias maneiras.

No nível de uma mensagem individual, identificação e autenticação é um serviço que envolve dois usuários, o emissor e o receptor da mensagem. O requisito básico é que o usuário do aplicativo que recebe a mensagem seja capaz de identificar e autenticar o usuário do aplicativo que enviou a mensagem. Observe que este requisito serve para autenticação de uma via, não de duas vias.

Dependendo de como seja implementado, os usuários e seus aplicativos podem precisar fazer interface, ou mesmo interagir, com o serviço. Além disso, quando e como o serviço será utilizado pode depender de onde os usuários e seus aplicativos estão localizados, e da natureza dos próprios aplicativos. É, portanto, natural considerar a implementação do serviço ao nível do aplicativo, ao invés de ao nível do link.

Se você considerar a implementação deste serviço ao nível do link, você pode precisar resolver questões tais como as seguintes:

- Em um canal de mensagens, como aplicar o serviço apenas às mensagens que precisam?
- Como habilitar usuários e seus aplicativos a fazer interface, ou interagir, com o serviço, se isso é um requisito?
- Em uma situação de multisalto, em que uma mensagem é enviada em mais de um canal de mensagens a caminho de seu destino, onde você chamará os componentes do serviço?

Aqui estão alguns exemplos de como o serviço de identificação e autenticação pode ser implementado no nível do aplicativo. O termo *saída API* significa tanto uma saída API, quanto uma saída cruzada da API.

- Quando um aplicativo coloca uma mensagem em uma fila, uma saída API pode adquirir um token de autenticação de um servidor de autenticação confiável, como Kerberos. A saída API pode incluir este token nos dados do aplicativo na mensagem. Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode pedir ao servidor de autenticação que autentique o emissor verificando o token.
- Quando um aplicativo põe uma mensagem em uma fila, uma saída API pode anexar os seguintes itens aos dados do aplicativo na mensagem:
  - O certificado digital do emissor
  - A assinatura digital do emissor

  Se diferentes algoritmos para gerar uma compilação da mensagem estiverem disponíveis para utilização, a saída API pode incluir o nome do algoritmo que ela utilizou.

  Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode executar as seguintes verificações:

  - A saída API pode validar o certificado digital verificando toda a cadeia de certificados até o certificado de CA raiz. Para fazer isto a saída da API deve ter acesso ao repositório de chaves que contém os certificados restantes na cadeia de certificados. Esta verificação proporciona garantia de que o emissor, identificado pelo Nome Distinto, seja o proprietário genuíno da chave pública contida no certificado.
  - A saída API pode verificar a assinatura digital utilizando a chave pública contida no certificado. Essa verificação autentica o emissor.

  O Nome Distinto do emissor pode ser enviado, ao invés do certificado digital inteiro. Neste caso, o repositório de chaves deve conter o certificado do emissor, de modo que a segunda saída API possa encontrar a chave pública do emissor. Outra possibilidade é enviar todos os certificados na cadeia de certificados.

- Quando um aplicativo põe uma mensagem em uma fila, o campo *UserIdentifier* no descritor da mensagem contém um ID do usuário associado ao aplicativo. O ID do usuário pode ser utilizado para identificar o emissor. Para ativar a autenticação, uma saída API pode anexar alguns dados, tal com uma senha criptografada, aos dados do aplicativo na mensagem. Quando a mensagem for recuperada pelo aplicativo receptor, uma segunda saída API pode autenticar o ID do usuário utilizando os dados que seguiram com a mensagem.

  Esta técnica pode ser considerada suficiente para mensagens que se originem em um ambiente controlado e confiável, e em circunstâncias em que um servidor de autenticação confiável ou suporte PKI não estejam disponíveis.

Trabalhando com Certificados Revogados

Os certificados digitais podem ser revogados pelas Autoridades de certificação. É possível verificar o status de revogação de certificados que usam OCSP ou CRLs nos servidores LDAP, dependendo da plataforma.

Durante o handshake TLS, os parceiros de comunicação se autenticam com certificados digitais. A autenticação pode incluir a verificação de que o certificado recebido ainda pode ser confiável. As Autoridades de certificação (CAs) revogam certificados por muitas razões, incluindo:

- O proprietário mudou para uma organização diferente.
- A chave privada não é mais secreta

As CAs publicam os certificados pessoais revogados em uma CRL (Lista de Certificados Revogados). Os certificados de CA que foram revogados são publicados em uma ARL (Lista de Autoridades Revogadas).

Nas plataformas a seguir, o suporte de SSL do IBM MQ verifica os certificados revogados usando o OCSP (Online Certificate Status Protocol) ou usando CRLs e ARLs em servidores LDAP (Lightweight Directory Access Protocol). OCSP é o método preferido.

- Linux
- UNIX
- Windows

IBM MQ classes for Java e IBM MQ classes for JMS não pode usar as informações do OCSP em um arquivo da tabela de definição de canal do cliente. No entanto, você pode configurar o OCSP conforme descrito em Usando Protocolo de Certificado Online.

Nas plataformas a seguir, o suporte de SSL do IBM MQ verifica os certificados revogados usando CRLs e ARLs apenas em servidores LDAP:

- IBM i
- z/OS

Para mais informações sobre Autoridades de certificação, consulte “Certificados Digitais” na página 9.

Verificação de OCSP/CRL

A verificação do Online Certificate Status Protocol (OCSP)/Lista de Revogação de Certificado (CRL) é realizada com relação aos certificados recebidos remotos. O processo verifica toda a cadeia envolvida desde o certificado pessoal do sistema remoto até o certificado raiz.

Usando o openSSL para verificar a validação do OCSP

Se a sua empresa usar o openSSL para validar o OCSP e você tentar usar uma conexão TLS do GSKit, será recebido um aviso de status UNKNOWN.

Isso ocorre porque todos os certificados na cadeia, além da raiz, são verificados pelo GSKit quanto ao status de revogação. A operação GSKit está de acordo com a RFC 5280, que é descrita na Política de

confiança do GSKit. O algoritmo GSKit tenta todas as origens disponíveis para obter informações de revogação, conforme descrito na RFC 5280 e na Política de confiança do GSKit.

Como a verificação de OCSP/CRL funciona no IBM MQ?

O IBM MQ suporta dois mecanismos para controle de comportamento ao verificar certificados com relação a terminais OCSP ou CRL nomeados, seja na extensão do certificado ou conforme definido nos objetos AUTHINFO:

- Os atributos **OCSPCheckExtensions**, **CDPCheckExtensions**e **OCSPAuthentication** da sub-rotina SSL do arquivo qm.inie
- Usando o parâmetro SSLCRLNL do gerenciador de filas e as configurações AUTHINFO OCSP e CRLLDAP. Consulte ALTER AUTHINFO e ALTER QMGR para obter mais informações.

Atenção:

O comando ALTER AUTHINFO com **AUTHTYPE(OCSP)** não se aplica para uso em Gerenciadores de Filas IBM i ou z/OS. No entanto, pode ser especificado nas plataformas a serem copiadas na tabela de definição de canal do cliente (CCDT) para uso do cliente.

Os atributos de sub-rotina SSL **OCSPCheckExtensions** e **CDPCheckExtensions** controlam se o IBM MQ verificará um certificado com relação ao servidor OCSP ou CRL detalhado na extensão AIA do certificado.

Se não estiver ativado, o servidor OCSP ou CRL na extensão do certificado não será contatado.

Se os servidores OCSP ou CRL forem detalhados por meio de objetos AUTHINFO e referenciados usando o atributo SSLCRLNL **QMGR**, durante o processamento de revogação de certificado, o IBM MQ tentará entrar em contato com esses servidores.

Importante: Apenas um objeto OCSP AUTHINFO pode ser definido na lista de nomes SSLCRLNL.

Se:

OCSPCheckExtensions=NO e **CDPCheckExtensions**=*NO* estão configurados e
Nenhum servidor OCSP ou CRL é definido em objetos AUTHINFO

nenhuma verificação de revogação de certificados é executada.

Ao verificar o status de revogação de um certificado, o IBM MQ entra em contato com os servidores OCSP ou CRL nomeados na ordem a seguir, se ativados:

1. O Servidor OCSP detalhado em um objeto **AUTHTYPE(OCSP)** e referenciado no atributo SSLCRLNL **QMGR**.
2. Os servidores OCSP detalhados na extensão AIA dos certificados, se **OCSPCheckExtensions**=*YES*.
3. Os servidores CRL detalhados na extensão **CRLDistributionPoints** dos certificados, se **CDPCheckExtensions**=*YES*.
4. Todos os servidores CRL detalhados em objetos **AUTHINFO(CRLLDAP)** e referenciados no atributo SSLCRLNL **QMGR**.

Ao verificar um certificado, se uma etapa resultar no servidor OCSP ou no servidor CRL retornando uma resposta definitiva REVOKED ou VALID para uma consulta do certificado, não serão realizadas verificações adicionais e o status do certificado será usado da maneira que ele foi apresentado para determinar se ele é confiável ou não.

Se um servidor OCSP ou servidor CRL retornar um resultado de UNKNOWN, o processamento continuará até que um servidor OCSP ou CRL retorne um resultado definitivo ou até que todas as opções sejam esgotadas.

O comportamento resultante de um certificado ser considerado revogado ou não, caso o status não possa ser determinado, é diferente para servidores OCSP e CRL:

- Para servidores CRL, se nenhum CRL puder ser obtido, o certificado será considerado NOT_REVOKED

- Para servidores OCSP, se nenhum status de revogação puder ser obtido de um servidor OCSP nomeado, o comportamento será controlado por meio do atributo **OCSPAuthentication** na sub-rotina SSL do arquivo qm.ini.

  É possível configurar esse atributo para bloquear uma conexão, permitir uma conexão ou permitir uma conexão com uma mensagem de aviso.

Será possível usar o atributo **SSLHTTPProxyName**=*string* na sub-rotina SSL dos arquivos qm.ini e mqclient.ini para as verificações de OCSP, se necessário. A sequência é o nome do host ou o endereço de rede do servidor de Proxy HTTP que deve ser usado pelo GSKit para verificações de OCSP.

No IBM MQ 9.1.5, é possível configurar o valor **OCSPTimeout** na sub-rotina SSL dos arquivos `qm.ini` ou `mqclient.ini` que configura o número de segundos que você deve aguardar um respondente OCSP ao executar uma verificação de revogação.

ULW Certificados Revogados e OCSP

O IBM MQ determina qual respondente Online Certificate Status Protocol (OCSP) usar e manipula a resposta recebida. Pode ser necessário concluir etapas para tornar o respondente do OCSP acessível.

Nota: Estas informações se aplicam apenas ao IBM MQ nos sistemas UNIX, Linux, and Windows.

Para verificar o status da revogação de um certificado digital usando OCSP, o IBM MQ pode usar dois métodos para determina com qual respondente OCSP entrar em contato:

- Usando a extensão de certificado AuthorityInfoAccess (AIA) no certificado a ser verificado.
- Usando uma URL especificada em um objeto de informação de autenticação ou especificada por um aplicativo cliente.

Uma URL especificada em um objeto de informações de autenticação ou por um aplicativo cliente que tem prioridade sobre uma URL em uma extensão de certificado de AIA.

Se a URL do respondente do OCSP estiver atrás de um firewall, reconfigure o firewall para que o respondente do OCSP possa ser acessado ou configure um servidor proxy do OCSP. Especifique o nome do servidor proxy usando a variável SSLHTTPProxyName na sub-rotina SSL. Nos sistemas do cliente, também é possível especificar o nome do servidor proxy usando a variável de ambiente MQSSLPROXY. Para obter mais detalhes, consulte as informações relacionadas.

Se você não estiver preocupado se os certificados TLS foram revogados, talvez porque esteja executando em um ambiente de teste, será possível configurar OCSPCheckExtensions para NO na sub-rotina SSL. Se você configurar essa variável, qualquer extensão de certificado AIA será ignorada. É possível que essa solução não seja aceita em um ambiente de produção, no qual você pode querer não permitir o acesso de usuários que possuírem certificados revogados.

A chamada para acessar o respondente do OCSP pode resultar em um dos três resultados a seguir:

válido
O certificado é válido.

Revogado
O certificado é revogado.

Desconhecido.
Esse resultado pode surgir por um dos três motivos:

- O IBM MQ não pode acessar o respondente OCSP.
- O respondente OCSP enviou uma resposta, mas o IBM MQ não pode verificar a assinatura digital da resposta.
- O respondente do OCSP enviou uma resposta indicando que ele não possui nenhum dado de revogação para o certificado.

Se o IBM MQ receber um resultado do OCSP de `Desconhecido`, seu comportamento dependerá da configuração do atributo OCSPAuthentication. Para gerenciadores de filas, este atributo é mantido em um dos locais a seguir:

- Linux UNIX Na sub-rotina SSL do arquivo `qm.ini` no UNIX and Linux.
- Windows No registro do Windows.

Este atributo pode ser configurado usando o IBM MQ Explorer. Para clientes, o atributo é mantido na sub-rotina de SSL do arquivo de configuração do cliente.

Se um resultado `Desconhecido` for recebido e OCSPAuthentication estiver configurado como REQUIRED (o valor padrão), o IBM MQ rejeitará a conexão e emitirá uma mensagem de erro de tipo AMQ9716. Se as mensagens de evento do SSL do gerenciador de filas estiverem ativadas, uma mensagem de evento SSL do tipo MQRC_CHANNEL_SSL_ERROR com ReasonQualifier configurado para MQRQ_SSL_HANDSHAKE_ERROR é gerada.

Se um resultado `Desconhecido` for recebido e OCSPAuthentication estiver configurado como OPTIONAL, o IBM MQ permitirá que o canal SSL seja iniciado e não são gerados avisos nem mensagens de eventos SSL.

Se um resultado `Desconhecido` for recebido e OCSPAuthentication estiver configurado como WARN, o canal SSL será iniciado, mas o IBM MQ emitirá uma mensagem de aviso do tipo AMQ9717 no log de erro. Se as mensagens de evento do SSL do gerenciador de filas estiverem ativadas, uma mensagem de evento SSL do tipo MQRC_CHANNEL_SSL_WARNING com ReasonQualifier configurado para MQRQ_SSL_UNKNOWN_REVOCATION é gerada.

Assinatura Digital das Respostas do OCSP

Um respondente do OCSP pode assinar suas respostas de uma de três maneiras. Seu respondente informará qual método é usado.

- A resposta do OCSP pode ser assinada digitalmente usando o mesmo certificado de CA que emitiu o certificado que estiver verificando. Nesse caso, não é necessário configurar nenhum certificado adicional; as etapas já concluídas para estabelecer a conectividade TLS são suficientes para verificar a resposta do OCSP.
- A resposta do OCSP pode ser assinada digitalmente usando outro certificado assinado pela mesma autoridade de certificação (CA) que emitiu o certificado que você está verificando. O certificado de assinatura é enviado junto com a resposta do OCSP nesse caso. O certificado que fluiu do respondente OCSP deve ter uma Extensão de Uso de Chave Estendida configurada como `id-kp-OCSPSigning` para que possa ser confiável para este propósito. Como a resposta do OCSP é enviada com o certificado que a assinou (e esse certificado é assinado por uma CA já confiável para a conectividade do TLS), nenhuma configuração de certificado adicional é necessária.
- A resposta do OCSP pode ser assinada digitalmente usando outro certificado que não esteja relacionado diretamente ao certificado que estiver verificando. Neste caso, a resposta do OCSP é assinada por um certificado emitido pelo próprio respondente do OCSP. Deve-se incluir uma cópia do certificado do respondente do OCSP para o banco de dados de chaves do cliente ou gerenciador de filas que executa a verificação de OCSP ; consulte “Incluindo um certificado de autoridade de certificação ou a parte pública de um certificado autoassinado em um repositório de chaves no UNIX, Linux, and Windows” na página 308 . Quando um certificado de CA é incluído, por padrão, ele é incluído como uma raiz confiável, que é a configuração necessária nesse contexto. Se este certificado não for incluído, o IBM MQ não poderá verificar a assinatura digital na resposta do OCSP e a verificação do OCSP resultará em um resultado Desconhecido, que pode fazer com que o IBM MQ feche o canal, dependendo do valor de OCSPAuthentication.

Online Certificate Status Protocol (OCSP) em aplicativos cliente Java e JMS

Devido a uma limitação da API Java, o IBM MQ pode usar a verificação de revogação de certificados do Online Certificate Status Protocol (OCSP) para soquetes seguros TLS somente quando o OCSP está ativado para o todo o processo de Java virtual machine (JVM). Existem duas maneiras de ativar o OCSP para todos os soquetes seguros na JVM:

- Edite o arquivo JRE java.security para incluir as definições de configuração do OCSP mostradas na Tabela 1 e reinicie o aplicativo.

- Use a API java.security.Security.setProperty(), sujeito a qualquer política do Java Security Manager em vigor.

No mínimo, é necessário especificar um dos valores ocsp.enable e ocsp.responderURL.

Nome da Propriedade	Descrição
ocsp.enable	Este valor da propriedade é `true` ou `false`. Se `true`, a verificação de OCSP é ativada ao realizar a verificação de revogação de certificados; se `false` ou não configurado, a verificação de OCSP está desativada.
ocsp.responderURL	Este valor de propriedade é uma URL que identifica o local do respondente do OCSP. Aqui está um exemplo; `ocsp.responderURL=http://ocsp.example.net:80`. Por padrão, o local do OCSP respondente é determinado implicitamente a partir do certificado que estiver sendo validado. A propriedade será usada quando a extensão Acesso de Informações de Autoridade (definida na RFC 3280) estiver ausente do certificado ou quando requerer substituição.
ocsp.responderCertSubjectName	Este valor da propriedade é o nome do assunto do certificado do respondente do OCSP. Aqui está um exemplo; `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Por padrão, o certificado do respondente do OCSP é aquele do emissor do certificado que está sendo validado. Esta propriedade identifica o certificado do respondente do OCSP quando o padrão não se aplica. Seu valor é um nome distinto de sequência (definido no RFC 2253) que identifica um certificado no conjunto de certificados que são fornecidos durante a validação do caminho do certificado. Nos casos em que o nome do assunto sozinho não é suficiente para identificar exclusivamente o certificado, as propriedades ocsp.responderCertIssuerName e ocsp.responderCertSerialNumber devem ser usadas. Quando esta propriedade for definida, então as propriedades ocsp.responderCertIssuerName e ocsp.responderCertSerialNumber serão ignoradas.
ocsp.responderCertIssuerName	Este valor da propriedade é o nome do emissor do certificado do respondente do OCSP. Aqui está um exemplo; `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Por padrão, o certificado do respondente do OCSP é aquele do emissor do certificado que está sendo validado. Esta propriedade identifica o certificado do respondente do OCSP quando o padrão não se aplica. Seu valor é um nome distinto de sequência (definido no RFC 2253) que identifica um certificado no conjunto de certificados que são fornecidos durante a validação do caminho do certificado. Quando esta propriedade for definida, a propriedade ocsp.responderCertSerialNumber também deve ser configurada. Essa propriedade é ignorada quando a propriedade ocsp.responderCertSubjectName está configurada.
ocsp.responderCertSerialNumber	Este valor da propriedade é o número de série do certificado do respondente do OCSP. Aqui está um exemplo; `ocsp.responderCertSerialNumber=2A:FF:00`. Por padrão, o certificado do respondente do OCSP é aquele do emissor do certificado que está sendo validado. Esta propriedade identifica o certificado do respondente do OCSP quando o padrão não se aplica. Este valor é uma sequência de dígitos hexadecimais (separadores de dois pontos ou espaço podem estar presentes) que identifica

Nome da Propriedade	Descrição
	um certificado no conjunto dos certificados fornecidos durante a validação do caminho do certificado. Quando esta propriedade for definida, a propriedade ocsp.responderCertIssuerName também deve ser configurada. Essa propriedade é ignorada quando a propriedade ocsp.responderCertSubjectName está configurada.

Antes de ativar do OCSP dessa forma, há várias considerações:

- Definir a configuração do OCSP afeta todos os soquetes seguros no processo da JVM. Em alguns casos, essa configuração pode ter efeitos colaterais indesejáveis quando a JVM é compartilhada com outro código do aplicativo que usa soquetes seguros TLS. Certifique-se de que a configuração do OCSP escolhido é adequada para todos os aplicativos que estão em execução na mesma JVM.
- Aplicar a manutenção para o seu JRE poderá sobrescrever o arquivo java.security. Tome cuidado ao aplicar correções temporárias do Java e manutenção do produto para evitar sobrescrever o arquivo java.security. Pode ser necessário reaplicar suas alterações java.security depois de aplicar a manutenção. Por essa razão, considere definir a configuração do OCSP usando a API java.security.Security.setProperty().
- Ativar a verificação de OCSP terá efeito somente se a verificação de revogação também estiver ativada. A verificação de revogação é ativada pelo método `PKIXParameters.setRevocationEnabled()`.
- Se você estiver usando o AMS Java Interceptor descrito em Ativando verificação de OCSP em interceptores nativos, tome cuidado para evitar o uso de uma configuração do OCSP java.security que entra em conflito com a configuração do OCSP AMS no arquivo de configuração de keystore.

Trabalhando com as Listas de Revogação de Certificados e Listas de Revogação de Autoridade

O suporte do IBM MQ para CRLs e ARLs varia por plataforma.

O suporte CRL e ARL em cada plataforma é o seguinte:

- No z/OS, o SSL do Sistema suporta as CRLs e ARLs armazenadas nos servidores LDAP pelo produto Tivoli Public Key Infrastructure.
- Em outras plataformas, o suporte CRL e ARL é compatível com as recomendações de perfil PKIX X.509 V2 CRL.

IBM MQ mantém um cache de CRLs e ARLs que foram acessadas nas últimas 12 horas.

Quando um gerenciador de filas ou IBM MQ MQI client recebe um certificado, ele verifica a CRL para confirmar se o certificado ainda é válido. O IBM MQ primeiro verifica no cache, se houver um cache. Se o CRL não estiver no cache, o IBM MQ interrogará os locais do servidor LDAP CRL na ordem em que eles ocorrem na lista de nomes de objetos de informações sobre autenticação especificados pelo atributo *SSLCRLNL*, até que o IBM MQ localize um CRL disponível. Se a lista de nomes não estiver especificada ou está especificada com um valor em branco, as CRLs não são verificadas.

Configurando Servidores LDAP

Configure a Estrutura em Árvore de Informações do Diretório LDAP para que reflita a hierarquia de Nomes Distintos de CAs. Faça isso usando arquivos de Formato de Troca de Dados LDAP.

Configure a estrutura do LDAP DIT (Directory Information Tree) para utilizar a hierarquia correspondente aos Nomes Distintos das CAs que emitem certificados e CRLs. Você pode definir a estrutura DIT com um arquivo que utiliza o LDAP LDIF (Data Interchange Format). Você também pode utilizar arquivos do LDIF para atualizar um diretório.

Arquivos LDIF são arquivos de texto ASCII que contém as informações exigidas para definir objetos dentro do diretório LDAP. Os arquivos LDIF contêm uma ou mais entradas, cada uma das quais compreende um Nome Distinto, pelo menos uma definição de classe de objeto e, como opção, várias definições de atributos.

O atributo `certificateRevocationList;binary` contém uma lista em formato binário de certificados de usuários revogados. O atributo `authorityRevocationList;binary` contém uma lista binária de certificados CA que foram revogados. Para uso com o TLS do IBM MQ, os dados binários para esses atributos devem em estar conformidade com o formato DER (Regras Distintas de Codificação). Para obter mais informações sobre os arquivos LDIF, consulte a documentação fornecida com o seu servidor LDAP.

A Figura 20 na página 347 mostra um arquivo LDIF de amostra que pode ser criado como entrada para o servidor LDAP carregar as CRLs (listas de revogação de certificado) e ARLs emitidas pela CA1, que é uma Autoridade de certificação imaginária com o Nome distinto "CN=CA1, OU=Test, O=IBM, C=GB", configurado pela Organização de teste na 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)
```

Figura 20. Arquivo LDIF de amostra para uma Autoridade de certificação. Isso poderá variar de implementação para implementação.

Figura 21 na página 347 mostra a estrutura DIT que o seu servidor LDAP cria ao carregar o arquivo LDIF de amostra mostrado no Figura 20 na página 347 juntamente com um arquivo semelhante para a CA2, uma Autoridade de certificação imaginária definida pela organização PKI, também dentro do IBM.

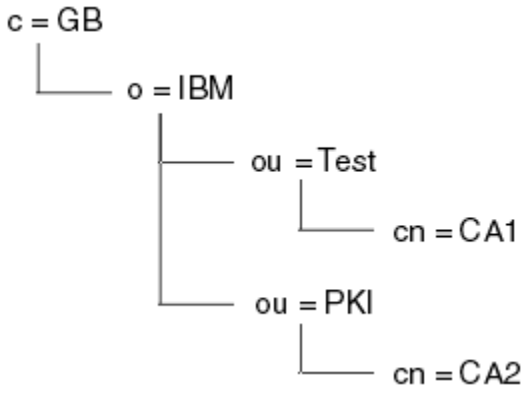


Figura 21. Exemplo de estrutura de Directory Information Tree do LDAP

O WebSphere MQ verifica ambas CRLs e ARLs.

Nota: Certifique-se de que a lista de controle de acesso para seu servidor LDAP permita que usuários autorizados leiam, pesquisem e comparem as entradas que contenham as CRLs e ARLs. O WebSphere MQ acessa o servidor LDAP usando as propriedades LDAPUSER e LDAPPWD do objeto AUTHINFO.

Configurando e Atualizando Servidores LDAP
Use este procedimento para configurar ou atualizar o servidor LDAP.

1. Obtenha as CRLs e ARLs em formato DER a partir da sua Autoridade ou Autoridades de Certificação.

2. Utilizando o editor de texto ou a ferramenta fornecida em seu servidor LDAP, crie um ou mais arquivos LDIF que contenham o Nome Distinto da CA e as definições da classe de objetos exigidas. Copie os dados do formato DER para o arquivo LDIF como os valores do atributo `certificateRevocationList;binary` atributo para CRLs, o atributo `authorityRevocationList;binary` para ARLs ou ambos.
3. Inicie seu servidor LDAP.
4. Inclua as entradas do arquivo LDIF ou arquivos que você criou na etapa “2” na página 348.

Depois de configurar o servidor LDAP CRL, verifique se ele está configurado corretamente. Primeiro, tente utilizar um certificado que não esteja revogado no canal, e verifique se o canal foi iniciado corretamente. Em seguida utilize um certificado revogado e verifique se o canal falhou ao iniciar.

Obtenha regularmente as CRLs atualizadas a partir das Autoridades de certificação. Tente fazer esta operação em seus servidores LDAP a cada 12 horas.

Acessando as CRLs e ARLs com um Gerenciador de Filas

Um gerenciador de filas é associado a um ou mais objetos de informação de autenticação, que contêm o endereço de um servidor de LDAP CRL. IBM i IBM MQ on IBM i se comporta de forma diferente de outras plataformas.

Observe que nesta seção, as informações sobre as CRLs (Certificate Revocation Lists) também se aplicam às ARLs (Authority Revocation Lists).

Informe ao gerenciador de filas como acessar as CRLs ao fornecê-los os objetos de informações de autenticação, cada qual mantendo o endereço de um servidor de CRL LDAP. Os objetos de informações sobre autenticação são mantidos em um lista de nomes, que é especificada no atributo de gerenciador de filas *SSLCRLNL*.

No seguinte exemplo, o MQSC é utilizado para especificar os parâmetros:

1. Defina os objetos de informações de autenticação usando o comando DEFINE AUTHINFO MQSC com o parâmetro AUTHTYPE definido para CRLLDAP. IBM i No IBM i, também é possível o comando CRTMQMAUTI CL.

   O valor CRLLDAP para o parâmetro AUTHTYPE indica que as CRLs são acessadas em servidores LDAP. Cada objeto de informações de autenticação com o tipo CRLLDAP que você criar contém o endereço de um servidor LDAP. Quando você tem mais de um objeto de informações sobre autenticação, os servidores LDAP para os quais eles apontam devem conter informações idênticas. Isso fornece continuidade de serviço caso ocorra uma ou mais falhas nos servidores LDAP.

   z/OS Além disso, somente no z/OS, todos os servidores LDAP devem ser acessados usando o mesmo ID do usuário e senha. O ID do usuário e senha utilizados são aqueles especificados no primeiro objeto AUTHINFO na lista de nomes.

   Em todas as plataformas, o ID do usuário e a senha são enviados não criptografados para o servidor LDAP.
2. Utilizando o comando DEFINE NAMELIST MQSC, defina uma lista de nomes para os nomes de seus objetos de informações de autenticação. z/OS No z/OS, assegure-se de que o atributo da lista de nomes NLTYPE esteja configurado como AUTHINFO.
3. Utilizando o comando ALTER QMGR MQSC, forneça a lista de nomes ao gerenciador de filas. Por exemplo:

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   em que `sslcrlnlname` é a sua lista de nomes de objetos de informações sobre autenticação

   Esse comando configura um atributo de gerenciador de filas chamado *SSLCRLNL*. O valor inicial do gerenciador de filas para este atributo está em branco.

IBM i No IBM i, é possível especificar os objetos de informações de autenticação, porém o gerenciador de filas não usa nem os objetos de informações de autenticação, nem uma lista de nomes de objetos de informações de autenticação. Apenas os clientes do IBM MQ que usam uma tabela de conexão de cliente gerada por um Gerenciador de Filas do IBM i usam as informações de autenticação especificadas para esse Gerenciador de Filas do IBM i. O atributo de gerenciador de filas *SSLCRLNL* no IBM i determina quais informações sobre autenticação são usadas por esses clientes. Consulte "Acessando CRLs e ARLs no IBM i" na página 349 para obter informações sobre como informar um gerenciador de filas do IBM i como acessar as CRLs.

É possível incluir até 10 conexões para servidores LDAP alternativos para a lista de nomes, para garantir a continuidade do serviço se um ou mais servidores LDAP falharem. Observe que os servidores LDAP devem conter informações idênticas.

IBM i *Acessando CRLs e ARLs no IBM i*

Use este procedimento para acessar CRLs ou ARLs no IBM i.

Observe que nesta seção, as informações sobre as CRLs (Certificate Revocation Lists) também se aplicam às ARLs (Authority Revocation Lists).

Siga estas etapas para configurar um local de CRL para um certificado específico no IBM i:

1. Acesse a interface DCM, conforme descrito em "Acessando DCM" na página 277.
2. Na categoria de tarefas **Gerenciar locais de CRL** no painel de navegação, clique em **Incluir local de CRL**. A página Gerenciar Locais de CRL é exibida no quadro de tarefas.
3. No campo **Nome do Local da CRL** , digite um nome do local da CRL, por exemplo `LDAP Server #1`
4. No campo **Servidor LDAP**, digite o nome do servidor LDAP.
5. No campo **Usar Secure Sockets Layer (SSL)**, selecione **Sim** se desejar conectar-se ao servidor LDAP usando TLS. Caso contrário, selecione **Não**.
6. No campo **Número da Porta**, digite um número da porta para o servidor LDAP, por exemplo, 389.
7. Se o seu servidor LDAP não permitir que usuários anônimos acessem o diretório, digite um nome distinto de login para o servidor no campo **Nome Distinto de Login**.
8. Clique em **OK**. O DCM informará que o local da CRL foi criado.
9. No painel de navegação, clique em **Selecionar um Armazenamento de Certificados**. A página Selecionar um Armazenamento de Certificados é exibida no quadro de tarefas.
10. Selecione a caixa de opção **Outro Armazenamento de Certificados do Sistema** e clique em **Continuar**. A página Armazenamento de Certificados e Senha é exibida.
11. No campo **Caminho e nome de arquivo de armazenamento de certificados**, digite o caminho e nome de arquivo IFS configurado quando "Criando um armazenamento de certificados no IBM i" na página 278.
12. Digite uma senha no campo **Senha do Armazenamento de Certificados**. Clique em **Continue**. A página Armazenamento de Certificados Atual é exibida no quadro de tarefas.
13. Na categoria de tarefas **Gerenciar Certificados** no painel de navegação, clique em **Atualizar Designação do Local da CRL**. A página Designação do Local de CRL é exibida no quadro de tarefas.
14. Selecione o botão de opção para o certificado de CA para o qual deseja atribuir o local da CRL. Clique em **Atualizar a Designação do Local da CRL**. A página Atualizar Designação do Local de CRL é exibida no quadro de tarefas.
15. Selecione o botão de opção para o local de CRL para o qual deseja atribuir o certificado. Clique em **Atualizar Designação**. O DCM informará que a designação foi atualizada

Observe que o DCM permite que você atribua um servidor LDAP diferente pela Autoridade de certificação.

Acessando CRLs e ARLs usando o IBM MQ Explorer

É possível usar o IBM MQ Explorer para informar a um gerenciador de filas como acessar CRLs.

Observe que nesta seção, as informações sobre as CRLs (Certificate Revocation Lists) também se aplicam às ARLs (Authority Revocation Lists).

Utilize o seguinte procedimento para definir uma conexão LDAP para uma CRL:

1. Certifique-se de que iniciou o gerenciador de filas.
2. Clique com o botão direito na pasta **Informações sobre autenticação** e clique em **Novo -> Informações sobre autenticação**. Na folha de propriedade que abre:
   a. Na primeira página **Criar Informações de Autenticação**, digite um nome para o objeto CRL (LDAP).
   b. Na página **Geral** de **Alterar Propriedades**, selecione o tipo de conexão. Opcionalmente é possível digitar uma descrição.
   c. Selecione a página **CRL(LDAP)** de **Alterar Propriedades**.
   d. Digite o nome do servidor LDAP como o nome da rede ou o endereço IP.
   e. Caso o servidor exija os detalhes de login, forneça o ID do usuário e, se for preciso, uma senha.
   f. Clique em **OK**.
3. Clique com o botão direito na pasta Lista de nomes e clique em **Nova-> Lista de nomes**. Na folha de propriedade que abre:
   a. Digite um nome para a lista de nomes.
   b. Inclua o nome do objeto CRL(LDAP) (da etapa "2.a" na página 350) na lista.
   c. Clique em **OK**.
4. Clique com o botão direito do mouse no gerenciador de filas, selecione **Propriedades** e selecione a página **SSL**:
   a. Selecione a caixa de entrada **Verificar certificados recebidos por este gerenciador de filas comparandos às Listas de Certificados Revogados**.
   b. Digite o nome da lista de nomes (da etapa "3.a" na página 350) no campo **Nomes da CRL**.

Acessando as CRLs e ARLs com um IBM MQ MQI client

Há três opções para especificar os servidores LDAP que contêm CRLs para verificar por um IBM MQ MQI client.

Observe que nesta seção, as informações sobre as CRLs (Certificate Revocation Lists) também se aplicam às ARLs (Authority Revocation Lists).

As três maneiras de especificar os servidores LDAP são as seguintes:

- Utilizando uma tabela de definição de canais
- Usando a estrutura de opções de configuração do SSL, MQSCO, ou uma chamada de MQCONNX
- Usando o Active Directory (em sistemas Windows com suporte ao Active Directory)

Para obter mais detalhes, consulte as informações relacionadas.

É possível incluir até 10 conexões para servidores LDAP alternativos, para garantir a continuidade do serviço se um ou mais servidores LDAP falharem. Observe que os servidores LDAP devem conter informações idênticas.

Não é possível acessar CRLs do LDAP a partir de um canal IBM MQ MQI client em execução no Linux (plataforma zSeries).

Local de um respondente OCSP e dos servidores LDAP que contêm CRLs

Em um sistema IBM MQ MQI client,é possível especificar o local de um respondente OCSP e dos servidores Lightweight Directory Access Protocol (LDAP) que contêm listas de revogação de certificado (CRLs).

É possível especificar esses locais de três maneiras descritas aqui, em ordem de precedência decrescente.

IBM i Para o IBM i, consulte Acessando CRLs e ARLs no IBM i.

Quando um aplicativo IBM MQ MQI client emite uma chamada MQCONNX

É possível especificar um respondente OCSP ou um servidor LDAP que contém CRLs em uma chamada **MQCONNX**.

Em uma chamada **MQCONNX**, a estrutura de opções de conexão, MQCNO, pode referenciar uma estrutura de opções de configuração de SSL, MQSCO. Por sua vez, a estrutura MQSCO pode referenciar uma ou mais estruturas de registro de informações sobre autenticação, MQAIR. Cada estrutura MQAIR contém todas as informações que um IBM MQ MQI client requer para acessar um respondente OCSP ou um servidor LDAP que contém CRLs. Por exemplo, um dos campos em uma estrutura MQAIR é a URL na qual um replicador pode ser contatado. Para obter mais informações sobre a estrutura MQAIR, consulte MQAIR - Registro de informações sobre autenticação.

Usando uma tabela de definição de canal de cliente (ccdt) para acessar um respondente OCSP ou servidores LDAP

Para que um IBM MQ MQI client pode acessar um respondente OCSP ou servidores LDAP que contêm CRLs, incluem os atributos de um ou mais objetos de informação de autenticação em uma tabela de definição de canal do cliente.

Em um gerenciador de filas do servidor é possível definir um ou mais objetos de informações sobre autenticação. Os atributos de um objeto de autenticação contêm todas as informações que são necessárias para acessar um respondente OCSP (em plataformas em que OCSP é suportado) ou um servidor LDAP que contém CRLs. Um dos atributos especifica a URL do respondente OCSP, outro especifica o endereço do host ou endereço IP de um sistema no qual um servidor LDAP é executado.

z/OS IBM i Um objeto de informação de autenticação com AUTHTYPE(OCSP) não se aplica para uso no IBM i ou z/OS os gerenciadores de filas, mas pode ser especificado nas plataformas a serem copiadas na tabela de definição de canal do cliente (CCDT) para uso do cliente.

Para ativar um IBM MQ MQI client para acessar um respondente OCSP ou servidores LDAP que contêm CRLs, os atributos de um ou mais objetos de informação de autenticação podem ser incluídos em uma tabela de definição de canal do cliente. É possível incluir atributos em uma das seguintes maneiras:

Multi

Nas plataformas do servidor AIX, Linux, IBM i, Solaris e Windows

É possível definir uma lista de nomes que contém os nomes de um ou mais objetos de informações de autenticação. Em seguida, é possível configurar o atributo de gerenciador de filas, **SSLCRLNL**, para o nome dessa lista de nomes.

Se você estiver usando CRLs, mais de um servidor LDAP poderá ser configurado para fornecer maior disponibilidade. A intenção é que cada servidor LDAP contenha as mesmas CRLs. Se um servidor LDAP estiver indisponível quando for necessário, um IBM MQ MQI client poderá tentar acessar outro.

Os atributos dos objetos de informação de autenticação identificados pela lista de nomes são referidos coletivamente aqui como o *local de revogação de certificado*. Ao configurar o atributo de gerenciador de filas, **SSLCRLNL**, para o nome da lista de nomes, o local de revogação de certificado é copiado para a tabela de definição de canal de cliente associada ao gerenciador de filas. Se a CCDT puder ser acessada a partir de um sistema do cliente como um arquivo compartilhado ou se a CCDT for então copiada em um sistema do cliente, o IBM MQ MQI client nesse sistema poderá usar o local de revogação de certificado na CCDT para acessar um replicador OCSP ou servidores LDAP que contêm CRLs.

Se o local de revogação de certificado do gerenciador de filas for mudado posteriormente, a mudança será refletida na CCDT associada ao gerenciador de filas. Se o atributo de gerenciador de filas, **SSLCRLNL**, for configurado em branco, o local de revogação de certificado será removido do CCDT. Estas alterações não são refletidas em nenhuma cópia da tabela em um sistema do cliente.

Se você requerer que o local de revogação de certificado nas extremidades do cliente e do servidor de um canal MQI seja diferente, e o gerenciador de filas do servidor for aquele que é usado para criar o local de revogação de certificado, será possível fazer isto conforme a seguir:

1. No gerenciador de filas do servidor, crie o local de revogação de certificado para uso no sistema do cliente.
2. Copie a CCDT contendo o local de revogação de certificado no sistema do cliente.
3. No gerenciador de filas do servidor, altere o local de revogação de certificado para o que é necessário na extremidade do servidor do canal MQI.
4. Na máquina cliente, é possível usar o comando **runmqsc** com o parâmetro **-n**.

Multi

Em plataformas do cliente AIX, Linux, IBM i, Solaris e Windows

É possível construir uma CCDT na máquina cliente usando o comando runmqsc com o parâmetro **-n** e os objetos **DEFINE AUTHINFO** no arquivo CCDT A ordem em que os objetos são definidos em é a ordem na qual eles são usados no arquivo. Qualquer nome que você possa usar em um objeto **DEFINE AUTHINFO** não será retido no arquivo. Somente números posicionais são usados quando você **DISPLAY** os objetos **AUTHINFO** em um arquivo CCDT.

Nota: Se o parâmetro **-n** for especificado, não se deve especificar qualquer outro parâmetro.

Usando o Active Directory no Windows

Windows

Nos sistemas Windows é possível usar o comando de controle **setmqcrl** para publicar as informações de CRL atuais no Active Directory.

O comando **setmqcrl** não publica informações de OCSP.

Para obter informações sobre este comando e sua sintaxe, consulte setmqcrl.

Acessando as CRLs e ARLs com o IBM MQ classes for Java e IBM MQ classes for JMS

O IBM MQ classes for Java e o IBM MQ classes for JMS acessam as CRLs de forma diferente de outras plataformas.

Para obter informações sobre como trabalhar com CRLs e ARLs com o IBM MQ classes for Java, consulte Usando listas de revogação de certificado

Para obter informações sobre como trabalhar com CRLs e ARLs com IBM MQ classes for JMS, consulte Propriedade de objeto SSLCERTSTORES

Manipulando Objetos de Informações de Autenticação

É possível manipular objetos de informações sobre autenticação usando os comandos MQSC ou PCF ou o IBM MQ Explorer.

Os seguintes comandos MQSC agem sobre objetos informações de autenticação:

- DEFINE AUTHINFO
- ALTER AUTHINFO
- DELETE AUTHINFO
- DISPLAY AUTHINFO

Para uma descrição completa desses comandos, veja Comandos MQSC.

Os seguintes comandos Programmable Command Format (PCF) agem sobre objetos de informações de autenticação:

- Criar Informações sobre Autenticação
- Copiar Informações sobre Autenticação

- Alterar Informações sobre Autenticação
- Excluir Informações sobre Autenticação
- Consultar Informações sobre Autenticação
- Consultar Nomes de Informações sobre Autenticação

Para obter uma descrição completa desses comandos, consulte Definições dos formatos de comando programáveis.

Em plataformas em que ele estiver disponível, também será possível usar o IBM MQ Explorer.

Linux UNIX Usando o Pluggable Authentication Method (PAM)

É possível usar o PAM apenas em plataformas UNIX and Linux. Um sistema típico sistema UNIX possui módulos PAM que implementam o mecanismo de autenticação tradicional; no entanto, pode haver mais. Assim como a tarefa básica de validação de senhas, os módulos PAM também podem ser chamados para realizar regras adicionais.

Os arquivos de configuração definem qual método de autenticação deve ser usado para cada aplicativo. Os aplicativos de exemplo incluem o login do terminal padrão, ftp e telnet.

A vantagem do PAM é que o aplicativo não precisa saber ou se importar sobre como o ID do usuário está realmente sendo autenticado. Desde que o aplicativo possa fornecer uma formulário correto de dados de autenticação para PAM, o mecanismo por trás dele é transparente.

O formulário de dados de autenticação depende do sistema que está sendo usado. Por exemplo, o IBM MQ obtém uma senha por meio de parâmetros, como a estrutura MQCSP usada na chamada de API `MQCONNX`.

Importante: Não é possível configurar o atributo **AUTHENMD** até que você instale o IBM MQ 8.0.0 Fix Pack 3 e, em seguida, reinicie o gerenciador de filas, usando um **-e CMDLEVEL=** *level* de *802* (no comando strmqm) para configurar o nível de comando necessário.

Configurando seu sistema para usar o PAM

O nome do serviço usado pelo IBM MQ ao chamar o PAM é *ibmmq*.

Observe que uma instalação do IBM MQ tenta manter uma configuração de PAM padrão que permite conexões de usuários do sistema operacional com base nos padrões conhecidos para os sistemas operacionais diferentes.

No entanto, seu administrador do sistema deve verificar se nas regras definidas no `/etc/pam.conf` ou no `/etc/pam.d/ibmmq`, os arquivos ainda são apropriados.

Autorizando o acesso aos objetos

Esta seção contém informações sobre como usar o gerenciador de autoridade de objeto e programas de saída de canal para controlar o acesso aos objetos.

ULW Em sistemas UNIX, Linux, and Windows. o acesso a objetos é controlado usando o gerenciador de autoridade de objeto (OAM). Esta coleção de tópicos contém informações sobre como usar a interface de comando para o OAM.

Esta seção também contém uma lista de verificação que é possível usar para determinar quais tarefas executar para aplicar segurança em seu sistema em todas as plataformas e as considerações para conceder aos usuários a autoridade para administrar o IBM MQ e trabalhar com os objetos do IBM MQ.

Se os mecanismos de segurança fornecidas não atenderem suas necessidades, é possível desenvolver seus próprios programas de saída de canal.

Determinando qual usuário é usado para autorização

As autoridades para acessar recursos são concedidas a grupos dos quais o usuário é membro ou, em determinados modos, diretamente ao usuário associado à conexão.. Durante o processo de conexão, e em particular para conexões remotas (cliente), essa identidade poderia ser alterada pela configuração do gerenciador de filas. Esta página lista os diferentes recursos do IBM MQ e suas opções de configuração que podem impactar a identidade de um aplicativo de conexão e a ordem de precedência na qual esses recursos entram em vigor

Recursos que podem modificar qual usuário é adotado

Os diferentes recursos que podem configurar qual usuário deve ser autorizado são os seguintes:

Usuário declarado do aplicativo
Quando uma conexão remota é iniciada pelo IBM MQ, o usuário do sistema operacional com o qual o processo está em execução é enviado para o gerenciador de filas de recebimento Esse usuário é enviado para assegurar que, se não existir nenhuma configuração adicional que modifique o usuário, haja um usuário que possa ser usado para verificação de autorização

Não é recomendado usar esse usuário como base para autorização, pois ele permite que as conexões declarem sua identidade sem qualquer validação do lado do servidor. Isso pode até incluir o usuário administrativo ('mqm ').

Configuração MCAUSER do Canal
Aplicativos que se conectam por meio de ligações de rede fazem isso usando uma definição de canal IBM MQ . As definições de canal suportam o atributo **MCAUSER** , que pode ser usado para especificar um usuário diferente a ser usado para autorização em vez do usuário declarado pelos aplicativos de conexão.

Autenticação de conexão ADOPTCTX
Os aplicativos podem especificar um usuário e uma senha a serem enviados para um gerenciador de filas para propósitos de autenticação Essas credenciais são autenticadas usando a configuração especificada para o recurso Autenticação de Conexão. A opção **ADOPTCTX** para Autenticação de Conexão controla se um usuário deve ser usado para autorização após ele ter sido validado com êxito Se configurado como YES, o usuário fornecido para autenticação será adotado para verificações de autorização.

Registro de autenticação de canal MCAUSER
Durante o processamento da conexão, o gerenciador de filas tentará localizar um registro de autenticação de canal correspondente à conexão. Se um registro de autenticação de canal for correspondido e seu valor de atributo **USERSRC** for configurado como MAP, IBM MQ mudará o usuário usado para autorizações para o valor do atributo **MCAUSER** .

Saídas de Segurança
Saídas de segurança são funções customizadas que podem ser gravadas e chamadas durante o processamento de segurança IBM MQ . Quando a função é chamada, ela é fornecida com uma cópia da estrutura MQCD que inclui vários campos relacionados ao usuário de conexões que serão usados para verificações de autorização... As saídas de segurança podem modificar esses campos para alterar o usuário que será autorizado

ordem de precedência

A tabela a seguir mostra a ordem de precedência para cada recurso de segurança descrito no “Recursos que podem modificar qual usuário é adotado” na página 354 quando o IBM MQ está selecionando um usuário para autorizar A ordem é do mais baixo para o mais alto, ou seja, um recurso de segurança que define um usuário na primeira linha é substituído por qualquer uma das outras linhas.

Tabela 68. Ordem de precedência para recursos de segurança

Ordem	**Recurso**
1 (mais baixo)	ID declarado do aplicativo

Tabela 68. Ordem de precedência para recursos de segurança (continuação)	
Ordem	**Recurso**
2	Atributo **MCAUSER** de definição de canal
3	Autenticação de conexão com **ADOPTCTX(YES)**
4	Registros de autenticação de canal com **USERSRC(MAP)**
5 (mais alto)	Saída de segurança

Implicações da adoção precoce

A autenticação de conexão e registros de autenticação de canal fornecem uma opção de configuração que controla quando a adoção do usuário de autenticação de conexão é executada. Essa configuração é referida como adoção antecipada.. Se a adoção antecipada estiver ativada, a adoção da identidade de autenticação de conexão ocorrerá antes que os registros de autenticação de canal sejam processados (o que significa que os registros de autenticação de canal substituem qualquer adoção do **CONNAUTH** .

Se desativada, a ordem será revertida-ou seja, os registros de autenticação de canal serão processados antes da adoção do **CONNAUTH** Nessa situação, a adoção da autenticação de conexão tem uma prioridade efetiva mais alta que a autenticação de canal.

A configuração padrão para adoção antecipada é `enabled`..

ULW Controlando o acesso a objetos usando o OAM no UNIX, Linux, and Windows

O gerenciador de autoridade de objeto (OAM) fornece uma interface de comando para conceder e revogar autoridade para objetos do IBM MQ.

Você deve estar adequadamente autorizado para usar esses comandos, conforme descrito em "Autoridade para administrar o IBM MQ no UNIX, Linux, and Windows" na página 406. Os IDs de usuários que estão autorizados a administrar o IBM MQ, tem autoridade de *super usuário* para o gerenciador de filas, o que significa que não é necessário lhes conceder permissão adicional para emitir quaisquer pedidos ou comandos MQI.

Linux UNIX Permissões baseadas em usuário do OAM no UNIX and Linux

A partir da IBM MQ 8.0, em sistemas UNIX and Linux, o gerenciador de autoridade de objeto (OAM) pode usar a autorização baseada em usuário, bem como uma autorização baseada em grupo.

Antes da IBM MQ 8.0, as listas de controle de acesso (ACLs) no UNIX and Linux eram baseadas apenas em grupos. A partir da IBM MQ 8.0, as ACLs são baseadas nos IDs de usuário e nos grupos e é possível usar o modelo baseado em usuário ou o modelo baseado em grupo para a autorização configurando o atributo **SecurityPolicy** para o valor apropriado, conforme descrito em Configurando os serviços instaláveis e em Configurando sub-rotinas do serviço de autorização no UNIX e no Linux.

Mudanças no comportamento da IBM MQ 8.0 e mais recente

A partir da IBM MQ 8.0, ao executar com a política baseada em usuário, alguns comandos retornam informações diferentes de versões anteriores do produto:

- Os comandos **dmpmqaut** e **dmpmqcfg** mostram registros baseados em usuário, como fazem as operações equivalentes do PCF.
- O plug-in do OAM para o IBM MQ Explorer mostra registros baseados em usuário e permite modificações baseadas em usuário.

- A função **Inquire** do OAM retorna resultados que mostram que ela é compatível com o usuário.

Usar o atributo **-p** no comando **setmqaut** não concede acesso a todos os usuários no mesmo grupo primário, quando as autorizações baseadas em usuário são ativadas no arquivo `qm.ini`, conforme descrito na sub-rotina Serviço do arquivo qm.ini.

Se você começar a empregar a autorização baseada em usuário e tiver muitos usuários, provavelmente haverá mais registros que são armazenados na fila AUTH do que com o modelo baseado em grupo, e o processo de autorização poderá demorar um pouco mais do que antes pois há mais registros a serem verificados. Não espera-se que este aumento seja significativo. Se necessário, é possível usar uma mistura de permissões de usuário e de grupo.

Considerações Sobre Migração

Se você alterar o modelo de grupo para usuário para um gerenciador de filas existente, não haverá efeito imediato. As autorizações que já foram feitas continuam a se aplicar. Qualquer usuário que se conecta ao gerenciador de filas recebe os mesmos privilégios que antes: a combinação de todos os grupos aos quais seu ID pertence. Quando novos comandos **setmqaut** forem emitidos para IDs do usuário, eles terão efeito imediato.

Se você criar um novo gerenciador de filas com a política do usuário, esse gerenciador de filas terá permissões apenas para o usuário que o criar (que é normalmente, mas não necessariamente, o ID do usuário `mqm`). Há também permissões que são concedidas automaticamente ao grupo `mqm`. No entanto, se você não tiver o `mqm` como o grupo primário, então o grupo `mqm` não será incluído no conjunto inicial de autorizações.

Se você mudar de uma política de usuário para grupo, as autorizações baseadas em usuário não serão automaticamente excluídas. No entanto, elas não serão mais usadas durante a verificação de permissões. Antes de reverter a política, salve a configuração atual, altere a política, reinicie o gerenciador de filas e, em seguida, reproduza o script. Como agora é um gerenciador de filas baseado em grupo, o efeito é que as regras desse ID do usuário serão armazenadas com base no grupo primário.

Conceitos relacionados

Gerenciador de autoridade de objeto (OAM)

Diretores e grupos no UNIX, no Linux e no Windows

Sub-rotina Service do arquivo qm.ini

Referências relacionadas

Comando **crtmqm** (criar gerenciador de filas)

ULW Concedendo acesso a um objeto do IBM MQ no UNIX, Linux, and Windows

Use o comando de controle **setmqaut**, o comando MQSC **SET AUTHREC** ou o comando PCF **MQCMD_SET_AUTH_REC** para fornecer aos usuários e grupos de usuários o acesso aos objetos do IBM MQ. Observe que no IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Para obter uma definição completa do comando de controle **setmqaut** e sua sintaxe, consulte setmqaut.

Para obter uma definição completa do comando MQSC **SET AUTHREC** e sua sintaxe, consulte SET AUTHREC.

Para obter uma definição completa do comando PCF **MQCMD_SET_AUTH_REC** e sua sintaxe, consulte Configurar registro de autoridade.

O gerenciador de filas deve estar em execução para usar esse comando. Quando você mudou o acesso de um diretor, as mudanças são refletidas imediatamente pelo OAM.

Para fornecer aos usuários acesso a um objeto, é necessário especificar:

- O nome do gerenciador de filas que possui os objetos com os quais você está trabalhando; se você não especificar o nome de um gerenciador de filas, o gerenciador de filas padrão será assumido.

- O nome e o tipo do objeto (para identificar o objeto exclusivamente). Você especifica o nome como um *perfil*; esse é o nome explícito do objeto ou um nome genérico, incluindo caracteres curinga. Para obter uma descrição detalhada de perfis genéricos e o uso de caracteres curinga dentro deles, consulte "Usando perfis genéricos do OAM no UNIX, Linux, and Windows" na página 358.
- Um ou mais nomes de principais e de grupos aos quais a autoridade se aplica.

  Se um ID do usuário contiver espaços, coloque-o entre aspas ao usar esse comando. Em sistemas Windows, é possível qualificar um ID do usuário com um nome de domínio. Se o ID do usuário real contiver um símbolo de arroba (@), substitua-o por @@ para mostrar que ele faz parte do ID do usuário, não do delimitador entre o ID do usuário e o nome do domínio.
- Uma lista de autorizações. Cada item da lista especifica um tipo de acesso que deve ser concedido a esse objeto (ou revogado dele). Cada autorização na lista é especificada como uma palavra-chave, prefixada com um sinal de mais (+) ou um sinal de menos (-). Use um sinal de mais para incluir a autorização especificada, e um sinal de menos para remover a autorização. Não deve haver espaços entre os sinais de + ou - e a palavra-chave.

  É possível especificar qualquer número de autorizações em um único comando. Por exemplo, a lista de autorizações para permitir que um usuário ou um grupo coloque mensagens em uma fila e navegue por elas, mas revogue o acesso para obter mensagens é:

```
+browse -get +put
```

Exemplos de como usar o comando `setmqaut`

Os seguintes exemplos mostram como usar o comando `setmqaut` para conceder e revogar permissões de uso de um objeto:

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
         -g groupa +browse -get +put
```

Nesse exemplo:

- `saturn.queue.manager` é o nome do gerenciador de filas
- `queue` é o tipo de objeto
- `RED.LOCAL.QUEUE` é o nome do objeto
- `groupa` é o identificador do grupo com autorizações que devem ser mudadas
- `+browse -get +put` é a lista de autorização para a fila especificada
  - `+browse` inclui autorização para navegar pelas mensagens na fila (para emitir **MQGET** com a opção de navegação)
  - `-get` remove a autorização para obter mensagens (**MQGET**) da fila
  - `+put` inclui autorização para colocar mensagens (**MQPUT**) na fila

O comando a seguir revoga a autoridade put na fila MyQueue do fvuser do diretor e dos grupos groupa e groupb. Em sistemas UNIX and Linux, este comando também revoga a autoridade put para todos os principais que estão no mesmo grupo primário que fvuser.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
         -g groupa -g groupb -put
```

Usando o comando `setmqaut` com um serviço de autorização diferente

Se você estiver usando seu próprio serviço de autorização em vez do OAM, é possível especificar o nome desse serviço no comando **setmqaut** para direcionar o comando para esse serviço. Você deverá especificar esse parâmetro se tiver vários componentes instaláveis em execução ao mesmo tempo; caso

contrário, a atualização será feita no primeiro componente instalável do serviço de autorização. Por padrão, esse é o OAM fornecido.

Observações de uso para SET AUTHREC

A lista de autorizações para incluir e a lista de autorizações para remover não devem se sobrepor. Por exemplo, você não pode incluir autoridade de exibição e remover a autoridade de exibição com o mesmo comando. Essa regra se aplica mesmo que as autoridades sejam expressas usando opções diferentes. Por exemplo, o comando falhará porque a autoridade DSP se sobrepõe com autoridade a ALLADM:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALLADM)
```

A exceção para esse comportamento de sobreposição é com a autoridade ALL. O comando a seguir inclui autoridades ALL primeiro, em seguida, remove a autoridade SETID:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(ALL) AUTHRMV(SETID)
```

O seguinte comando remove autoridades ALL primeiro, em seguida, inclui a autoridade DSP:

```
SET AUTHREC PROFILE(*) OBJTYPE(QUEUE) PRINCIPAL(PRINC01) AUTHADD(DSP) AUTHRMV(ALL)
```

Independentemente da ordem em que são fornecidos no comando, ALL são processados primeiro.

ULW Usando perfis genéricos do OAM no UNIX, Linux, and Windows

Use perfis genéricos do OAM para configurar, em uma única operação, os privilégios de um usuário para muitos objetos; em vez de ter que emitir comandos **setmqaut** separados ou comandos **SET AUTHREC** com relação a cada objeto individual quando ele for criado. Observe que no IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC** .

O uso de perfis genéricos nos comandos setmqaut ou SET AUTHREC permite configurar uma autoridade genérica para todos os objetos que se ajustarem a esse perfil.

Esta coleção de tópicos descreve o uso de perfis genéricos em mais detalhes.

Usando Caracteres Curinga em Perfis OAM

O que torna um perfil genérico é o uso de caracteres especiais (caracteres curinga) no nome do perfil. Por exemplo, o caractere curinga de ponto de interrogação (?) corresponde a qualquer caractere único em um nome. Portanto, se você especificar `ABC.?EF`, a autorização fornecida a esse perfil se aplicará a qualquer objeto com os nomes `ABC.DEF`, `ABC.CEF`, `ABC.BEF`, etc.

Os caracteres curinga disponíveis são:

?

Use o ponto de interrogação (?) em vez de qualquer caractere. Por exemplo, `AB.?D` aplica-se aos objetos `AB.CD`, `AB.ED` e `AB.FD`.

*****

Use o asterisco (*) como:

- Um *qualificador* em um nome de perfil para corresponder a qualquer qualificador em um nome de objeto. Um qualificador é a parte de um nome de objeto delimitado por um ponto. Por exemplo, em `ABC.DEF.GHI`, os qualificadores são `ABC`, `DEF` e `GHI`.

  Por exemplo, `ABC.*.JKL` aplica-se aos objetos `ABC.DEF.JKL` e `ABC.GHI.JKL`. (Observe que ele **não** se aplica ao `ABC.JKL`; * usado nesse contexto sempre indica um qualificador.)
- Um caractere dentro de um qualificador em um nome de perfil para corresponder a zero ou mais caracteres dentro do qualificador em um nome de objeto.

  Por exemplo, `ABC.DE*.JKL` aplica-se aos objetos `ABC.DE.JKL`, `ABC.DEF.JKL` e `ABC.DEGH.JKL`.

**

Use o asterisco duplo (**) **uma vez** em um nome de perfil como:

- O nome do perfil inteiro para corresponder a todos os nomes de objeto. Por exemplo, se você usar `-t prcs` para identificar processos, em seguida, usar ** como o nome do perfil, você mudará as autorizações para todos os processos.
- Como o qualificador inicial, do meio ou final em um nome de perfil para corresponder a zero ou mais qualificadores em um nome de objeto. Por exemplo, `**.ABC` identifica todos os objetos com o qualificador final ABC.

É possível usar apenas o asterisco duplo ** como um qualificador completo:

```
**.DEF
  ABC.**
  A*.**
```

mas não como

```
A**
```

caso contrário, você receberá a mensagem AMQ7226E: `O nome do perfil é inválido.`

Nota: Ao usar caracteres curinga em sistemas UNIX e Linux, você **deve** colocar o nome do perfil entre aspas simples.

Prioridades do Perfil

Um ponto importante a ser entendido ao usar perfis genéricos é a prioridade que os perfis recebem ao decidirem quais autoridades aplicar a um objeto que está sendo criado. Por exemplo, suponha que você emitiu estes comandos:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

O primeiro fornece autoridade put para todas as filas para o fred principal com nomes que correspondem ao perfil AB. *; O segundo fornece autoridade get para os mesmos tipos de fila que correspondem ao perfil AB.C*.

Suponha que agora você crie uma fila chamada AB.CD. De acordo com as regras para correspondência de curinga, setmqaut poderia ser aplicado a essa fila. Portanto, ele tem autoridade put ou get?

Para localizar a resposta, você aplica a regra que, sempre que vários perfis puderem se aplicar a um objeto, **apenas o mais específico será aplicado**. A maneira de aplicação dessa regra é comparando-se os nomes dos perfis da esquerda para a direita. Sempre que forem diferentes, um caractere não genérico será mais específico do que um genérico. Portanto, neste exemplo, o AB.CD da fila possui autoridade **get** (AB.C* é mais específico do que AB.*).

Ao comparar os caracteres genéricos, a ordem de *especificidade* é:

1. ?
2. *
3. **

Fazendo Dump de Configurações do Perfil

Para obter uma definição completa do comando de controle **dmpmqaut** e sua sintaxe, consulte dmpmqaut.

Para obter uma definição completa do comando MQSC **DISPLAY AUTHREC** e sua sintaxe, consulte DISPLAY AUTHREC.

Para obter uma definição completa do comando PCF **MQCMD_INQUIRE_AUTH_RECS** e sua sintaxe, consulte Consultar registros de autoridade.

Os seguintes exemplos mostram o uso do comando de controle **dmpmqaut** para fazer dump de registros de autoridade de perfis genéricos:

1. Este exemplo faz dump de todos os registros de autoridade com um perfil que corresponde à fila a.b.c do principal user1.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

   O dump resultante é semelhante a isto:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

   Nota: Embora os usuários do UNIX e Linux possam utilizar a opção `-p` para o comando **dmpmqaut**, eles deverão usar `-g groupname` em seu lugar ao definir autorizações.

2. Este exemplo faz dump de todos os registros de autoridade com um perfil que corresponde à fila a.b.c.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

   O dump resultante é semelhante a isto:

```
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. Este exemplo faz dump de todos os registros de autoridade para o perfil a.b. *, de fila do tipo

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

   O dump resultante é semelhante a isto:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

4. Este exemplo faz dump de todos os registros de autoridade para o gerenciador de filas qmX.

```
dmpmqaut -m qmX
```

   O dump resultante é semelhante a isto:

```
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. Este exemplo faz dump de todos os nomes de perfis e tipos de objetos para o gerenciador de filas qmX.

```
dmpmqaut -m qmX -l
```

   O dump resultante é semelhante a isto:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Nota: Somente para o IBM MQ for Windows, todos os principais exibidos incluem informações de domínio, por exemplo:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW *Usando caracteres curinga em perfis do OAM no UNIX, Linux, and Windows*

Use caracteres curinga em um nome de perfil do Object Authority Manager (OAM) para que esse perfil seja aplicável a mais de um objeto.

O que torna um perfil genérico é o uso de caracteres especiais (caracteres curinga) no nome do perfil. Por exemplo, o caractere curinga de ponto de interrogação (?) corresponde a qualquer caractere único em um nome. Portanto, se você especificar `ABC.?EF`, a autorização fornecida a esse perfil se aplicará a qualquer objeto com os nomes `ABC.DEF`, `ABC.CEF`, `ABC.BEF`, etc.

Os caracteres curinga disponíveis são:

?

Use o ponto de interrogação (?) em vez de qualquer caractere. Por exemplo, `AB.?D` aplica-se aos objetos `AB.CD`, `AB.ED` e `AB.FD`.

*****

Use o asterisco (*) como:

- Um *qualificador* em um nome de perfil para corresponder a qualquer qualificador em um nome de objeto. Um qualificador é a parte de um nome de objeto delimitado por um ponto. Por exemplo, em `ABC.DEF.GHI`, os qualificadores são `ABC`, `DEF` e `GHI`.

  Por exemplo, `ABC.*.JKL` aplica-se aos objetos `ABC.DEF.JKL` e `ABC.GHI.JKL`. (Observe que ele **não** se aplica ao `ABC.JKL`; * usado nesse contexto sempre indica um qualificador.)
- Um caractere dentro de um qualificador em um nome de perfil para corresponder a zero ou mais caracteres dentro do qualificador em um nome de objeto.

Por exemplo, ABC.DE*.JKL aplica-se aos objetos ABC.DE.JKL, ABC.DEF.JKL e ABC.DEGH.JKL.

**

Use o asterisco duplo (**) **uma vez** em um nome de perfil como:

- O nome do perfil inteiro para corresponder a todos os nomes de objeto. Por exemplo, se você usar `-t prcs` para identificar processos, em seguida, usar ** como o nome do perfil, você mudará as autorizações para todos os processos.
- Como o qualificador inicial, do meio ou final em um nome de perfil para corresponder a zero ou mais qualificadores em um nome de objeto. Por exemplo, **.ABC identifica todos os objetos com o qualificador final ABC.

Nota: Ao usar caracteres curinga em sistemas do UNIX and Linux, você **deve** colocar o nome do perfil entre aspas simples.

ULW *Prioridades de perfil no UNIX, Linux, and Windows*

Mais de um perfil genérico pode aplicar-se a um único objeto. Quando for esse o caso, a regra mais específica se aplicará.

Um ponto importante a ser entendido ao usar perfis genéricos é a prioridade que os perfis recebem ao decidirem quais autoridades aplicar a um objeto que está sendo criado. Por exemplo, suponha que você emitiu estes comandos:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

O primeiro fornece autoridade put para todas as filas para o fred principal com nomes que correspondem ao perfil AB. *; O segundo fornece autoridade get para os mesmos tipos de fila que correspondem ao perfil AB.C*.

Suponha que agora você crie uma fila chamada AB.CD. De acordo com as regras para correspondência de curinga, setmqaut poderia ser aplicado a essa fila. Portanto, ele tem autoridade put ou get?

Para localizar a resposta, você aplica a regra que, sempre que vários perfis puderem se aplicar a um objeto, **apenas o mais específico será aplicado**. A maneira de aplicação dessa regra é comparando-se os nomes dos perfis da esquerda para a direita. Sempre que forem diferentes, um caractere não genérico será mais específico do que um genérico. Portanto, neste exemplo, o AB.CD da fila possui autoridade **get** (AB.C* é mais específico do que AB.*).

Ao comparar os caracteres genéricos, a ordem de *especificidade* é:

1. ?
2. *
3. **

Consulte SET AUTHREC para as informações equivalentes ao usar este comando MQSC.

ULW *Fazendo dump das configurações de perfil no UNIX, Linux, and Windows*

Use o comando de controle **dmpmqaut** , o comando MQSC **DISPLAY AUTHREC** ou o comando PCF **MQCMD_INQUIRE_AUTH_RECS** para fazer dump das autorizações atuais associadas a um perfil especificado.. Observe que no IBM MQ Appliance é possível usar apenas o comando **DISPLAY AUTHREC** .

Para obter uma definição completa do comando de controle **dmpmqaut** e sua sintaxe, consulte dmpmqaut.

Para obter uma definição completa do comando MQSC **DISPLAY AUTHREC** e sua sintaxe, consulte DISPLAY AUTHREC.

Para obter uma definição completa do comando PCF **MQCMD_INQUIRE_AUTH_RECS** e sua sintaxe, consulte Consultar registros de autoridade.

Os seguintes exemplos mostram o uso do comando de controle **dmpmqaut** para fazer dump de registros de autoridade de perfis genéricos:

1. Este exemplo faz dump de todos os registros de autoridade com um perfil que corresponde à fila a.b.c do principal user1.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

   O dump resultante é semelhante a este exemplo:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

   Nota: Usuários do UNIX and Linux não podem usar a opção `-p`; eles devem usar `-g groupname`.

2. Este exemplo faz dump de todos os registros de autoridade com um perfil que corresponde à fila a.b.c.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

   O dump resultante é semelhante a este exemplo:

```
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. Este exemplo faz dump de todos os registros de autoridade para o perfil a.b. *, de fila do tipo

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

   O dump resultante é semelhante a este exemplo:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

4. Este exemplo faz dump de todos os registros de autoridade para o gerenciador de filas qmX.

```
dmpmqaut -m qmX
```

   O dump resultante é semelhante a este exemplo:

```
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. Este exemplo faz dump de todos os nomes de perfis e tipos de objetos para o gerenciador de filas qmX.

```
dmpmqaut -m qmX -l
```

   O dump resultante é semelhante a este exemplo:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Nota: Somente para o IBM MQ for Windows, todos os principais exibidos incluem informações de domínio, por exemplo:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

ULW Exibindo configurações de acesso no UNIX, Linux, and Windows

Use o comando de controle **dspmqaut** , o comando MQSC **DISPLAY AUTHREC** ou o comando PCF **MQCMD_INQUIRE_ENTITY_AUTH** para visualizar as autorizações que um proprietário ou grupo específico possui para um objeto específico Observe que no IBM MQ Appliance, é possível usar somente o comando **DISPLAY AUTHREC**.

O gerenciador de filas deve estar em execução para usar esse comando. Ao mudar o acesso de um diretor, as mudanças são refletidas imediatamente pelo OAM. A autorização pode ser exibida para apenas um grupo ou diretor de cada vez.

Para obter uma definição completa do comando de controle **dmpmqaut** e sua sintaxe, consulte dmpmqaut.

Para obter uma definição completa do comando MQSC **DISPLAY AUTHREC** e sua sintaxe, consulte DISPLAY AUTHREC.

Para obter uma definição completa do comando PCF **MQCMD_INQUIRE_AUTH_RECS** e sua sintaxe, consulte Consultar registros de autoridade.

O exemplo a seguir mostra o uso do comando de controle **dspmqaut** para exibir as autorizações que o grupo `GpAdmin` tem para uma definição de processo chamada `Annuities` que está no gerenciador de filas `QueueMan1`

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

ULW Mudando e revogando o acesso a um objeto do IBM MQ no UNIX, Linux, and Windows

Para mudar o nível de acesso que um usuário ou grupo tem para um objeto, use o comando de controle **setmqaut**, o comando MQSC **DELETE AUTHREC** ou o comando PCF **MQCMD_DELETE_AUTH_REC**.

MQ Appliance Observe que no IBM MQ Appliance é possível usar apenas o comando **DELETE AUTHREC** .

O processo de remover o usuário de um grupo é descrito em:

- Windows "Criando e gerenciando grupos no Windows" na página 146
- AIX "Criando e gerenciando grupos no AIX" na página 144
- Solaris "Criando e gerenciando grupos no Solaris" na página 145
- Linux "Criando e gerenciando grupos no Linux" na página 144

.

O ID do usuário que cria um objeto do IBM MQ é concedido autoridades de controle totais para esse objeto. Se você remover este ID do usuário do grupo mqm local (ou o grupo Administradores em sistemas Windows) essas autoridades não serão revogadas. Use o comando de controle **setmqaut** ou o comando PCF **MQCMD_DELETE_AUTH_REC** para revogar o acesso a um objeto para o ID do usuário que o criou, depois de removê-lo do grupo mqm ou do grupo de Administradores.

Para obter uma definição completa do comando de controle setmqaut e sua sintaxe, consulte setmqaut.

Para obter uma definição completa do comando MQSC **DELETE AUTHREC** e sua sintaxe, consulte DELETE AUTHREC.

Para obter uma definição completa do comando PCF **MQCMD_DELETE_AUTH_REC** e sua sintaxe, consulte Excluir registro de autoridade.

Windows No Windows, a partir do IBM MQ 8.0, é possível excluir as entradas OAM correspondentes a uma conta do usuário específica do Windows a qualquer momento usando o parâmetro **-u** *SID* do **setmqaut**.

Antes do IBM MQ 8.0, você teve de excluir as entradas OAM correspondentes a uma conta de usuário específica do Windows antes de excluir o perfil do usuário. Foi impossível remover as entradas OAM após remover a conta do usuário.

ULW Evitando verificações de acesso de segurança nos sistemas UNIX, Linux, and Windows

Para desligar toda verificação de segurança, é possível desativar o gerenciador de autoridade de objeto (OAM). Isso pode ser adequado para um ambiente de teste. Depois de desativar ou remover o OAM, não é possível incluir um OAM em um gerenciador de filas existente.

Se você decidir que não deseja executar verificações de segurança (por exemplo, em um ambiente de teste), poderá desativar o OAM em uma de duas maneiras:

- Antes de criar um gerenciador de filas, configure a variável de ambiente do sistema operacional MQSNOAUT.

  Consulte Descrições de variáveis de ambiente para obter informações sobre as implicações da configuração da variável MQSNOAUT e como configurar MQSNOAUT em Windows e UNIX.
- Edite o arquivo de configuração do gerenciador de filas para remover o serviço.

Se você usar o comando **setmqaut** ou **dspmqaut** enquanto o OAM estiver desativado, observe os pontos a seguir:

- O OAM não valida o diretor ou o grupo especificado, isto é, o comando pode aceitar valores inválidos.

- O OAM não executa verificações de segurança e indica que todos os principais e grupos têm autorização para executar todas as operações de objeto aplicáveis.

Aviso: Quando um OAM é removido, ele não pode ser colocado de volta em um gerenciador de filas existente. Isso ocorre porque o OAM precisa estar ativo no horário de criação do objeto. Para usar o IBM MQ OAM novamente depois que ele foi removido, reconstrua o gerenciador de filas.

Conceitos relacionados

Serviços e componentes instaláveis para UNIX, Linux e Windows

Tarefas relacionadas

Configurando serviços instaláveis

Referências relacionadas

Informações de referência de serviços instaláveis

Concedendo acesso necessário para recursos

Use este tópico para determinar quais tarefas executar para aplicar segurança em seu sistema IBM MQ no UNIX, no Linux, no Windows, no IBM i e no z/OS.

Sobre esta tarefa

Durante esta tarefa, você decide quais ações são necessárias para aplicar o nível apropriado de segurança para os elementos de sua instalação do IBM MQ. Cada tarefa individual para a qual você é encaminhado fornece instruções passo a passo para todas as plataformas.

Procedimento

1. Você precisa limitar o acesso ao gerenciador de filas para determinados usuários?
   a) Não: não executar ação adicional.
   b) Sim: Acesse a próxima pergunta.
2. Esses usuários precisam de acesso administrativo parcial em um subconjunto de recursos de gerenciadores de filas?
   a) Não: Acesse a próxima pergunta.
   b) Sim: Consulte “Concedendo Acesso Administrativo Parcial em um Subconjunto de Recursos do Gerenciador de Filas” na página 367.
3. Esses usuários precisam de acesso administrativo total em um subconjunto de recursos de gerenciadores de filas?
   a) Não: Acesse a próxima pergunta.
   b) Sim: Consulte “Concedendo Acesso Administrativo Total em um Subconjunto de Recursos do Gerenciador de Filas” na página 376.
4. Esses usuários precisam de acesso somente leitura a todos os recursos de gerenciadores de filas?
   a) Não: Acesse a próxima pergunta.
   b) Sim: Consulte “Concedendo Acesso somente Leitura a todos os Recursos em um Gerenciador de Filas” na página 383.
5. Esses usuários precisam de acesso administrativo total em todos recursos de gerenciadores de filas?
   a) Não: Acesse a próxima pergunta.
   b) Sim: Consulte “Concedendo Acesso Administrativo Total a todos os Recursos em um Gerenciador de Filas” na página 385.
6. Você precisa que os aplicativos de usuários se conectem ao gerenciador de filas?
   a) Não: Desative a conectividade, conforme descrito em “Removendo a Conectividade com o Gerenciador de Filas” na página 386
   b) Sim: Consulte “Permitindo que Aplicativos de Usuário se Conectem ao Gerenciador de Filas” na página 387.

Multi z/OS Concedendo Acesso Administrativo Parcial em um Subconjunto de Recursos do Gerenciador de Filas

É necessário fornecer a determinados usuários acesso administrativo parcial a alguns recursos do gerenciador de filas, mas não a todos. Use esta tabela para determinar as ações que precisam ser executadas.

Tabela 69. Concedendo acesso administrativo parcial para um subconjunto de recursos do gerenciador de filas

Os usuários precisam administrar objetos deste tipo	**Executar esta ação**
Filas	Conceda acesso administrativo parcial às filas necessárias, conforme descrito em "Concedendo Acesso Administrativo Limitado a algumas Filas" na página 367
tópicos	Conceda acesso administrativo parcial aos tópicos necessários, conforme descrito em "Concedendo Acesso Administrativo Limitado a alguns Tópicos" na página 369
Canais	Conceda acesso administrativo parcial aos canais necessários, conforme descrito em "Concedendo Acesso Administrativo Limitado a alguns Canais" na página 370
O gerenciador de filas	Conceda acesso administrativo parcial ao gerenciador de filas, conforme descrito em "Concedendo Acesso Administrativo Limitado a um Gerenciador de Filas" na página 371
Processos	Conceda acesso administrativo parcial aos processos necessários, conforme descrito em "Concedendo Acesso Administrativo Limitado a alguns Processos" na página 372
Listas de Nomes	Conceda acesso administrativo parcial às listas de nomes necessárias, conforme descrito em "Concedendo Acesso Administrativo Limitado a algumas Listas de Nomes" na página 374
Serviços	Conceda acesso administrativo parcial aos serviços necessários, conforme descrito em "Concedendo Acesso Administrativo Limitado a alguns Serviços" na página 375

Concedendo Acesso Administrativo Limitado a algumas Filas

Conceda acesso administrativo parcial a algumas filas em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a algumas filas para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux

- UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
  ```

- IBM i
  Para o IBM i, emita o comando a seguir:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS Para o z/OS, emita os comandos a seguir para conceder acesso a uma fila especificada:

  ```
  RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
  PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Para especificar quais comandos MQSC o usuário pode executar na fila, emita os comandos a seguir para cada comando MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction. QType UACC(NONE)
  PERMIT QMgrName. ReqdAction. QType CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Para permitir que o usuário use o comando DISPLAY QUEUE, emita os seguintes comandos:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY. QType UACC(NONE)
  PERMIT QMgrName.DISPLAY. QType CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

  ReqdAction
  A ação que você está permitindo que o grupo execute:

  – ULW Nos sistemas UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +dlt, +dsp. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.

  – IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMDLT, *ADMDSP. A autorização *ALLADM é equivalente a todas essas autorizações individuais.

  – z/OS No z/OS, um dos valores ALTER, CLEAR, DELETE ou MOVE.

Nota: Conceder +crt para filas torna indiretamente o usuário ou o grupo um administrador. Não use a autoridade +crt para conceder acesso administrativo limitado a algumas filas.

QType

Para o comando DISPLAY, um dos valores QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE ou QCLUSTER.

Para outros valores de *ReqdAction*, um dos valores QLOCAL, QALIAS, QMODEL ou QREMOTE.

Concedendo Acesso Administrativo Limitado a alguns Tópicos

Conceda acesso administrativo parcial a alguns tópicos em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a alguns tópicos para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW

  Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
  ```

- IBM i

  Para o IBM i, emita o comando a seguir:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS Para z/OS, emita os seguintes comandos:

  ```
  RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
  PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Esses comandos concedem acesso ao tópico especificado. Para determinar quais comandos MQSC o usuário pode executar no tópico, emita os seguintes comandos para cada comando MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.TOPIC UACC(NONE)
  PERMIT QMgrName. ReqdAction.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Para permitir que o usuário use o comando DISPLAY TOPIC, emita os seguintes comandos:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.TOPIC UACC(NONE)
  PERMIT QMgrName.DISPLAY.TOPIC CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

ReqdAction
A ação que você está permitindo que o grupo execute:

- ULW Em sistemas UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +dsp. +ctrl. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.
- IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL. A autorização *ALLADM é equivalente a todas essas autorizações individuais.
- z/OS No z/OS, um dos valores ALTER, CLEAR, DEFINE, DELETE ou MOVE.

Concedendo Acesso Administrativo Limitado a alguns Canais

Conceda acesso administrativo parcial a alguns canais em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a alguns canais para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- IBM i
  No IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS No z/OS:

```
RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Esses comandos concedem acesso ao canal especificado. Para determinar quais comandos MQSC o usuário pode executar no canal, emita os seguintes comandos para cada comando MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.CHANNEL UACC(NONE)
PERMIT QMgrName. ReqdAction.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Para permitir que o usuário use o comando DISPLAY CHANNEL, emita os seguintes comandos:

```
RDEFINE MQCMDS QMgrName.DISPLAY.CHANNEL UACC(NONE)
PERMIT QMgrName.DISPLAY.CHANNEL CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

ReqdAction
A ação que você está permitindo que o grupo execute:

- ULW No UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +dsp. +ctrl, +ctrlx. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.
- IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. A autorização *ALLADM é equivalente a todas essas autorizações individuais.
- z/OS No z/OS, um dos valores ALTER, CLEAR, DEFINE, DELETE ou MOVE.

Concedendo Acesso Administrativo Limitado a um Gerenciador de Filas

Conceda acesso administrativo parcial a um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado para executar algumas ações no gerenciador de filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW

  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
  ```

- IBM i

  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS

  No z/OS:

  Para determinar quais comandos MQSC você pode executar no gerenciador de filas, emita os comandos a seguir para cada comando MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.QMGR UACC(NONE)
  PERMIT QMgrName. ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Para permitir que o usuário use o comando DISPLAY QMGR, emita os seguintes comandos:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
  PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

  ReqdAction
  A ação que você está permitindo que o grupo execute:

  – ULW No UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +dsp. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.

    Embora +set seja uma autorização do MQI e não considerada administrativa normalmente, conceder +set no gerenciador de filas pode levar indiretamente à autoridade administrativa total. Não conceda +set a usuários e aplicativos ordinários.

  – IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. A autorização *ALLADM é equivalente a todas essas autorizações individuais.

Concedendo Acesso Administrativo Limitado a alguns Processos

Conceda acesso administrativo parcial a alguns processos em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a alguns processos para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- IBM i

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW

  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
  ```

- IBM i

  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.PROCESS. ObjectProfile UACC(NONE)
  PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Esses comandos concedem acesso ao canal especificado. Para determinar quais comandos MQSC o usuário pode executar no canal, emita os seguintes comandos para cada comando MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.PROCESS UACC(NONE)
  PERMIT QMgrName. ReqdAction.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Para permitir que o usuário use o comando DISPLAY PROCESS, emita os seguintes comandos:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.PROCESS UACC(NONE)
  PERMIT QMgrName.DISPLAY.PROCESS CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

  ReqdAction
  A ação que você está permitindo que o grupo execute:

  – ULW No UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +dsp. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.

– IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP. A autorização *ALLADM é equivalente a todas essas autorizações individuais.

– z/OS No z/OS, um dos valores ALTER, CLEAR, DEFINE, DELETE ou MOVE.

Concedendo Acesso Administrativo Limitado a algumas Listas de Nomes

Conceda acesso administrativo parcial a algumas listas de nomes em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a algumas listas de nomes para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
  ```

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(ReqdAction) MQMNAME('
  QMgrName ')
  ```

- z/OS No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
  PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Esses comandos concedem acesso à lista de nomes especificada. Para determinar quais comandos MQSC o usuário pode executar na lista de nomes, emita os seguintes comandos para cada comando MQSC:

  ```
  RDEFINE MQCMDS QMgrName. ReqdAction.NAMELIST UACC(NONE)
  PERMIT QMgrName. ReqdAction.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
  ```

  Para permitir que o usuário use o comando DISPLAY NAMELIST, emita os seguintes comandos:

  ```
  RDEFINE MQCMDS QMgrName.DISPLAY.NAMELIST UACC(NONE)
  PERMIT QMgrName.DISPLAY.NAMELIST CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
  ```

  Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

ReqdAction
A ação que você está permitindo que o grupo execute:

- ULW No UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +ctrl, +ctrlx, +dsp. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.
- IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. A autorização *ALLADM é equivalente a todas essas autorizações individuais.
- z/OS No z/OS, um dos valores ALTER, CLEAR, DEFINE, DELETE ou MOVE.

Concedendo Acesso Administrativo Limitado a alguns Serviços

Conceda acesso administrativo parcial a alguns serviços em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo limitado a alguns serviços para algumas ações, use os comandos apropriados de seu sistema operacional. z/OS Note que os objetos de serviço não existem no z/OS.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- No IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction) MQMNAME('
QMgrName ')
```

- z/OS No z/OS:

Esses comandos concedem acesso ao serviço especificado. Para determinar quais comandos MQSC o usuário pode executar no serviço, emita os seguintes comandos para cada comando MQSC:

```
RDEFINE MQCMDS QMgrName. ReqdAction.SERVICE UACC(NONE)
PERMIT QMgrName. ReqdAction.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Para permitir que o usuário use o comando DISPLAY SERVICE, emita os seguintes comandos:

```
RDEFINE MQCMDS QMgrName.DISPLAY.SERVICE UACC(NONE)
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

ReqdAction
A ação que você está permitindo que o grupo execute:

- ULW Nos sistemas UNIX, Linux, and Windows, qualquer combinação das autorizações a seguir: +chg, +clr, +crt, +dlt, +ctrl, +ctrlx, +dsp. A autorização +alladm é equivalente a +chg +clr +dlt +dsp.
- IBM i No IBM i, qualquer combinação das autorizações a seguir: *ADMCHG, *ADMCLR, *ADMCRT, *ADMDLT, *ADMDSP, *CTRL, *CTRLX. A autorização *ALLADM é equivalente a todas essas autorizações individuais.

Concedendo Acesso Administrativo Total em um Subconjunto de Recursos do Gerenciador de Filas

É necessário fornecer a determinados usuários acesso administrativo total a alguns recursos do gerenciador de filas, mas não a todos. Use estas tabelas para determinar as ações que precisam ser executadas.

Tabela 70. Concedendo acesso administrativo completo para um subconjunto de recursos do gerenciador de filas

Os usuários precisam administrar objetos deste tipo	**Executar esta ação**
Filas	Conceda acesso administrativo total às filas necessárias, conforme descrito em “Concedendo Acesso Administrativo Total a algumas Filas” na página 377
tópicos	Conceda acesso administrativo total aos tópicos necessários, conforme descrito em “Concedendo Acesso Administrativo Total a alguns Tópicos” na página 378
Canais	Conceda acesso administrativo total aos canais necessários, conforme descrito em “Concedendo Acesso Administrativo Total a alguns Canais” na página 379

Tabela 70. Concedendo acesso administrativo completo para um subconjunto de recursos do gerenciador de filas (continuação)	
Os usuários precisam administrar objetos deste tipo	**Executar esta ação**
O gerenciador de filas	Conceda acesso administrativo total ao gerenciador de filas, conforme descrito em “Concedendo Acesso Administrativo Total a um Gerenciador de Filas” na página 380
Processos	Conceda acesso administrativo total aos processos necessários, conforme descrito em “Concedendo Acesso Administrativo Total a alguns Processos” na página 380
Listas de Nomes	Conceda acesso administrativo total às listas de nomes necessárias, conforme descrito em “Concedendo Acesso Administrativo Total a algumas Listas de Nomes” na página 381
Serviços	Conceda acesso administrativo total aos serviços necessários, conforme descrito em “Concedendo Acesso Administrativo Total a alguns Serviços” na página 382

Concedendo Acesso Administrativo Total a algumas Filas

Conceda acesso administrativo total a algumas filas em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a algumas filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
  ```

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME(' QMgrName
  ')
  ```

- z/OS
  No z/OS:

```
RDEFINE MQADMIN QMgrName.QUEUE. ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a alguns Tópicos

Conceda acesso administrativo total a alguns tópicos em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a alguns tópicos para algumas ações, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- IBM i
  No IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  No z/OS:

```
RDEFINE MQADMIN QMgrName.TOPIC. ObjectProfile UACC(NONE)
PERMIT QMgrName.TOPIC. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a alguns Canais

Conceda acesso administrativo total a alguns canais em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a alguns canais, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
  ```

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS
  No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
  PERMIT QMgrName.CHANNEL. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a um Gerenciador de Filas

Conceda acesso administrativo total a um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total ao gerenciador de filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -t qmgr -g GroupName +alladm
  ```

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS
  No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
  PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a alguns Processos

Conceda acesso administrativo total a alguns processos em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a alguns processos, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
  ```

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS
  No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.CHANNEL. ObjectProfile UACC(NONE)
  PERMIT QMgrName.PROCESS. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a algumas Listas de Nomes

Conceda acesso administrativo total a algumas listas de nomes em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a algumas listas de nomes, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i

- Linux
- UNIX
- Windows

Nota: No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW

  No UNIX, Linux, and Windows:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
  ```

- IBM i

  No IBM i:

  ```
  GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM) MQMNAME('
  QMgrName ')
  ```

- z/OS

  No z/OS:

  ```
  RDEFINE MQADMIN QMgrName.NAMELIST. ObjectProfile UACC(NONE)
  PERMIT QMgrName.NAMELIST. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a alguns Serviços

Conceda acesso administrativo total a alguns serviços em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder acesso administrativo total a alguns serviços, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- Windows

Nota: No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- IBM i
  No IBM i:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('
QMgrName ')
```

- z/OS
  No z/OS:

```
RDEFINE MQADMIN QMgrName.SERVICE. ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE. ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo Acesso somente Leitura a todos os Recursos em um Gerenciador de Filas

Conceda acesso somente leitura a todos os recursos em um gerenciador de filas, a cada usuário ou grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Use o assistente Incluir autoridades baseadas na função ou os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Depois de mudar quaisquer detalhes de autorização, execute uma atualização de segurança usando o comando REFRESH SECURITY.

Procedimento

- Usando o assistente:

a) Na área de janela do Navegador IBM MQ Explorer , clique com o botão direito do mouse no gerenciador de filas e clique em **Autoridades de Objetos** > **Incluir Autoridades Baseadas em Função**

   O assistente Incluir Autoridades Baseadas na Função é aberto.

- Windows UNIX

  Para sistemas UNIX e Windows, emita os comandos a seguir:

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
+put
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +inq
setmqaut -m QMgrName -n ** -t clntconn -g GroupName +dsp
setmqaut -m QMgrName -n ** -t authinfo -g GroupName +dsp
setmqaut -m QMgrName -n ** -t listener -g GroupName +dsp
setmqaut -m QMgrName -n ** -t namelist -g GroupName +dsp
setmqaut -m QMgrName -n ** -t process -g GroupName +dsp
setmqaut -m QMgrName -n ** -t service -g GroupName +dsp
setmqaut -m QMgrName -t qmgr -g GroupName +dsp +inq +connect
```

  As autoridades específicas para o SYSTEM.ADMIN.COMMAND.QUEUE e SYSTEM.MQEXPLORER.REPLY.MODEL são necessários apenas se você desejar utilizar o IBM MQ Explorer

- IBM i

  Para IBM i, emita os seguintes comandos:

```
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

  Para z/OS, emita os seguintes comandos:

```
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)
```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName

  O nome do gerenciador de filas.

  z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

GroupName
O nome do grupo que receberá acesso.

Concedendo Acesso Administrativo Total a todos os Recursos em um Gerenciador de Filas

Conceda acesso administrativo total a todos os recursos em um gerenciador de filas, a cada usuário ou grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

É possível usar o assistente Incluir autoridades baseadas em função ou os comandos apropriados para seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Notes: ULW

1. Se você estiver usando o **runmqsc** para administrar o gerenciador de fila em vez do IBM MQ Explorer, deverá conceder autoridade para consultar, obter e procurar o SYSTEM.MQSC.REPLY.QUEUE, e você não precisa conceder nenhuma autoridade no SYSTEM.MQEXPLORER.REPLY.MODEL fila.
2. Ao conceder a um usuário acesso a todos os recursos em um gerenciador de filas, há alguns comandos que o usuário não pode executar, a menos que esse usuário tenha acesso de leitura ao arquivo `qm.ini`. Isso ocorre devido a restrições sobre os usuários não `mqm` poderem ler o arquivo `qm.ini`.

   O usuário não pode emitir os comandos a seguir, a menos que você tenha concedido a esse usuário acesso de leitura ao arquivo qm.ini:

   - Definindo um canal configurado para usar TLS
   - Definindo um canal usando variáveis de inserção de configuração automática definidas no `qm.ini`

Procedimento

- Se você estiver usando o assistente, na área de janela do IBM MQ Explorer Navigator, clique com o botão direito no Gerenciador de Filas e clique em **Autoridades do objeto** > **Incluir autoridades baseadas em função**.

  O assistente Incluir Autoridades Baseadas na Função é aberto.

- Linux UNIX

  Para sistemas UNIX and Linux, emita os comandos a seguir:

```
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
```

Consulte **setmqaut** para obter mais informações sobre `@class`

- Windows

Para sistemas Windows, emita os mesmos comandos para sistemas UNIX and Linux, mas usando o nome do perfil @CLASS em vez de @class.

- IBM i

Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER(' GroupName ') AUT(*ALLADM) MQMNAME(' QMgrName ')
```

- z/OS

Para z/OS, emita os seguintes comandos:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

GroupName
O nome do grupo que receberá acesso.

Removendo a Conectividade com o Gerenciador de Filas

Para que aplicativos de usuário não se conectem ao gerenciador de filas, remova sua autoridade de conexão com ele.

Sobre esta tarefa

Revogue a autoridade de todos os usuários de conexão com o gerenciador de filas usando o comando apropriado de seu sistema operacional.

Em sistemas UNIX, Linux, Windows e IBM i, também é possível usar o comando DELETE AUTHREC.

Nota: No IBM MQ Appliance é possível usar somente o comando **DELETE AUTHREC**.

Procedimento

- ULW

Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- IBM i

Para o IBM i, emita o comando a seguir:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- z/OS

Para z/OS, emita os seguintes comandos:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

Não emita comandos PERMIT.

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas.

z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

GroupName
O nome do grupo cujo acesso será negado.

Permitindo que Aplicativos de Usuário se Conectem ao Gerenciador de Filas

Você deseja permitir que o aplicativo de usuário se conecte ao gerenciador de filas. Use as tabelas deste tópico para determinar quais ações executar.

Primeiro, determine se os aplicativos clientes se conectarão ao seu Gerenciador de Filas.

Se nenhum dos aplicativos que irão se conectar ao gerenciador de filas for aplicativo cliente, desative o acesso remoto, conforme descrito em "Desativando o Acesso Remoto ao Gerenciador de Filas" na página 395.

Se um ou mais dos aplicativos que irão se conectar ao gerenciador de filas forem aplicativos clientes, proteja a conectividade remota, conforme descrito em "Protegendo a Conectividade Remota no Gerenciador de Filas" na página 387.

Em ambos os casos, configure a segurança de conexão, conforme descrito em "Configurando a Segurança de Conexão" na página 395

Para controlar o acesso a recursos de cada usuário que se conectar ao gerenciador de filas, consulte a tabela a seguir. Se a instrução na primeira coluna for verdadeira, execute a ação listada na segunda coluna.

Declaração	Execute esta ação
Você tem aplicativos que usam filas	Consulte "Controlando o Acesso de Usuário a Filas" na página 396
Você tem aplicativos que usam tópicos	Consulte o "Controlando o Acesso de Usuário aos Tópicos" na página 402.
Você tem aplicativos que consultam o objeto de gerenciador de filas	Consulte o "Concedendo autoridade para consultar em um gerenciador de filas" na página 404.
Você tem aplicativos que usam objetos de processos	Consulte "Concedendo autoridade para acessar processos" na página 405
Você tem aplicativos que usam listas de nomes	Consulte "Concedendo autoridade para acessar listas de nomes" na página 406

Protegendo a Conectividade Remota no Gerenciador de Filas

É possível assegurar a conectividade remota com o gerenciador de filas usando TLS, uma saída de segurança, registros de autenticação de canal ou uma combinação desses métodos.

Sobre esta tarefa

Você conecta um cliente ao gerenciador de filas usando um canal de conexão do cliente na estação de trabalho do cliente e um canal de conexão do servidor no servidor. Proteja essas conexões de uma das seguintes maneiras.

Procedimento

1. Usando TLS com registros de autenticação de canal:
   a) Evite que qualquer nome distinto (DN) abra um canal, usando um registro de autenticação de canal SSLPEERMAP para mapear todos os DNs para USERSRC(NOACCESS).
   b) Permita que DNs específicos ou conjuntos de DNs abram um canal, usando um registro de autenticação de canal SSLPEERMAP para mapeá-los para USERSRC(CHANNEL).
2. Usando TLS com uma saída de segurança:
   a) Configure MCAUSER no canal de conexão do servidor para um identificador de usuários sem privilégios.
   b) Grave uma saída de segurança para designar um valor MCAUSER, dependendo do valor do DN TLS que ele recebe nos campos SSLPeerNamePtr e SSLPeerNameLength passados para a saída na estrutura MQCD.
3. Usando TLS com valores de definição de canal fixos:
   a) Configure SSLPEER no canal de conexão do servidor para um valor específico ou limite o intervalo de valores.
   b) Configure MCAUSER no canal de conexão do servidor para o ID do usuário com o qual o canal deve ser executado.
4. Usando registros de autenticação de canal em canais que não usam TLS:
   a) Evite que qualquer endereço IP abra canais, usando um registro de autenticação de canal de mapeamento de endereço com ADDRESS(*) e USERSRC(NOACCESS).
   b) Permita que endereços IP específicos abram canais, usando registros de autenticação de canal de mapeamento de endereço para esses endereços com USERSRC(CHANNEL).
5. Usando uma saída de segurança:
   a) Grave uma saída de segurança para autorizar conexões com base em qualquer propriedade escolhida, por exemplo, o endereço IP de origem.
6. Também é possível usar registros de autenticação de canal com uma saída de segurança ou usar todos os três métodos, se suas circunstâncias específicas exigirem.

Bloqueando Endereços IP Específicos
É possível evitar que um canal específico aceite uma conexão de entrada de um endereço IP, ou evitar que o gerenciador de filas inteiro permita o acesso a partir de um endereço IP, usando um registro de autenticação de canal.

Antes de começar

Ative registros de autenticação de canal executando o comando a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Sobre esta tarefa

Para desaprovar canais específicos para aceitação de uma conexão de entrada e assegurar que conexões sejam aceitas apenas ao usar o nome de canal correto, um tipo de regra pode ser usado para bloquear endereços IP. Para desaprovar um endereço IP a acessar o gerenciador de fias inteiro, você normalmente usaria um firewall para bloqueá-lo permanentemente. Entretanto, um outro tipo de regra pode ser usado para permitir que você bloqueie alguns endereços temporariamente, por exemplo, enquanto você estiver aguardando pela atualização do firewall.

Procedimento

- Para bloquear endereços IP do uso de um canal específico, configure um registro de autenticação de canal usando o comando MQSC **SET CHLAUTH**, ou o comando PCF **Set Channel Authentication Record**.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

Existem três partes para o comando:

SET CHLAUTH (*generic-channel-name*)
Use esta parte do comando para controlar se você deseja bloquear uma conexão para o gerenciador de filas inteiro, canal único ou intervalo de canais. O que você colocou aqui determina quais áreas estão cobertas.

Por exemplo:

- SET CHLAUTH('*') - bloqueia todos os canais em um gerenciador de filas, ou seja, todo o gerenciador de filas
- SET CHLAUTH('SYSTEM.*') - bloqueia todos os canais iniciados com SYSTEM.
- SET CHLAUTH('SYSTEM.DEF.SVRCONN') - bloqueia o canal SYSTEM.DEF.SVRCONN

Tipo de regra CHLAUTH
Use esta parte do comando para especificar o tipo de comando e determinar se você deseja fornecer um único endereço ou uma lista de endereços.

Por exemplo:

- TYPE(ADDRESSMAP) - use ADDRESSMAP se você deseja fornecer um único endereço ou um endereço curinga. Por exemplo, ADDRESS('192.168.*') bloqueia quaisquer conexões provenientes de um endereço IP com início no 192.168.

  Para obter mais informações sobre como filtrar endereços IP com padrões, consulte Endereços IP genéricos.
- TYPE(BLOCKADDR) - Use BLOCKADDR se você deseja fornecer uma lista de endereços para o bloqueio.

Parâmetros Adicionais
Esses parâmetros são dependentes do tipo de regra usada na segunda parte do comando:

- Para TYPE(ADDRESSMAP), use o ADDRESS
- Para TYPE(BLOCKADDR), use o ADDRLIST

Referências relacionadas
SET CHLAUTH

Bloqueando temporariamente endereços IP específicos se o gerenciador de filas não estiver em execução
Você pode desejar bloquear determinados endereços IP ou intervalos de endereços, quando o gerenciador de filas não estiver em execução e não é possível, portanto, emitir comandos MQSC. É possível bloquear temporariamente os endereços IP em uma base excepcional modificando o arquivo `blockaddr.ini`.

Sobre esta tarefa

O arquivo `blockaddr.ini` contém uma cópia das definições de BLOCKADDR que são usadas pelo Gerenciador de Filas. Esse arquivo é lido pelo listener se o listener é iniciado antes do gerenciador de filas. Nessas circunstâncias, o listener utiliza quaisquer valores que você tenha incluído manualmente no arquivo `blockaddr.ini`

No entanto, esteja ciente de que quando o Gerenciador de Filas é iniciado, ele grava o conjunto de definições de BLOCKADDR no arquivo `blockaddr.ini`, substituindo qualquer edição manual que você possa ter feito. Da mesma forma, sempre que você incluir ou excluir uma definição de BLOCKADDR usando o comando **SET CHLAUTH**, o arquivo `blockaddr.ini` é atualizado. É possível, portanto, tornar as mudanças permanentes para as definições de BLOCKADDR somente usando o comando **SET CHLAUTH** quando o gerenciador de filas estiver em execução.

Procedimento

1. Abra o arquivo `blockaddr.ini` em um editor de texto.
   O arquivo está localizado no diretório de dados do gerenciador de filas.
2. Inclua endereços IP como pares de valor de palavra-chave simples, em que a palavra-chave é `Addr`.
   Para obter informações sobre filtrar endereços IP com padrões, consulte Endereços IP genéricos.
   Por exemplo:

```
Addr = 192.0.2.0
Addr = 192.0.*
Addr = 192.0.2.1-8
```

Tarefas relacionadas

"Bloqueando Endereços IP Específicos" na página 388
É possível evitar que um canal específico aceite uma conexão de entrada de um endereço IP, ou evitar que o gerenciador de filas inteiro permita o acesso a partir de um endereço IP, usando um registro de autenticação de canal.

Referências relacionadas

SET CHLAUTH

Bloqueando IDs de Usuários Específicos
É possível evitar que usuários específicos usem um canal especificando IDs de usuários que, se declarados, fazem com que o canal termine. Faça isso configurando um registro de autenticação de canal de canal.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
A lista de usuários fornecida em um TYPE(BLOCKUSER) se aplica somente a canais SVRCONN e não a canais de gerenciador de filas para gerenciador de filas.
userID1 e *userID2* são cada um o ID de um usuário que deve ser evitado de usar o canal. Também é possível especificar o valor especial `*MQADMIN` para fazer referência a usuários administrativos privilegiados. Para obter informações adicionais sobre usuários privilegiados, consulte "Usuários Privilegiados" na página 336. Para obter informações adicionais sobre `*MQADMIN`, consulte SET CHLAUTH.

Referências relacionadas

SET CHLAUTH

Mapeando um Gerenciador de Filas Remoto para um ID do Usuário MCAUSER
É possível usar um registro de autenticação de canal para configurar o atributo MCAUSER de um canal de acordo com o gerenciador de filas a partir do qual o canal está conectando.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Sobre esta tarefa

Como opção, é possível restringir os endereços IP aos quais a regra se aplica.

Observe que essa técnica não se aplica a canais de conexão do servidor. Se você especificar o nome de um canal de conexão do servidor nos comandos a seguir, isso não tem efeito.

Procedimento

- Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

  ```
  SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user)
  ```

  generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
  generic-partner-qmgr-name é o nome do gerenciador de filas ou um padrão que inclui o símbolo de asterisco (*) como um curinga que corresponde ao nome do gerenciador de filas.
  user é o ID do usuário a ser usado para todas as conexões do gerenciador de filas especificado.
- Para restringir esse comando a determinados endereços IP, inclua o parâmetro **ADDRESS** da seguinte forma:

  ```
  SET CHLAUTH(' generic-channel-name ') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
  ) USERSRC(MAP) MCAUSER(user) ADDRESS(
  generic-ip-address)
  ```

  generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
  generic-ip-address é um endereço único ou um padrão que inclui o símbolo de asterisco (*) como um curinga ou o hífen (-) para indicar um intervalo, que corresponda ao endereço. Para obter informações adicionais sobre endereços IP genéricos, consulte Endereços IP genéricos.

Referências relacionadas

SET CHLAUTH

Mapeando um ID de usuário cliente para um ID do usuário MCAUSER

É possível usar um registro de autenticação de canal para mudar o atributo MCAUSER de um canal de conexão do servidor, de acordo com o ID do usuário recebido de um cliente.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Sobre esta tarefa

Observe que essa técnica se aplica somente a canais de conexão do servidor. Não tem nenhum efeito em outros tipos de canais.

Procedimento

Configure um registro de autenticação de canal usando o comando MQSC **SET CHLAUTH**ou o comando PCF **Set Channel Authentication Record** . Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
client-user-name é o ID do usuário associado com a conexão de clientes, o valor poderia ser declarado pelo aplicativo cliente, alterado pela autenticação de conexão usando adoção antecipada ou configurado por meio de uma saída do canal.
user é o ID do usuário a ser usado em vez de o nome de usuário do cliente.

Referências relacionadas
SET CHLAUTH
Atributos da sub-rotina de canais (ChlauthEarlyAdopt)

Mapeando um Nome Distinto de SSL ou TLS para um ID do Usuário MCAUSER
É possível usar um registro de autenticação de canal para configurar o atributo MCAUSER de um canal de acordo com o Nome Distinto (DN) recebido.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP)
SSLPEER(generic-ssl-peer-name) SSLCERTI(generic-issuer-name)
USERSRC(MAP) MCAUSER(user)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
generic-ssl-peer-name é uma d que segue as regras de padrão do IBM MQ para valores de SSLPEER. Consulte Regras do IBM MQ para valores SSLPEER.
user é o ID do usuário a ser usado para todas as conexões usando o DN especificado.
generic-issuer-name refere-se ao DN do emissor do certificado para corresponder. Esse parâmetro é opcional mas é necessário usá-lo para evitar de corresponder de maneira falsa ao certificado errado, se várias autoridades de certificação estiverem em uso.

Referências relacionadas
SET CHLAUTH

Bloqueando Acesso de um Gerenciador de Filas Remotas
É possível usar um registro de autenticação de canal para evitar que um gerenciador de filas remotas inicie canais.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Sobre esta tarefa

Observe que essa técnica não se aplica a canais de conexão do servidor. Se você especificar o nome de um canal de conexão do servidor no comando a seguir, ele não tem efeito.

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(QMGRMAP) QMNAME(' generic-partner-qmgr-name ')
USERSRC(NOACCESS)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
generic-partner-qmgr-name é o nome do gerenciador de filas ou um padrão que inclui o símbolo de asterisco (*) como um curinga que corresponde ao nome do gerenciador de filas.

Referências relacionadas

SET CHLAUTH

Bloqueando o acesso para um ID de usuário cliente

É possível usar um registro de autenticação de canal para evitar que um ID de usuário cliente estabeleça uma conexão de canal.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Sobre esta tarefa

Observe que essa técnica se aplica somente a canais de conexão do servidor. Não tem nenhum efeito em outros tipos de canais.

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(USERMAP) CLNTUSER(' client-user-name ')
USERSRC(NOACCESS)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
client-user-name é o ID do usuário associado com a conexão de clientes, o valor poderia ser declarado pelo aplicativo cliente, alterado pela autenticação de conexão usando adoção antecipada ou configurado por meio de uma saída do canal.

Referências relacionadas

SET CHLAUTH

Bloqueando o acesso para um Nome Distinto SSL ou TLS
É possível usar um registro de autenticação de canal para evitar que um Nome Distinto (DN) TLS inicie canais.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP)
SSLPEER('generic-ssl-peer-name') SSLCERTI(generic-issuer-name)
USERSRC(NOACCESS)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
generic-ssl-peer-name é uma d que segue as regras de padrão do IBM MQ para valores de SSLPEER. Consulte Regras do IBM MQ para valores SSLPEER.
generic-issuer-name refere-se ao DN do emissor do certificado para corresponder. Esse parâmetro é opcional mas é necessário usá-lo para evitar de corresponder de maneira falsa ao certificado errado, se várias autoridades de certificação estiverem em uso.

Referências relacionadas
SET CHLAUTH

Mapeando um Endereço IP para um ID do Usuário MCAUSER
É possível usar um registro de autenticação de canal para configurar o atributo MCAUSER de um canal de acordo com o endereço IP a partir do qual a conexão é recebida.

Antes de começar

Certifique-se de que os registros de autenticação de canal são ativados como a seguir:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procedimento

Configure um registro de autenticação de canal usando o comando de MQSC **SET CHLAUTH**, ou o comando de PCF **Set Channel Authentication Record**. Por exemplo, é possível emitir o comando de MQSC:

```
SET CHLAUTH(' generic-channel-name ') TYPE(ADDRESSMAP) ADDRESS(' generic-ip-address ')
USERSRC(MAP) MCAUSER(user)
```

generic-channel-name é o nome de um canal para o qual você deseja acesso ao controle, ou um padrão incluindo o símbolo asterisco (*) como um curinga que corresponde ao nome de canal.
user é o ID do usuário a ser usado para todas as conexões usando o DN especificado.
generic-ip-address é o endereço a partir do qual a conexão está sendo feita ou um padrão que inclui o asterisco (*) como um curinga ou o hífen (-) para indicar um intervalo, que corresponda ao endereço.

Referências relacionadas
SET CHLAUTH

Desativando o Acesso Remoto ao Gerenciador de Filas

Para que os aplicativos clientes não sejam conectados ao gerenciador de filas, desative o acesso remoto a eles.

Sobre esta tarefa

Evite que aplicativos clientes sejam conectados ao gerenciador de filas em uma das seguintes maneiras:

Procedimento

- Exclua todos os canais de conexão do servidor usando o comando MQSC **DELETE CHANNEL**.
- Configure o identificador de usuários do agente do canal de mensagens (MCAUSER) do canal com um ID do usuário sem direitos de acesso, usando o comando MQSC **ALTER CHANNEL**.

Configurando a Segurança de Conexão

Conceda a autoridade de conexão com o gerenciador de filas a cada usuário ou grupo de usuários que tiver uma necessidade de negócios.

Sobre esta tarefa

Para configurar a segurança de conexão, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  No UNIX, Linux, and Windows:

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

- IBM i
  No IBM i:

  ```
  GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM) USER('GroupName') AUT(*CONNECT)
  ```

- z/OS
  No 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)
  ```

  Estes comandos concedem autoridade para conectar-se para lote, CICS, IMS e o inicializador de canais (CHIN). Se você não usar um tipo particular de conexão, omita os comandos relevantes.

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Conceitos relacionados

“Perfis de Segurança de Conexão para o Inicializador de Canais” na página 199
Perfis para verificação de conexões do inicializador de canais são compostos pelo nome do gerenciador de filas ou do grupo de filas compartilhadas, seguido pela palavra *CHIN*. Conceda ao ID do usuário usado pelo espaço de endereço de tarefa iniciada do inicializador de canais o acesso READ para o perfil de conexão.

Controlando o Acesso de Usuário a Filas

Você deseja controlar o acesso ao aplicativo a filas. Use este tópico para determinar quais ações executar.

Para cada instrução verdadeira na primeira coluna, execute a ação indicada na segunda coluna.

Declaração	Ação
O aplicativo obtém mensagens de uma fila	Consulte “Concedendo autoridade para obter mensagens de filas” na página 396
O aplicativo configura contexto	Consulte “Concedendo autoridade para configurar o contexto” na página 397
O aplicativo passa contexto	Consulte “Concedendo autoridade para passar o contexto” na página 398
O aplicativo coloca mensagens em uma fila armazenada em cluster	Consulte “Autorizando a Colocação de Mensagens em Filas de Cluster Remotas” na página 464
O aplicativo coloca mensagens em uma fila local	Consulte “Concedendo autoridade para colocar mensagens em uma fila local” na página 399
O aplicativo coloca mensagens em uma fila modelo	Consulte “Concedendo autoridade para colocar mensagens em uma fila modelo” na página 400
O aplicativo coloca mensagens em uma fila remota	Consulte “Concedendo autoridade para colocar mensagens em uma fila do cluster remoto” na página 401

Concedendo autoridade para obter mensagens de filas
Conceda a autoridade para obter mensagens de uma fila ou um conjunto de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para obter mensagens de algumas filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX

- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME(' QMgrName ')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para configurar o contexto
Conceda a autoridade para configurar contexto em uma mensagem que está sendo colocada, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para configurar contexto em algumas filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita um dos comandos a seguir:
  - Para configurar apenas contexto de identidade:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
```

  - Para configurar todo o contexto:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
```

Nota: Para usar a autoridade `setid` ou `setall`, as autorizações devem ser concedidas tanto no objeto de filas apropriado como também no objeto de gerenciador de filas.

- Para o IBM i, emita um dos comandos a seguir:
  - Para configurar apenas contexto de identidade:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('
QMgrName ')
```

  - Para configurar todo o contexto:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL) MQMNAME('
QMgrName ')
```

- Para o z/OS, emita um dos conjuntos de comandos a seguir:
  - Para configurar apenas contexto de identidade:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

  - Para configurar todo o contexto:

```
RDEFINE MQQUEUE QMgrName. ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo autoridade para passar o contexto
Conceda a autoridade para passar contexto de uma mensagem recuperada para uma que está sendo colocada, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para passar contexto em algumas filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- IBM i

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- ULW
  Para sistemas UNIX, Linux, and Windows, emita um dos comandos a seguir:
  - Para passar apenas contexto de identidade:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Para passar todo o contexto:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
    ```

- IBM i
  Para o IBM i, emita um dos comandos a seguir:
  - Para passar apenas contexto de identidade:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID) MQMNAME('
    QMgrName ')
    ```

  - Para passar todo o contexto:

    ```
    GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL) MQMNAME('
    QMgrName ')
    ```

- z/OS
  Para o z/OS, emita os comandos a seguir para transmitir o contexto de identidade ou todo o contexto:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo autoridade para colocar mensagens em uma fila local
Conceda a autoridade para colocar mensagens em uma fila local ou um conjunto de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para colocar mensagens em algumas filas locais, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX

- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para colocar mensagens em uma fila modelo
Conceda a autoridade para colocar mensagens em uma fila modelo ou um conjunto de filas modelo, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Filas modelo são usadas para criar filas dinâmicas. Você deve, portanto, conceder autoridade para ambas as filas, modelo e dinâmica. Para conceder essas autoridades, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita os comandos a seguir:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Para IBM i, emita os seguintes comandos:

```
GRTMQMAUT OBJ(' ModelQueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

- Para z/OS, emita os seguintes comandos:

```
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)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ModelQueueName
O nome da fila modelo em que as filas dinâmicas se baseiam.

ObjectProfile
O nome do perfil da fila dinâmica ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para colocar mensagens em uma fila do cluster remoto
Conceda a autoridade para colocar mensagens em uma fila cluster remoto ou um conjunto de filas a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para colocar uma mensagem em uma fila do cluster remoto, é possível colocá-la em uma definição local de uma fila remota ou uma fila remota completa. Se você estiver usando uma definição local de uma fila remota, você precisa de autoridade para colocar o objeto local: consulte "Concedendo autoridade para colocar mensagens em uma fila local" na página 399. Se você estiver usando uma fila remota completa, você precisa de autoridade para colocar a fila remota. Conceda esta autoridade usando os comandos apropriados para seu sistema operacional.

O comportamento padrão é realizar o controle de acesso no SYSTEM.CLUSTER.TRANSMIT.QUEUE. Observe que esse comportamento se aplica mesmo se você estiver usando diversas filas de transmissão.

O comportamento específico descrito neste tópico se aplica apenas quando você tiver configurado o atributo **ClusterQueueAccessControl** no arquivo qm.ini para ser *RQMNome*, conforme descrito no tópico Sub-rotina de segurança, e tiver reiniciado o gerenciador de filas.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- IBM i

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -t rqmname -n
ObjectProfile -g GroupName +put
```

Observe que é possível usar o objeto *rqmname* somente para filas de cluster remoto.

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
QMgrName')
```

Observe que é possível usar o objeto RMTMQMNAME somente para filas de cluster remoto.

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQQUEUE)
ID(GroupName) ACCESS(UPDATE)
```

Observe que é possível usar o nome do gerenciador de filas remotas (ou grupo de filas compartilhadas) somente para filas de clusters remotos.

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do gerenciador de filas remotas ou do perfil genérico para o qual mudar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Controlando o Acesso de Usuário aos Tópicos

É necessário controlar o acesso de aplicativos aos tópicos. Use este tópico para determinar quais ações executar.

Para cada instrução verdadeira na primeira coluna, execute a ação indicada na segunda coluna.

Tabela 71. Controlando o Acesso de Usuário aos Tópicos

Declaração	**Ação**
O aplicativo publica mensagens em um tópico	Consulte “Concedendo autoridade para publicar mensagens em um tópico” na página 402
O aplicativo assina um tópico	Consulte “Concedendo autoridade para assinar tópicos” na página 403

Concedendo autoridade para publicar mensagens em um tópico

Conceda a autoridade para publicar mensagens em um tópico ou um conjunto de tópicos, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para publicar mensagens em alguns tópicos, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux

- UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('
QMgrName ')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

  Os nomes das variáveis possuem os seguintes significados:

  QMgrName
  O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

  ObjectProfile
  O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

  GroupName
  O nome do grupo que receberá acesso.

Concedendo autoridade para assinar tópicos
Conceda a autoridade para assinar um tópico ou um conjunto de tópicos, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para assinar alguns tópicos, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('
QMgrName ')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para consultar em um gerenciador de filas

Conceda a autoridade para consultar em um gerenciador de filas, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para consultar em um gerenciador de filas, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME(' QMgrName
')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Esses comandos concedem acesso ao gerenciador de filas especificado. Para permitir que o usuário use o comando MQINQ, emita os seguintes comandos:

```
RDEFINE MQCMDS QMgrName.MQINQ.QMGR UACC(NONE)
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para acessar processos

Conceda a autoridade para acessar um processo ou um conjunto de processos, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para acessar alguns processos, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i
- Linux
- UNIX
- IBM i

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ(' ObjectProfile ') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME(' QMgrName
')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

Concedendo autoridade para acessar listas de nomes

Conceda a autoridade para acessar uma lista de nomes ou um conjunto de listas de nomes, a cada grupo de usuários com uma necessidade de negócios para isso.

Sobre esta tarefa

Para conceder a autoridade para acessar algumas listas de nomes, use os comandos apropriados de seu sistema operacional.

Nas plataformas a seguir, também é possível usar o comando SET AUTHREC:

- IBM i IBM i
- Linux Linux
- UNIX UNIX
- IBM i Windows

Nota: MQ Appliance No IBM MQ Appliance é possível usar apenas o comando **SET AUTHREC**.

Procedimento

- Para sistemas UNIX, Linux, and Windows, emita o comando a seguir:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
+all
```

- Para o IBM i, emita o comando a seguir:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

ObjectProfile
O nome do perfil de objeto ou do perfil genérico do qual alterar as autorizações.

GroupName
O nome do grupo que receberá acesso.

ULW Autoridade para administrar o IBM MQ no UNIX, Linux, and Windows

Os administradores do IBM MQ podem usar todos os comandos do IBM MQ e conceder autoridades para outros usuários. Quando administradores emitem comandos para gerenciadores de filas remotas, ele devem ter a autoridade necessária no gerenciador de filas remotas. Considerações adicionais se aplicam aos sistemas Windows.

Os administradores do IBM MQ têm autoridade para usar todos os comandos do IBM MQ (incluindo os comandos para conceder autoridades do IBM MQ para outros usuários).

Para ser um administrador do IBM MQ, deve-se ser membro de um grupo especial denominado grupo **mqm**.

Windows Como alternativa, apenas no Windows , as contas locais podem administrar o IBM MQ se forem membros do grupo de Administradores em sistemas Windows .

Atenção: É possível incluir seu usuário do Azure AD no grupo mqm usando um comando de administrador. Por exemplo, use o comando `net localgroup mqm AzureAD\<your userID> /add`. Em seguida, execute comandos de administração do IBM MQ ou use o IBM MQ Explorer.

O grupo **mqm** é criado automaticamente quando o IBM MQ está instalado. É possível incluir usuários adicionais no grupo para permitir que eles executem a administração. Todos os membros desse grupo possuem acesso a todos os recursos. Esse acesso pode ser revogado somente removendo um usuário do grupo **mqm** e emitindo o comando **REFRESH SECURITY**.

Os administradores podem usar comandos de controle para administrar o IBM MQ. Um desses comandos de controle é **setmqaut**, que é usado para conceder autoridades a outros usuários para permitir que eles acessem ou controlem os recursos do IBM MQ. Os comandos PCF para gerenciar os registros de autoridade estão disponíveis a não administradores aos quais tenham sido concedidas autoridades dsp e chg no gerenciador de filas. Para obter mais informações sobre o gerenciamento de autoridades usando comandos PCF, veja Formatos de comando programável.

Os administradores devem ter as autoridades requeridas para os comandos MQSC serem processados pelo gerenciador de fila remoto. O IBM MQ Explorer emite comandos PCF (formato de comando programável) para executar tarefas de administração. Os administradores não requerem autoridades adicionais para usar o IBM MQ Explorer para administrar um gerenciador de filas no sistema local. Quando o IBM MQ Explorer é usado para administrar um gerenciador de filas em outro sistema, os administradores devem ter as autoridades necessárias para que os comandos PCF sejam processados pelo gerenciador de filas remoto.

Atenção: No IBM MQ 8.0, você não precisa ser um administrador para usar o comando de controle **runmqsc**, que emite comandos do IBM MQ Script (MQSC).

Quando **runmqsc** é utilizado no modo indireto para enviar comandos MQSC para um gerenciador de fila remoto, cada comando será encapsulado dentro de um comando PCF Escape.

Para obter mais informações sobre verificações de autoridade quando os comandos PCF e MQSC são processados, consulte os seguintes tópicos:

- Para comandos PCF que operam em gerenciadores de filas, filas, processos, listas de nomes e objetos de informações sobre autenticação, consulte Autoridade para trabalhar com objetos do IBM MQ. Consulte esta seção para obter os comandos MQSC equivalentes encapsulados nos comandos PCF Escape.
- Para comandos PCF que operam em canais, iniciadores de canais, listeners e clusters, consulte Segurança de Canal.
- Para comandos PCF que operam em registros de autoridade, consulte verificação de autoridade para comandos PCF
- z/OS Para comandos MQSC que são processados pelo servidor de comando no IBM MQ for z/OS, consulte Segurança do comando e segurança de recurso do comando no z/OS .

Além disso, em sistemas Windows , a conta SYSTEM tem acesso total aos recursos do IBM MQ

Em plataformas UNIX and Linux, um ID do usuário especial de **mqm** também é criado, para uso somente pelo produto. Ele nunca deverá estar disponível para usuários não privilegiados. Todos os objetos do IBM MQ são de propriedade do ID do usuário **mqm**.

Em sistemas Windows , os membros do grupo de Administradores também podem administrar qualquer gerenciador de filas, assim como a conta SYSTEM Também é possível criar um grupo **mqm** de domínio no

controlador de domínio que contenha todos os IDs de usuários privilegiados ativos dentro do domínio e incluí-lo no grupo **mqm** local. Alguns comandos, por exemplo **crtmqm**, manipulam as autoridades nos objetos IBM MQ e, portanto, precisam de autoridade para trabalhar com esses objetos (conforme descrito nas seções a seguir). Os membros do grupo **mqm** têm autoridade para trabalhar com todos os objetos, mas pode haver circunstâncias nos sistemas Windows em que a autoridade será negada se você tiver um usuário local e um usuário autenticado pelo domínio com o mesmo nome. Isso é descrito no "Principais e grupos no UNIX, Linux, and Windows" na página 411.

Versões do Windows com um recurso Controle de Conta do Usuário (UAC) restringem as ações que os usuários podem executar em certos recursos do sistema operacional, mesmo que sejam membros do grupo Administradores. Se o seu ID do usuário está no grupo Administradores, mas não no grupo **mqm**, deve-se usar um prompt de comandos elevado para emitir comandos administrativos do IBM MQ, como **crtmqm**, caso contrário, o erro `AMQ7077: você não está autorizado a executar a operação solicitada` é gerado. Para abrir um prompt de comandos elevado, clique com o botão direito no item de menu iniciar ou ícone para o prompt de comandos e selecione **Executar como administrador**.

Você não precisa ser um membro do grupo **mqm** para executar as ações a seguir:

- Emita os comandos a partir de um programa de aplicativo que emite os comandos PCF ou comandos MQSC em um comando Escape PCF, a menos que os comandos manipulem os iniciadores de canal. (Esses comandos são descritos em "Protegendo Definições do Inicializador de Canais" na página 112).
- Emita as chamadas MQI a partir de um programa de aplicativo (a menos que você queira usar as ligações de caminho rápido na chamada `MQCONNX`).
- Use o comando `crtmqcvx` para criar um fragmento de código que executa conversão de dados em estruturas de tipo de dados.
- Usar o comando `dspmq` para exibir gerenciadores de filas.
- Use o comando `dspmqtrc` para exibir a saída de rastreio formatado do IBM MQ.

Uma limitação de 12 caracteres aplica-se ao grupo e aos IDs do usuário.

As plataformas UNIX and Linux geralmente restringem o comprimento de um ID do usuário a 12 caracteres. O AIX 5.3 aumentou esse limite, mas o IBM MQ ainda observa uma restrição de 12 caracteres em todas as plataformas UNIX and Linux. Se você usar um ID do usuário com mais de 12 caracteres, o IBM MQ substitui-o com o valor de `UNKNOWN`. Não defina um ID do usuário com um valor de `UNKNOWN`.

ULW Gerenciando o grupo mqm no UNIX, Linux, and Windows

Usuários no grupo mqm são concedidos privilégios administrativos completos sobre o IBM MQ. Por esta razão, não é necessário inscrever usuários comuns e de aplicativos no grupo mqm. O grupo mqm deve conter contas somente dos administradores do IBM MQ.

Estas tarefas estão descritas em:

- Windows Criando e gerenciando grupos no Windows
- AIX Criando e gerenciando grupos no AIX
- Solaris Criando e gerenciando grupos no Solaris
- Linux Criando e gerenciando grupos no Linux

Windows Se o seu controlador de domínio é executado no Windows 2000 ou Windows 2003 ou mais recente, seu administrador de domínio pode ter que configurar uma conta especial para o IBM MQ usar. Para obter mais informações, consulte Configurando o IBM MQ com o Prepare IBM MQ Wizard e Criando e configurando contas de domínio do Windows para o IBM MQ.

ULW Autoridade para trabalhar com objetos do IBM MQ no UNIX, Linux, and Windows

Todos os objetos são protegidos pelo IBM MQ e deve ser concedida autoridade apropriada aos diretores para acessá-los. Diferentes principais precisam de diferentes direitos de acesso a diferentes objetos.

Gerenciadores de filas, filas, definições de processos, listas de nomes, canais, canais de conexão do cliente, listeners, serviços e objetos de informações sobre autenticação são todos acessados a partir de aplicativos que usam chamadas MQI ou comandos PCF. Esses são todos os recursos protegidos pelo IBM MQ e os aplicativos precisam ser concedida permissão para acessá-los. A entidade que faz a solicitação pode ser um usuário, um programa de aplicativo que emite uma chamada MQI ou um programa de administração que emite um comando PCF. O identificador do solicitante é referido como o *principal*.

Diferentes grupos de principais podem receber diferentes tipos de autoridade de acesso ao mesmo objeto. Por exemplo, para uma fila específica, um grupo pode ter permissão para executar ambas as operações put e get; outro grupo pode ter permissão somente para navegar pela fila (MQGET com a opção de navegação). De forma semelhante, alguns grupos podem ter as autoridades put e get para uma fila, mas podem não ter permissão para alterar atributos da fila ou para excluí-la.

Algumas operações são especialmente sigilosas e devem ser limitadas a usuários privilegiados. Por exemplo:

- Acesso a algumas filas especiais, como filas de transmissão ou a fila de comandos SYSTEM.ADMIN.COMMAND.QUEUE
- Execução de programas que usam opções de contexto completas de MQI
- Criação e exclusão de filas de aplicativos

Permissão de acesso completo a um objeto é determinada automaticamente para o ID do usuário que criou o objeto e para todos os membros do grupo mqm (e aos membros do grupo Administradores local em sistemas Windows).

Conceitos relacionados

“Autoridade para administrar o IBM MQ no UNIX, Linux, and Windows” na página 406
Os administradores do IBM MQ podem usar todos os comandos do IBM MQ e conceder autoridades para outros usuários. Quando administradores emitem comandos para gerenciadores de filas remotas, ele devem ter a autoridade necessária no gerenciador de filas remotas. Considerações adicionais se aplicam aos sistemas Windows.

ULW Quando verificações de segurança são feitas no UNIX, Linux, and Windows

As verificações de segurança são feitas geralmente ao conectar-se a um gerenciador de filas, abrir ou fechar objetos e colocar ou obter mensagens.

As verificações de segurança feitas para um aplicativo típico são as seguintes:

Conectando-se ao gerenciador de filas (chamadas MQCONN ou MQCONNX)
Eta é a primeira vez que o aplicativo é associado a um determinado gerenciador de filas. O gerenciador de filas interroga o ambiente operacional para descobrir o ID do usuário associado ao aplicativo. O IBM MQ, em seguida, verifica se o ID do usuário está autorizado a se conectar ao gerenciador de filas e retém o ID do usuário para verificações futuras.

Os usuários não têm de efetuar sign on para o IBM MQ; o IBM MQ assume que os usuários efetuaram sign on ao sistema operacional subjacente e foram autenticados por ele.

Abrindo o objeto (chamadas MQOPEN ou MQPUT1)
Os objetos do IBM MQ são acessados abrindo o objeto e emitindo comandos com relação a ele. Todas as verificações de recursos são executadas quando o objeto é aberto, em vez de quando ele é realmente acessado. Isso significa que a solicitação de **MQOPEN** deve especificar o tipo de acesso necessário (por exemplo, se o usuário deseja apenas pesquisar o objeto ou executar uma atualização, como colocar mensagens em uma fila).

O IBM MQ verifica o recurso que é nomeado na solicitação **MQOPEN**. Para um objeto de fila de alias ou fila remota, a autorização usada é aquela do próprio objeto, não da fila à qual a fila do alias ou a fila remota é resolvida. Isso significa que o usuário não precisa de permissão para acessá-la. Limite a autoridade para criar filas a usuários privilegiados. Se você não fizer isto, os usuários podem efetuar bypass do controle de acesso normal simplesmente criando um alias. Se uma fila remota for referida explicitamente com ambos os nomes, da fila e do gerenciador de filas, a fila de transmissão associada ao gerenciador de filas remotas será verificada.

A autoridade para uma fila dinâmica baseia-se naquela da fila modelo da qual se deriva, mas não é necessariamente a mesma. Isso é descrito na Nota "1" na página 132.

O ID do usuário usado pelo gerenciador de filas para verificações de acesso é o ID do usuário obtido do ambiente operacional do aplicativo conectado ao gerenciador de filas. Um aplicativo adequadamente autorizado pode emitir uma chamada **MQOPEN** especificando um ID do usuário alternativo; as verificações de controle de acesso são então feitas no ID do usuário alternativo. Isso não altera o ID do usuário associado ao aplicativo, apenas aquele usado para verificações de controle de acesso.

Colocando e obtendo mensagens (chamadas MQPUT ou MQGET)
Não são executadas verificações de controle de acesso.

Fechando o objeto (MQCLOSE)
Não são executadas verificações de controle de acesso, a menos que o **MQCLOSE** resulte na exclusão de uma fila dinâmica. Neste caso, há uma verificação para ver se o ID do usuário tem autorização para excluir a fila.

Inscrevendo-se em um tópico (MQSUB)
Quando um aplicativo é subscrito para um tópico, ele especifica o tipo de operação que precisa executar. Ele estará criando uma nova assinatura, alterando uma assinatura existente ou continuando uma assinatura existente sem alterá-la. Para cada tipo de operação, o gerenciador de filas verifica se o ID do usuário que está associado ao aplicativo possui a autoridade para executar a operação.

Quando um aplicativo é subscrito para um tópico, as verificações de autoridade são executadas com relação aos objetos de tópicos que estão localizados na árvore de tópicos ou acima do ponto na árvore de tópicos no qual a aplicativo foi subscrito. As verificações de autoridade podem envolver verificações em mais de um objeto de tópico.

O ID do usuário que o gerenciador de fila utiliza para as verificações de autoridade é o ID obtido do sistema operacional quando o aplicativo estabelece conexão com o gerenciador de fila.

O gerenciador de filas executa verificações de autoridade em filas de assinantes, mas não em filas gerenciadas.

ULW Como o controle de acesso é implementado pelo IBM MQ no UNIX, Linux, and Windows

O IBM MQ usa os serviços de segurança fornecidos pelo sistema operacional subjacente, usando o gerenciador de autoridade de objeto. O IBM MQ fornece comandos para criar e manter listas de controle de acesso.

Uma interface de controle de acesso chamada Interface de serviço de autorização é parte do IBM MQ. O IBM MQ fornece uma implementação de um gerenciador de controle de acesso (em conformidade com a Interface de serviço de autorização) conhecido como o *gerenciador de autoridade de objeto (OAM)*. Isso é automaticamente instalado e ativado para cada gerenciador de filas que você criar, a menos que você especifique de outra maneira, (conforme descrito em "Evitando verificações de acesso de segurança nos sistemas UNIX, Linux, and Windows" na página 365). O OAM pode ser substituído por qualquer usuário ou componente gravado do fornecedor que esteja em conformidade com a Interface de serviço de autorização.

O OAM explora os recursos de segurança do sistema operacional subjacente, usando IDs de usuário e de grupo do sistema operacional. Os usuários podem acessar objetos do IBM MQ somente se eles tiverem a autoridade correta. "Controlando o acesso a objetos usando o OAM no UNIX, Linux, and Windows" na página 355 descreve como conceder e revogar essa autoridade.

O OAM mantém uma lista de controle de acesso (ACL) para cada recurso que controla. Os dados de autorização são armazenados em uma fila local chamada SYSTEM.AUTH.DATA.QUEUE. O acesso a essa fila é restrito a usuários no grupo mqm e, adicionalmente, no Windows, a usuários no grupo Administradores e usuários com login efetuado com o ID SYSTEM. O acesso de usuário à fila não pode ser alterado.

O IBM MQ fornece comandos para criar e manter listas de controle de acesso. Para obter informações adicionais sobre esses comandos, consulte "Controlando o acesso a objetos usando o OAM no UNIX, Linux, and Windows" na página 355.

O IBM MQ transmite o OAM uma solicitação contendo um diretor, um nome de recurso e um tipo de acesso. O OAM concede ou rejeita o acesso com base na ACL que mantém. O IBM MQ segue a decisão do OAM; se o OAM não puder tomar uma decisão, o IBM MQ não permitirá o acesso.

ULW Identificando o ID do usuário no UNIX, Linux, and Windows

O gerenciador de autoridade de objeto identifica o diretor que está solicitando acesso a um recurso. O ID do usuário usado como o principal varia de acordo com o contexto.

O gerenciador de autoridade de objeto (OAM) deve ser capaz de identificar quem está solicitando acesso a um recurso específico. O IBM MQ usa o termo *diretor* para fazer referência a este identificador. O principal é estabelecido quando o aplicativo se conecta ao gerenciador de filas pela primeira vez; ele é determinado pelo gerenciador de filas a partir do ID do usuário associado ao aplicativo de conexão. (Se o aplicativo emitir chamadas XA sem se conectar ao gerenciador de filas, o ID do usuário associado ao aplicativo que emite a chamada xa_open será usado para verificações de autoridade pelo gerenciador de filas.)

Em sistemas UNIX and Linux, as rotinas de autorização verificam o ID do usuário real (efetuado log in) ou o ID do usuário efetivo associado ao aplicativo. O ID do usuário verificado pode depender do tipo de ligação. Para obter detalhes, consulte Serviços Instaláveis.

O IBM MQ propagará o ID do usuário recebido do sistema no cabeçalho da mensagem (estrutura do MQMD) de cada mensagem como a identificação do usuário. Esse identificador faz parte das informações de contexto da mensagem e é descrito em "Autoridade de contexto no UNIX, Linux, and Windows" na página 413. Os aplicativos não podem alterar essas informações, a não ser que tenham sido autorizados a alterar as informações de contexto.

ULW *Principais e grupos no UNIX, Linux, and Windows*

Principais podem pertencer a grupos. Concedendo acesso de recurso a grupos em vez de indivíduos, é possível reduzir a quantidade de administração requeridos. As Listas de controle de acesso (ACLs) baseiam-se em ambos os grupos e IDs de usuário.

Por exemplo, é possível definir um grupo consistindo em usuários que desejam executar um determinado aplicativo. Outros usuários podem receber acesso a todos os recursos que precisam, incluindo seus IDs de usuário no grupo apropriado.

Este processo de definição e gerenciamento de grupos está descrito para plataformas específicas:

- Windows Criando e gerenciando grupos no Windows
- AIX Criando e gerenciando grupos no AIX
- Solaris Criando e gerenciando grupos no Solaris
- Linux Criando e gerenciando grupos no Linux

Um principal pode pertencer a mais de um grupo (seu conjunto de grupos). Ele tem a agregação de todas as autoridades concedidas a cada grupo em seu conjunto de grupos. Essas autoridades são armazenadas em cache, portanto, quaisquer mudanças feitas na associação ao grupo do principal não são reconhecidas até que o gerenciador de filas seja reiniciado, a menos que você emita o comando MQSC **REFRESH SECURITY** (ou seu equivalente PCF).

Linux UNIX Sistemas UNIX and Linux

A partir da IBM MQ 8.0, as listas de controle de acesso (ACLs) são baseadas nos IDs de usuário e nos grupos e é possível usá-las para a autorização configurando o atributo **SecurityPolicy** para o valor apropriado, conforme descrito em Configurando os serviços instaláveis e em Configurando as sub-rotinas do serviço de autorização no UNIX e no Linux.

A partir da IBM MQ 8.0, é possível usar o *modelo baseado em usuário* para autorização, o que permite usar usuários e grupos. No entanto, ao especificar um usuário no comando setmqaut, as novas permissões se aplicam somente a esse usuário e não os grupos aos quais esse usuário pertence. Para obter mais informações, consulte Permissões baseadas em usuário do OAM em sistemas UNIX e Linux.

Ao usar o *modelo baseado em grupo* para autorização, o grupo primário ao qual o ID do usuário pertence é incluído na ACL. O ID do usuário individual não é incluído e autoridade é concedida a todos os membros desse grupo. Por causa disso, observe que é possível, acidentalmente, mudar a autoridade de um diretor mudando a autoridade de outro diretor no mesmo grupo.

Todos os usuários são nominalmente designados ao grupo de usuários padrão nobody e, por padrão, nenhuma autorização é fornecida a esse grupo. É possível mudar a autorização no grupo nobody para conceder acesso a recursos do IBM MQ para usuários sem as autorizações específicas.

Não defina um ID do usuário com o valor UNKNOWN. O valor UNKNOWN é usado quando um ID do usuário é muito longo, portanto, os IDs de usuário arbitrários usariam as autoridades de acesso de UNKNOWN.

Os IDs de usuário podem conter até 12 caracteres e nomes de grupos com até 12 caracteres.

Windows Sistemas Windows

As ACLs baseiam-se em IDs de usuário e grupos. As verificações são as mesmas para o UNIX. É possível ter usuários diferentes em domínios diferentes com o mesmo ID do usuário. O IBM MQ permite que os IDs de usuário sejam qualificados por um nome de domínio para que estes usuários possam receber diferentes níveis de acesso.

O nome do grupo pode, opcionalmente, incluir um nome de domínio, especificado nos formatos a seguir:

```
GroupName@domain domain_name\group_name
```

Grupos globais são marcadas pelo OAM somente em dois casos:

1. A sub-rotina de segurança do gerenciador de filas inclui a configuração: GroupModel=GlobalGroups. Consulte Segurança.
2. O gerenciador de filas está usando um grupo de acesso de segurança alternativo. Consulte **crtmqm** .

Os IDs de usuário podem conter até 20 caracteres, nomes de domínio até 15 caracteres e nomes de grupos até 64 caracteres.

O OAM verifica, primeiramente, o banco de dados de segurança local, em seguida, o banco de dados de domínio primário e, finalmente, o banco de dados de qualquer domínio confiável. O primeiro ID do usuário encontrado é usado pelo OAM para verificação. Cada um desses IDs de usuário pode ter associações diferentes ao grupo em um determinado computador.

Alguns comandos de controle (por exemplo, **crtmqm**) mudam autoridades em objetos do IBM MQ usando o gerenciador de autoridade de objeto (OAM). O OAM procura nos banco de dados de segurança na ordem fornecida no parágrafo precedente para determinar os direitos de autoridade de um determinado ID do usuário. Como resultado, a autoridade determinada pelo OAM pode substituir o fato de que um ID do usuário é um membro do grupo mqm local. Por exemplo, se você emitir o comando **crtmqm** a partir de um ID do usuário autenticado por um controlador de domínio que tenha associação do grupo mqm local por meio de um grupo global, o comando falhará se o sistema tiver um usuário local com o mesmo nome que não está no grupo mqm local.

Para obter mais informações sobre como configurar o atributo **SecurityPolicy** no Windows, consulte Serviços instaláveis e Configurando sub-rotinas de serviço de autorização no Windows.

Windows *Identificadores de segurança (SIDs) do Windows*

O IBM MQ no Windows usa o SID no local onde ele está disponível. Se um SID do Windows não for fornecido com um pedido de autorização, o IBM MQ identifica o usuário com base no nome do usuário sozinho, mas isso pode resultar na autoridade errada sendo concedida.

Nos sistemas Windows, o identificador de segurança (SID) é usado para completar o ID do usuário. O SID contém informações que identificam os detalhes completos da conta do usuário no banco de dados do gerente de contas de segurança (SAM) do Windows no qual o usuário está definido. Quando uma mensagem é criada no IBM MQ for Windows, o IBM MQ armazena o SID no descritor de mensagens. Quando o IBM MQ no Windows executa verificações de autorização, ele usa o SID para consultar as informações completas do banco de dados do SAM. (O banco de dados do SAM em que o usuário está definido deve estar acessível para que essa consulta seja bem-sucedida.)

Por padrão, se um SID do Windows não for fornecido com um pedido de autorização, o IBM MQ identificará o usuário com base no nome do usuário sozinho. Ele faz isso procurando nos bancos de dados de segurança na seguinte ordem:

1. O banco de dados de segurança local
2. O banco de dados de segurança do domínio primário
3. O banco de dados de segurança de domínios confiáveis

Se o nome do usuário não for exclusivo, a autoridade incorreta do IBM MQ pode ser concedida. Para evitar esse problema, inclua um SID em cada pedido de autorização; o SID é usado pelo IBM MQ para estabelecer credenciais do usuário.

Para especificar que todas as solicitações de autorização devem incluir um SID, use **regedit**. Configure SecurityPolicy como NTSIDsRequired.

ULW Autoridade de usuário alternativo no UNIX, Linux, and Windows

É possível especificar que um ID do usuário possa usar a autoridade de outro usuário quando acessar um objeto do IBM MQ. Isso é denominado *autoridade de usuário alternativo* e é possível usar isso em qualquer objeto do IBM MQ.

A autoridade de usuário alternativo é essencial onde um servidor recebe solicitações de um programa e deseja assegurar que o programa possui a autoridade necessária para a solicitação. O servidor pode ter a autoridade necessária, mas precisa saber se o programa tem a autoridade para as ações solicitadas.

Por exemplo, suponha que um programa do servidor em execução com um ID do usuário PAYSERV recupere uma mensagem de solicitação de uma fila que foi colocada na fila pelo ID do usuário USER1. Quando o programa do servidor recebe a mensagem de solicitação, ele processa a solicitação e coloca a resposta de volta na fila de resposta especificada com a mensagem de solicitação. Em vez de usar seu próprio ID do usuário (PAYSERV) para autorizar a abertura da fila de resposta, o servidor pode especificar um ID do usuário diferente, neste caso, USER1. Neste exemplo, é possível usar a autoridade de usuário alternativo para controlar se PAYSERV tem permissão para especificar USER1 como um ID do usuário alternativo ao abrir a fila de resposta.

O ID do usuário alternativo é especificado no campo **AlternateUserId** do descritor de objeto.

ULW Autoridade de contexto no UNIX, Linux, and Windows

Contexto são informações que se aplicam a uma determinada mensagem e está contido no descritor de mensagens, MQMD, que faz parte da mensagem. Aplicativos podem especificar os dados de contexto quando uma chamada MQOPEN ou MQPUT é feita.

As informações de contexto são fornecidas em duas seções:

Seção de Identidade
De quem a mensagem veio. Ela consiste nos campos `UserIdentifier`, `AccountingToken` e `ApplIdentityData`.

Seção de Origem
De onde a mensagem veio, e quando ela foi colocada na fila. Ela consiste nos campos `PutApplType`, `PutApplName`, `PutDate`, `PutTime` e `ApplOriginData`.

Aplicativos podem especificar os dados de contexto quando uma chamada `MQOPEN` ou `MQPUT` é feita. Esses dados podem ser gerados pelo aplicativo, passados de outra mensagem ou gerados pelo gerenciador de filas, por padrão. Por exemplo, dados de contexto podem ser usados por programas do servidor para verificar a identidade do solicitante, testar se a mensagem veio de um aplicativo em execução com um ID do usuário autorizado.

Um programa do servidor pode usar `UserIdentifier` para determinar o ID do usuário de um usuário alternativo. Use a autorização de contexto para controlar se o usuário pode especificar qualquer uma das opções de contexto em qualquer chamada `MQOPEN` ou `MQPUT1`.

Consulte Controlando informações de contexto para obter informações sobre as opções de contexto, e Visão geral para MQMD para descrições dos campos do descritor de mensagens relacionadas ao contexto.

Implementando o controle de acesso em saídas de segurança

É possível implementar o controle de acesso em uma saída de segurança usando o MCAUserIdentifier ou o gerenciador de autoridade de objeto.

MCAUserIdentifier

Cada instância de um canal atual tem uma estrutura de definição de canais associada, MQCD. Os valores iniciais dos campos no MQCD são determinados pela definição de canal que é criada por um administrador do IBM MQ. Em particular, o valor inicial de um dos campos, *MCAUserIdentifier* , é determinado pelo valor do parâmetro MCAUSER no comando DEFINE CHANNEL ou pelo equivalente a MCAUSER, se a definição de canais for criada de outra forma.

A estrutura MQCD passa para um programa de saída de canal quando é chamada por um MCA. Quando chamada, a saída de segurança pode alterar o valor de *MCAUserIdentifier*, substituindo qualquer valor especificado na definição de canais.

Multi Em Multiplataformas, a menos que o valor de *MCAUserIdentifier* esteja em branco, o gerenciador de filas usa o valor de *MCAUserIdentifier* como ID do usuário para verificações de autoridade quando um MCA tenta acessar os recursos do gerenciador de filas após ele ter se conectado ao gerenciador de filas. Se o valor de *MCAUserIdentifier* estiver em branco, o gerenciador de fila utilizará então o ID do usuário padrão do MCA. Isso se aplica aos canais RCVR, RQSTR, CLUSRCVR e SVRCONN. Para MCAs de envio, o ID do usuário padrão sempre é usado para verificações de autoridade, mesmo que o valor de *MCAUserIdentifier* não esteja em branco.

z/OS No z/OS, o gerenciador de filas pode usar o valor de *MCAUserIdentifier* para verificações de autoridade, contanto que não esteja em branco. Para MCAs de recepção e MCAs de conexão do servidor, o gerenciador de fila utiliza o valor *MCAUserIdentifier* para verificações de autoridade dependendo:

- Do valor do parâmetro PUTAUT na definição do canal
- O perfil do RACF usado para as verificações
- Do nível de acesso do ID do usuário do espaço de endereço do inicializador de canais do perfil RESLEVEL

Para MCAs de envio, depende:

- De o MCA ser um originador da chamada ou um receptor
- Do nível de acesso do ID do usuário do espaço de endereço do inicializador de canais do perfil RESLEVEL

O ID do usuário que uma saída de usuário armazena no *MCAUserIdentifier* pode ser adquirido de várias formas. Estes são alguns exemplos:

- Visto que não existe saída de segurança na extremidade do cliente de um canal MQI, um ID do usuário associado ao aplicativo do cliente IBM MQ realiza fluxo de mensagens a partir da conexão do cliente ao MCA de conexão do servidor MCA quando o aplicativo cliente emite uma chamada MQCONN.O MCA da conexão do servidor armazena este ID do usuário no campo *RemoteUserIdentifier* na estrutura de definição do canal, MQCD. Se o valor de *MCAUserIdentifier* estiver em branco nesse momento, o MCA armazenará o mesmo ID do usuário no *MCAUserIdentifier*. Se o MCA não armazenar o ID do usuário em *MCAUserIdentifier*, uma saída de segurança poderá fazê-lo posteriormente configurando *MCAUserIdentifier* com o valor de *RemoteUserIdentifier*.

  Se o ID do usuário que flui do sistema do cliente estiver entrando em um novo domínio de segurança e não for válido no sistema do servidor, a saída de segurança poderá substituir o ID do usuário por um que seja válido e armazenar o ID do usuário substituto no *MCAUserIdentifier*.
- O ID do usuário pode ser enviado pela saída de segurança do parceiro em uma mensagem de segurança.

  Em um canal de mensagens, uma saída de segurança chamada pelo MCA de envio pode enviar o ID do usuário sob o qual o MCA de envio está sendo executado. Uma saída de segurança chamada pelo MCA receptor pode então armazenar o ID do usuário no *MCAUserIdentifier* . Da mesma forma, em um canal de MQI, uma saída de segurança na extremidade do cliente do canal pode enviar o ID do usuário associado ao aplicativo do IBM MQ MQI client. Uma saída de segurança na parte do servidor do canal pode então armazenar o ID do usuário no *MCAUserIdentifier*. Como no exemplo anterior, se o ID do usuário não for válido no sistema de destino, a saída de segurança pode substituir o ID do usuário por um que seja válido e armazenar o substituto no *MCAUserIdentifier*.

  Se um certificado digital foi recebido como parte do serviço de identificação e autenticação, uma saída de segurança poderá mapear o Nome Distinto no certificado para um ID do usuário que seja válido no sistema de destino. Ele pode então armazenar o ID do usuário no *MCAUserIdentifier*.
- Se for usado TLS no canal, o Nome Distinto (DN) do parceiro será passado para a saída no campo SSLPeerNamePtr do MQCD e o DN do emissor desse certificado será passado para a saída no campo SSLRemCertIssNamePtr do MQCXP.

Para obter mais informações sobre o campo *MCAUserIdentifier*, a estrutura de definição de canal, MQCD e a estrutura de parâmetros de saída de canal, MQCXP, consulte Chamadas de saída do canal e estrutura de dados. Para obter mais informações sobre o ID do usuário que flui de um sistema do cliente em um canal MQI, consulte Controle de Acesso.

Nota: Os aplicativos de saída de segurança construídos antes da liberação do IBM WebSphere MQ 7.1 podem requerer atualização. Para obter mais informações, consulte Programas de saída de segurança de canal.

Autenticação do usuário do gerenciador de autoridade de objeto do IBM MQ

Em conexões do IBM MQ MQI client, as saídas de segurança podem ser usadas para modificar ou criar a estrutura MQCSP usada na autenticação do usuário gerenciador de autoridade de objeto (OAM). Isso é descrito em Programas de saída do canal para canais do sistema de mensagens

Implementando controle de acesso em saídas de mensagem

Talvez seja necessário usar uma saída de mensagem para substituir um ID do usuário por outro.

Considere um aplicativo cliente que envia uma mensagem para um aplicativo do servidor. O aplicativo do servidor pode extrair o ID do usuário do campo *UserIdentifier* no descritor de mensagens e, contanto que tenha autoridade de usuário alternativa, solicitar que o gerenciador de filas use esse ID do usuário para verificações de autoridade quando ele acessa recursos do IBM MQ em nome do cliente.

Se o parâmetro PUTAUT estiver definido como CTX (ou ALTMCA no z/OS) na definição de canal, o ID do usuário no campo *UserIdentifier* de cada mensagem de entrada será usado para verificações de autoridade quando o MCA abrir a fila de destino.

Em certas circunstâncias, quando uma mensagem de relatório é gerada, é colocada utilizando a autoridade do ID do usuário no campo *UserIdentifier* da mensagem que está causando o relatório. Em particular, os relatórios COD (confirm-on-delivery) e relatórios de expiração são sempre colocados com essa autoridade.

Em decorrência dessas situações, será necessário substituir um ID do usuário por outro no campo *UserIdentifier* à medida que uma mensagem entrar em um novo domínio de segurança. Isso pode ser feito por uma saída de mensagem na extremidade receptora do canal. Alternativamente, você pode garantir que o ID do usuário no campo *UserIdentifier* de uma mensagem de entrada seja definido no novo domínio de segurança.

Se uma mensagem de entrada contiver um certificado digital para o usuário do aplicativo que enviou a mensagem, uma saída de mensagem poderá validar o certificado e mapear o Nome Distinto no certificado para um ID do usuário que seja válido no sistema receptor. Ela poderá definir o campo *UserIdentifier* no descritor de mensagem desse ID do usuário.

Se for necessário que uma saída de mensagem altere o valor do campo *UserIdentifier* em uma mensagem de entrada, poderá ser apropriado que a saída autentique o emissor da mensagem ao mesmo tempo. Para obter mais detalhes, consulte “Mapeamento de identidade em saídas de mensagem” na página 339.

Implementando o controle de acesso na saída de API e saída cruzada da API

Uma saída da API ou saída cruzada da API pode fornecer controles de acesso para suplementar aqueles fornecidos pelo IBM MQ. Especificamente, a saída pode fornecer controle de acesso no nível de mensagem. A saída pode assegurar que um aplicativo coloque ou obtenha de uma fila somente mensagens que satisfaçam determinados critérios.

Considere os seguintes exemplos:

- Uma mensagem contém informações sobre um pedido. Quando um aplicativo tenta colocar uma mensagem em uma fila, uma saída API ou saída cruzada da API pode verificar se o valor total do pedido é menor do que algum limite prescrito.
- Mensagens chegam a uma fila de destino a partir de gerenciadores de filas remotos. Quando um aplicativo tenta obter uma mensagem da fila, uma saída API ou saída cruzada da API pode verificar se o emissor da mensagem está autorizado a enviar uma mensagem para a fila.

Autorização LDAP

É possível usar a autorização de LDAP para remover a necessidade de um ID do usuário local.

Disponibilidade de autorização de LDAP em plataformas suportadas

A autorização do LDAP está disponível nas seguintes plataformas:

- UNIX
- IBM i
- Windows

Atenção:

Por meio da disponibilidade geral do IBM MQ 9.0, essa funcionalidade está disponível em todos os gerenciadores de filas novos ou migrados de uma liberação anterior.

Visão geral da autorização LDAP

Com autorização LDAP, comandos que manipulam a configuração de autorização, como **setmqaut** e **DISPLAY AUTHREC**, podem processar Nomes Distintos. Anteriormente, os usuários eram autenticados pela comparação de suas credenciais com o máximo de caracteres disponíveis que existem para usuários e grupos no sistema operacional local.

Atenção: Se você tiver executado o comando **DEFINE AUTHINFO**, deve-se reiniciar o gerenciador de filas. Se você não reiniciar o gerenciador de filas, o comando setmqaut não retornará o resultado correto.

Se um usuário fornece um ID do usuário em vez de um Nome distinto, o ID do usuário é processado. Por exemplo, quando há uma mensagem de entrada em um canal com PUTAUT(CTX), os caracteres no ID do usuário são mapeados para um Nome distinto LDAP e as verificações de autorização apropriadas são feitas.

Outros comandos como **DISPLAY CONN**, continuam a funcionar e mostram o valor real para o ID do usuário, ainda que esse ID de usuário possa não existir, de fato, no S.O. local.

UNIX Quando a autorização do LDAP estiver em vigor, o gerenciador de filas sempre usará o modelo de usuário de segurança em plataformas UNIX, independentemente do atributo **SecurityPolicy** no arquivo qm.ini. Portanto, configurar permissões para um usuário individual afeta somente esse usuário e ninguém mais que pertença a qualquer um dos grupos desse usuário.

Como com o modelo de SO, um usuário ainda tem a autoridade combinada que foi designada a ambos os individuais e para todos os grupos (se houver algum) para o qual o usuário pertence.

Por exemplo, suponha que os registros a seguir foram definidos em um repositório LDAP.

- Na classe **inetOrgPerson**:

```
dn="cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry"
        email=JohnDoe1@yourcompany.com [longer than 12 characters]
        shortu=jodoe
        Phone=1234567
```

- Na classe **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"
```

Para propósitos de autenticação, um gerenciador de filas usando esse servidor LDAP deve ter sido definido para que seu valor **CONNAUTH** aponte para um objeto **AUTHINFO** do tipo IDPWLDAP e cujos atributos de resolução do nome relevantes estão provavelmente configurados como a seguir:

```
USRFIELD(email) SHORTUSR(shortu)
BASEDNU(ou=users,o=yourcompany,c=yourcountry) CLASSUSR(inetOrgPerson)
```

Dada essa configuração para autenticação, um aplicativo pode concluir o campo CSPUserID, usado na chamada MQCNO, com um dos conjuntos de valores a seguir:

```
" cn=JohnDoe ", " JohnDoe1@yourcompany.com ", " email=JohnDoe1@yourcompany.com "
```

ou

```
" cn=JohnDoe, ou=users, o=ibm, c=uk ", " shortu=jodoe "
```

Em qualquer caso, o sistema pode usar os valores fornecidos para autenticar o contexto do S.O. de "jodoe".

Configurando autorizações

Como você usa o nome abreviado ou **USRFIELD** para configurar autorizações.

A abordagem de trabalhar com vários formatos, descrita em “Autorização LDAP” na página 416, continua para os comandos de autorização, com uma extensão adicional que o shortname ou o USRFIELD pode ser usado em um modo sem enfeites.

A sequência de caracteres especifica um atributo específico no registro LDAP ao nomear usuários (diretores) para autorização.

Importante: A sequência de caracteres não deve conter o caractere =, porque este caractere não pode ser usado em um ID do usuário do sistema operacional.

Se você transmitir um nome do principal para o OAM para autorização que é potencialmente um `shortname`, a sequência de caracteres deve caber em 12 caracteres. O algoritmo de mapeamento primeiro tenta resolver a um DN usando o atributo SHORTUSR na sua consulta LDAP.

Se isso falhar com um erro UNKNOWN_ENTITY ou se a sequência especificada não puder ser uma `shortname`, uma tentativa adicional será feita usando o atributo USRFIELD para construir a consulta LDAP.

Atenção: Se você executou o comando DEFINE AUTHINFO, deve-se reiniciar o gerenciador de filas. Se você não reiniciar o gerenciador de filas, o comando setmqaut não retornará o resultado correto.

Para processar autorizações do usuário, as configurações do comando setmqaut a seguir são todas equivalentes.

Tabela 72. Configurações de autorização do usuário

Comando:	**Nota**
`setmqaut -m QM -t qmgr -p jodoe +connect`	Este é um nome simples, não qualificado, resolvido por meio de SHORTUSR.
`setmqaut -m QM -t qmgr -pJohnDoe1@yourcompany.com +connect`	Além disso, um nome simples, não qualificado, resolvendo através de USRFIELD para a mesma entidade.
`setmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com +connect`	Usando um atributo denominado.
`setmqaut -m QM -t qmgr -p "phone=1234567" +connect`	Usando outro atributo denominado que não precisa ser qualquer um desses configurados no objeto AUTHINFO.

É possível usar o comando MQSC SET AUTHREC como uma alternativa para o comando **setmqaut**:

```
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('JohnDoe1@yourcompany.com') AUTHADD(connect)
```

ou o comando Set Authority Record (MQCMD_SET_AUTH_REC) PCF com o elemento MQCACF_PRINCIPAL_ENTITY_NAMES que contém a sequência:

```
 "cn=JohnDoe,ou=users,o=yourcompany,c=yourcountry"
```

Ao processar grupos, não há ambiguidade sobre o processamento de `shortname`, pois não há requisito para ajustar qualquer forma de um nome do grupo em 12 caracteres. Portanto, não há equivalente do atributo SHORTUSR para os grupos.

Isso significa que os exemplos de sintaxe descritos em Tabela 73 na página 419 são válidos, supondo que você tenha configurado o objeto AUTHINFO com os atributos estendidos e configurado para:

```
GRPFIELD(longname)
BASEDNG(ou=groups,o=yourcompany,c=yourcountry ) CLASSGRP(groupOfNames)
```

Tabela 73. Configurações de autorização de grupo	
Comando:	**Nota**
`setmqaut -m QM -t qmgr -g ApplicationGroupA +connect`	Usando GRPFIELD para resolver
`setmqaut -m QM -t qmgr -g longname=ApplicationGroupA +connect`	Nomeando um único atributo
`setmqaut -m QM -t qmgr -g "cn=Application Group A,ou=groups,o=yourcompany,c=yourcountry" +connect`	Usando o DN completo

É possível usar o comando MQSC SET AUTHREC como uma alternativa para o comando precedente **setmqaut**:

```
SET AUTHREC OBJTYPE(QMGR) GROUP('ApplicationGroupA')
      AUTHADD(connect)
```

ou o comando Set Authority Record (MQCMD_SET_AUTH_REC) PCF com o elemento MQCACF_GROUP_ENTITY_NAMES que contém a sequência:

```
 "ApplicationGroupA"
```

Importante:

Qualquer formato que você use para fazer referência a um nome, seja para usuário ou grupo, deve ser possível derivar um DN exclusivo.

Portanto, por exemplo, não se deve ter dois registros distintos que tenham "`shortu=jodoe`".

Se um DN exclusivo único não pode ser determinado, o OAM retorna MQRC_UNKNOWN_ENTITY.

Exibindo as autorizações

Vários métodos de exibir a autorização de usuários ou grupos.

comando dspmqaut

O método mais simples para exibir as autorizações disponíveis para um usuário ou grupo é usar o comando dspmqaut.

É possível usar uma consulta em qualquer uma das variações de sintaxe para identificar um usuário ou grupo. Observe que a saída de comando repete a identidade no formato especificado na linha de comandos. A saída não relata sobre o DN completo resolvido.

Por exemplo:

```
dspmqaut -m QM -t qmgr -p johndoe
Entity johndoe has the following authorizations for object QM:
    connect
```

ou

```
dspmqaut -m QM -t qmgr -p email=JohnDoe1@yourcompany.com
Entity email=JohnDoe1@yourcompany.com has the following authorizations for object QM:
    connect
```

comandos dmpmqaut e dmpmqcfg

O comando dmpmqaut e seus equivalentes MQSC ou PCF pode especificar o diretor ou grupo em qualquer um dos formatos suportados, como as tabelas **setmqaut** descritas em "Configurando autorizações" na página 417. No entanto, diferentemente de **dspmqaut**, o comando **dmpmqaut** sempre relata o DN completo.

```
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
```

Da mesma forma, o comando dmpmqcfg, que não tem nenhuma filtragem nos registros selecionados, sempre mostrará o DN completo em um formato que pode ser reproduzido posteriormente.

```
dmpmqcfg -m QM -x authrec
-----------------------------------
SET AUTHREC PROFILE(SELF) +
    PRINCIPAL('cn=JohnDoe, ou=users, o=yourcompany, c=yourcountry') +
    OBJTYPE(QMGR)
    AUTHADD(CONNECT)
```

Outras contraprestações ao usar a autorização LDAP

Uma breve descrição das mudanças no Message Queue Interface (MQI) e outros comandos MQSC e PCF dos quais você precisa estar ciente ao usar a autorização LDAP do IBM MQ 9.0.0.

ADOPTCTX

Não há nenhum requisito para que os aplicativos forneçam informações de autenticação ou para que o atributo ADOPTCTX seja definido como YES.

Se um aplicativo não autenticar explicitamente ou se **ADOPTCTX** for definida como NO para o objeto CONNAUTH ativo, o contexto de identidade associado ao aplicativo será obtido a partir do ID do usuário do sistema operacional.

Quando as autorizações precisam ser aplicadas, esse contexto é mapeado para uma identidade de LDAP usando as mesmas regras como para os comandos setmqaut.

Parâmetros de entrada para chamadas MQI

MQOPEN, MQPUT1 e MQSUB têm estruturas que permitem que um ID de usuário alternativo seja especificado.

Se esses campos são usados, o ID do usuário de 12 caracteres é mapeado para um DN usando as mesmas regras como nos comandos **setmqaut**, **dmpmqaut** e **dspmqaut**.

MQPUT e MQPUT1 também permitem que os programas adequadamente autorizados configurem o MQMD do campo UserIdentifier. O valor deste campo não é fiscalizado durante o processo PUT e pode ser definido com qualquer valor.

Como de costume, no entanto, o valor **UserIdentifier** pode ser usado para autorização em estágios posteriores do processamento de mensagens, por exemplo, quando PUTAUT(CTX) é definido em um canal de recebimento.

Nesse ponto, o identificador será verificado para obter autorização usando a configuração do gerenciador de filas de recebimento, que pode ser LDAP ou baseado no sistema operacional.

Parâmetros de saída para chamadas MQI

Sempre que um ID do usuário for fornecido para um programa em uma estrutura MQI será a versão do nome abreviado de 12 caracteres de associado à conexão.

Por exemplo, o valor de **MQAXC.UserId** para Saídas de API é o nome abreviado retornado do mapeamento do LDAP.

Outros comandos administrativos MQSC e PCF

Comandos que mostram informações do usuário no status do objeto como DISPLAY CONN USERID retornam o nome curto de 12 caracteres associado ao contexto. O DN completo não é mostrado.

Comandos que permitem que a asserção de identidades, como as regras de mapeamento CHLAUTH ou os valores de MCAUSER para os canais, podem assumir valores até o comprimento máximo definido para esses atributos (atualmente 64 caracteres).

Não há mudança para a sintaxe. Quando a autorização é necessária para essa identidade, ela é internamente mapeada para um DN usando as mesmas regras como para os comandos **setmqaut**, **dmpmqaut** e **dspmqaut**.

Isso significa que o valor MCAUSER em uma definição de canal pode não ser exibido como a mesma sequência que DISPLAY CHSTATUS, mas eles se referem à mesma identidade.

Por exemplo:

```
DEFINE CHL(SV1) CHLTYPE(SVRCONN) MCAUSER('cn=JohnDoe')
DEFINE CHL(SV2) CHLTYPE(SVRCONN) MCAUSER('jodoe')
DEFINE CHL(SV3) CHLTYPE(SVRCONN) MCAUSER('JohnDoe1@yourcompany.com')
```

Em seguida, DISPLAY CHSTATUS(*) ALL mostra o valor SHORTUSR, *MCAUSER(jodoe)* para todas as conexões.

Mudando entre modelos de autorização SO e LDAP

Como alternar entre os diferentes métodos de autorização em plataformas diferentes.

O atributo CONNAUTH dos pontos de gerenciador de filas em um objeto AUTHINFO. Quando o objeto é do tipo IDPWLDAP, um repositório LDAP é usado para autenticação.

Agora é possível aplicar um método de autorização para esse mesmo objeto, o que permite continuar com a autorização baseada em S.O. ou trabalhar com autorização LDAP

Plataformas UNIX e IBM i

O gerenciador de filas pode ser alternado a qualquer momento entre os modelos SO e LDAP. É possível mudar a configuração e fazer essa configuração ativa usando o comando REFRESH SECURITY TYPE (CONNAUTH).

Por exemplo, se esse objeto já foi configurado com as informações de conexão para autenticação:

```
ALTER AUTHINFO(MYLDAP) AUTHTYPE(IDPWLDAP) +
        AUTHORMD(SEARCHGRP) +
        BASEDNG('ou=groups,o=ibm,c=uk') +
        <other attributes>
ALTER QMGR CONNAUTH(MYLDAP)
REFRESH SECURITY
```

Windows

Se uma mudança na configuração da autoridade envolver a comutação entre os modelos OS e LDAP, o gerenciador de filas deverá ser reiniciado para que a mudança entre em vigor. Caso contrário, será possível fazer a mudança ativa usando o comando REFRESH SECURITY TYPE (CONNAUTH).

Regras de processamento

Ao alternar do SO para autorização do LDAP, quaisquer regras de autoridade existentes do SO que foram configuradas se tornam inativas e invisíveis.

Comandos como **dmpmqaut** não exibem as regras do SO. Da mesma forma, quando comutar de volta do LDAP para SO, quaisquer autorizações LDAP definidas se tornarem inativas e invisíveis, restaurando as regras de SO originais.

Se você deseja fazer backup das definições de um gerenciador de filas por qualquer razão, usando o comando **dmpmqcfg**, então esse backup conterá apenas as regras que são definidas para o método de autorização em vigor no momento do backup.

LDAP de LDAP

Uma visão geral de como cada plataforma administra o LDAP.

Ao usar autorização LDAP, a associação do grupo mqm (ou equivalente) no sistema operacional não é tão importante. Ser um membro desse grupo controla apenas se os comandos da linha de comandos determinados podem ser processados.

Em particular, deve-se estar nesse grupo para emitir os comandos strmqm e endmqm.

Quando o gerenciador de filas estiver em execução, agora existem limites na conta totalmente privilegiada. Independentemente do ID do usuário da pessoa que emite o comando **strmqm**, outros usuários pertencentes ao grupo do SO mqm (ou equivalente) não obtém privilégios especiais.

As autorizações de outros usuários são baseadas em quais grupos LDAP eles pertencem. Um uso não qualificado do nome do grupo mqm nos comandos como **setmqaut** não pode mapear para qualquer grupo LDAP.

Plataformas UNIX

UNIX

Depois que o gerenciador de filas está em execução, a única conta com privilégios completos automáticos é o usuário real que iniciou o gerenciador de filas.

O ID do mqm ainda existe e é usado como o proprietário de recursos do sistema operacional, como arquivos, porque mqm é o ID efetivo no qual o gerenciador de filas está em execução. No entanto, o usuário mqm não será automaticamente capaz de executar tarefas administrativas controladas pelo OAM.

IBM i

IBM i

No IBM i, as contas automaticamente privilegiadas são as que iniciam o gerenciador de filas e o ID do QMQM.

Ambos os IDs são necessários, porque o ID do usuário que inicia o gerenciador de filas é necessário apenas para iniciar o sistema. Uma vez em execução, os processos do gerenciador de filas têm somente autoridade QMQM.

Plataformas Windows

Windows

No Windows, as contas automaticamente privilegiadas completas é o usuário do SO que iniciou o gerenciador de filas e também o usuário que executará os processos do gerenciador de filas principal, como MUSR_MQADMIN, se o gerenciador de filas foi iniciado como um serviço do Windows.

Ao executar em modo de autorização do LDAP, o Windows se comportará de forma muito semelhante às plataformas UNIX. Ele lida com nomes abreviados de 12 caracteres e DNs completos.

Script da amostra

Como é útil ter um grupo capaz de fazer administração completa em um gerenciador de filas, um script de amostra é fornecido em plataformas UNIX como:

```
MQ_INSTALLATION_PATH/samp/bin/amqauthg.sh
```

Esta amostra usa dois parâmetros:

- Um nome do gerenciador de filas
- Um nome do grupo LDAP

A amostra processa os comandos setmqaut, concedendo autoridade total para todos os objetos. Este é o mesmo script que é gerado peloIBM MQ Explorer Assistente OAM para funções administrativas. Por exemplo, o código é iniciado:

```
setmqaut -t q -m qmgr -n "**" +alladm +allmqi -g
      groupname
```

Confidencialidade das mensagens

Para manter a confidencialidade, criptografe suas mensagens. Há vários métodos de criptografia de mensagens no IBM MQ, dependendo de suas necessidades.

Sua opção de CipherSpec determina o nível de confidencialidade que você possui.

Se você precisa de proteção de dados de ponta a ponta no nível do aplicativo para sua infraestrutura do sistema de mensagens de ponto a ponto, é possível usar o Advanced Message Security para criptografar as mensagens ou escrever sua própria saída da API ou saída cruzada da API.

Se você precisar criptografar mensagens somente enquanto elas estão sendo transportadas por meio de um canal, porque você tem a segurança adequada em seus gerenciadores de filas, será possível usar TLS ou escrever seus próprios programas de saída de segurança, saída de mensagem ou saída de envio e recebimento.

V 9.1.4 z/OS Se você precisar criptografar mensagens em repouso em um gerenciador de filas, poderá usar a criptografia do conjunto de dados do z/OS nesse gerenciador de filas.

Para obter informações adicionais sobre Advanced Message Security, consulte “Planejamento para o Advanced Message Security” na página 105. O uso de TLS com o IBM MQ é descrito em “Protocolos de segurança TLS no IBM MQ” na página 24. O uso de programas de saída em criptografia de mensagem é descrito em “Implementando confidencialidade em programas de saída do usuário” na página 452.

Consulte a seção Confidencialidade para dados em repouso no IBM MQ for z/OS com criptografia do conjunto de dados. para obter mais informações sobre a criptografia do conjunto de dados do z/OS.

Tarefas relacionadas

Conectando dois gerenciadores de filas usando TLS

Conectando um Cliente a um Gerenciador de Filas de Forma Segura

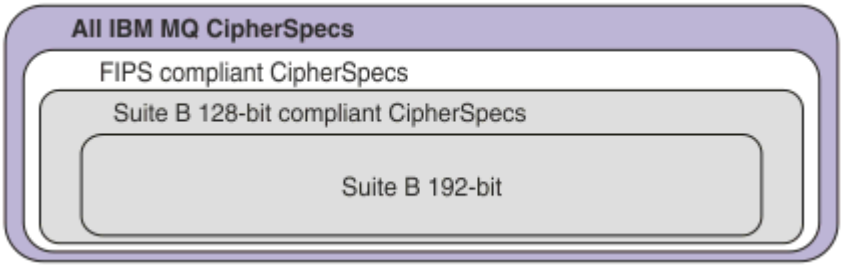
Ativando CipherSpecs

Ative um CipherSpec usando o parâmetro **SSLCIPH** no comando MQSC **DEFINE CHANNEL** ou no comando MQSC **ALTER CHANNEL** .

Alguns dos CipherSpecs que podem ser usados com IBM MQ são compatíveis com FIPS. Alguns dos CipherSpecs compatíveis com FIPS também são compatíveis com Suite B, embora outros, como TLS_RSA_WITH_AES_256_CBC_SHA, não sejam.

Todos os CipherSpecs compatíveis com o Conjunto B também são compatíveis com FIPS. Todos os CipherSpecs compatíveis com o Suite B caem em dois grupos: 128 bit (por exemplo, ECDHE_ECDSA_AES_128_GCM_SHA256) e 192 bit (por exemplo, ECDHE_ECDSA_AES_256_GCM_SHA384),

O diagrama a seguir ilustra o relacionamento entre estes subconjuntos:



Em IBM MQ 8.0.0 Fix Pack 3 , o número de CipherSpecs suportados foi reduzido.

V 9.1.1 Para obter informações sobre como configurar CipherSpecs padrão, consulte "Valores de CipherSpec padrão ativados no IBM MQ" na página 428. Também é possível fornecer um conjunto alternativo de CipherSpecs que são ativados para uso com os canais do MQ. Consulte "Fornecendo uma lista customizada de CipherSpecs ativados em multiplataformas" na página 429.

Para obter informações sobre a ativação de CipherSpecs descontinuados, consulte "Ativando CipherSpecs descontinuados em multiplataformas" na página 430 ou "Ativando CipherSpecs descontinuados no z/OS" na página 430. Para obter uma lista de CipherSpecs que podem ser reativados para uso com o IBM MQ, consulte "CipherSpecs descontinuado" na página 433.

ULW V 9.1.4 No IBM MQ 9.1.4, o IBM MQ suporta o protocolo de segurança TLS 1.3 no UNIX, Linux, and Windows. Para obter informações sobre o uso dessas CipherSpecs, consulte "Usando o TLS 1.3 no IBM MQ" na página 428 e "IBM MQ MQI client e TLS 1.3" na página 428.

Os CipherSpecs que você usa com o suporte do IBM MQ TLS

As especificações de código que é possível usar com o gerenciador de filas do IBM MQ são listadas automaticamente na tabela a seguir. Ao exigir um certificado pessoal, você especifica um tamanho de chave para o par de chaves público e particular. O tamanho da chave que é usado durante o handshake TLS é o tamanho armazenado no certificado, a menos que ele seja determinado pelo CipherSpec, conforme indicado na tabela:

Tabela 74. CipherSpecs que podem ser usados com o suporte TLS do IBM MQ

Suporte da plataforma "1" na página 427	**Nome do CipherSpec**	**Código Hex**	**Protocolo utilizado**	**Integridade de dados**	**Algoritmo de criptografia (bits de criptografia)**	**FIPS** "2" na página 427	**Conjunto B**
V 9.1.4 V 9.1.4 **CipherSpecs de alias**							
Todos(as)	ANY_TLS13_OR_HIGHER "3" na página 427 "4" na página 427 "5" na página 427	N/D	Negociado	Negociado	Negociado	Negociado	Negociado
Todos(as)	ANY_TLS13 "4" na página 427 "5" na página 427 "6" na página 427	N/D	TLS 1.3	Negociado	Negociado	Negociado	Negociado
Todos(as)	ANY_TLS12_OR_HIGHER "4" na página 427 "5" na página 427 "7" na página 427	N/D	Negociado	Negociado	Negociado	Negociado	Negociado

Tabela 74. CipherSpecs que podem ser usados com o suporte TLS do IBM MQ (continuação)

Suporte da plataforma "1" na página 427	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS "2" na página 427	Conjunto B
Todos(as)	ANY_TLS12 "8" na página 427	N/D	TLS 1.2	Negociado	Negociado	Negociado	Negociado
Todos(as)	ANY "9" na página 427	N/D	Negociado	Negociado	Negociado	Negociado	Negociado
V 9.1.4 V 9.1.4 **CipherSpecs para o TLS 1.3**							
Todos(as)	TLS_AES_128_GCM_SHA256 "4" na página 427	1301	TLS 1.3	GCM	AES-128 com GCM (128)	Sim	No
Todos(as)	TLS_AES_256_GCM_SHA384 "4" na página 427	1302	TLS 1.3	GCM	AES-256 com GCM (256)	Sim	No
Todos(as)	TLS_CHACHA20_POLY1305_SHA256 "4" na página 427	1303	TLS 1.3	POLY1305	CHACHA20 (256)	No	No
ULW	TLS_AES_128_CCM_SHA256	1304	TLS 1.3	CBC-MAC	AES-128 com CTR (128)	Sim	No
ULW	TLS_AES_128_CCM_8_SHA256 "11" na página 427	1305	TLS 1.3	CBC-MAC	AES-128 com CTR (128)	Sim	No
CipherSpecs para o TLS 1.2							
Todos(as)	TLS_RSA_WITH_AES_128_CBC_SHA256 "10" na página 427	003C	TLS 1.2	SHA-256	AES (128)	Sim	No
Todos(as)	TLS_RSA_WITH_AES_256_CBC_SHA256 "10" na página 427 "12" na página 427	003D	TLS 1.2	SHA-256	AES (256)	Sim	No
Todos(as)	TLS_RSA_WITH_AES_128_GCM_SHA256 "10" na página 427 "13" na página 427	009C	TLS 1.2	SHA-256 e AEAD GCM	AES (128)	Sim	No
Todos(as)	TLS_RSA_WITH_AES_256_GCM_SHA384 "10" na página 427 "12" na página 427 "13" na página 427	009D	TLS 1.2	SHA-384 e AEAD GCM	AES (256)	Sim	No
Todos(as)	ECDHE_ECDSA_AES_128_CBC_SHA256 "10" na página 427	C023	TLS 1.2	SHA-256	AES (128)	Sim	No
Todos(as)	ECDHE_ECDSA_AES_256_CBC_SHA384 "10" na página 427 "12" na página 427	C024	TLS 1.2	SHA-384	AES (256)	Sim	No
Todos(as)	ECDHE_RSA_AES_128_CBC_SHA256 "10" na página 427	C027	TLS 1.2	SHA-256	AES (128)	Sim	No
Todos(as)	ECDHE_RSA_AES_256_CBC_SHA384 "10" na página 427 "12" na página 427	C028	TLS 1.2	SHA-384	AES (256)	Sim	No

Tabela 74. CipherSpecs que podem ser usados com o suporte TLS do IBM MQ (continuação)

Suporte da plataforma “1” na página 427	**Nome do CipherSpec**	**Código Hex**	**Protocolo utilizado**	**Integridade de dados**	**Algoritmo de criptografia (bits de criptografia)**	**FIPS** “2” na página 427	**Conjunto B**
Multi	ECDHE_ECDSA_AES_128_GCM_SHA256 “12” na página 427 “13” na página 427	C02B	TLS 1.2	SHA-256 e AEAD GCM	AES (SHA384)	Sim	128 bits
Multi	ECDHE_ECDSA_AES_256_GCM_SHA384 “12” na página 427 “13” na página 427	C02C	TLS 1.2	SHA-384 e AEAD GCM	AES (SHA384)	Sim	192 bits
Todos(as)	ECDHE_RSA_AES_128_GCM_SHA256 “13” na página 427	C02F	TLS 1.2	SHA-256 e AEAD GCM	AES (128)	Sim	No
Todos(as)	ECDHE_RSA_AES_256_GCM_SHA384 “12” na página 427 “13” na página 427	C030	TLS 1.2	AEAD AES-128 GCM	AES (SHA384)	Sim	No

Tabela 74. CipherSpecs que podem ser usados com o suporte TLS do IBM MQ (continuação)

Suporte da plataforma "1" na página 427	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS "2" na página 427	Conjunto B

Notas:

1. Para obter uma lista de plataformas cobertas por cada ícone da plataforma, consulte Liberação e ícones de plataforma na documentação do produto.
2. Especifica se o CipherSpec é certificado por FIPS em uma plataforma certificada por FIPS. Consulte Federal Information Processing Standards (FIPS) para obter uma explicação do FIPS.
3. ULW A CipherSpec do alias ANY_TLS13_OR_HIGHER negocia o nível mais alto de segurança que a extremidade remota permitirá, mas se conectará apenas usando um protocolo TLS 1.3 ou superior.
4. z/OS Para usar o TLS 1.3 ou o ANY CipherSpec, no IBM MQ for z/OS, o sistema operacional deve ser z/OS 2.4 ou mais recente.
5. IBM i Para usar o TLS 1.3 ou o ANY CipherSpec no IBM i, a versão do sistema operacional subjacente deve suportar o TLS 1.3. Consulte Suporte TLS do sistema para TLSv1.3 para obter mais informações.
6. ULW A CipherSpec do alias ANY_TLS13 representa um subconjunto de CipherSpecs aceitáveis que usam o protocolo TLS 1.3, conforme listado nesta tabela para cada plataforma.
7. ULW A CipherSpec do alias ANY_TLS12_OR_HIGHER negocia o nível mais alto de segurança que a extremidade remota permitirá, mas se conectará apenas usando um protocolo TLS 1.2 ou superior.
8. O CipherSpec ANY_TLS12 representa um subconjunto de CipherSpecs aceitáveis que usam o protocolo TLS 1.2, conforme listado nesta tabela para cada plataforma.
9. ULW A CipherSpec do alias ANY negocia o nível mais alto de segurança que a extremidade remota permitirá.
10. IBM i Esses CipherSpecs não são ativados em sistemas IBM i 7.4 que têm o Valor do sistema QSSLCSLCTL configurado como *OPSSYS.
11. ULW Esses CipherSpecs usam um Integrity Check Value (ICV) com 8 octetos ao invés de um ICV com 16 octetos.
12. Esse CipherSpec não pode ser usado para assegurar uma conexão a partir do IBM MQ Explorer até um gerenciador de filas a menos que os arquivos de política sem restrição sejam aplicados ao JRE usado pelo Explorer.
13. Windows Linux Seguindo uma recomendação do GSKit, o TLS 1.2 GCM CipherSpecs tem uma restrição que significa que após 2 registros TLS24.5 serem enviados, usando a mesma chave de sessão, a conexão é finalizada com a mensagem AMQ9288E. Essa restrição do GCM está ativa, independentemente do modo FIPS que está sendo utilizado

    Para evitar que esse erro ocorra. Evite usar Cifras TLS 1.2 GCM , ative a reconfiguração de chave secreta ou inicie o gerenciador de filas ou o cliente do IBM MQ com a variável de ambiente `GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE` configurada. Para bibliotecas do GSKit , deve-se configurar essa variável de ambiente nos dois lados da conexão e aplicá-la às conexões do cliente para o gerenciador de filas e do gerenciador de filas para as conexões do gerenciador de filas. Observe que essa configuração afeta clientes .NET não gerenciados, mas não clientes Java ou gerenciados .NET . Para obter mais informações, consulte AES-GCM restrição de cifra.

    Essa restrição não se aplica ao IBM MQ for z/OS.

Usando o TLS 1.3 no IBM MQ

ULW V 9.1.4

No IBM MQ 9.1.4, o IBM MQ suporta o TLS 1.3 no UNIX, Linux, and Windows. Em qualquer instalação suportada, novos gerenciadores de filas são criados com uma entrada na sub-rotina SSL do arquivo `qm.ini` que lê:

```
SSL:
  AllowTLSV13=TRUE
```

Nota: O arquivo `qm.ini` pode ser localizado no diretório *<data directory>*/qmgrs/*<qmgr name>*

Se o gerenciador de filas tiver sido criado usando uma versão do IBM MQ anterior à IBM MQ 9.1.4, mas posteriormente for iniciado usando a IBM MQ 9.1.4 ou mais recente, ele não terá o conjunto de propriedades **AllowTLSV13**. Se você desejar ativar o TLS 1.3, deve-se editar o `qm.ini file` e incluir na propriedade conforme mostrado no exemplo (incluindo a sub-rotina "SSL:" se ela ainda não existir).

Essa propriedade do arquivo .ini ativa o TLS 1.3, o que permite o uso de CipherSpecs TLS 1.3. De acordo com a especificação do TLS 1.3, serão rejeitadas quaisquer tentativas de comunicação com um CipherSpec fraco, independentemente dele estar ou não ativado no IBM MQ. Os CipherSpecs que o TLS 1.3 considera fracos são CipherSpecs que atendem a um ou mais dos critérios a seguir:

- Usa o protocolo SSL 3.0.
- usam RC4 ou RC2 como o algoritmo de criptografia.
- têm um tamanho de chave de criptografia (bits) igual ou menor que 112.

Essas restrições são sinalizadas com a Nota [10] na Tabela 1 de CipherSpecs descontinuados.

Caso seja necessário continuar usando esses CipherSpecs, deve-se desativar o modo TLS 1.3. Para isso, edite o arquivo `qm.ini` do gerenciador de filas e mude a configuração da propriedade **AllowTLSV13** para:

```
SSL:
  AllowTLSV13=FALSE
```

Nota: Com essa configuração em vigor, não é possível usar especificações de código do TLS 1.3.

IBM MQ MQI client e TLS 1.3

ULW V 9.1.4

Ao usar o cliente do IBM MQ MQI client, o valor de **AllowTLSV13** será inferido, a menos que ele seja explicitamente especificado na sub-rotina SSL do arquivo `mqclient.ini` que está sendo usado pelo aplicativo.

- Se algum CipherSpecs fraco estiver ativado, **AllowTLSV13** será configurado como FALSE e nenhum CipherSpecs TLS 1.3 poderá ser usado.
- Caso contrário, **AllowTLSV13** será configurado como TRUE e os novos CipherSpecs TLS 1.3 e os CipherSpecs de alias poderão ser usados.

Valores de CipherSpec padrão ativados no IBM MQ

Multi V 9.1.1

Na configuração padrão, o IBM MQ fornece suporte para o protocolo TLS 1.2 e vários algoritmos criptográficos usando CipherSpecs. Para fins de compatibilidade, o IBM MQ também pode ser configurado para usar protocolos SSL 3.0 e TLS 1.0 e vários algoritmos criptográficos que são conhecidos por serem fracos ou suscetíveis a vulnerabilidades de segurança. A lista de CipherSpecs que estão ativados na configuração padrão pode ser mudada pela aplicação da manutenção.

É possível configurar o IBM MQ para restringir ou permitir o uso de CipherSpecs usando os controles a seguir:

- permitir somente os CipherSpecs compatíveis com o FIPS 140-2 usando SSLFIPS.
- ULW permitir somente os CipherSpecs compatíveis com o NSA Suite B usando SUITEB.
- ULW permitir uma lista customizada de CipherSpecs usando **AllowedCipherSpecs** ou a variável de ambiente **AMQ_ALLOWED_CIPHERS**.
- ULW permitir o uso de CipherSpecs descontinuados usando **AllowWeakCipher** ou a variável de ambiente **AMQ_SSL_WEAK_CIPHER_ENABLE**.
- z/OS permitir o uso de CipherSpecs descontinuados usando instruções DD no CHINIT JCL.

Nota: Se você especificar uma lista customizada de CipherSpecs usando **AllowedCipherSpecs** ou **AMQ_ALLOWED_CIPHERS**, isso substituirá a ativação de quaisquer CipherSpecs descontinuados. Observe que, ao usar restrições de NSA Suite B ou FIPS 140-2 em combinação com uma lista CipherSpec customizada, deve-se assegurar-se de que a lista customizada contenha apenas CipherSpecs permitidos pelas configurações do Suite B ou FIPS 140-2.

Fornecendo uma lista customizada de CipherSpecs ativados em multiplataformas

Multi V 9.1.1

É possível fornecer um conjunto alternativo de CipherSpecs ativados para uso com os canais do IBM MQ, seja usando a variável de ambiente **AMQ_ALLOWED_CIPHERS** ou o atributo de sub-rotina SSL **AllowedCipherSpecs** do arquivo `.ini`. Você pode desejar usar essa configuração para restringir os listeners do IBM MQ de aceitar solicitações de início de canal recebidas, a menos que eles usem um dos CipherSpecs nomeados. Essa funcionalidade pode ser usada para controlar os CipherSpecs que são incluídos nos CipherSpecs ANY*.

A variável de ambiente **AMQ_ALLOWED_CIPHERS** ou o atributo de sub-rotina SSL **AllowedCipherSpecs** aceita:

- Um nome de CipherSpec único ou
- Uma lista separada por vírgula de nomes de IBM MQ CipherSpec para ativar novamente ou
- O valor especial de ALL, representando todos os CipherSpecs (não recomendado).

Nota: Ativar especificações de código **ALL** não é recomendado, pois isso ativará os protocolos SSL 3.0 e TLS 1.0 e um grande número de algoritmos criptográficos fracos.

Se essa configuração estiver definida, ela substituirá a lista de CipherSpec padrão e fará com que o IBM MQ ignore as configurações de descontinuação de cifra fraca (veja abaixo):

- Os listeners do IBM MQ aceitarão somente as propostas de SSL/TLS que usam um dos CipherSpecs nomeados.
- Os canais do IBM MQ permitirão somente um valor de SSLCIPH em branco ou um dos CipherSpecs nomeados.
- A conclusão dos valores de SSLCIPH da guia **runmqsc** restringe os valores de conclusão a um dos CipherSpecs nomeados.

Por exemplo, se você quer apenas permitir que canais sejam definidos/alterados e que listeners aceitem ECDHE_RSA_AES_128_GCM_SHA256 ou ECDHE_ECDSA_AES_256_GCM_SHA384, é possível configurar o seguinte no arquivo `qm.ini`:

```
SSL:
  AllowedCipherSpecs=ECDHE_RSA_AES_128_GCM_SHA256, ECDHE_ECDSA_AES_256_GCM_SHA384
```

Observe que as cifras usadas pelos canais AMQP ou MQTT podem ser restritas usando as configurações de arquivo java.security.

Ativando CipherSpecs descontinuados em multiplataformas

Multi

Por padrão, você não tem permissão para especificar um CipherSpec descontinuado em uma definição de canal. Se você tentar especificar um CipherSpec descontinuado em Multiplataformas, receberá a mensagem AMQ8242: definição de SSLCIPH incorreta e PCF retorna MQRCCF_SSL_CIPHER_SPEC_ERROR.

Não é possível iniciar um canal com um CipherSpec descontinuado. Se você tentar fazer isso com um CipherSpec descontinuado, o sistema retornará MQCC_FAILED (2), juntamente com um **Reason** de MQRC_SSL_INITIALIZATION_ERROR (2393) para o cliente.

É possível re-ativar uma ou mais das CipherSpecs descontinuadas para definição de canais, no tempo de execução no servidor, configurando a variável de ambiente **AMQ_SSL_WEAK_CIPHER_ENABLE**.

A variável de ambiente **AMQ_SSL_WEAK_CIPHER_ENABLE** aceita:

- Um nome de CipherSpec único ou
- Uma lista separada por vírgula de nomes de IBM MQ CipherSpec para ativar novamente ou
- O valor especial de ALL, representando todos os CipherSpecs (não recomendado).

Nota: Reativar especificações de código ALL não é recomendado, pois isso ativará os protocolos SSL 3.0 e TLS 1.0 e um grande número de algoritmos criptográficos fracos.

Por exemplo, se você desejar ativar novamente ECDHE_RSA_RC4_128_SHA256, configure a seguinte variável de ambiente:

```
export AMQ_SSL_WEAK_CIPHER_ENABLE=ECDHE_RSA_RC4_128_SHA256
```

ou, alternativamente mude a sub-rotina SSL no arquivo qm.ini configurando:

```
SSL:
  AllowTLSV1=Y
  AllowWeakCipherSpec=ECDHE_RSA_RC4_128_SHA256
```

Ativando CipherSpecs descontinuados no z/OS

z/OS

Por padrão, você não tem permissão para especificar um CipherSpec descontinuado em uma definição de canal. Se você tentar especificar um CipherSpec descontinuado no z/OS, receberá a mensagem CSQM102E ou a mensagem CSQX674E.

Para ativar cipherspecs fracos (descontinuados), você precisa definir a instrução DD a seguir na JCL CHINIT:

```
JCL: //CSQXWEAK DD DUMMY
```

Nota: Nem todos os CipherSpecs descontinuados requerem o uso dessa instrução DD, consulte a nota 11 na tabela dentro de "CipherSpecs descontinuado" na página 433

Para ativar o protocolo SSL 3.0 descontinuado, também é necessário definir a instrução DD a seguir na JCL CHINIT:

```
JCL: //CSQXSSL3 DD DUMMY
```

V 9.1.0 Para ativar o protocolo TLS 1.0 descontinuado, também é necessário definir a instrução DD a seguir na JCL CHINIT:

```
JCL: //TLS10ON DD DUMMY
```

Observe que o nome do cartão DD é TLS100N, para significar que o TLS 1.0 está ATIVADO e não TLS100N.

Para DESATIVAR o TLS 1.0, use a instrução a seguir:

```
JCL: //TLS10OFF DD DUMMY
```

Se você não quiser negociar com o listener usando especificações de cifras fracas ou quebradas, será necessário definir a instrução DD a seguir no JCL CHINIT:

```
JCL: //WCIPSOFF DD DUMMY
```

Se desejar negociar apenas com o listener usando as especificações de cifra listadas na lista de especificações de cifra padrão **System SSL** , será necessário definir a instrução DD a seguir na JCL CHINIT:

```
JCL: //GSKDCIPS DD DUMMY
```

CipherSpecs de nível mínimo versus nível fixo

ULW V 9.1.4

O IBM MQ suporta dois tipos diferentes de CipherSpecs:

- CipherSpecs de **nível mínimo** são aqueles que não configuram um limite superior, por exemplo ANY, ANY_TLS12_OR_HIGHER ou ANY_TLS13_OR_HIGHER.
- CipherSpecs de **nível fixo** são aqueles que identificam um protocolo específico, por exemplo ANY_TLS12 e ANY_TLS13 ou um algoritmo específico, tal como ECDHE_ECDSA_3DES_EDE_CBC_SHA256

Para maximizar a simplicidade da configuração mantendo a segurança, o uso de CipherSpecs de **nível mínimo** é recomendado em ambos os lados do canal. Isso permite que suas comunicações suportem e usem automaticamente uma versão mais alta do protocolo TLS quando os dois lados suportam uma nova versão sem a necessidade de mudar a configuração dos dois lados.

Usando um **nível mínimo** CipherSpec no lado inicial, mas um **nível fixo** CipherSpec no lado de recebimento poderia resultar na conexão sendo rejeitada e mensagens AMQ9631 e AMQ9641 sendo emitidas.

Consulte “Relacionamento entre as configurações do CipherSpec de alias” na página 436 para tabelas contendo resultados diferentes para configurações de Alias CipherSpec .

Conceitos relacionados

“Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45
Este tópico fornece informações sobre como escolher os certificados digitais e do CipherSpecs para sua política de segurança, delineando o relacionamento entre os certificados digitais e de CipherSpecs no IBM MQ.

“CipherSpecs e CipherSuites” na página 19
Os protocolos de segurança criptográficos devem concordar sobre os algoritmos usados por uma conexão segura. CipherSpecs e CipherSuites definem combinações específicas de algoritmos.

“Configurando o IBM MQ para o Conjunto B” na página 42
O IBM MQ pode ser configurado para operar em conformidade com o padrão do Conjunto B da NSA nas plataformas Windows, UNIX and Linux.

“FIPS (Federal Information Processing Standards)” na página 33
Este tópico apresenta o Federal Information Processing Standards (FIPS) Cryptomodule Validation Program do National Institute of Standards and Technology dos EUA e as funções criptográficas que podem ser usadas nos canais TLS.

Tarefas relacionadas

Migrando configurações de segurança existentes para usar o CipherSpec ANY_TLS12_OR_HIGHER

Referências relacionadas
DEFINE CHANNEL
ALTER CHANNEL
Alterar, Copiar e Criar Canal

ULW AES-restrição de cifra doGCM

Um guia para as restrições que são impostas às cifras AES-GCM quando usadas para a criptografia TLS. Essas restrições são impostas pelas organizações IETF e NIST e requerem que a mesma chave de sessão não seja usada para transferir com segurança mais de 2 registros TLS$^{24.5}$ ao usar cifras AES-GCM .

Para obter mais informações sobre essas restrições, consulte a Seção RFC 9325 4.4 Limites no Uso da Chave e Seção RFC 8446 5.5

O IBM MQ não implementa a funcionalidade criptográfica diretamente Em vez disso, várias bibliotecas criptográficas diferentes são usadas para fornecer a funcionalidade TLS e Advanced Message Security . Nos sistemas operacionais Windows, Linuxe AIX , a biblioteca criptográfica que o IBM MQ usa é GSKit Para aplicativos, as bibliotecas C e .NET não gerenciadas usam GSKit para funcionalidade criptográfica. A implementação dos algoritmos de criptografia AES-GCM por GSKit inclui as restrições especificadas pelo grupo de padrões. Além disso, essas restrições são ativadas por padrão.. Dessa forma, a IBM MQ comunicação TLS, ao usar cifras AES-GCM , será finalizada se mais de 2 registros TLS$^{24.5}$ forem transmitidos usando a mesma chave de sessão.

Nota: Essa restrição não está presente nas plataformas IBM i, IBM Z ou IBM MQ for HPE NonStop ou aplicativos Java/JMSgerenciados .NET porque bibliotecas criptográficas diferentes são usadas e essas bibliotecas não implementaram a mesma restrição.

Se um canal IBM MQ permanecer em execução por tempo suficiente para que mais de 2 registros TLS$^{24.5}$ sejam transmitidos usando a mesma chave de sessão, a biblioteca criptográfica subjacente terminará a conexão. Isso faz o canal ser finalizado e uma mensagem de erro AMQ9288E é gerada. Os aplicativos que tiverem sua comunicação finalizada dessa maneira receberão um código de retorno `MQRC_CONNECTION_BROKEN` de qualquer operação IBM MQ que estiver sendo executada

A finalização da conexão pode ser executada em qualquer extremidade da comunicação, mas apenas em extremidades que estão usando GSKit para a funcionalidade criptográfica.

Conselhos para atenuar a restrição

Algumas opções para como evitar ou manipular comunicações que são finalizadas devido a essa restrição são as seguintes::

Usar clientes reconectáveis
Os aplicativos podem ser configurados para tentar automaticamente uma reconexão, se uma conexão falhar. Isso inclui conexões que são finalizadas devido à restrição do GCM Quando configurado para reconexão, o aplicativo cliente é restaurado automaticamente em qualquer ponto de falha e quaisquer identificadores para objetos abertos são restaurados Isso é feito sem retornar para o código do aplicativo.

Para obter mais informações, consulte Reconexão automática do cliente.

Configure um valor de reconfiguração de chave secreta
IBM MQ pode ser configurado para solicitar uma reconfiguração de chave de sessão após um número configurável de bytes ter sido transferido através de um canal Ao atingir esse limite, o IBM MQ solicita que a camada de criptografia execute uma reconfiguração de chave de sessão, resultando em uma nova chave de sessão.

É importante observar que o valor especificado é o número de bytes transferidos, que está relacionado ao tamanho das mensagens enviadas pelo IBM MQ. A restrição está no número de registros TLS enviados. Não há um mapeamento direto entre bytes de mensagens e registros TLS, pois um registro TLS pode enviar um número máximo de bytes dependentes da Maximum Transmission Unit (MTU) da rede. Quaisquer mensagens enviadas maiores que esse valor são transmitidas como diversos registros TLS. O valor de MTU varia entre as redes. Além disso, há

outras razões pelas quais um registro TLS pode precisar ser enviado fora da transmissão de dados de mensagem do IBM MQ , por exemplo, IBM MQ Verificações de pulsação, alertas TLS, outras mensagens de protocolo IBM MQ Esses registros TLS adicionais contam para o número máximo de registros TLS, mas não são contados no valor de reconfiguração de chave secreta IBM MQ .

Reconfigurar regularmente uma chave de sessão usando a reconfiguração de chave secreta pode evitar que o canal seja finalizado devido à restrição AES-GCM .

Para obter mais informações, consulte Reconfigurando chaves secretas SSL e TLS.

V 9.1.4 **Usar especificações de código TLS 1.3**

Embora a restrição AES-GCM ainda esteja presente ao usar o protocolo TLS 1.3 , o protocolo TLS 1.3 suporta a execução automática de uma reconfiguração de chave de sessão sem a necessidade de interromper as comunicações TLS Isso permite que o GSKit gerencie a reconfiguração da chave de sessão quando for necessário sem IBM MQ precisar solicitar uma reconfiguração de chave secreta.

Para obter mais informações, consulte Usando o TLS 1.3 em IBM MQ em “Ativando CipherSpecs” na página 423

Desativar a restrição AES-GCM

Se necessário, a restrição poderá ser desativada configurando a variável de ambiente **GSK_ENFORCE_GCM_RESTRICTION=GSK_FALSE** para desativar a restrição AES-GCM . Isso permite que qualquer número de registros TLS seja enviado usando a mesma chave de sessão. Se escolher essa mitigação, a variável de ambiente deverá ser configurada em cada extremidade de comunicação que usa GSKit para comunicações seguras.

Aviso: Essa opção não é recomendada porque, após mais de 2 registros TLS[24.5] terem sido enviados, é possível que os invasores executem a análise nos registros enviados para determinar a chave de sessão em uso. Quando a chave de sessão tiver sido determinada, toda a comunicação existente e futura usando essa chave de sessão será comprometida.

CipherSpecs descontinuado

Uma lista de CipherSpecs descontinuados que é possível usar com o IBM MQ, se necessário.

Para obter informações sobre a ativação de CipherSpecs descontinuados, consulte “Ativando CipherSpecs descontinuados em multiplataformas” na página 430 ou “Ativando CipherSpecs descontinuados no z/OS” na página 430.

Os CipherSpecs descontinuados que podem ser usados com suporte de TLS do IBM MQ são listados na tabela a seguir.

Tabela 75. CipherSpecs descontinuados que podem ser reativados para uso com o IBM MQ

Suporte da plataforma “1” na página 436	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS “2” na página 436	Conjunto B	Atualizar quando descontinuado
CipherSpecs para o SSL 3.0								
IBM i	AES_SHA_US “3” na página 436	002F	SSL 3.0	SHA-1	AES (128)	No	No	9.0.0.0
Todos(as)	DES_SHA_EXPORT “3” na página 436 “4” na página 436 “5” na página 436	0009	SSL 3.0	SHA-1	DES (56)	No	No	9.0.0.0
ULW	DES_SHA_EXPORT1024 “3” na página 436 “6” na página 436	0062	SSL 3.0	SHA-1	DES (56)	No	No	9.0.0.0

Tabela 75. CipherSpecs descontinuados que podem ser reativados para uso com o IBM MQ (continuação)

Suporte da plataforma "1" na página 436	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS "2" na página 436	Conjunto B	Atualizar quando descontinuado
ULW	FIPS_WITH_DES_CBC_SHA "3" na página 436	FEFE	SSL 3.0	SHA-1	DES (56)	Não "7" na página 436	No	9.0.0.0
ULW	FIPS_WITH_3DES_EDE_CBC_SHA "3" na página 436	FEFF	SSL 3.0	SHA-1	3DES (168)	Não "8" na página 436	No	9.0.0.1 e 9.0.1
Todos(as)	NULL_MD5 "3" na página 436	0001	SSL 3.0	MD5	Nenhum	No	No	9.0.0.1
Todos(as)	NULL_SHA "3" na página 436	0002	SSL 3.0	SHA-1	Nenhum	No	No	9.0.0.1
Todos(as)	RC2_MD5_EXPORT "3" na página 436 "4" na página 436 "5" na página 436	0006	SSL 3.0	MD5	RC2 (40)	No	No	9.0.0.0
Todos(as)	RC4_MD5_EXPORT "4" na página 436 "3" na página 436	0003	SSL 3.0	MD5	RC4 (40)	No	No	9.0.0.0
Todos(as)	RC4_MD5_US "3" na página 436	0004	SSL 3.0	MD5	RC4 (128).	No	No	9.0.0.0
Todos(as)	RC4_SHA_US "3" na página 436 "5" na página 436	0005	SSL 3.0	SHA-1	RC4 (128).	No	No	9.0.0.0
ULW	RC4_56_SHA_EXPORT1024 "3" na página 436 "6" na página 436	0064	SSL 3.0	SHA-1	RC4 (56)	No	No	9.0.0.0
Todos(as)	TRIPLE_DES_SHA_US "3" na página 436 "5" na página 436	000A	SSL 3.0	SHA-1	3DES (168)	No	No	9.0.0.1 e 9.0.1
CipherSpecs para o TLS 1.0								
IBM i	TLS_RSA_EXPORT_WITH_RC2_40_MD5 "3" na página 436	0006	TLS 1.0	MD5	RC2 (40)	No	No	9.0.0.0
IBM i	TLS_RSA_EXPORT_WITH_RC4_40_MD5 "3" na página 436 "4" na página 436	0003	TLS 1.0	MD5	RC4 (40)	No	No	9.0.0.0
Todos(as)	TLS_RSA_WITH_DES_CBC_SHA "3" na página 436	0009	TLS 1.0	SHA-1	DES (56)	Não "9" na página 436	No	9.0.0.0
IBM i	TLS_RSA_WITH_NULL_MD5 "3" na página 436	0001	TLS 1.0	MD5	Nenhum	No	No	9.0.0.1
IBM i	TLS_RSA_WITH_NULL_SHA "3" na página 436	0002	TLS 1.0	SHA-1	Nenhum	No	No	9.0.0.1

Tabela 75. CipherSpecs descontinuados que podem ser reativados para uso com o IBM MQ (continuação)

Suporte da plataforma "1" na página 436	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS "2" na página 436	Conjunto B	Atualizar quando descontinuado
IBM i	TLS_RSA_WITH_RC4_128_MD5 "3" na página 436	0004	TLS 1.0	MD5	RC4 (128).	No	No	9.0.0.0
z/OS ULW	TLS_RSA_WITH_AES_128_CBC_SHA "10" na página 436	002F	TLS 1.0	SHA-1	AES (128)	Sim	No	9.0.5
z/OS ULW	TLS_RSA_WITH_AES_256_CBC_SHA "6" na página 436 "10" na página 436	0035	TLS 1.0	SHA-1	AES (256)	Sim	No	9.0.5
Todos(as)	TLS_RSA_WITH_3DES_EDE_CBC_SHA	000A	TLS 1.0	SHA-1	3DES (168)	Sim	No	9.0.0.1 e 9.0.1
CipherSpecs para o TLS 1.2								
ULW	ECDHE_ECDSA_NULL_SHA256 "3" na página 436	C006	TLS 1.2	SHA-1	Nenhum	No	No	9.0.0.1
ULW	ECDHE_ECDSA_RC4_128_SHA256 "3" na página 436	C007	TLS 1.2	SHA-1	RC4 (128).	No	No	9.0.0.0
ULW IBM i	ECDHE_RSA_NULL_SHA256 "3" na página 436	C010	TLS 1.2	SHA-1	Nenhum	No	No	9.0.0.1
ULW IBM i	ECDHE_RSA_RC4_128_SHA256 "3" na página 436	C011	TLS 1.2	SHA-1	RC4 (128).	No	No	9.0.0.0
ULW	TLS_RSA_WITH_NULL_NULL "3" na página 436	0000	TLS 1.2	Nenhum	Nenhum	No	No	9.0.0.1
Todos(as)	TLS_RSA_WITH_NULL_SHA256 "3" na página 436	003B	TLS 1.2	SHA-256	Nenhum	No	No	9.0.0.1
ULW	TLS_RSA_WITH_RC4_128_SHA256 "3" na página 436	0005	TLS 1.2	SHA-1	RC4 (128).	No	No	9.0.0.0
ULW	ECDHE_ECDSA_3DES_EDE_CBC_SHA256	C0008	TLS 1.2	SHA-1	3DES (168)	Sim	No	9.0.0.1 e 9.0.1
ULW IBM i	ECDHE_RSA_3DES_EDE_CBC_SHA256	C012	TLS 1.2	SHA-1	3DES (168)	Sim	No	9.0.0.1 e 9.0.1

Tabela 75. CipherSpecs descontinuados que podem ser reativados para uso com o IBM MQ (continuação)

Suporte da plataforma "1" na página 436	Nome do CipherSpec	Código Hex	Protocolo utilizado	Integridade de dados	Algoritmo de criptografia (bits de criptografia)	FIPS "2" na página 436	Conjunto B	Atualizar quando descontinuado

Notas:

1. Para obter uma lista de plataformas cobertas por cada ícone da plataforma, consulte Liberação e ícones de plataforma na documentação do produto.
2. Especifica se o CipherSpec é certificado por FIPS em uma plataforma certificada por FIPS. Consulte Federal Information Processing Standards (FIPS) para obter uma explicação do FIPS.
3. ULW Esses CipherSpecs são desativados quando o TLS 1.3 é ativado (por meio da propriedade AllowTLSV13 no `qm.ini`).

   z/OS Os gerenciadores de filas criados em IBM MQ for z/OS 9.2.0 ou posterior ativam o TLS 1.3 por padrão, que desativa esses CipherSpecs. Será possível ativar esses CipherSpecs, se necessário, desligando o TLS V1.3. Isso é feito incluindo **AllowTLSV13**=*FALSE* à sub-rotina TransportSecurity do conjunto de dados QMINI no gerenciador de filas JCL. Os gerenciadores de filas migrados para o IBM MQ for z/OS 9.2.0 de uma versão anterior não têm o TLS 1.3 ativado por padrão e, portanto, têm esses CipherSpecs ativados.
4. O tamanho de chave de handshake máximo é 512 bits. Caso nenhum dos certificados trocados durante o protocolo de reconhecimento do SSL tenha um tamanho de chave superior a 512 bits, uma chave de 512 bits temporária será gerada para uso durante o protocolo de reconhecimento.
5. Esses CipherSpecs não são mais suportados pelo IBM MQ classes for Java ou IBM MQ classes for JMS. Para obter mais informações, consulte SSL/TLS CipherSpecs e CipherSuites em IBM MQ classes for Java ou SSL/TLS CipherSpecs e CipherSuites em IBM MQ classes for JMS.
6. O tamanho de chave de handshake é 1024 bits.
7. Este CipherSpec era certificado FIPS 140-2 antes de 19 de Maio de 2007. O nome do `FIPS_WITH_DES_CBC_SHA` é histórico e reflete o fato de que esse CipherSpec era anteriormente (mas não é mais) compatível com FIPS. Esse CipherSpec foi descontinuado e seu uso não é recomendado.
8. O nome do `FIPS_WITH_3DES_EDE_CBC_SHA` é histórico e reflete o fato de que esse CipherSpec era anteriormente (mas não é mais) compatível com FIPS. O uso deste CipherSpec está descontinuado.
9. Este CipherSpec era certificado FIPS 140-2 antes de 19 de Maio de 2007.
10. z/OS Reativar apenas esses CipherSpecs não requer o uso da instrução CSQXWEAK DD.

Conceitos relacionados

"Certificados digitais e compatibilidade de CipherSpec no IBM MQ" na página 45
Este tópico fornece informações sobre como escolher os certificados digitais e do CipherSpecs para sua política de segurança, delineando o relacionamento entre os certificados digitais e de CipherSpecs no IBM MQ.

Referências relacionadas

DEFINE CHANNEL
ALTER CHANNEL

Relacionamento entre as configurações do CipherSpec de alias

As tabelas a seguir mostram o comportamento esperado quando TLS1.3 não está ativado no cliente, no gerenciador de fila ou em ambos e quando TLS1.3 está ativado no cliente e no gerenciador de filas.

As tabelas a seguir mostram o relacionamento entre diferentes configurações de CipherSpec de alias e o resultado esperado. Tabela 76 na página 437 mostra o comportamento esperado quando o TLS 1.3 não está ativado no cliente, no servidor ou em ambos. A Tabela 77 na página 437 mostra o comportamento esperado quando o TLS 1.3 está ativado no cliente e no servidor Em ambos os casos, o CipherSpecs para o cliente é mostrado no eixo Y da tabela e o CipherSpecs para o servidor é mostrado no eixo X da tabela.

Nota: Em que a entrada indica *provável falha* , isso ocorre porque, se o TLS 1.3 ou TLS 1.2 CipherSpec específico usado for o CipherSpec mais forte para o cliente e o gerenciador de filas, o handshake TLS será resolvido para usá-lo e, portanto, corresponderá ao valor SSCIPH do canal.

Tabela 76. Comportamento esperado quando o TLS 1.3 não está ativado no cliente, no servidor ou em ambos

	Servidor			
Client	**CipherSpec específico do TLS 1.2**	**QUALQUER**	**ANY_ TLS12**	**ANY_TLS12_ OR_HIGHER**
CipherSpec específico do TLS 1.2	Connects	Connects	Connects	Connects
qualquer um	*Com probabilidade de falha*	Connects	Connects	Connects
ANY_ TLS12	*Com probabilidade de falha*	Connects	Connects	Connects
ANY_TLS12_ OR_HIGHER	*Com probabilidade de falha*	Connects	Connects	Connects

Tabela 77. Comportamento esperado quando o TLS 1.3 está ativado no cliente e no servidor

	Servidor						
Client	**CipherSpec específico do TLS 1.2**	**CipherSpec específico do TLS 1.3**	**QUALQUER**	**ANY_TLS 12**	**ANY_TLS 13**	**ANY_TLS12_ OR_HIGHER**	**ANY_TLS13_ OR_HIGHER**
CipherSpec específico do TLS 1.2	Connects	**Com falhas**	Connects	Connects	**Com falhas**	Connects	**Com falhas**
CipherSpec específico do TLS 1.3	**Com falhas**	Connects	Connects	**Com falhas**	Connects	Connects	Connects
qualquer um	**Com falhas**	*Com probabilidade de falha*	Connects	**Com falhas**	Connects	Connects	Connects
ANY_TLS12	*Com probabilidade de falha*	**Com falhas**	Connects	Connects	**Com falhas**	Connects	**Com falhas**
ANY_TLS13	**Com falhas**	*Com probabilidade de falha*	Connects	**Com falhas**	Connects	Connects	Connects
ANY_TLS12_ OR_HIGHER	**Com falhas**	*Com probabilidade de falha*	Connects	**Com falhas**	Connects	Connects	Connects

Tabela 77. Comportamento esperado quando o TLS 1.3 está ativado no cliente e no servidor (continuação)							
	Servidor						
Client	**CipherSpec específico do TLS 1.2**	**CipherSpec específico do TLS 1.3**	**QUALQUER**	**ANY_TLS12**	**ANY_TLS13**	**ANY_TLS12_OR_HIGHER**	**ANY_TLS13_OR_HIGHER**
ANY_TLS13_OR_HIGHER	**Com falhas**	*Com probabilidade de falha*	Connects	**Com falhas**	Connects	Connects	Connects

Conceitos relacionados

"Certificados digitais e compatibilidade de CipherSpec no IBM MQ" na página 45
Este tópico fornece informações sobre como escolher os certificados digitais e do CipherSpecs para sua política de segurança, delineando o relacionamento entre os certificados digitais e de CipherSpecs no IBM MQ.

"CipherSpecs e CipherSuites" na página 19
Os protocolos de segurança criptográficos devem concordar sobre os algoritmos usados por uma conexão segura. CipherSpecs e CipherSuites definem combinações específicas de algoritmos.

"Ativando CipherSpecs" na página 423
Ative um CipherSpec usando o parâmetro **SSLCIPH** no comando MQSC **DEFINE CHANNEL** ou no comando MQSC **ALTER CHANNEL** .

Tarefas relacionadas

Migrando configurações de segurança existentes para usar o CipherSpec ANY_TLS12_OR_HIGHER

Obtendo informações sobre CipherSpecs usando o IBM MQ Explorer

É possível usar o IBM MQ Explorer para exibir descrições de CipherSpecs.

Utilize o seguinte procedimento para obter informações sobre o CipherSpecs no "Ativando CipherSpecs" na página 423:

1. Abra o IBM MQ Explorer e expanda a pasta **Gerenciadores de Filas**.
2. Certifique-se de que iniciou o gerenciador de filas.
3. Selecione o Gerenciador de Filas com o qual deseja trabalhar e clique em **Canais**.
4. Clique com o botão direito no canal que deseja trabalhar e selecione **Propriedades**.
5. Selecione a página de propriedades **SSL**.
6. Selecione da lista o CipherSpec com o qual quer trabalhar. Uma descrição é exibida na janela abaixo da lista.

Alternativas para a Especificação do CipherSpecs

Para as plataformas em que o sistema operacional fornece suporte do TLS, é possível que o sistema suporte novos CipherSpecs. Você pode especificar um novo CipherSpec com o parâmetro SSLCIPH, mas o valor que você fornecer dependerá da sua plataforma.

Nota: Esta seção não se aplica aos sistemas UNIX, Linux ou Windows, porque os CipherSpecs são fornecidos com o produto IBM MQ, portanto, novos CipherSpecs não se tornam disponíveis depois do envio.

Para aquelas plataformas em que o sistema operacional fornece suporte do TLS, é possível que o seu sistema suporte os novos CipherSpecs que não estão incluídos em "Ativando CipherSpecs" na página 423. Você pode especificar um novo CipherSpec com o parâmetro SSLCIPH, mas o valor que você fornecer dependerá da sua plataforma. Em todos os casos, a especificação deve corresponder a um CipherSpec do TLS que seja válido e suportado pela versão de TLS que seu sistema está executando.

IBM i

Uma cadeia de dois caracteres que representa um valor hexadecimal.

Para obter mais informações sobre os valores permitidos, consulte o ponto três na seção Notas de uso de Configurar informações de caracteres para uma sessão segura.

Atenção: Não é necessário especificar valores de cifras hexadecimais no SSLCIPH, já que o valor não especifica claramente qual cifra será usada e a opção de qual protocolo será usado está indeterminada. A utilização de valores de cifras hexadecimais pode levar a erros de incompatibilidade de CipherSpec.

Você pode utilizar o comando CHGMQMCHL ou CRTMQMCHL para especificar o valor, por exemplo:

```
CRTMQMCHL CHLNAME(' channel name ') SSLCIPH(' hexadecimal value ')
```

Também é possível usar o comando ALTER QMGR MQSC para configurar o parâmetro **SSLCIPH**.

z/OS

Uma sequência de quatro caracteres que representa um valor hexadecimal. Os códigos hexadecimais correspondem aos valores definidos no protocolo TLS.

Para obter mais informações, consulte as Definições do conjunto de cifras onde há uma lista de todas as especificações de cifras TLS 1.0, TLS 1.2 e TLS 1.3 na forma de códigos hexadecimais de 4 dígitos.

Considerações para clusters do IBM MQ

Com clusters do IBM MQ é mais seguro usar os nomes de CipherSpec no “Ativando CipherSpecs” na página 423. Se você usar uma especificação alternativa, tenha em mente que a especificação pode não ser válida em outras plataformas. Para obter informações adicionais, consulte “SSL/TLS e clusters” na página 467.

Especificando um CipherSpec para um IBM MQ MQI client

Você tem três opções para especificar um CipherSpec para um IBM MQ MQI client.

Estas opções são as seguintes:

- Utilizando uma tabela de definição de canais
- Usando o campo SSLCipherSpec na estrutura MQCD, no MQCD_VERSION_7 ou mais recente, em uma chamada MQCONNX.
- Usando o Active Directory (em sistemas Windows com suporte ao Active Directory)

Especificando um CipherSuite com o IBM MQ classes for Java e IBM MQ classes for JMS

O IBM MQ classes for Java e o IBM MQ classes for JMS especificam CipherSuites diferentemente de outras plataformas.

Para obter informações sobre como especificar um CipherSuite com o IBM MQ classes for Java, consulte Suporte de Segurança da Camada de Transporte (TLS) para o Java

Para obter informações sobre como especificar um CipherSuite com o IBM MQ classes for JMS, consulte Usando a Segurança da Camada de Transporte (TLS) com o IBM MQ classes for JMS

Especificando um CipherSpec para IBM MQ.NET

Para o IBM MQ.NET é possível especificar o CipherSpec usando a classe MQEnvironment ou usando o MQC.SSL_CIPHER_SPEC_PROPERTY na hashtable das propriedades da conexão.

Para obter informações sobre como especificar um CipherSpec para o cliente não gerenciado do .NET, consulte Ativando o TLS para o cliente não gerenciado do .NET

Para obter informações sobre como especificar um CipherSpec para o cliente gerenciado do .NET, consulte Suporte de CipherSpec para cliente gerenciado do .NET

z/OS Uso de AT-TLS com o IBM MQ for z/OS

A Segurança da Camada de Transporte Transparente do Aplicativo (AT-TLS) fornece suporte de TLS para aplicativos z/OS sem que esses aplicativos tenham que implementar o suporte de TLS, ou até mesmo saber que o TLS está sendo usado. O AT-TLS está disponível somente no z/OS.

O AT-TLS pode ser usado com todas as versões do IBM MQ for z/OS.

Antes de fazer uso de AT-TLS com o IBM MQ for z/OS, certifique-se de entender o “Restrições” na página 442 envolvido.

Para usar a Segurança da Camada de Transporte Transparente do Aplicativo, defina instruções de política contendo um conjunto de regras que são usadas pelo z/OS Communications Server para decidir quais conexões TCP/IP têm o TLS ativado de forma transparente.

O IBM MQ for z/OS tem sua própria implementação TLS, que requer que os canais tenham o parâmetro SSLCIPH configurado com uma CipherSpec suportada.

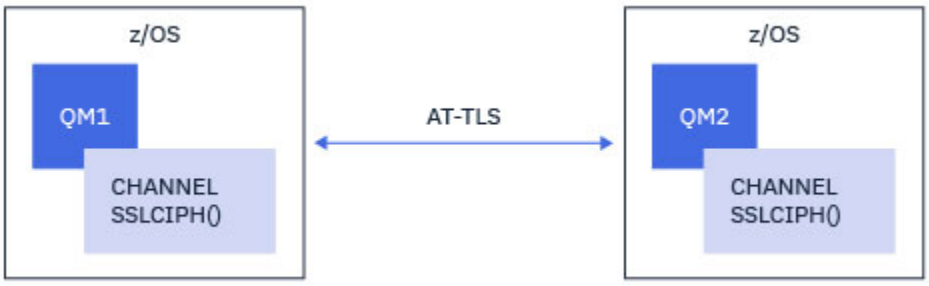
Ao decidir ativar o TLS em um canal, o administrador do IBM MQ pode decidir usar o AT-TLS ou o TLS do IBM MQ. A decisão é frequentemente feita com base em se o AT-TLS é usado para outro middleware ou por causa de implicações de desempenho. Para uma comparação básica do desempenho do AT-TLS e do TLS do IBM MQ, consulte MP16: Planejamento de capacidade e ajuste para o IBM MQ for z/OS.

Situações

O uso do AT-TLS com o IBM MQ é suportado nos cenários a seguir:

Cenário 1

Entre dois Gerenciadores de Filas do IBM MQ for z/OS em que ambos os lados do canal usam AT-TLS. Ou seja, nenhum canal especifica o atributo SSLCIPH. Esta abordagem pode ser usada com qualquer canal de mensagem.

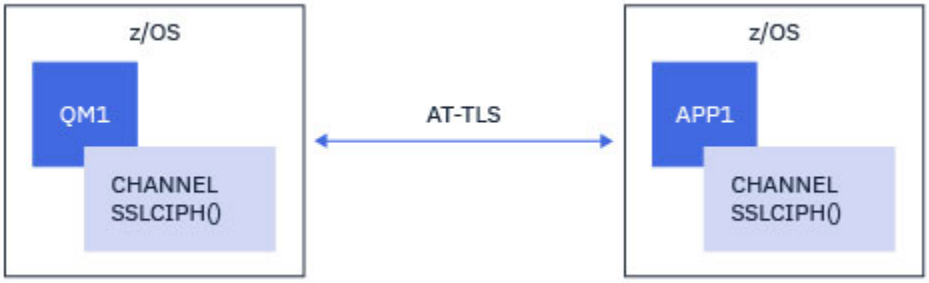


A implementação deste cenário consiste na definição de duas políticas de AT-TLS, uma para cada lado do canal. Essas políticas são as mesmas usadas com o Cenário 3.

Por exemplo, se o canal estivesse mudando do uso de uma única CipherSpec denominada para o AT-TLS, o canal de saída usaria a política do “Configurando o AT-TLS em um canal de saída por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec denominado” na página 443 e o canal de entrada usaria a política do “Configurando o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec de nominado” na página 446.

Cenário 2

Entre um Gerenciador de Filas do IBM MQ for z/OS e um aplicativo cliente IBM MQ Java executando no z/OS em que ambos os lados do canal usam AT-TLS. Ou seja, nem o canal de conexão do servidor, nem o canal de conexão do cliente especifica o atributo SSLCIPH.

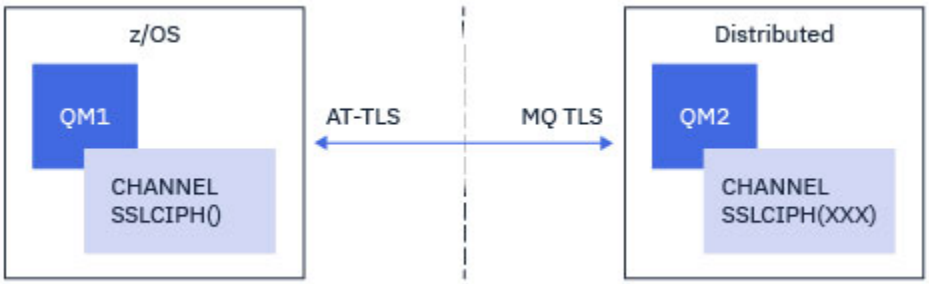


A implementação deste cenário consiste na definição de duas políticas de AT-TLS, uma para cada lado do canal. Essas políticas são as mesmas usadas com o Cenário 3.

Por exemplo, se o canal estivesse mudando do uso de uma única CipherSpec denominada para o AT-TLS, o canal de conexão do cliente usaria a política do "Configurando o AT-TLS em um canal de saída por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec denominado" na página 443 e o canal de conexão do servidor usaria a política do "Configurando o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec de nominado" na página 446.

Cenário 3

Entre um Gerenciador de Filas do IBM MQ for z/OS e um Gerenciador de Filas em execução no IBM MQ for Multiplatforms, em que o Gerenciador de Filas do IBM MQ for z/OS usa o AT-TLS e o Gerenciador de Filas do IBM MQ for Multiplatforms usa o TLS do IBM MQ. Isto se aplica a todos os tipos de canal de mensagens diferentes do emissor de cluster e do receptor de cluster.

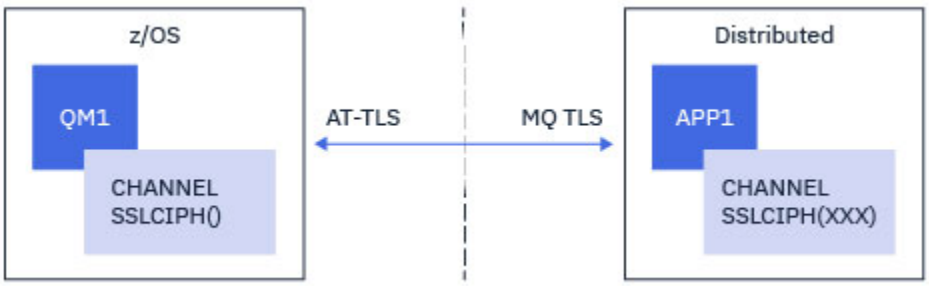


Consulte "Configurando o AT-TLS em um canal de saída por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec denominado" na página 443 para um exemplo de configuração de AT-TLS para canais de saída do Gerenciador de Filas do IBM MQ for z/OS para o Gerenciador de Filas do IBM MQ for Multiplatforms e "Configurando o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec de nominado" na página 446 para um exemplo de configuração de AT-TLS para canais de entrada do Gerenciador de Filas do IBM MQ for Multiplatforms para o Gerenciador de Filas do IBM MQ for z/OS.

A mesma configuração de AT-TLS pode ser usada quando ambos os Gerenciadores de Filas estão no z/OS, mas o Gerenciador de Filas no lado direito não foi configurado para usar o AT-TLS.

Cenário 4

Entre um Gerenciador de Filas do IBM MQ for z/OS e um aplicativo cliente em execução no IBM MQ for Multiplatforms, em que o Gerenciador de Filas do IBM MQ for z/OS usa AT-TLS e o aplicativo cliente usa o TLS do IBM MQ especificando o atributo SSLCIPH com uma CipherSpec única denominada.



Este cenário requer uma única política AT-TLS que atenda aos mesmos requisitos dos utilizados por um canal de mensagem de entrada; consulte “Configurando o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec de nominado” na página 446.

A mesma configuração de AT-TLS pode ser usada quando o aplicativo cliente é um aplicativo Java e também está em execução no z/OS, mas não foi configurado para usar o AT-TLS.

Restrições

O IBM MQ for z/OS não é ciente do AT-TLS, portanto, existem várias restrições que se aplicam com os cenários precedentes:

- O AT-TLS em combinação com o TLS do IBM MQ não funciona com canais emissores e receptores de cluster.
- Os Gerenciadores de Filas do IBM MQ for z/OS não são cientes de que estão usando o AT-TLS e não recebem nenhuma informação de certificado de seu Gerenciador de Filas ou cliente parceiro. Portanto, os atributos a seguir não têm efeito no lado do z/OS de um canal usando o AT-TLS:
  - Os atributos de canal SSLCAUTH e SSLPEER
  - O atributo SSLRKEYC do Gerenciador de Filas
  - Os atributos SSLPEERMAP de regras CHLAUTH
- O uso da renegociação de chave secreta do TLS requer que ambos os lados do canal usem o TLS do IBM MQ. Portanto, um Gerenciador de Filas do IBM MQ for Multiplatforms, ou cliente, não deve ter a renegociação de chave secreta do TLS ativada se estiver se conectando a um Gerenciador de Filas do IBM MQ for z/OS usando o AT-TLS.

  Para desativar a renegociação de chave secreta TLS para um gerenciador de filas, configure o parâmetro SSLRKEYC do gerenciador de filas para `0`. Para um cliente, configure o parâmetro relevante para `0` dependendo do tipo do cliente. Para obter detalhes sobre como fazer isso, consulte “Reconfigurando as chaves secretas SSL e TLS” na página 450.

Instruções de configuração de AT-TLS

O AT-TLS é configurado usando um conjunto de instruções. Os utilizados nos cenários documentados neste tópico são:

TTLSRule
Especifica um conjunto de critérios para correspondência de uma conexão TCP/IP com uma configuração de TLS. Isto, por sua vez, refere-se aos outros tipos de instrução.

TTLSGroupAction
Especifica se a `TTLSRule` de referência está ativado ou não.

TTLSEnvironmentAction
Especifica a configuração detalhada para a `TTLSRule` de referência e referencia uma série de outras instruções.

TTLSKeyringParms
Referencia o conjunto de chaves que deve ser usado pelo AT-TLS.

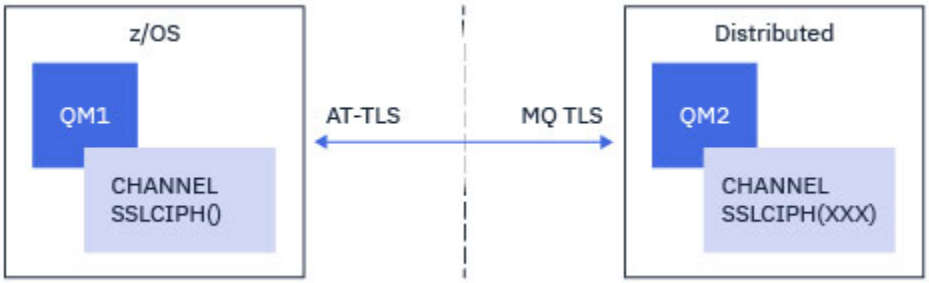
TTLSCipherParms
Define os conjuntos de cifras que devem ser usados.

TTLSEnvironmentAdvancedParms
Define quais protocolos TLS ou SSL estão ativados.

Atenção: Há outras Instruções de política AT-TLS com AT-TLS que não são documentadas aqui, e poderiam ser usadas com o IBM MQ dependendo da necessidade. No entanto, o IBM MQ somente foi testado com as políticas descritas neste tópico.

Configurando o AT-TLS em um canal de saída por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec denominado

Como você configura o AT-TLS em um canal de saída por meio de um Gerenciador de Filas IBM MQ for z/OS para um Gerenciador de Filas IBM MQ for Multiplatforms. Neste caso, o canal no Gerenciador de Filas z/OS é um canal emissor que não possui o conjunto de atributos SSLCIPH, e o canal no Gerenciador de Filas não z/OS é um canal receptor com o conjunto de atributos SSLCIPH configurado para um único CipherSpec denominado.



Neste exemplo, um par de canais emissor / receptor existente, que usa o TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec será ajustado para que o canal emissor use AT-TLS em vez de IBM MQ TLS.

Outros protocolos TLS e CipherSpecs podem ser usados fazendo pequenos ajustes na configuração. Outros tipos de canal de mensagens, além de canais emissores e receptores de cluster, poderiam ser usados sem alteração na configuração de AT-TLS.

Procedimento

Etapa 1: Pare o canal

Etapa 2: Crie e aplique uma política AT-TLS

É necessário criar as instruções AT-TLS a seguir para este cenário:

1. Uma instrução TTLSRule para corresponder as conexões de saída do espaço de endereço do iniciador do canal para o endereço IP e número da porta do canal receptor de destino. Esses valores devem corresponder às informações utilizadas no CONNAME do canal emissor. Aqui, mais filtragem foi incluída para corresponder a um nome de tarefa do iniciador de canal específico.

```
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
}
```

A regra anterior corresponde às conexões que vão para o endereço IP 123.456.78.9 na porta 1414 por meio da tarefa CSQ1CHIN.

Mais opções avançadas de filtragem são descritas em TTLSRule.

2. Uma instrução TTLSGroupAction ativando a regra. O `TTLSRule` referencia o `TTLSGroupAction` usando a propriedade **`TTLSGroupActionRef`**.

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Uma instrução TTLSEnvironmentAction está associada com o `TTLSRule` pela propriedade **`TTLSEnvironmentActionRef`**. Um `TTLSEnvironmentAction` configura o Ambiente TLS e especifica qual conjunto de chaves a utilizar.

```
TTLSEnvironmentAction               CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                     CLIENT
  TTLSKeyringParmsRef               CSQ1-KEYRING
  TTLSCipherParmsRef                CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef   CSQ1-ENVIRONMENT-ADVANCED
}
```

4. Uma instrução TTLSKeyringParms é associada ao `TTLSEnvironmentAction` pela propriedade **`TTLSKeyringParmsRef`** e define o conjunto de chaves usado por AT-TLS.

   O conjunto de chaves deve conter certificados confiáveis pelo Gerenciador de Filas remoto não z/OS. Este conjunto de chaves pode ser definido da mesma forma que um conjunto de chaves usado pelo inicializador de canal; consulte “Configurando seu sistema z/OS para usar TLS” na página 258.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Uma instrução TTLSCipherParms associada com o `TTLSEnvironmentAction` pela propriedade **`TTLSCipherParmsRef`**

   Esta instrução deve conter um único nome de conjunto de cifras que deve ser o equivalente ao nome de CipherSpec do IBM MQ usado no canal receptor de destino.

   Nota: Os nomes de conjunto de cifras AT-TLS não correspondem necessariamente aos nomes de CipherSpec do IBM MQ. No entanto, é possível localizar o nome do conjunto de cifras AT-TLS que corresponde a um nome IBM MQ CipherSpec localizando o nome IBM MQ CipherSpec da tabela a seguir e fazendo referência cruzada da coluna de código de quatro caracteres com a coluna de caractere expandida da Tabela 2 no tópico TTLSCipherParms .

Tabela 78. Converter de códigos de quatro caracteres para nomes de CipherSpec

Código de quatro caracteres	Protocolo	Ativado por padrão	Nome do CipherSpec
0001	SSL 3.0	No	NULL_MD5
0002	SSL 3.0	No	NULL_SHA
0003	SSL 3.0	No	RC4_MD5_EXPORT
0004	SSL 3.0	No	RC4_MD5_US
0005	SSL 3.0	No	RC4_SHA_US
0006	SSL 3.0	No	RC2_MD5_EXPORT
0008	SSL 3.0	No	DES_SHA_EXPORT
0009	TLS 1.0	Sim	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	No	TRIPLE_DES_SHA_US
000A	TLS 1.0	Sim	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Sim	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Sim	TLS_RSA_WITH_AES_256_CBC_SHA
003B	TLS 1.2	Sim	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	Sim	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	Sim	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	Sim	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Sim	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Sim	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Sim	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. Uma instrução TTLSEnvironmentAdvancedParms é associada ao TTLSEnvironmentAction pela propriedade **TTLSEnvironmentAdvancedParmsRef** ..

   Essa instrução pode ser usada para especificar quais protocolos SSL e TLS estão ativados. Com IBM MQ você deve ativar apenas o protocolo único que corresponde ao nome do conjunto de cifras usado na instrução TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

O conjunto completo de instruções é o seguinte e deve ser aplicado ao agente de política:

```
TTLSRule                      CSQ1-TO-REMOTE
{
  LocalAddr                   ALL
  RemoteAddr                  123.456.78.9
  RemotePortRange             1414
  Jobname                     CSQ1CHIN
  Direction                   OUTBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-OUTBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-OUTBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        ON
  TLSv1.3        OFF
}
```

Etapa 3: Remover SSLCIPH do z/OS canal

Remova o CipherSpec do canal z/OS usando o comando a seguir:

```
ALTER CHANNEL(channel-name) CHLTYPE(SDR) SSLCIPH(' ')
```

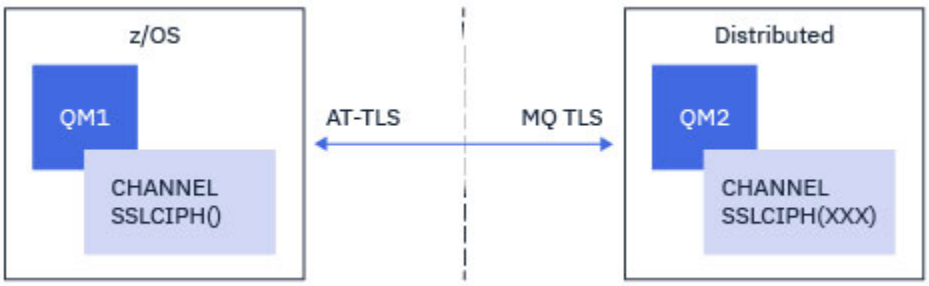
Etapa 4: Iniciar o canal

Uma vez que o canal tenha iniciado, ele estará usando uma combinação de AT-TLS e TLS do IBM MQ.

Atenção: As instruções AT-SLT anteriores são apenas uma configuração mínima Há outras Instruções de política AT-TLS com AT-TLS que não são documentadas aqui, e poderiam ser usadas com o IBM MQ dependendo da necessidade. No entanto, o IBM MQ foi testado apenas com as políticas descritas

Configurando o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms usando um único CipherSpec de nominado

Como você configura o AT-TLS em um canal de entrada por meio de um Gerenciador de Filas IBM MQ for Multiplatforms para um Gerenciador de Filas IBM MQ for z/OS. Neste caso, o canal no Gerenciador de Filas z/OS é um canal receptor que não possui o conjunto de atributos SSLCIPH, e o canal no Gerenciador de Filas não z/OS é um canal emissor com o conjunto de atributos SSLCIPH configurado para um único CipherSpec denominado.



Neste exemplo, um par de canais emissor / receptor existente, que usa o TLS 1.2 TLS_RSA_WITH_AES_256_GCM_SHA384 CipherSpec será ajustado para que o canal receptor use AT-TLS em vez de IBM MQ TLS.

Outros protocolos TLS e CipherSpecs podem ser usados fazendo pequenos ajustes na configuração. Outros tipos de canal de mensagens, além de canais emissores e receptores de cluster, poderiam ser usados sem alteração na configuração de AT-TLS.

Procedimento

Etapa 1: Pare o canal

Etapa 2: Crie e aplique uma política AT-TLS

É necessário criar as instruções AT-TLS a seguir para este cenário:

1. Uma instrução TTLSRule para corresponder conexões de entrada com o espaço de endereço do iniciador do canal por meio do endereço IP do canal emissor. Aqui, mais filtragem foi incluída para corresponder a um nome de tarefa do iniciador de canal específico.

```
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
}
```

   As correspondências de regra anteriores com relação às conexões que vão para a tarefa CSQ1CHIN na porta local 1414 do endereço IP remoto 123.456.78.9.

   Mais opções avançadas de filtragem são descritas em TTLSRule.

2. Uma instrução TTLSGroupAction ativando a regra. O `TTLSRule` referencia o `TTLSGroupAction` usando a propriedade **`TTLSGroupActionRef`**.

```
TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}
```

3. Uma instrução TTLSEnvironmentAction está associada com o `TTLSRule` pela propriedade **`TTLSEnvironmentActionRef`**. Um `TTLSEnvironmentAction` configura o Ambiente TLS e especifica qual conjunto de chaves a utilizar.

```
TTLSEnvironmentAction                 CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                       SERVER
  TTLSKeyringParmsRef                 CSQ1-KEYRING
  TTLSCipherParmsRef                  CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef     CSQ1-ENVIRONMENT-ADVANCED
}
```

O AT-TLS fornece a capacidade de conceder autenticação mútua, que é o equivalente a utilizar o atributo de canal SSLCAUTH. Isso é feito por ter uma instrução `TTLSEnvironmentAction` com um valor **HandshakeRole** de *ServerWithClientAuth* para a instrução de entrada `TTLSEnvironmentAction`.

4. Uma instrução TTLSKeyringParms é associada ao `TTLSEnvironmentAction` pela propriedade **TTLSKeyringParmsRef** e define o conjunto de chaves usado por AT-TLS.

   O conjunto de chaves deve conter certificados confiáveis pelo Gerenciador de Filas remoto não z/OS. Este conjunto de chaves pode ser definido da mesma forma que um conjunto de chaves usado pelo inicializador de canal; consulte "Configurando seu sistema z/OS para usar TLS" na página 258.

```
TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}
```

5. Uma instrução TTLSCipherParms associada com o `TTLSEnvironmentAction` pela propriedade **TTLSCipherParmsRef**

   Esta instrução deve conter um único nome de conjunto de cifras que deve ser o equivalente ao nome de CipherSpec do IBM MQ usado no canal emissor remoto.

   Nota: Os nomes de conjunto de cifras AT-TLS não correspondem necessariamente aos nomes de CipherSpec do IBM MQ. No entanto, é possível localizar o nome do conjunto de cifras AT-TLS que corresponde a um nome IBM MQ CipherSpec localizando o nome IBM MQ CipherSpec da tabela a seguir e fazendo referência cruzada da coluna de código de quatro caracteres com a coluna de caractere expandida da Tabela 2 no tópico TTLSCipherParms .

Tabela 79. Converter de códigos de quatro caracteres para nomes de CipherSpec

Código de quatro caracteres	Protocolo	Ativado por padrão	Nome do CipherSpec
0001	SSL 3.0	No	NULL_MD5
0002	SSL 3.0	No	NULL_SHA
0003	SSL 3.0	No	RC4_MD5_EXPORT
0004	SSL 3.0	No	RC4_MD5_US
0005	SSL 3.0	No	RC4_SHA_US
0006	SSL 3.0	No	RC2_MD5_EXPORT
0008	SSL 3.0	No	DES_SHA_EXPORT
0009	TLS 1.0	Sim	TLS_RSA_WITH_DES_CBC_SHA
000A	SSL 3.0	No	TRIPLE_DES_SHA_US
000A	TLS 1.0	Sim	TLS_RSA_WITH_3DES_EDE_CBC_SHA
002F	TLS 1.0	Sim	TLS_RSA_WITH_AES_128_CBC_SHA
0035	TLS 1.0	Sim	TLS_RSA_WITH_AES_256_CBC_SHA

Tabela 79. Converter de códigos de quatro caracteres para nomes de CipherSpec (continuação)			
Código de quatro caracteres	**Protocolo**	**Ativado por padrão**	**Nome do CipherSpec**
003B	TLS 1.2	Sim	TLS_RSA_WITH_NULL_SHA256
003C	TLS 1.2	Sim	TLS_RSA_WITH_AES_128_CBC_SHA256
003D	TLS 1.2	Sim	TLS_RSA_WITH_AES_256_CBC_SHA256
C023	TLS 1.2	Sim	ECDHE_ECDSA_AES_128_CBC_SHA256
C024	TLS 1.2	Sim	ECDHE_ECDSA_AES_256_CBC_SHA384
C027	TLS 1.2	Sim	ECDHE_RSA_AES_128_CBC_SHA256
C028	TLS 1.2	Sim	ECDHE_RSA_AES_256_CBC_SHA384

```
TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}
```

6. Uma instrução TTLSEnvironmentAdvancedParms é associada ao TTLSEnvironmentAction pela propriedade **TTLSEnvironmentAdvancedParmsRef** ..

   Essa instrução pode ser usada para especificar quais protocolos SSL e TLS estão ativados. Com IBM MQ você deve ativar apenas o protocolo único que corresponde ao nome do conjunto de cifras usado na instrução TTLSCipherParms .

```
TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3           OFF
  TLSv1           OFF
  TLSv1.1         OFF
  SecondaryMap    OFF
  TLSv1.2         ON
  TLSv1.3         OFF
}
```

O conjunto completo de instruções é o seguinte e deve ser aplicado ao agente de política:

```
TTLSRule                      REMOTE-TO-CSQ1
{
  LocalAddr                   ALL
  LocalPortRange              1414
  RemoteAddr                  123.456.78.9
  Jobname                     CSQ1CHIN
  Direction                   INBOUND
  TTLSGroupActionRef          CSQ1-GROUP-ACTION
  TTLSEnvironmentActionRef    CSQ1-INBOUND-ENVIRONMENT-ACTION
}

TTLSGroupAction             CSQ1-GROUP-ACTION
{
  TTLSEnabled               ON
}

TTLSEnvironmentAction             CSQ1-INBOUND-ENVIRONMENT-ACTION
{
  HandshakeRole                   CLIENT
  TTLSKeyringParmsRef             CSQ1-KEYRING
  TTLSCipherParmsRef              CSQ1-CIPHERPARM
  TTLSEnvironmentAdvancedParmsRef CSQ1-ENVIRONMENT-ADVANCED
}

TTLSKeyringParms            CSQ1-KEYRING
{
  Keyring                   MQCHIN/CSQ1RING
}

TTLSCipherParms             CSQ1-CIPHERPARM
{
  V3CipherSuites            TLS_RSA_WITH_AES_256_GCM_SHA384
}

TTLSEnvironmentAdvancedParms CSQ1-ENVIRONMENT-ADVANCED
{
  SSLv3          OFF
  TLSv1          OFF
  TLSv1.1        OFF
  SecondaryMap   OFF
  TLSv1.2        OFF
  TLSv1.3        ON
}
```

Etapa 3: Remover SSLCIPH do z/OS canal

Remova o CipherSpec do canal z/OS usando o comando a seguir:

```
ALTER CHANNEL(channel-name) CHLTYPE(RCVR) SSLCIPH(' ')
```

Etapa 4: Iniciar o canal

Uma vez que o canal tenha iniciado, ele estará usando uma combinação de AT-TLS e TLS do IBM MQ.

Atenção: As instruções AT-SLT anteriores são apenas uma configuração mínima Há outras Instruções de política AT-TLS com AT-TLS que não são documentadas aqui, e poderiam ser usadas com o IBM MQ dependendo da necessidade. No entanto, o IBM MQ foi testado apenas com as políticas descritas

Reconfigurando as chaves secretas SSL e TLS

O IBM MQ suporta a reinicialização de chaves secretas em gerenciadores de filas e clientes.

As chaves secretas são reconfiguradas quando um número especificado de bytes criptografados de dados passa pelo canal. Se as pulsações de canal forem ativadas, a chave secreta será reconfigurada de os dados serem enviados ou recebidos após uma pulsação de canal.

O valor de reconfiguração de chave é sempre configurado pelo lado inicial do canal do IBM MQ.

Gerenciador de filas

Para um gerenciador de filas, use o comando **ALTER QMGR** com o parâmetro **SSLRKEYC** para definir os valores usados durante a renegociação.

IBM i No IBM i, use **CHGMQM** com o parâmetro **SSLRSTCNT**.

Cliente MQI

Por padrão, os clientes MQI não renegociam a chave secreta. É possível fazer um cliente MQI renegociar a chave em qualquer uma das três formas. Na lista a seguir, os métodos são mostrados em ordem de prioridade. Se você especificar diversos valores, o valor de prioridade mais alto será usado.

1. Usando o campo KeyResetCount na estrutura MQSCO em uma chamada MQCONNX
2. Usando a variável de ambiente MQSSLRESET
3. Configurando o atributo SSLKeyResetCount no arquivo de configuração do cliente MQI

Essas variáveis podem ser configuradas para um número inteiro no intervalo de 0 a 999999999, representando o número de bytes não criptografados enviados e recebidos em uma conversa TLS antes de a chave secreta TLS ser renegociada. A especificação de um valor igual a 0 indica que as chaves secretas TLS nunca serão renegociadas. Se você especificar uma contagem de reconfiguração de chave secreta TLS no intervalo de 1 byte a 32 KB, os canais TLS usarão uma contagem de reconfiguração de chave secreta de 32 KB. Isto é para evitar reconfigurações de chave excessivas que ocorreriam para valores pequenos de reconfiguração de chave secreta TLS.

Se um valor maior que zero for especificado e as pulsações de canal forem ativadas para o canal, a chave secreta também será renegociada antes dos dados da mensagem serem enviados ou recebidos após uma pulsação de canal.

A contagem de bytes até a próxima renegociação de chave secreta é reconfigurada após cada renegociação bem-sucedida.

Para obter detalhes integrais da estrutura MQSCO, veja KeyResetCount (MQLONG). Para obter detalhes completos de MQSSLRESET, consulte MQSSLRESET. Para obter mais informações sobre o uso de TLS no arquivo de configuração do cliente, veja Sub-rotina de SSL do arquivo de configuração do cliente.

Java

Para o IBM MQ classes for Java, um aplicativo pode reconfigurar a chave secreta de uma das maneiras a seguir:

- Configurando o campo sslResetCount na classe MQEnvironment.
- Configurando uma propriedade de ambiente MQC.SSL_RESET_COUNT_PROPERTY em um objeto Hashtable. O aplicativo designa, então, a hashtable para o campo `properties` na classe MQEnvironment ou passa a hashtable para um objeto MQQueueManager em seu construtor.

Se o aplicativo usar mais de uma dessas maneiras, as regras usuais de precedência se aplicam. Consulte Classe com.ibm.mq.MQEnvironment para as regras de precedência.

O valor do campo sslResetCount ou a propriedade de ambiente MQC.SSL_RESET_COUNT_PROPERTY representa o número total de bytes enviados e recebidos pelo código do cliente IBM MQ classes for Java antes que a chave secreta seja renegociada. O número de bytes enviados é o número antes da criptografia e o número de bytes recebidos é o número após a decriptografia. O número de bytes também inclui informações de controle enviadas e recebidas pelo cliente IBM MQ classes for Java.

Se a contagem de reconfiguração for zero, que é o valor padrão, a chave secreta nunca será renegociada. A contagem de reconfiguração será ignorada se nenhum CipherSuite for especificado.

JMS

Para o IBM MQ classes for JMS, a propriedade SSLRESETCOUNT representa o número total de bytes enviados e recebidos por uma conexão antes que chave secreta que é usada para criptografia seja

renegociada. O número de bytes enviados é o número antes da criptografia e o número de bytes recebidos é o número após a decriptografia. O número de bytes também inclui informações de controle enviadas e recebidas pelo IBM MQ classes for JMS. Por exemplo, para configurar um objeto ConnectionFactory que possa ser usado para criar uma conexão por meio de um canal MQI ativado por TLS (Segurança da Camada de Transporte) com uma chave secreta que seja renegociada após a passagem de 4 MB de dados, emita o comando a seguir para JMSAdmin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Se o valor de SSLRESETCOUNT for zero, que é o valor padrão, a chave secreta nunca será renegociada. A propriedade SSLRESETCOUNT será ignorada se SSLCIPHERSUITE não estiver configurado.

.NET

Para clientes não gerenciados do .NET, a propriedade de número inteiro SSLKeyResetCount indica o número de bytes não criptografados enviados e recebidos em uma conversa TLS antes que a chave secreta seja renegociada.

Para obter informações sobre o uso das propriedades de objeto no IBM MQ classes for .NET, consulte Obtendo e definindo os valores de atributo.

Para clientes gerenciados .NET, a classe SSLStream não suporta reconfiguração/renegociação de chave secreta. No entanto, para ser consistente com outros clientes IBM MQ , o cliente IBM MQ gerenciado .NET permite que os aplicativos definam SSLKeyResetCount. Para obter mais informações, veja Reconfiguração ou renegociação de chave secreta.

XMS .NET

Para clientes não gerenciados XMS .NET, veja Conexões seguras com um gerenciador de filas do IBM MQ.

Referências relacionadas
ALTER QMGR
DISPLAY QMGR
Alterar Gerenciador da Fila de Mensagens (CHGMQM)
Exibir Gerenciador da Fila de Mensagens (DSPMQM)

Implementando confidencialidade em programas de saída do usuário

Implementando confidencialidade em saídas de segurança

As saídas de segurança podem exercer uma função no serviço de confidencialidade gerando e distribuindo a chave simétrica para criptografia e decriptografia de dados que flui no canal. Uma técnica comum aplicada utiliza a tecnologia PKI.

Uma saída de segurança gera um valor de dados aleatório, criptografa-os com a tecla pública do gerenciador ou usuário de fila que a saída do parceiro está representando e envia os dados criptografados a seu parceiro em uma mensagem de segurança. A saída de segurança do parceiro decriptografa os valores de dados aleatórios com a tecla privativa do gerenciador ou usuário de fila que os está representando. Cada saída de segurança pode agora utilizar o valor de dados aleatórios para derivar a chave simétrica, independentemente de outros utilizando um algoritmo conhecido de ambos. De forma alternativa, podem usar o valor de dados aleatórios como a chave.

Se a primeira saída de segurança não autenticou seu parceiro até então, a mensagem de segurança seguinte enviada pelo parceiro poderá conter uma valor inesperado criptografado com a chave simétrica. A primeira saída de segurança pode então autenticar seu parceiro verificando se a saída de segurança dele conseguiu criptografar o valor esperado corretamente.

As saídas de segurança podem também usar esta oportunidade para concordar o algoritmo para criptografia e decriptografia de dados que fluem no canal, se mais de um algoritmo estiver disponível para uso.

Implementando confidencialidade em saídas de mensagem

Uma saída de mensagem na extremidade de envio de um canal pode criptografar os dados do aplicativo em uma mensagem e outra saída na extremidade de recepção do canal pode descriptografar os dados. Por razões de desempenho, um algoritmo de tecla simétrica é normalmente utilizado para este propósito. Para obter mais informações sobre como a chave simétrica pode ser gerada e distribuída, consulte “Implementando confidencialidade em programas de saída do usuário” na página 452.

Os cabeçalhos de uma mensagem, como da fila de transmissão, MQXQH, que inclui o descritor da mensagem interna, não devem ser criptografados por uma saída de mensagem. Isso porque a conversão de dados dos cabeçalhos da mensagem ocorre depois que uma saída de mensagem é chamada na extremidade de envio ou antes de ser chamada na extremidade de recepção. Se os cabeçalhos forem criptografados, a conversão de dados falhará e o canal parará.

Implementando confidencialidade em saídas de envio e de recebimento

As saídas de envio e recebimento podem ser utilizadas para criptografar e descriptografar dados que passam por um canal. Elas são mais apropriadas que as saídas de mensagens que fornecem esse serviço pelos seguintes motivos:

- Em um canal de mensagem, os cabeçalhos da mensagem podem ser criptografados assim como os dados do aplicativo nas mensagens.
- As saídas de envio e recebimento podem ser usadas em canais MQI assim como em canais de mensagens. Os parâmetros nas chamadas MQI podem não conter dados sensíveis do aplicativo que tenham que ser protegidos enquanto passam em um canal MQI. Portanto, é possível usar as mesmas saídas de envio e recebimento nos dois tipos de canais.

A confidencialidade na saída da API e saída cruzada da API

Os dados do aplicativo em uma mensagem podem ser criptografados por uma saída API ou saída cruzada da API quando a mensagem for colocada pelo aplicativo de envio e decriptografada por uma segunda saída quando a mensagem for recuperada pelo aplicativo de recebimento. Por razões de desempenho, um algoritmo de chave simétrica é normalmente usado para este propósito. No entanto, ao nível do aplicativo, em que muitos usuários podem estar enviando mensagens uns aos outros, o problema é como assegurar que somente o receptor pretendido de uma mensagem seja capaz de decriptografá-la. Uma solução é utilizar uma chave simétrica diferente para cada par de usuários que enviem mensagens uns aos outros. Mas essa solução pode ser difícil e demorada para administrar, particularmente se os usuários pertencerem a organizações diferentes. Um modo padrão de resolver este problema é conhecido como *envelopamento digital* e utiliza tecnologia PKI.

Quando um aplicativo coloca uma mensagem em uma fila, uma saída API ou saída cruzada da API gera uma chave simétrica aleatória e usa a chave para criptografar os dados do aplicativo na mensagem. A saída criptografa a chave simétrica com a chave pública do receptor desejado. Então, ela substitui os dados do aplicativo na mensagem pelos dados criptografados do aplicativo e a chave simétrica criptografada. Deste modo, somente o receptor pretendido poderá decriptografar a chave simétrica e, portanto, os dados do aplicativo. Se uma mensagem criptografada tiver mais de um possível receptor desejado, a saída poderá criptografar uma cópia da chave simétrica para cada receptor desejado.

Se diferentes algoritmos para criptografar e decriptografar dados do aplicativo estiverem disponíveis para uso, a saída poderá incluir o nome do algoritmo que foi usado.

V 9.1.4 z/OS Confidencialidade para dados em repouso no IBM MQ for z/OS com criptografia do conjunto de dados

O IBM MQ for z/OS pode reforçar os dados de clientes e de configuração gravando-os nos conjuntos de dados de log ativo, nos conjuntos de dados de log de archive, nos conjuntos de páginasconjuntos de dados de autoinicialização (BSDS) e nos V 9.1.5 conjuntos de dados de mensagens compartilhadas (SMDS).

O z/OS fornece criptografia eficiente e baseada em políticas dos conjuntos de dados. O IBM MQ for z/OS suporta a criptografia do conjunto de dados do z/OS:

- Conjuntos de dados de log ativos; consulte a nota “1” na página 454
- Conjuntos de dados de log de archive; consulte a nota “2” na página 454
- Conjuntos de páginas; consulte a nota “1” na página 454
- BSDS; consulte a nota “2” na página 454
- Conjuntos de dados CSQINP*; consulte a nota “2” na página 454
- V 9.1.5 SMDS; consulte a nota “3” na página 454

Isso fornece confidencialidade de dados em repouso em um gerenciador de filas individual do z/OS.

Notes:

1. A partir da IBM MQ 9.1.4, o IBM MQ for z/OS suporta a criptografia de conjunto de dados do z/OS para logs ativos e conjuntos de páginas.
2. A criptografia de conjunto de dados para conjuntos de dados de logs de archive, BSDS e CSQINP* é suportada em todas as versões do IBM MQ for z/OS.
3. V 9.1.5 A partir da IBM MQ 9.1.5, o IBM MQ for z/OS suporta a criptografia de conjunto de dados do z/OS para SMDS.
4. O IBM MQ Advanced Message Security fornece um mecanismo alternativo de proteção de dados em repouso. Além disso, o AMS também protege dados na memória e em andamento

Consulte Usando os aperfeiçoamentos de criptografia do conjunto de dados do z/OS para obter mais informações sobre a criptografia de conjunto de dados do z/OS.

A configuração da criptografia do conjunto de dados do z/OS está fora do controle do IBM MQ for z/OS. As configurações de criptografia entram em vigor quando o conjunto de dados é criado.

Isso significa que quaisquer conjuntos de dados existentes precisam ser recriados antes que uma nova política de criptografia do conjunto de dados possa ser usada.

O IBM MQ for z/OS pode ser executado com uma mistura de conjuntos de dados criptografados e não criptografados, mas uma configuração padrão criptografaria todos ou nenhum dos conjuntos de dados usados.

V 9.1.4 z/OS Visão geral de etapas para criptografar um conjunto de dados do IBM MQ for z/OS

Como criptografar um conjunto de dados do IBM MQ for z/OS.

Antes de começar

Deve-se assegurar de ter configurado a criptografia de conjunto de dados do z/OS corretamente em sua empresa. Se você estiver configurando a criptografia do conjunto de dados em um grupo de compartilhamento de filas, deve-se configurar a criptografia do conjunto de dados do z/OS para compartilhamento de dados.

Nota: Um conjunto de dados criptografados do z/OS deve ser um conjunto de dados de formato estendido.

Procedimento

1. Configure no RACF a chave de criptografia e o `key-label` a serem usados a fim de criptografar o conjunto de dados.
2. Crie um perfil para o `key-label` na classe CSFKEYS do RACF.
3. Conceda acesso READ ao ID do usuário do gerenciador de filas e a quaisquer outros IDs de usuário que precisem de acesso aos dados criptografados.

   Isso pode incluir IDs de usuário que são usados para executar utilitários de impressão em relação ao conjunto de dados. Por exemplo, o usuário que estivesse executando CSQUTIL SCOPY precisaria decriptografar o conjunto de páginas relevante.
4. Associe o `key-label` de criptografia com o nome do conjunto de dados.

   É possível fazer isso usando uma classe de dados SMS ou um segmento DFP do RACF para o nome do conjunto de dados ou qualificador de alto nível.

   Também é possível associar o `key-label` ao conjunto de dados quando o conjunto de dados é alocado.
5. Renomeie qualquer conjunto de dados existente usando IDCAMS ALTER.
6. Realoque o conjunto de dados com os atributos apropriados.
7. Copie o conteúdo do conjunto de dados renomeado para o novo conjunto de dados usando IDCAMS REPRO.

   Os dados são criptografados pela ação de copiá-los no conjunto de dados.
8. Repita as etapas de “4” na página 455 a “6” na página 455 para quaisquer outros conjuntos de dados que precisem ser criptografados.

V 9.1.4 z/OS Exemplo de como criptografar logs ativos do gerenciador de filas

Os tópicos a seguir o guiarão durante o processo de ativação da criptografia de conjunto de dados em logs ativos existentes.

Nota: O processo para outros conjuntos de dados é semelhante ao de logs ativos.

Nesse exemplo:

- O gerenciador de filas CSQ1 é executado sob o usuário QMCSQ1 e tem os conjuntos de dados de logs ativos CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002 e assim por diante
- O ambiente de hardware e software é capaz de usar a criptografia de conjunto de dados do z/OS
- O RACF é usado como o SAF
- O gerenciador de filas foi interrompido

Realize o procedimento na ordem a seguir:

1. “Configurando a chave de criptografia do conjunto de dados para o gerenciador de filas” na página 455
2. “Configurando a criptografia de conjunto de dados para os conjuntos de dados de log” na página 456

V 9.1.4 z/OS Configurando a chave de criptografia do conjunto de dados para o gerenciador de filas

Como configurar uma chave de criptografia de conjunto de dados para um gerenciador de filas.

Sobre esta tarefa

Esta tarefa é um pré-requisito para “Configurando a criptografia de conjunto de dados para os conjuntos de dados de log” na página 456.

Procedimento

1. Configure uma chave de dados de criptografia de bits AES-256 com um rótulo, por exemplo, CSQ1DSKY, usando o z/OS programa utilitário gerador de chaves (KGUP).
2. Defina o perfil CSFKEYS do RACF para a chave de criptografia CSQ1DSKY, emitindo o comando a seguir:

   ```
   RDEFINE CSFKEYS CSQ1DSKY UACC(NONE)
   ```

3. Configure o segmento ICSF do perfil para permitir que a chave seja usada como uma chave protegida, emitindo o comando a seguir:

   ```
   RALTER CSFKEYS CSQ1DSKY ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
   ```

4. Permita que o gerenciador de filas use a chave de criptografia concedendo acesso QMCSQ1 READ ao perfil, emitindo o comando a seguir:

   ```
   PERMIT CSQ1DSKY CLASS(CSFKEYS) ID(QMCSQ1) ACCESS(READ)
   ```

   Forneça o mesmo acesso a qualquer usuário administrativo que precise ler ou gravar no conjunto de dados criptografados.
5. Atualize a classe CSFKEYS emitindo o comando a seguir.

   ```
   SETROPTS RACLIST(CSFKEYS) REFRESH
   ```

Como proceder a seguir

Configurar a criptografia do conjunto de dados para os conjuntos de dados conforme descrito em “Configurando a criptografia de conjunto de dados para os conjuntos de dados de log” na página 456

V 9.1.4 z/OS Configurando a criptografia de conjunto de dados para os conjuntos de dados de log

Como configurar a criptografia nos conjuntos de dados de log.

Antes de começar

Assegure-se de ter lido:

A visão geral das etapas para criptografar um conjunto de dados do IBM MQ for z/OS e de ter realizado o procedimento em
“Configurando a chave de criptografia do conjunto de dados para o gerenciador de filas” na página 455

Sobre esta tarefa

Esse método usa o segmento DFP de um perfil genérico de RACF, de modo que você possa usar a chave de criptografia para todos os novos conjuntos de dados que correspondam ao perfil.

Como alternativa, é possível configurar e usar uma classe de dados do SMS ou o rótulo da chave pode ser especificado diretamente ao alocar o conjunto de dados.

Conforme descrito anteriormente, neste exemplo, o gerenciador de filas CSQ1 é executado no usuário QMCSQ1 e possui os conjuntos de dados de logs ativos CSQ1.LOGS.LOGCOPY1.DS001, CSQ1.LOGS.LOGCOPY1.DS002 e assim por diante.

Procedimento

1. Crie o perfil genérico se ele não existir, emitindo o comando a seguir:

   ```
   ADDSD 'CSQ1.LOGS.*' UACC(NONE)
   ```

2. Permita que o usuário do gerenciador de filas altere o acesso ao perfil, emitindo o comando a seguir:

```
PERMIT 'CSQ1.LOGS.*' ID(QMCSQ1) ACCESS(ALTER)
```

Além disso, permita o acesso apropriado necessário para qualquer usuário administrativo.

3. Inclua o segmento do DFP com o rótulo da chave de criptografia emitindo o comando a seguir:

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

Nota: Deve-se usar a mesma chave de criptografia usada em configurando a chave de criptografia do conjunto de dados para o gerenciador de filas.

4. Atualize os perfis de conjunto de dados genéricos emitindo o comando a seguir:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Renomeie cada conjunto de dados de log para um backup, em seguida, recrie e restaure os dados, usando IDCAMS. O fragmento de JCL a seguir converte CSQ1.LOGS.LOGCOPY1.DS001:

   a) Renomear o conjunto de dados para um backup

```
//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) Redefinir o conjunto de dados.

   O novo conjunto de dados será criptografado devido ao perfil do RACF.

   Nota: Substitua ++EXTDCLASS++ pelo nome da classe de dados de formato estendido que você deseja usar para o conjunto de dados.

```
//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) Copie os dados do backup no conjunto de dados recriados.

   Essa etapa criptografa os dados:

```
//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)
```

Como proceder a seguir

Repita a Etapa “5” na página 457 para todos os conjuntos de dados de log ativos.

Somente uma única chave de criptografia é requerida e todos os conjuntos de dados podem ser associados ao mesmo rótulo de chave.

Reinicie o gerenciador de filas CSQ1. Use a saída por meio do comando DISPLAY LOG para verificar se os conjuntos de dados de log foram criptografados.

V 9.1.4 z/OS Considerações para a criptografia do conjunto de dados do z/OS em um grupo de filas compartilhadas

Cada gerenciador de filas em um grupo de filas compartilhadas (QSG) deve ser capaz de ler os logs, o BSDS V 9.1.5 e os conjuntos de dados de mensagens compartilhadas (SMDS), de todos os outros gerenciadores de filas no QSG.

Isso significa que cada sistema no qual um membro do QSG pode ser executado deve atender aos requisitos para a criptografia do conjunto de dados do z/OS e todos os rótulos de chaves e chaves de criptografia usados para proteger os conjuntos de dados para cada gerenciador de filas no QSG devem estar disponíveis em cada sistema.

Um gerenciador de filas anterior ao IBM MQ for z/OS 9.1.3 não pode acessar um conjunto de dados de log ativo criptografado.

V 9.1.5 Um gerenciador de filas anterior ao IBM MQ for z/OS 9.1.3 não pode acessar um SMDS criptografado.

V 9.1.5 Antes de fazer uso da criptografia de conjunto de dados do z/OS, é necessário migrar todos os gerenciadores de filas em um QSG para pelo menos o IBM MQ for z/OS 9.1.3.

Se um gerenciador de filas em um QSG tiver sido iniciado com qualquer conjunto de dados do log ativo criptografado e qualquer outro gerenciador de filas no QSG tiver sido iniciado, mas não tiver sido iniciado pela última vez com uma versão do IBM MQ for z/OS que suporte logs ativos criptografados, o gerenciador de filas com o log ativo criptografado finalizará de maneira anormal com o código de encerramento anormal 5C6-00F50033.

V 9.1.5 É possível converter um QSG para usar logs ativos criptografados e SMDS sem uma indisponibilidade completa ao:

1. Migrar cada gerenciador de filas para pelo menos a IBM MQ 9.1.5 por sua vez.
2. Converter logs ativos para conjuntos de dados criptografados para cada gerenciador de filas por sua vez. Isso requer que o gerenciador de filas seja encerrado e, em seguida, reiniciado.

   Ao mesmo tempo, é provável que os conjuntos de páginas e os logs de archive também sejam ativados para conjuntos de dados criptografados, mas isso não afeta a migração do QSG.

   O procedimento para conversão de cada conjunto de dados é descrito em “Exemplo de como criptografar logs ativos do gerenciador de filas” na página 455
3. Converter SMDS em conjuntos de dados criptografados para cada estrutura de CF individual, por sua vez, ao:
   a. Emitindo o comando RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name) para suspender o acesso do gerenciador de filas ao SMDS.

      Observe que durante esse tempo, os dados sobre as filas compartilhadas associadas ao SMDS estão temporariamente indisponíveis.
   b. Converter cada conjunto de dados que compõe o SMDS em conjuntos de dados criptografados, usando o procedimento descrito em “Exemplo de como criptografar logs ativos do gerenciador de filas” na página 455.
   c. Emitindo o comando RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name) para retomar o acesso do gerenciador de filas ao SMDS.

Atenção: É necessário encerrar o gerenciador de filas de maneira limpa antes de converter os logs e a recuperação da estrutura do recurso de acoplamento pode não ser possível durante a conversão, pois os conjuntos de dados de logs ativos estarão temporariamente indisponíveis.

V 9.1.4 z/OS Considerações sobre migração para versão anterior ao usar a criptografia de conjunto de dados do z/OS

É necessário considerar o seguinte ao migrar para uma versão anterior um gerenciador de filas, que possui um ou mais conjuntos de dados criptografados.

A criptografia do conjunto de dados do z/OS é suportada nos conjuntos de dados do IBM MQ for z/OS a seguir:

- Conjuntos de dados do log ativo
- Conjuntos de dados do log de archive
- Conjuntos de páginas
- BSDS
- V 9.1.5 SMDS
- Conjuntos de dados CSQINP*

Não há considerações de migração para versão anterior para BSDS, log de archive ou conjuntos de dados CSINP*.

No entanto, há considerações para

- V 9.1.5 SMDS
- Conjunto de páginas e
- Log Ativo

conjuntos de dados, já que o uso deles com a criptografia do conjunto de dados do z/OS não é suportado em liberações de suporte de longo prazo IBM MQ for z/OS 9.1.0e anteriores.

Antes da migração para versão anterior, todas as políticas de criptografia para o V 9.1.5 SMDS, conjunto de páginas e conjuntos de dados de log ativos precisam ser removidos e os dados decriptografados. Este processo está descrito em “Removendo a criptografia do conjunto de dados de um conjunto de dados” na página 459.

Atenção: Se o gerenciador de filas a ser migrado para uma versão anterior fizer parte de um grupo de filas compartilhadas (QSG), leia primeiro a seção “Considerações do grupo de filas compartilhadas” na página 461.

Removendo a criptografia do conjunto de dados de um conjunto de dados

Este exemplo descreve como remover a criptografia do conjunto de dados do conjunto de dados de log CSQ1.LOGS.LOGCOPY1.DS001. É possível usar um processo equivalente para V 9.1.5 SMDS e conjuntos de páginas.

O exemplo presume que:

- RACF é o SAF
- O gerenciador de filas que usa o conjunto de dados foi interrompido
- O rótulo da chave de criptografia foi associado ao perfil do RACF genérico CSQ1.LOGS.*

Execute o seguinte procedimento:

1. Copie os dados do conjunto de dados em um conjunto de dados de backup.
   a. Defina um conjunto de dados de backup que não esteja associado a um rótulo chave criptografado.

      Nota: Substitua ++EXTDCLASS++ pelo nome da classe de dados de formato estendido que você deseja usar para o conjunto de dados.

      ```
      //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. Copie os dados do conjunto de dados original para o backup. Esta etapa decriptografa os dados.

```
//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. Exclua o conjunto de dados original

```
//DELETE   EXEC PGM=IDCAMS,REGION=0M
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  /*-------------------------------------------------------------*/
  /* DELETE ORIGINAL                                             */
  /*-------------------------------------------------------------*/
  DELETE ('CSQ1.LOGS.LOGCOPY1.DS001')
/*
```

d. Renomeie o backup para o nome do conjunto de dados original. Os dados permanecem não criptografados

```
//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. Opcionalmente, repita esse processo para outros conjuntos de dados que tenham um rótulo de chave de criptografia associado a eles por meio do CSQ1.LOGS.* perfil genérico.
3. Opcionalmente, se todos os conjuntos de dados associados ao CSQ1.LOGS.* perfil genérico foi decriptografado, remova o DATAKEY associado ao perfil genérico emitindo o comando a seguir

```
ALTDSD 'CSQ1.LOGS.*' DFP(RESOWNER(QMCSQ1) DATAKEY(CSQ1DSKY))
```

4. Atualize os perfis de conjunto de dados genéricos emitindo o comando a seguir:

```
SETROPTS GENERIC(DATASET) REFRESH
```

5. Reiniciar o gerenciador de filas.
6. Se a chave de criptografia não for mais necessária, exclua-a e exclua seu perfil RACF associado da classe CSFKEYS.

Considerações do grupo de filas compartilhadas

Se um gerenciador de filas que faz parte de um grupo de filas compartilhadas for migrado para versão anterior do IBM MQ for z/OS que não suporta a criptografia do conjunto de dados, todos os conjuntos de dados de log ativos V 9.1.5 e o SMDS de todos os gerenciadores de filas no QSG precisarão ter suas políticas de criptografia de conjunto de dados removidas e seus dados decriptografados.

Isso se aplica independentemente de um único membro do QSG ser migrado para versão anterior ou todos os membros do QSG.

É possível realizar a remoção de políticas de criptografia e a decriptografia de dados, sem uma indisponibilidade completa de QSG ao:

1. Encerrar cada gerenciador de filas no QSG por vez, remover as políticas de criptografia e decriptografar os dados de seus logs ativos, usando o processo descrito em "Removendo a criptografia do conjunto de dados de um conjunto de dados" na página 459.

   Se o gerenciador de filas tiver de ser migrado para versão anterior, o conjunto de páginas dele também deverá ser decriptografado no momento. Em seguida, reinicie o gerenciador de filas.

2. V 9.1.5 Remover as políticas de criptografia e decriptografar os dados para o SMDS de cada estrutura de CF individual, por sua vez, ao:

   a. Emitindo o comando

   ```
   RESET SMDS(*) ACCESS(DISABLED) CFSTRUCT(structure-name)
   ```

   para suspender o acesso do gerenciador de filas ao SMDS. Durante este tempo, os dados sobre as filas compartilhadas associadas ao SMDS estarão temporariamente indisponíveis.

   b. Seguindo o processo em "Removendo a criptografia do conjunto de dados de um conjunto de dados" na página 459 para cada conjunto de dados que compõe o SMDS.

   c. Emitindo o comando

   ```
   RESET SMDS(*) ACCESS(ENABLED) CFSTRUCT(structure-name)
   ```

   para retomar o acesso do gerenciador de filas ao SMDS.

Usando a criptografia de conjunto de dados do z/OS com um gerenciador de filas que não a suporta

Se você acidentalmente migrar um gerenciador de filas para uma versão anterior do IBM MQ for z/OS que não suporte a criptografia de conjunto de dados, esquecer-se de remover as políticas de criptografia e decriptografar os dados, você obterá um erro quando o gerenciador de filas tentar acessar o conjunto de dados.

O erro depende do tipo de conjunto de dados e é mostrado na tabela a seguir.

Nota: Se um ou mais desses erros ocorrerem, será necessário seguir os processos descritos em "Removendo a criptografia do conjunto de dados de um conjunto de dados" na página 459 para o conjunto de dados afetado. Eles podem ser executados sem mudar a versão do IBM MQ for z/OS.

Conjunto de dados	**Erro se o gerenciador de filas não suportar a criptografia do conjunto de dados do z/OS**
Conjunto de páginas 0	Finalização anormal de 5C6-00C91400 no início do gerenciador de filas
Conjuntos de páginas 1 a 99	MQRC 2193 "Erro de conjunto de páginas" ao acessar o conjunto de páginas, por exemplo, em MQPUT
Log Ativo	Finalização anormal de 5C6-00E80084 no início do gerenciador de filas

Conjunto de dados	Erro se o gerenciador de filas não suportar a criptografia do conjunto de dados do z/OS
V 9.1.5 SMDS	A mensagem IEC161I-122 registrou "O conjunto de dados tem um KEYLABEL, mas o usuário não especificou que o aplicativo poderia manipular a criptografia". O SMDS marcou AVAIL(ERROR).

Integridade de dados de mensagens

Para manter a integridade dos dados é possível usar vários tipos de programa de saída de usuário para fornecer trechos de mensagens ou assinaturas digitais para suas mensagens.

Integridade de dados

Implementando integridade de dados em mensagens

Ao usar TLS, sua opção de CipherSpec determina o nível de integridade de dados na empresa. Se você usar o IBM MQ Advanced Message Service (AMS), é possível especificar a integridade para uma mensagem exclusiva.

Implementando integridade de dados em saídas de mensagem

Uma mensagem pode ser assinada digitalmente por uma saída de usuário na extremidade de envio de um canal. A assinatura digital pode então ser verificada por uma saída de mensagem na extremidade de recepção de um canal para detectar se a mensagem foi modificada deliberadamente.

Alguma proteção pode ser proporcionada utilizando-se uma compilação de mensagens ao invés de uma assinatura digital. Uma compilação de mensagens pode ser efetiva contra violação casual ou indiscriminada, mas não evita que pessoas mais informadas alterem ou substituam a mensagem e gerem uma compilação completamente nova. Isto é particularmente verdadeiro quando o algoritmo utilizado para gerar a compilação da mensagem é bem conhecido.

Implementando integridade de dados em saídas de envio e recebimento

Em um canal de mensagem, as saídas de mensagem são mais apropriadas para fornecer esse serviço porque uma saída pode acessar uma mensagem inteira. Em um canal MQI, os parâmetros nas chamadas MQI podem conter dados do aplicativo que precisem de proteção e somente as saídas de envio e recebimento podem fornecer essa proteção.

Implementando integridade de dados na saída da API ou saída cruzada da API

Uma mensagem pode ser assinada digitalmente por uma saída API ou saída cruzada da API ao ser colocada pelo aplicativo de envio. A assinatura digital pode então ser verificada por uma segunda saída quando a mensagem for recuperada pelo aplicativo receptor para detectar se a mensagem foi modificada deliberadamente.

Alguma proteção pode ser proporcionada utilizando-se uma compilação de mensagens ao invés de uma assinatura digital. Uma compilação de mensagens pode ser efetiva contra violação casual ou indiscriminada, mas não evita que pessoas mais informadas alterem ou substituam a mensagem e gerem uma compilação completamente nova. Isso é particularmente verdadeiro se o algoritmo que é usado para gerar o trecho da mensagem é conhecido,

Outras informações

Consulte a seção sobre “Ativando CipherSpecs” na página 423 para obter mais informações sobre como assegurar a integridade dos dados.

Tarefas relacionadas

Conectando dois gerenciadores de filas usando TLS

Conectando um Cliente a um Gerenciador de Filas de Forma Segura

Auditing

É possível procurar por intrusões de segurança ou tentativas de intrusão usando mensagens do evento. Também é possível verificar a segurança do seu sistema usando o IBM MQ Explorer.

Para detectar tentativas de executar ações não autorizadas como conectar-se a um gerenciador de filas ou colocar uma mensagem em uma fila, examine as mensagens de eventos produzidas por seus gerenciadores de filas, sobretudo mensagens de eventos de autoridade. Para obter mais informações sobre mensagens de eventos do gerenciador de filas, consulte Eventos de filas do gerenciador e para obter mais informações sobre o monitoramento de eventos em geral, consulte Monitoramento de eventos.

Mantendo Clusters Seguros

Autorize ou evite que os gerenciadores de filas juntem os clusters ou coloquem as mensagens nas filas de cluster. Force um gerenciador de filas para deixar um cluster. Leve em conta algumas considerações adicionais ao configurar o TLS para clusters.

Parando o envio de mensagens por gerenciadores de filas desautorizados

Evite que os gerenciadores de filas desautorizados enviem mensagens para seu gerenciador de filas usando uma saída de segurança do canal.

Antes de começar

O armazenamento em cluster não tem efeito na maneira como as saídas de segurança funcionam. Você pode restringir o acesso a um gerenciador de filas da mesma maneira que faria em um ambiente de enfileiramento distribuído.

Sobre esta tarefa

Evite que os gerentes de filas selecionados enviem mensagens ao seu gerenciador de filas:

Procedimento

1. Defina um programa de saída de segurança do canal na definição de canal CLUSRCVR.
2. Grave um programa que autentica gerenciadores de filas que estão tentando enviar mensagens em seu canal do receptor de clusters e nega-lhes o acesso se não estiverem autorizados.

Como proceder a seguir

Os programas de saída de segurança do canal são chamados na inicialização e na rescisão de MCA.

Parando a Colocação de Mensagens de Gerenciadores de Filas Desautorizados em suas Filas

Use o canal para colocar o atributo de autoridade no canal do receptor de clusters para parar os gerenciadores de filas não autorizados de colocar mensagens nas suas filas. Autorize um gerenciador de filas remotas remoto verificando o ID do usuário na mensagem usando o RACF no z/OS ou o OAM em outras plataformas.

Sobre esta tarefa

Use as instalações de segurança de uma plataforma e o mecanismo de controle de acesso no IBM MQ para controlar o acesso às filas.

Procedimento

1. Para evitar que determinados gerenciadores de filas coloquem mensagens em uma fila, use os recursos de segurança disponíveis em sua plataforma.

   Por exemplo:

   - O RACF ou outros gerenciadores de segurança externa no IBM MQ for z/OS
   - O gerenciador de autoridade de objeto (OAM) em outras plataformas.
2. Use a autoridade put, PUTAUT, o atributo CLUSRCVR na definição de canal.

   O atributo PUTAUT permite que você especifique quais os identificadores de usuário devem ser usados para estabelecer a autoridade para colocar uma mensagem em uma fila.

   As opções no atributo PUTAUT são:

   DEF
   Use o ID do usuário padrão. No z/OS, a verificação pode envolver usar ambos o ID do usuário da rede o derivado de MCAUSER.

   CTX
   Use o ID do usuário nas informações de contexto associadas à mensagem. No z/OS a verificação pode envolver o uso do ID do usuário recebido da rede ou daquele derivado de MCAUSER ou ambos. Use esta opção se o link for confiável e autenticado.

   ONLYMCA (somente z/OS)
   Igual a DEF, mas qualquer ID do usuário recebido da rede não é usado. Use esta opção se o link não for confiável. Você deseja permitir somente um conjunto específico de ações nele, que são definidos para o MCAUSER.

   ALTMCA (somente z/OS)
   Como para CTX, mas qualquer ID do usuário recebido da rede não é usado.

Autorizando a Colocação de Mensagens em Filas de Cluster Remotas

No z/OS configure uma autorização para colocar em uma fila de clusters usando o RACF. Em outras plataformas, autorize o acesso para se conectar aos gerenciadores de filas e para colocar nas filas nos gerenciadores de filas.

Sobre esta tarefa

O comportamento padrão é realizar o controle de acesso no SYSTEM.CLUSTER.TRANSMIT.QUEUE. Observe que esse comportamento se aplica mesmo se você estiver usando diversas filas de transmissão.

O comportamento específico descrito neste tópico se aplica apenas quando você tiver configurado o atributo **ClusterQueueAccessControl** no arquivo qm.ini para ser *RQMNome*, conforme descrito no tópico Sub-rotina de segurança, e tiver reiniciado o gerenciador de filas.

Procedimento

- Para z/OS, emita os seguintes comandos:

```
RDEFINE MQQUEUE QMgrName.QUEUE. QueueName UACC(NONE)
PERMIT QMgrName.QUEUE. QueueName CLASS(MQADMIN) ID(GroupName) ACCESS(UPDATE)
```

- Para sistemas UNIX, Linux, and Windows, emita os comandos a seguir:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

- Para IBM i, emita os seguintes comandos:

```
GRTMQMAUT OBJ(' QMgrName ') OBJTYPE(*MQM) USER(GroupName) AUT(*CONNECT)
GRTMQMAUT OBJ(' QueueName ') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME(' QMgrName ')
```

O usuário pode colocar mensagens apenas na fila de clusters especificada, e em nenhuma outra fila de clusters.

Os nomes das variáveis possuem os seguintes significados:

QMgrName
O nome do gerenciador de filas. No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.

GroupName
O nome do grupo que receberá acesso.

QueueName
Nome da fila ou perfil genérico para o qual mudar as autorizações.

Como proceder a seguir

Se você especificar uma fila de resposta quando colocar uma mensagem em uma fila de clusters, o aplicativo consumidor deverá ter autoridade para enviar a resposta. Configure essa autoridade seguindo as instruções em "Concedendo autoridade para colocar mensagens em uma fila do cluster remoto" na página 401.

Conceitos relacionados

Sub-rotina de segurança no qm.ini

Impedindo que Gerenciadores de Filas se Juntem a um Cluster

Se um gerenciador de filas nocivo se unir a um cluster é difícil evitar o recebimento de mensagens que você não deseja que ele receba.

Procedimento

Se você desejar assegurar que somente determinados gerenciadores de filas autorizados se juntar a um cluster, você tem a opção de três técnicas:

- Usar registros de autenticação de canal, é possível bloquear a conexão do canal do cluster com base em: o endereço IP remoto, o nome do gerenciador de filas remotas ou o Nome distinto TLS fornecido pelo sistema remoto.
- Gravar um programa de saída para evitar que gerenciadores de filas não autorizados gravem em `SYSTEM.CLUSTER.COMMAND.QUEUE`. Não restrinja o acesso a `SYSTEM.CLUSTER.COMMAND.QUEUE` de forma que nenhum gerenciador de filas possa gravar nele ou você impediria que qualquer gerenciador de filas se junte ao cluster.
- Um programa de saída de segurança na definição de canal `CLUSRCVR`.

Saídas de segurança nos canais de cluster

Considerações extra ao usar saídas de segurança em canais de cluster.

Sobre esta tarefa

Quando um canal do emissor de clusters é iniciado pela primeira vez, ele usa atributos definidos manualmente por um administrador do sistema. Quando o canal é interrompido e reiniciado, ele seleciona os atributos da definição do canal do receptor de clusters correspondente. A definição de canal do emissor de clusters original é sobrescrita com os novos atributos, incluindo o atributo `SecurityExit`.

Procedimento

1. Deve-se definir uma saída de segurança em ambas as extremidades do emissor de cluster e o receptor de cluster de um canal.

   A conexão inicial deve ser feita com um handshake de saída de segurança, mesmo que o nome de saída de segurança seja enviado a partir da definição do receptor de cluster.
2. Valide o `PartnerName` na estrutura `MQCXP` na saída de segurança.

   A saída deve permitir que o canal inicie somente se o gerenciador de filas do parceiro estiver autorizado
3. Projete a saída de segurança na definição do receptor de cluster para ser iniciada pelo destinatário.
4. Se você projetá-la como iniciada pelo emissor, um gerenciador de filas não autorizado sem uma saída de segurança poderá unir-se ao cluster porque nenhuma verificação de segurança será executada.

   Não até o canal ser interrompido e reiniciado pode o nome `SCYEXIT` ser enviado a partir da definição do receptor de cluster e verificações de segurança integral feita.
5. Para visualizar a definição de canal do emissor de clusters que está atualmente em uso, use o comando:

   ```
   DISPLAY CLUSQMGR( queue manager ) ALL
   ```

   O comando exibe os atributos que foram enviados a partir da definição do receptor de clusters.
6. Para visualizar a definição original, use o comando:

   ```
   DISPLAY CHANNEL( channel name ) ALL
   ```
7. Você pode precisar definir uma saída de autodefinição de canal `CHADEXIT`, no gerenciador de filas do emissor de cluster, se os gerenciadores de filas estiverem em plataformas diferentes.

   Use a saída de definição automática de canal para configurar o atributo `SecurityExit` para um formato apropriado para a plataforma de destino.
8. Implementar e configurar a saída de segurança.

   z/OS z/OS

   O módulo de carregamento de saída de segurança deve estar no conjunto de dados especificado na instrução `CSQXLIB DD` do procedimento de espaço de endereço do inicializador de canais.

   ULW Sistemas Windows, UNIX and Linux

   - A biblioteca de vínculo dinâmico de saída de segurança deve estar no caminho especificado no atributo `SCYEXIT` da definição de canal.
   - A biblioteca de vínculo dinâmico de saída de autodefinição de canal deve estar no caminho especificado no atributo `CHADEXIT` da definição do gerenciador de filas.

Forçando Gerenciadores de Filas Indesejáveis a Sair de um Cluster

Forçar um gerenciador de filas indesejado para deixar um cluster, emitindo o comando `RESET CLUSTER` em um gerenciador de filas de repositório completo.

Sobre esta tarefa

É possível forçar um gerenciador de filas indesejado para deixar um cluster. Se, por exemplo, um gerenciador de filas for excluído mas seus canais do receptor de clusters ainda estiverem definidos no cluster. Você pode desejar organizar.

Somente gerenciadores de fila de repositório completo têm autorização para ejetar um gerenciador de filas de um cluster.

Nota: Embora usar o comando RESET CLUSTER coercivamente remove um gerenciador de filas de um cluster, o uso de RESET CLUSTER por si só não impede que o gerenciador de filas se una ao cluster posteriormente. Para assegurar que o gerenciador de filas não se unirá novamente ao cluster, siga as etapas detalhadas em "Impedindo que Gerenciadores de Filas se Juntem a um Cluster" na página 465.

Siga este procedimento para ejetar o gerenciador de filas OSLO do cluster NORWAY:

Procedimento

1. Em um gerenciador de filas de repositório completo, emita o comando:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Como alternativa use o QMID em vez de QMNAME no comando:

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

   Nota: QMID é uma sequência, portanto, o valor de qmid deve ser colocado entre aspas simples, por exemplo, QMID('FR01_2019-07-15_14.42.42').

Resultados

O gerenciador de filas que é removido à força não muda; suas definições de cluster local mostram que ele está no cluster. As definições em todos os outros gerenciadores de filas não mostram isso no cluster.

Impedindo que gerenciadores de filas recebam mensagens

É possível evitar que um gerenciador de filas do cluster receba mensagens que ele não está autorizado a receber, usando programas de saída.

Sobre esta tarefa

É difícil parar a definição de uma fila por um gerenciador de filas que é membro de um cluster. Há um risco de que um gerenciador de filas nocivo se una a um cluster e defina sua própria instância de uma das filas no cluster. Agora ele pode receber mensagens que ele não está autorizado a receber. Para impedir que um gerenciador de filas receba mensagens, use uma das seguintes opções determinado no procedimento.

Procedimento

- Um programa de saída do canal em cada canal do emissor de clusters. O programa de saída usa o nome de conexão para determinar a adequação do gerenciador de filas de destino para que as mensagens sejam enviadas.
- Um programa de saída de carga de do cluster que usa os registros de destino para determinar a adequação da fila de destino e do gerenciador de filas para ser enviadas as mensagens.

SSL/TLS e clusters

Ao configurar o TLS para clusters, esteja ciente que uma definição de canal CLUSRCVR é propagada para outros gerenciadores de filas como um canal CLUSSDR autodefinido. Se um canal CLUSRCVR usar TLS, você deverá configurar o TLS em todos os gerenciadores de filas que se comunicarem usando o canal.

Para obter informações adicionais sobre o TLS, consulte "Protocolos de segurança TLS no IBM MQ" na página 24. O conselho lá geralmente é aplicável aos canais do cluster, mas talvez você deseje fornecer alguma consideração especial ao seguinte:

Em um cluster do IBM MQ uma determinada definição de canal CLUSRCVR é frequentemente propagada a muitos outros gerenciadores de filas nos quais é transformada em um CLUSSDR definido automaticamente. Subsequentemente o CLUSSDR definido automaticamente é usado para iniciar um

canal para o CLUSRCVR. Se o CLUSRCVR for configurado para conectividade TLS, as considerações a seguir se aplicarão:

- Todos os gerenciadores de filas que desejam se comunicar com este CLUSRCVR devem ter acesso ao suporte de TLS. Esta provisão de TLS deve suportar CipherSpec para o canal.
- Os diferentes gerenciadores de filas para os quais os canais do emissor de clusters definidos automaticamente foram propagados terão, cada, um nome distinto diferente associado. Se a verificação de peer de nome distinto deve ser usada no CLUSRCVR ela deve ser configurada para que todos os nomes distintos que serão recebidos sejam correspondidos com sucesso.

  Por exemplo, vamos assumir que todos os gerenciadores de filas que hospedarão os canais do emissor de clusters que se conectarão a um determinado CLUSRCVR possuem certificados associados. Também vamos assumir que os nomes distintos em todos estes certificados definam o país como UK, a organização como IBM, a unidade da organização como IBM MQ Development e que todos possuam nomes comuns no formato DEVT.QMnnn, em que nnn é numérico.

  Neste caso, um valor SSLPEER de C=UK, O=IBM, OU=IBM MQ Development, CN=DEVT.QM* no CLUSRCVR permitirá que todos os canais do receptor de clusters necessários sejam conectados com sucesso, mas evitará a conexão de canais do receptor de clusters não desejados.
- Se cadeias de CipherSpec customizadas forem usadas, esteja ciente de que os formatos de cadeia customizados não são permitidos em todas as plataformas. Um exemplo disso é que a sequência do CipherSpec RC4_SHA_US tem um valor de 05 no IBM i, mas não é uma especificação válida em sistemas UNIX, Linux ou Windows. Portanto, se os parâmetros SSLCIPH customizados forem usados em um CLUSRCVR, todos os canais de emissor de cluster autodefinidos resultantes deverão residir nas plataformas nas quais o suporte de TLS subjacente implementa esse CipherSpec e nas quais ele pode ser especificado com o valor customizado. Se não for possível selecionar um valor para o parâmetro SSLCIPH que será entendido em todo o seu cluster, será preciso uma saída de autodefinição de canal para mudá-lo para algo que as plataformas que estão sendo usadas entendam. Use as sequências textuaisCipherSpec quando possível (por exemplo, TLS_RSA_WITH_AES_128_CBC_SHA).

Um parâmetro SSLCRLNL se aplica a um gerenciador de filas individual e não é propagado a outros gerenciadores de filas em um cluster.

Fazendo upgrade de gerenciadores de filas e canais em cluster para SSL/TLS

Faça upgrade dos canais do cluster um por vez, mudando todos os canais CLUSRCVR antes dos canais CLUSSDR.

Antes de começar

Considere as considerações a seguir, como elas podem afetar sua escolha de CipherSpec para um cluster:

- Alguns CipherSpecs não estão disponíveis em todas as plataformas. Tome cuidado ao escolher um CipherSpec que é suportado por todos os gerenciadores de filas no cluster.
- Alguns CipherSpecs podem ser novos na liberação atual do IBM MQ e não são suportados em releases anteriores. Um cluster contendo gerenciadores de filas em execução em diferentes liberações do MQ somente poderá usar os CipherSpecs suportados por cada liberação.

  Para usar um novo CipherSpec dentro de um cluster, primeiro deve-se migrar todos os gerenciadores de filas do cluster para a liberação atual.
- Alguns CipherSpecs requerem um tipo específico de certificado digital para ser usado, especialmente aquelas que usam Elliptic Curve Cryptography.

Atenção: Não é possível usar uma combinação de certificados assinados por Curva elíptica e certificados assinados por RSA nos gerenciadores de filas que você deseja associar como parte de um cluster.

Os gerenciadores de filas em um cluster devem todos usar certificados assinados por RSA ou certificados assinados pela EC, não uma mistura de ambos.

Veja “Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45 para obter mais informações.

Faça upgrade de todos os gerenciadores de filas no cluster para o IBM MQ V8 ou mais recente, se eles já não estiverem nesses níveis. Distribua os certificados e chaves para que o TLS funcione a partir de cada um deles.

Se desejar fazer upgrade de tom ou usar o ANY_TLS12 CipherSpecs, você deverá fazer upgrade de todos os gerenciadores de fila no cluster para IBM MQ 9.1.2 ou superior.

Se você desejar fazer upgrade para ou usar qualquer um dos outros CipherSpecs de Alias (ANY_TLS13, ANY_TLS12, ANY_TLS12_OR_HIGHERe assim por diante), deverá fazer upgrade de todos os gerenciadores de filas no cluster para IBM MQ 9.1.4 ou superior.

Sobre esta tarefa

Mude os canais CLUSRCVR antes dos canais CLUSSDR.

Procedimento

1. Alterne os canais CLUSRCVR para TLS em qualquer ordem desejada, mudando um CLUSRCVR por vez e permita que as mudanças fluam por meio do cluster antes de mudar o próximo.

   Importante: Certifique-se de não alterar o caminho reverso até que as alterações para o canal atual tenham sido distribuídas por todo o cluster.
2. Opcional: Alterne todos os canais CLUSSDR manuais para TLS.

   Isto não possui qualquer efeito na operação do cluster, a menos que você use o comando REFRESH CLUSTER com a opção REPOS(YES).

   Nota: Para clusters grandes, o uso do comando **REFRESH CLUSTER** pode ser disruptivo para o cluster enquanto ele estiver em andamento e novamente em intervalos de 27 dias depois disso, quando os objetos do cluster enviarem automaticamente atualizações de status para todos os gerenciadores de filas interessados Consulte Atualizando em um grande cluster pode afetar o desempenho e disponibilidade do cluster.
3. Use o comando DISPLAY CLUSQMGR para assegurar que a nova configuração de segurança tenha sido propagada por todo o cluster.
4. Reinicie os canais para usar TLS e execute REFRESH SECURITY (SSL).

Conceitos relacionados

“Ativando CipherSpecs” na página 423
Ative um CipherSpec usando o parâmetro **SSLCIPH** no comando MQSC **DEFINE CHANNEL** ou no comando MQSC **ALTER CHANNEL** .

“Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45
Este tópico fornece informações sobre como escolher os certificados digitais e do CipherSpecs para sua política de segurança, delineando o relacionamento entre os certificados digitais e de CipherSpecs no IBM MQ.

Informações relacionadas

Armazenamento em Cluster: Usando Melhores Práticas de REFRESH CLUSTER

Desativando SSL/TLS em gerenciadores de filas e canais em cluster

Para desativar o TLS, configure o parâmetro SSLCIPH como ' ' Desative TLS nos canais de cluster individualmente, mudando todos os canais do receptor de clusters antes dos canais do emissor de clusters.

Sobre esta tarefa

Mude um canal do receptor de clusters por vez e permita que as mudanças fluam através do antes de mudar o próximo.

Importante: Assegure-se de não mudar o caminho reverso até que as mudanças para o canal atual tenham sido distribuídas por todo o cluster.

Procedimento

1. Configure o valor do parâmetro SSLCIPH como `' '`, uma sequência de caracteres vazia em uma aspa única IBM i ou `*NONE` no IBM i .

   É possível desativar TLS nos canais do receptor de clusters em qualquer ordem desejada.

   Observe que as mudanças fluem na direção oposta nos canais nos quais você deixa o TLS ativo.
2. Verifique se o novo valor é refletido em todos os outros Gerenciadores de Filas usando o comando **DISPLAY CLUSQMGR(*)** ALL.
3. Desligue o TLS em todos os canais do emissor de clusters manuais.

   Isto não possui qualquer efeito na operação do cluster, a menos que você use o comando **REFRESH CLUSTER** com a opção REPOS(YES).

   Para clusters grandes, o uso do comando **REFRESH CLUSTER** pode ser disruptivo para o cluster enquanto ele está em andamento e novamente em intervalos regulares, quando os objetos de cluster enviam automaticamente atualizações de status para todos os gerenciadores de filas interessados. Consulte Atualizando em um cluster grande pode afetar o desempenho e disponibilidade do cluster para obter mais informações.
4. Pare e reinicie os canais do emissor de clusters.

Segurança de Publicação/Assinatura

Os componentes e as interações que estão envolvidos na publicação/assinatura estão descritos como uma introdução para as explicações mais detalhadas e exemplos a seguir.

Existem inúmeros componentes envolvidos na publicação e assinatura para um tópico. Alguns dos relacionamentos de segurança entre eles estão ilustrados em Figura 22 na página 471 e descritos no seguinte exemplo.

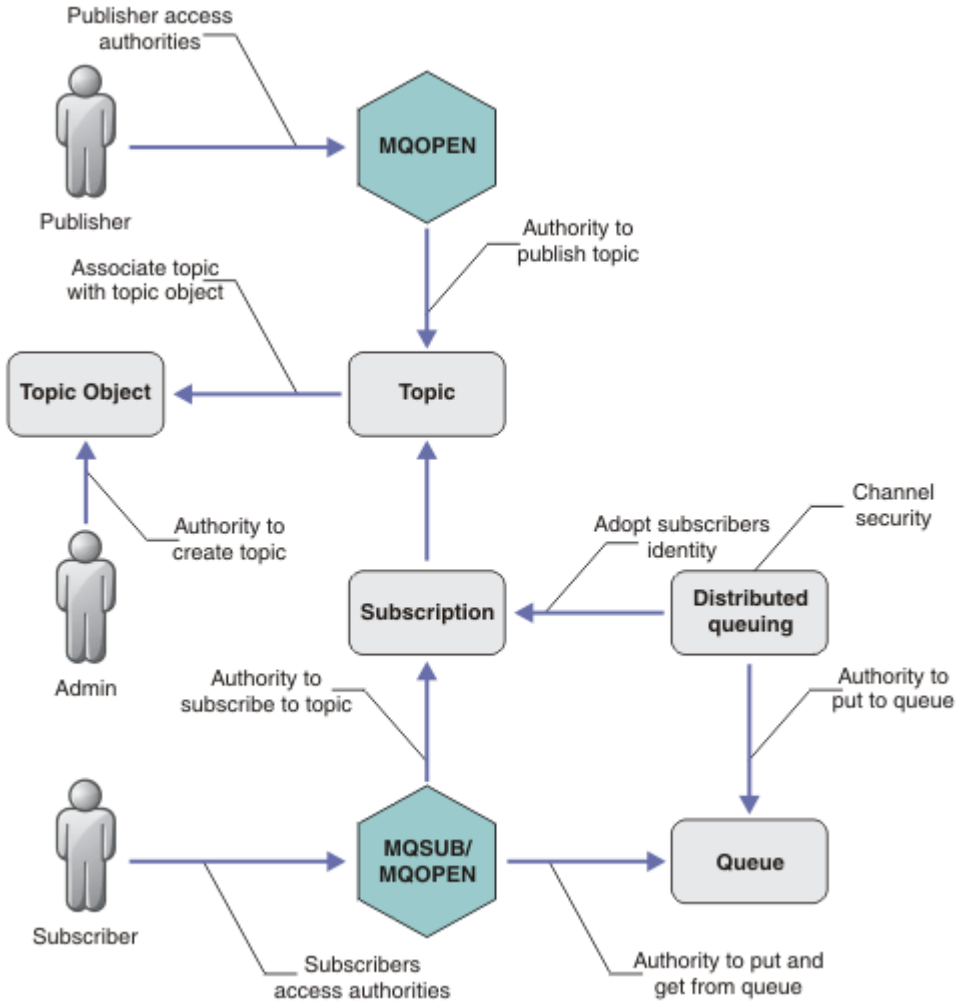


Figura 22. Publicar/assinar relacionamentos de segurança entre vários componentes

Tópicos

Os tópicos são identificados por sequências de tópicos e geralmente organizados em árvores; consulte Árvores de tópicos. É necessário associar um tópico a um objeto do tópico para controlar o acesso ao tópico. O "Modelo de Segurança do Tópico" na página 473 explica como proteger os tópicos usando os objetos do tópico.

Objetos de tópico administrativo

É possível controlar quem tem acesso a um tópico e para qual propósito, usando o comando **setmqaut** com uma lista de objetos de tópico administrativo. Consulte os exemplos, "Conceder acesso a um usuário para assinar um tópico" na página 478 e "Conceder acesso a um usuário para publicar um tópico" na página 485. z/OS Para controlar o acesso a objetos de tópico em z/OS, consulte Perfis para a segurança de tópico.

Assinaturas

Subscreva-se em um ou mais tópicos, criando uma assinatura que fornece uma sequência de tópicos, que pode incluir curingas, para corresponder nas sequências de tópicos das publicações. Para obter detalhes adicionais, consulte:

Subscrever usando um objeto do tópico

"Subscrevendo Usando o Nome do Objeto de Tópico" na página 474

Subscrever usando um tópico

"Subscrevendo Usando a Sequência de Tópicos na Qual o Nó de Tópico não Existe" na página 475

Subscrever usando um tópico com curingas

"Subscrevendo Usando uma Sequência de Tópicos que Contém Caracteres Curinga" na página 475

Uma assinatura contém informações sobre a identidade do assinante e a identidade da fila de destino na qual as publicações devem ser colocadas. Ela também contém informações sobre como a publicação deve ser colocada na fila de destino.

Assim como definir quais assinantes possuem autoridade para se subscrever em certos tópicos, é possível restringir as assinaturas para que sejam usadas por um assinante individual. Também é possível controlar quais informações sobre o assinante são usadas pelo gerenciador de filas quando as publicações forem colocadas na fila de destino. Consulte o "Segurança de assinatura" na página 491.

Filas

A fila de destino é uma fila importante para proteger. É local para o assinante e as publicações que correspondiam à assinatura são colocadas nele. Você precisa considerar o acesso à fila de destino a partir de duas perspectivas:

1. Colocando uma publicação na fila de destino.
2. Obtendo a publicação da fila de destino.

O gerenciador de filas coloca uma publicação na fila de destino usando uma identidade fornecida pelo assinante. O assinante ou um programa que delegou a tarefa de obter as publicações, obtém as mensagens da fila. Consulte o "Autoridade para Filas de Destino" na página 476.

Não há nenhum alias de objeto do tópico, mas é possível usar uma fila de alias como o alias para um objeto do tópico. Se fizer isso, e também verificar a autoridade para usar o tópico para publicação ou assinatura, o gerenciador de filas verificará a autoridade para usar a fila.

"Segurança de Publicação/Assinatura entre os Gerenciadores de Filas" na página 492

Sua permissão para publicar ou subscrever em um tópico é verificada no gerenciador de filas locais usando as identidades e autorizações locais. A autorização não depende de o tópico ser definido ou não, nem de onde está definido. Consequentemente, você precisa executar a autorização de tópico em cada gerenciador de filas em um cluster quando os tópicos em cluster forem usados.

Nota: O modelo de segurança para tópicos difere do modelo de segurança para filas. É possível alcançar o mesmo resultado para as filas definindo um alias da fila localmente para cada fila em cluster.

Os gerenciadores de fila trocam assinaturas em um cluster. Na maioria as configurações de cluster do IBM MQ, os canais são configurados com PUTAUT=DEF para colocar mensagens em filas de destino usando a autoridade do processo do canal. É possível modificar a configuração do canal para usar PUTAUT=CTX para requerer que o usuário assinante tenha autoridade para propagar uma assinatura para outro gerenciador de filas em um cluster.

"Segurança de Publicação/Assinatura entre os Gerenciadores de Filas" na página 492 descreve como alterar as suas definições de canal para controlar quem tem permissão para propagar as assinaturas em outros servidores no cluster.

Autorização

É possível aplicar autorização em objetos de tópico, assim como filas e outros objetos. Existem três operações de autorização, `pub`, `sub` e `resume` que permitem a você aplicar apenas nos tópicos. Os detalhes estão descritos em Especificando Autoridades para Diferentes Tipos de Objeto.

Chamadas de função

Nos programas de publicação e assinatura, como em programas enfileirados, as verificações de autorização são feitas quando os objetos são abertos, criados, alterados ou excluídos. As verificações não são feitas quando as chamadas `MQPUT` ou `MQGET` MQI são feitas para colocar e obter as publicações.

Para publicar um tópico, execute um MQOPEN no tópico, que executa as verificações de autorização. As mensagens publicadas na manipulação de tópico que usam o comando MQPUT, que não executa nenhuma autorização.

Para subscrever-se em um tópico, geralmente execute um comando MQSUB para criar ou retornar a assinatura e também para abrir a fila de destino para receber as publicações. Como alternativa, execute um MQOPEN separado para abrir a fila de destino e, em seguida, execute o MQSUB para criar ou retomar a assinatura.

Independente das chamadas que você usar, o gerenciador de filas verificar se é possível se subscrever no tópico e obter as publicações resultantes da fila de destino. Se a fila de destino não for gerenciada, as verificações de autorização também serão feitas para que o gerenciador de filas consiga colocar as publicações na fila de destino. Ela usa a identidade que adotou de uma assinatura correspondente. É assumido que o gerenciador de filas sempre consegue colocar as publicações nas filas de destino gerenciadas.

Papéis

Os usuários estão envolvidos em quatro funções na execução de aplicativos de publicação/assinatura:

1. Publisher
2. Assinante
3. Administrador do tópico
4. IBM MQ Administrador - membro do grupo mqm

Defina os grupos com autorizações apropriadas correspondentes às funções de administração do tópico, publicação e assinatura. Em seguida, é possível designar os diretores desses grupos autorizando-os a executar tarefas específicas de publicação e assinatura.

Além disso, você precisa estender as autorizações de operações administrativas para o administrador das filas e canais responsáveis por mover as publicações e assinaturas.

Modelo de Segurança do Tópico

Apenas os objetos de tópico definido possuem atributos de segurança associados. Para uma descrição de objetos de tópico, consulte Objetos de tópico administrativo. Os atributos de segurança especificam se um ID do usuário especificado ou grupo de segurança, tem permissão para executar uma operação de assinatura ou publicação em cada objeto do tópico.

Os atributos de segurança são associados ao nó de administração apropriado na árvore de tópicos. Quando uma verificação de autoridade é feita para um determinado ID do usuário durante uma operação de assinatura ou publicação, a autoridade concedida será baseada nos atributos de segurança do nó associado da árvore de tópicos.

Os atributos de segurança são uma lista de controle de acesso, que indica qual autoridade um determinado ID do usuário do sistema operacional ou grupo de segurança tem para o objeto do tópico.

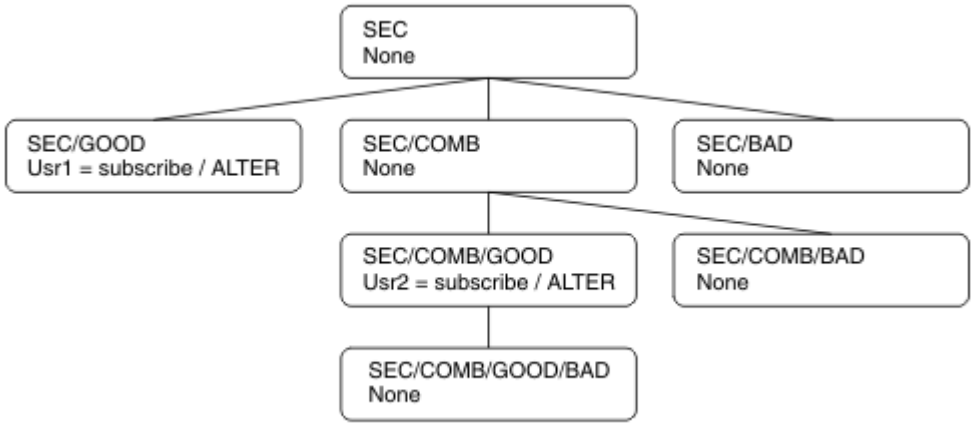
Considere o seguinte exemplo no qual os objetos do tópico foram definidos com os atributos de segurança ou autoridades mostradas:

Tabela 80. Autoridades de Objeto do Tópico de Exemplo

Nome do tópico	**Cadeia do tópico**	**Autoridades - não z/OS**	**autoridades do z/OS**
SECROOT	SEC	Nenhum	Nenhum
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Nenhum	Nenhum HLQ.SUBSCRIBE.SECBAD

Tabela 80. Autoridades de Objeto do Tópico de Exemplo (continuação)			
Nome do tópico	**Cadeia do tópico**	**Autoridades - não z/OS**	**autoridades do z/OS**
SECCOMB	SEC/COMB	Nenhum	Nenhum HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Nenhum	Nenhum HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Nenhum	Nenhum HLQ.SUBSCRIBE.SECCOMBN

A árvore de tópicos com os atributos de segurança associados em cada nó pode ser representada da seguinte maneira:



Os exemplos listados fornecem as seguintes autorizações:

- No nó-raiz da árvore /SEC, nenhum usuário tem autoridade nesse nó.
- usr1 recebeu autoridade de assinatura para o objeto /SEC/GOOD
- usr2 recebeu autoridade de assinatura para o objeto /SEC/COMB/GOOD

Subscrevendo Usando o Nome do Objeto de Tópico

Ao subscrever em um objeto do tópico especificando o nome MQCHAR48, o nó correspondente na árvore de tópicos está localizado. Se os atributos de segurança associados ao nó indicarem que o usuário tem autoridade para se subscrever, então o acesso será concedido.

Se o usuário não tiver acesso concedido, o nó pai na árvore determinará se o usuário tem autoridade para se subscrever no nível de nó pai. Em caso positivo, o acesso é concedido. Em caso negativo, o pai desse nó será considerado. A recursão continua até que seja localizado um nó que conceda autoridade de assinatura para o usuário. A recursão para quando o nó-raiz é considerado sem que a autoridade tenha sido concedida. No último caso, o acesso é negado.

Em resumo, se algum nó no caminho conceder autoridade para se subscrever nesse usuário ou aplicativo, o assinante terá permissão para se subscrever nesse nó ou em qualquer local abaixo desse nó na árvore de tópicos.

O nó-raiz no exemplo é SEC.

O usuário recebe autoridade de assinatura, se a lista de controle de acesso indicar que o ID do usuário em si tem autoridade ou se um grupo de segurança do sistema operacional do qual o ID do usuário é membro tiver autoridade.

Assim, por exemplo:

- Se `usr1` tentar se subscrever, usando uma sequência de tópicos de `SEC/GOOD`, a assinatura seria alocada porque o ID do usuário tem acesso ao nó associado a esse tópico. No entanto, se `usr1` tentou se subscrever usando a sequência de tópicos `SEC/COMB/GOOD` a assinatura não seria permitida porque o ID do usuário não tem acesso ao nó associado.
- Se o `usr2` tentar se subscrever, usando uma sequência de tópicos de `SEC/COMB/GOOD`, a assinatura seria alocada porque o ID do usuário tem acesso ao nó associado ao tópico. No entanto, se `usr2` tentou se subscrever ao `SEC/GOOD` a assinatura não seria permitida porque o ID do usuário não tem acesso ao nó associado.
- Se `usr2` tentar se subscrever usando uma sequência de tópicos de `SEC/COMB/GOOD/BAD`, a assinatura seria permitida porque o ID do usuário tem acesso ao nó-pai `SEC/COMB/GOOD`.
- Se `usr1` ou `usr2` tentar se subscrever usando uma sequência de tópicos de `/SEC/COMB/BAD`, nenhum seria permitido porque não possuem acesso ao nó de tópico associado, ou nós pais desse tópico.

Uma operação de assinatura que especifica o nome de um objeto do tópico que não existe resulta em um erro de MQRC_UNKNOWN_OBJECT_NAME.

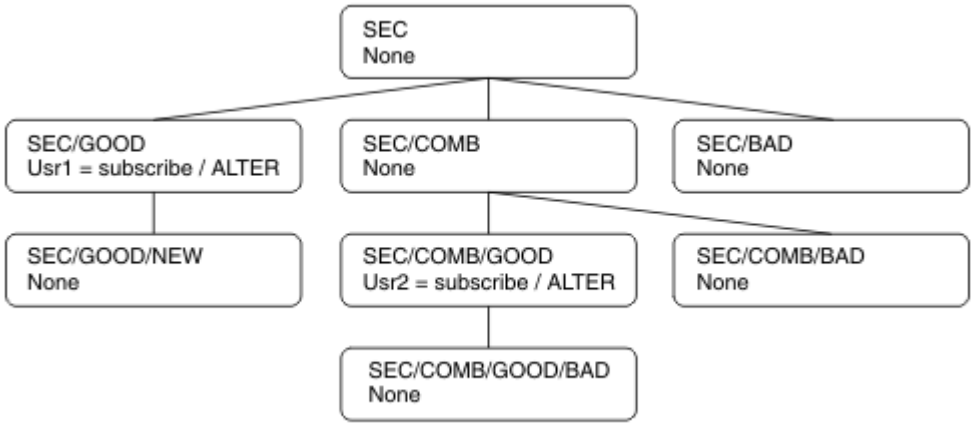
Subscrevendo Usando a Sequência de Tópicos na Qual o Nó de Tópico Existe

O comportamento é igual ao quando especificar o tópico pelo nome do objeto MQCHAR48.

Subscrevendo Usando a Sequência de Tópicos na Qual o Nó de Tópico não Existe

Considere o caso de uma assinatura de aplicativo, especificando uma sequência de tópicos que representa um nó de tópico que não existe atualmente na árvore de tópicos. A verificação de autoridade é executada conforme descrito na seção anterior. A verificação inicia com o nó pai do qual é representado pela sequência de tópicos. Se a autoridade for concedida, um novo nó que representa a sequência de tópicos será criado na árvore de tópicos.

Por exemplo, `usr1` tenta se subscrever em um tópico `SEC/GOOD/NEW`. A autoridade é concedida porque `usr1` tem acesso ao nó-pai `SEC/GOOD`. Um novo nó de tópico é criado na árvore conforme o seguinte diagrama é mostrado. O novo nó de tópico não é um objeto do tópico, ele não tem qualquer atributo de segurança associado diretamente; os atributos são herdados do seu pai.



Subscrevendo Usando uma Sequência de Tópicos que Contém Caracteres Curinga

Considere o caso de subscrever usando uma sequência de tópicos que contém um caractere curinga. A verificação de autoridade é feita no nó na árvore de tópicos que corresponde à parte completa da sequência de tópicos.

Portanto, se um aplicativo se subscrever ao SEC/COMB/GOOD/*, uma verificação de autoridade será executada conforme detalhado nas duas seções anteriores no nó SEC/COMB/GOOD na árvore de tópicos.

De maneira semelhante, se um aplicativo precisar ser subscrever ao SEC/COMB/*/GOOD, uma verificação de autoridade será executada no nó SEC/COMB.

Autoridade para Filas de Destino

Ao se inscrever em um tópico, um dos parâmetros é o identificador hobj de uma fila que foi aberta para saída para receber as publicações.

Se hobj não for especificado, mas estiver em branco, uma fila gerenciada será criada se as condições a seguir se aplicarem:

- A opção MQSO_MANAGED foi especificada.
- A assinatura não existe.
- A criação é especificada.

Se hobj estiver em branco e você estiver mudando ou retomando uma assinatura existente, a fila de destino fornecida anteriormente poderá ser gerenciada ou não gerenciada.

O aplicativo ou o usuário que faz a solicitação MQSUB deve ter a autoridade para colocar as mensagens na fila de destino que forneceu; na realidade, a autoridade para fazer com que as mensagens publicadas sejam colocadas nessa fila. A verificação de autoridade segue as regras existentes para a verificação de segurança da fila.

A verificação de segurança inclui verificações alternativas de contexto e ID do usuário onde necessário. Para conseguir configurar alguns dos campos de contexto de Identidade você deve especificar a opção MQSO_SET_IDENTITY_CONTEXT bem como a opção MQSO_CREATE ou MQSO_ALTER. Não é possível configurar qualquer um dos campos de contexto de Identidade em uma solicitação MQSO_RESUME.

Se o destino for uma fila gerenciada, nenhuma verificação de segurança será executada no destino gerenciado. Se tiver permissão para se subscrever em um tópico, é assumido você pode usar os destinos gerenciados.

Publicando Usando o Nome do Tópico ou Sequência de Tópicos Onde Existir o Nó de Tópico

O modelo de segurança para publicação é o mesmo que para assinatura, com exceção dos curingas. Publicações não contêm curingas; portanto, não há nenhum caso de uma sequência de tópicos contendo curingas para ser considerado.

As autoridades para publicar e subscrever são distintas. Um usuário ou grupo pode ter a autoridade para executar uma sem conseguir necessariamente executar a outra.

Ao publicar em um objeto do tópico especificando o nome MQCHAR48 ou a sequência de tópicos, o nó correspondente na árvore de tópicos será localizado. Se os atributos de segurança associados ao nó de tópico indicarem que o usuário tem autoridade para publicar, o acesso será concedido.

Se o acesso não for concedido, o nó pai na árvore determinará se o usuário tem autoridade para publicar nesse nível. Em caso positivo, o acesso é concedido. Em caso negativo, a recursão continuará até que seja localizado um nó que conceda autoridade de publicação ao usuário. A recursão para quando o nó-raiz é considerado sem que a autoridade tenha sido concedida. No último caso, o acesso é negado.

Em resumo, se algum nó no caminho conceder autoridade para publicar nesse usuário ou aplicativo, o publicador terá permissão para publicar nesse nó ou em qualquer lugar abaixo desse nó na árvore de tópicos.

Publicando Usando o Nome do Tópico ou Sequência de Tópicos Onde não Existir o Nó de Tópico

Assim como na operação de assinatura, quando um aplicativo é publicado, especificando uma sequência de tópicos que representa um nó de tópico que não existe atualmente na árvore de tópicos, a verificação de autoridade é executada iniciando com o pai do nó representado pela sequência de tópicos. Se a autoridade for concedida, um novo nó que representa a sequência de tópicos será criado na árvore de tópicos.

Publicando Usando uma Fila de Alias que Resolve em um Objeto de Tópico

Se você publicar usando uma fila de alias que é resolvida em um objeto de tópico, a verificação de segurança ocorrerá na fila de alias e no tópico subjacente no qual é resolvido.

A verificação de segurança na fila de alias verifica se o usuário tem autoridade para colocar as mensagens nessa fila de alias e a verificação de segurança no tópico verifica se o usuário pode publicar nesse tópico. Quando uma fila de alias é resolvida para outra fila, as verificações não são feitas na fila subjacente. A verificação de autoridade é executada de maneira diferente para os tópicos e as filas.

Fechando uma Assinatura

Ocorre uma verificação de segurança adicional se você fechar a assinatura usando a opção `MQCO_REMOVE_SUB` se não criar a assinatura sob esta manipulação.

Uma verificação de segurança é executada para assegurar que tenha a autoridade correta para fazer isso porque a ação resulta na remoção da assinatura. Os atributos de segurança associados ao nó de tópico indicam que o usuário tem autoridade e, em seguida, o acesso é concedido. Em caso negativo, o nó-pai na árvore é considerado para determinar se o usuário tem autoridade para fechar a assinatura. A recursão continua até que a autoridade seja concedida ou o nó-raiz seja atingido.

Definindo, Alterando e Excluindo uma Assinatura

Nenhuma verificação de segurança de assinatura é executada quando uma assinatura for criada administrativamente, em vez de usar uma solicitação de API `MQSUB`. O administrador já recebeu esta autoridade por meio do comando.

As verificações de segurança são executadas para assegurar que as publicações podem ser colocadas na fila de destino associadas à assinatura. As verificações são executadas da mesma maneira que para uma solicitação `MQSUB`.

O ID do usuário que é usado para essas verificações de segurança depende do comando sendo emitido. Se o parâmetro **SUBUSER** for especificado, ele afetará a maneira como a verificação é executada, conforme mostrado em Tabela 81 na página 477:

Tabela 81. IDs de Usuário Usados para Verificações de Segurança para Comandos

Comando:	SUBUSER especificado e em branco	SUBUSER especificado e concluído	SUBUSER não especificado
	Use o ID de administrador		Use o ID do usuário a partir da assinatura LIKE

Tabela 81. IDs de Usuário Usados para Verificações de Segurança para Comandos (continuação)			
Comando:	**SUBUSER especificado e em branco**	**SUBUSER especificado e concluído**	**SUBUSER não especificado**
	Use o ID de administrador		Use o ID do.DEFAULT.SU usuário aB - se estiver partir daem branco, assinaturause o ID de SYSTEMadministrador
	Use o ID de administrador		Use o ID do usuário a partir da assinatura existente

A única verificação de segurança executada ao excluir as assinaturas usando o comando DELETE SUB é a verificação de segurança de comando.

Exemplo de configuração de segurança de publicação/assinatura

Esta seção descreve um cenário que tem o controle de acesso configurado em tópicos de uma maneira que permita que o controle de segurança seja aplicado conforme necessário.

Conceder acesso a um usuário para assinar um tópico

Este tópico é o primeiro em uma lista de tarefas que informam como conceder acesso aos tópicos por mais de um usuário.

Sobre esta tarefa

Esta tarefa assume que nenhum objeto de tópico administrativo existe nem quaisquer perfis foram definidos para assinatura ou publicação. Os aplicativos estão criando novas assinaturas em vez de continuar as existentes e estão fazendo isso usando somente a sequência de tópicos.

Um aplicativo pode fazer uma assinatura fornecendo um objeto do tópico, uma sequência de tópicos ou uma combinação de ambos. Independentemente do caminho o aplicativo selecione, o efeito é fazer uma assinatura em um determinado ponto na árvore de tópicos. Se este ponto na árvore de tópicos for representado por um objeto de tópico administrativo, um perfil de segurança será verificado com base no nome do objeto do tópico.

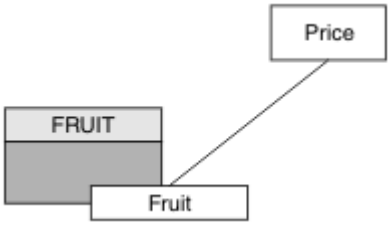


Figura 23. Exemplo de acesso do objeto do tópico

Tabela 82. Acesso ao objeto do tópico de exemplo		
Tópico	**Acesso de assinatura necessário**	**Objeto do Tópico**
Preço (Real R$)	Nenhum usuário	Nenhum
Preço/Fruta	USER1	FRUTA

Defina um novo objeto do tópico conforme a seguir:

Procedimento

1. Emita o comando MQSC `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Conceda acesso como a seguir:
   - z/OS **z/OS** :

     Conceda acesso a USER1 para assinar o tópico `"Price/Fruit"` concedendo o acesso do usuário ao perfil `hlq.SUBSCRIBE.FRUIT`. Faça isso usando os comandos RACF a seguir:

     ```
     RDEFINE MXTOPIC hlq.SUBSCRIBE.FRUIT UACC(NONE)
     PERMIT hlq.SUBSCRIBE.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
     ```

   - Em outras plataformas:

     Conceda acesso a USER1 para assinar o tópico `"Price/Fruit"` concedendo o acesso do usuário ao objeto FRUIT. Faça isso usando o comando de autorização para a plataforma:

     ULW **Sistemas Windows, UNIX and Linux**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

     IBM i **IBM i**

     ```
     GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*SUB)
     ```

Resultados

Quando USER1 tenta assinar o tópico `"Price/Fruit"` o resultado é sucesso.

Quando USER2 tenta assinar o tópico `"Price/Fruit"` o resultado é uma falha com uma mensagem `MQRC_NOT_AUTHORIZED`, juntamente com:

- z/OS No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Em outras plataformas, o evento de autorização a seguir:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  ```

```
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- IBM i No IBMi, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Observe que esta é uma ilustração do que você vê; não todos os campos.

Conceder acesso a um usuário para assinar um tópico mais fundo na árvore

Este tópico é o segundo em uma lista de tarefas que informam como conceder acesso aos tópicos por mais de um usuário.

Antes de começar

Este tópico usa a configuração descrita em "Conceder acesso a um usuário para assinar um tópico" na página 478.

Sobre esta tarefa

Se o ponto na árvore de tópicos no qual o aplicativo faz a assinatura não é representado por um objeto de tópico administrativo, mova para cima na árvore até que o objeto do tópico administrativo pai mais próximo seja localizado. O perfil de segurança é verificado com base no nome do objeto do tópico.

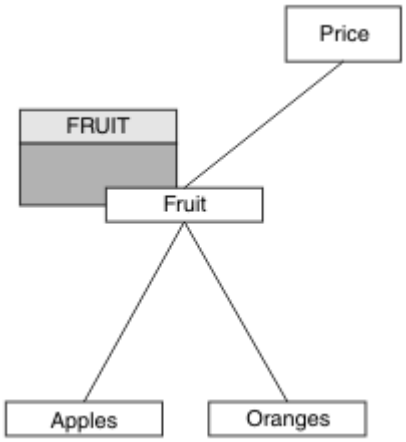


Figura 24. Exemplo de concessão de acesso a um tópico em uma árvore de tópicos

Tabela 83. Requisitos de acesso para tópicos de exemplo e objetos de tópico

Tópico	Acesso de assinatura necessário	Objeto do Tópico
Preço (Real R$)	Nenhum usuário	Nenhum
Preço/Fruta	USER1	FRUTA
Preço/Fruta/ Maçãs	USER1	
Preço/Fruta/ Laranjas	USER1	

Na tarefa anterior USER1 foi concedido acesso para assinar o tópico "Price/Fruit" concedendo acesso ao perfil hlq.SUBSCRIBE.FRUIT no z/OS e assine o acesso ao perfil FRUIT em outras plataformas. Esse perfil único também concede acesso para assinar USER1 para "Price/Fruit/Apples", "Price/Fruit/Oranges" e "Price/Fruit/#".

Quando USER1 tenta assinar o tópico "Price/Fruit/Apples" o resultado é sucesso.

Quando USER2 tenta assinar o tópico "Price/Fruit/Apples" o resultado é uma falha com uma mensagem MQRC_NOT_AUTHORIZED, juntamente com:

- No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Em outras plataformas, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Apples"
```

Observe o seguinte :

- As mensagens que você recebe no z/OS são idênticas àquelas recebidas na tarefa anterior como os mesmos objetos e perfis de objeto estão controlando o acesso.
- A mensagem do evento que você recebe em outras plataformas é semelhante à recebida na tarefa anterior, mas a sequência de tópicos real é diferente.

Garanta acesso a outro usuário para assinar somente o tópico dentro da árvore

Este tópico é o terceiro em uma lista de tarefas que informam como conceder acesso para assinar tópicos por mais de um usuário.

Antes de começar

Este tópico usa a configuração descrita em “Conceder acesso a um usuário para assinar um tópico mais fundo na árvore” na página 480.

Sobre esta tarefa

Na tarefa anterior foi recusado o acesso do USER2 ao tópico "Price/Fruit/Apples". Esse tópico informa como conceder acesso a esse tópico, mas não para quaisquer outros tópicos.

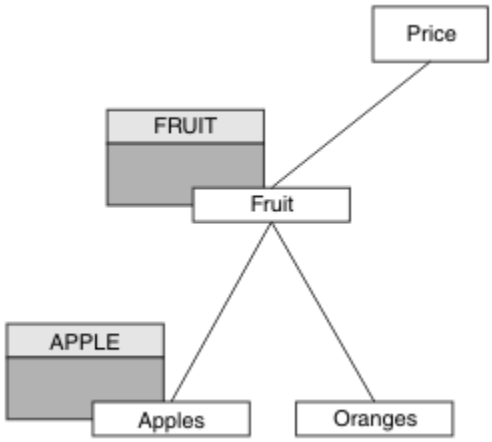


Figura 25. Concedendo acesso a tópicos específicos em uma árvore de tópicos

Tabela 84. Requisitos de acesso para tópicos de exemplo e objetos de tópico		
Tópico	**Acesso de assinatura necessário**	**Objeto do Tópico**
Preço (Real R$)	Nenhum usuário	Nenhum
Preço/Fruta	USER1	FRUTA
Preço/Fruta/ Maçãs	USER1 e USER2	APPLE
Preço/Fruta/ Laranjas	USER1	

Defina um novo objeto do tópico conforme a seguir:

Procedimento

1. Emita o comando MQSC `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Conceda acesso como a seguir:

- z/OS **z/OS** :

  Na tarefa anterior USER1 foi concedido acesso para assinar o tópico `"Price/Fruit/Apples"` concedendo o acesso do usuário ao perfil `hlq.SUBSCRIBE.FRUIT`.

  Este perfil único também concedeu acesso ao USER1 para assinar `"Price/Fruit/Oranges"` `"Price/Fruit/#"` e esse acesso permanece mesmo com a inclusão do objeto do tópico novo e os perfis associados a ele.

  Conceder acesso a USER2 para assinar o tópico `"Price/Fruit/Apples"` concedendo o acesso do usuário ao perfil `hlq.SUBSCRIBE.APPLE`. Faça isso usando os comandos RACF a seguir:

  ```
  RDEFINE MXTOPIC hlq.SUBSCRIBE.APPLE UACC(NONE)
  PERMIT hlq.SUBSCRIBE.FRUIT APPLE(MXTOPIC) ID(USER2) ACCESS(ALTER)
  ```

- Em outras plataformas:

  Na tarefa anterior USER1 recebeu acesso para assinar o tópico `"Price/Fruit/Apples"` concedendo ao usuário acesso de assinatura ao perfil `FRUIT`.

Este perfil único também concedeu acesso USER1 para acessar "Price/Fruit/Oranges" e "Price/Fruit/#" e esse acesso permanece mesmo com a inclusão do novo objeto do tópico e os perfis associados a ele.

Conceda acesso a USER2 para assinar o tópico "Price/Fruit/Apples" concedendo o acesso à assinatura do usuário para o perfil APPLE. Faça isso usando o comando de autorização para a plataforma:

ULW **Sistemas Windows, UNIX and Linux**

```
setmqaut -t topic -n APPLE -p USER2 +sub
```

IBM i **IBM i**

```
GRTMQAUT OBJ(APPLE) OBJTYPE(*TOPIC) USER(USER2) AUT(*SUB)
```

Resultados

No z/OS, quando USER1 tenta assinar o tópico "Price/Fruit/Apples" a primeira verificação de segurança no perfil hlq.SUBSCRIBE.APPLE falha, mas ao mover a árvore do perfil para cima o perfil hlq.SUBSCRIBE.FRUIT permite que o USER1 assine, portanto, a assinatura é bem-sucedida e nenhum código de retorno será enviado para a chamada MQSUB. No entanto, uma mensagem RACF ICH é gerada para a primeira verificação:

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Quando USER2 tenta assinar o tópico "Price/Fruit/Apples" o resultado é sucesso porque a verificação de segurança aprova o primeiro perfil.

Quando USER2 tenta assinar o tópico "Price/Fruit/Oranges" o resultado será uma falha com uma mensagem MQRC_NOT_AUTHORIZED juntamente com:

- z/OS No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

  ```
  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.FRUIT ...

  ICH408I USER(USER2   ) ...
    hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
  ```

- ULW Nas plataformas Windows, UNIX and Linux o evento de autorização a seguir:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

- IBM i No IBMi, o evento de autorização a seguir:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

A desvantagem dessa configuração é que, no z/OS, você receberá mensagens ICH adicionais no console. É possível evitar isso se você proteger a árvore de tópicos de maneira diferente.

Mudar o controle de acesso para evitar mensagens adicionais

Este tópico é o quarto em uma lista de tarefas que informam como conceder acesso para assinar tópicos por mais de um usuário e para evitar mensagens ICH408I adicionais do RACF no z/OS.

Antes de começar

Este tópico aprimora a configuração descrita em "Garanta acesso a outro usuário para assinar somente o tópico dentro da árvore" na página 481 para que você evite mensagens de erro adicionais.

Sobre esta tarefa

Esse tópico informa como conceder acesso a tópicos mais profundos na árvore e como remover o acesso ao tópico para baixo na árvore quando nenhum usuário requerer isso.

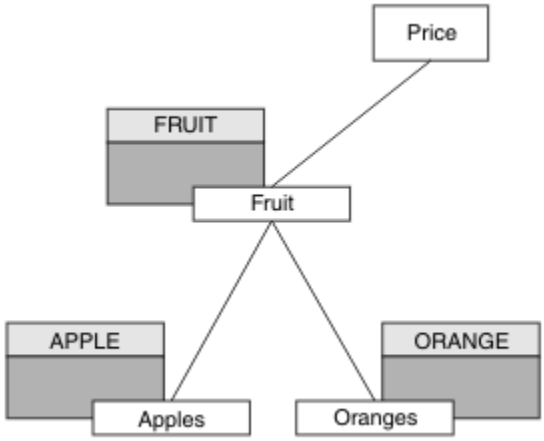


Figura 26. Exemplo de concessão do controle de acesso para evitar mensagens adicionais.

Defina um novo objeto do tópico conforme a seguir:

Procedimento

1. Emita o comando MQSC `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Conceda acesso como a seguir:

   - z/OS **z/OS** :

     Defina um novo perfil e inclua acesso àquele perfil e aos perfis existentes. Faça isso usando os comandos RACF a seguir:

     ```
     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)
     ```

   - Em outras plataformas:

     Configure o acesso equivalente usando os comandos de autorização para a plataforma:

     ULW **Sistemas Windows, UNIX and Linux**

     ```
     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)
```

Resultados

No z/OS, quando USER1 tenta assinar o tópico `"Price/Fruit/Apples"` a primeira verificação de segurança no perfil `hlq.SUBSCRIBE.APPLE` é bem-sucedida.

Da mesma forma, quando o USER2 tenta assinar o tópico `"Price/Fruit/Apples"` o resultado é sucesso porque a verificação de segurança aprova o primeiro perfil.

Quando USER2 tenta assinar o tópico `"Price/Fruit/Oranges"` o resultado será uma falha com uma mensagem `MQRC_NOT_AUTHORIZED` juntamente com:

- **z/OS** No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.ORANGE ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- **ULW** Em outras plataformas, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

- **IBM i** No IBMi, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

Conceder acesso a um usuário para publicar um tópico

Este tópico é o primeiro uma em uma lista de tarefas que informam como conceder acesso para publicar os tópicos por mais de um usuário.

Sobre esta tarefa

Esta tarefa assume que nenhum objeto de tópico administrativo exista no lado direito da árvore de tópicos, nem quaisquer perfis foram definidos para publicação. A suposição usada é que os publicadores estão usando somente a sequência de tópicos.

Um aplicativo pode publicar em um tópico fornecendo um objeto do tópico, uma sequência de tópicos ou uma combinação de ambos. Qualquer forma o aplicativo seleciona, o efeito é publicar em um determinado ponto na árvore de tópicos. Se este ponto na árvore de tópicos for representado por um objeto de tópico administrativo, um perfil de segurança será verificado com base no nome do objeto do tópico. Por exemplo:

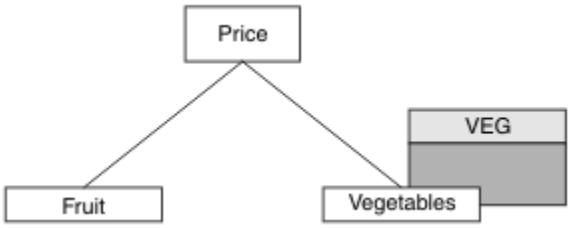


Figura 27. Concedendo acesso de publicação a um tópico

Tabela 85. Exemplo de requisitos de acesso de publicação		
Tópico	**Acesso de publicação necessário**	**Objeto do Tópico**
Preço (Real R$)	Nenhum usuário	Nenhum
Preço/Vegetais	USER1	VEG

Defina um novo objeto do tópico conforme a seguir:

Procedimento

1. Emita o comando MQSC `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Conceda acesso como a seguir:

- z/OS **z/OS** :

  Conceda acesso para USER1 para publicar no tópico `"Price/Vegetables"` concedendo o acesso do usuário ao perfil `hlq.PUBLISH.VEG`. Faça isso usando os comandos RACF a seguir:

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.VEG UACC(NONE)
  PERMIT hlq.PUBLISH.VEG CLASS(MXTOPIC) ID(USER1) ACCESS(UPDATE)
  ```

- Em outras plataformas:

  Conceda acesso para USER1 para publicar no tópico `"Price/Vegetables"` concedendo o acesso do usuário ao perfil VEG. Faça isso usando o comando de autorização para a plataforma:

  ULW **Sistemas Windows, UNIX and Linux**

  ```
  setmqaut -t topic -n VEG -p USER1 +pub
  ```

  IBM i **IBM i**

  ```
  GRTMQAUT OBJ(VEG) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
  ```

Resultados

Quando USER1 tenta publicar no tópico `"Price/Vegetables"` o resultado é sucesso; ou seja, a chamada MQOPEN é bem-sucedida.

Quando USER2 tentar publicar no tópico `"Price/Vegetables"` a chamada MQOPEN falhará com uma mensagem `MQRC_NOT_AUTHORIZED`, juntamente com:

- z/OS No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- ULW Em outras plataformas, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

- IBM i No IBMi, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Observe que esta é uma ilustração do que você vê; não todos os campos.

Conceder acesso a um usuário para publicar em um tópico dentro da árvore

Este tópico é o segundo em uma lista de tarefas que informam como conceder acesso a publicação em tópicos por mais de um usuário.

Antes de começar

Este tópico usa a configuração descrita em “Conceder acesso a um usuário para publicar um tópico” na página 485.

Sobre esta tarefa

Se o ponto na árvore de tópicos no qual o aplicativo publicar não for representado por um objeto do tópico administrativo, mova a árvore para cima até onde o objeto do tópico administrativo pai mais próximo está localizado. O perfil de segurança é verificado com base no nome do objeto do tópico.

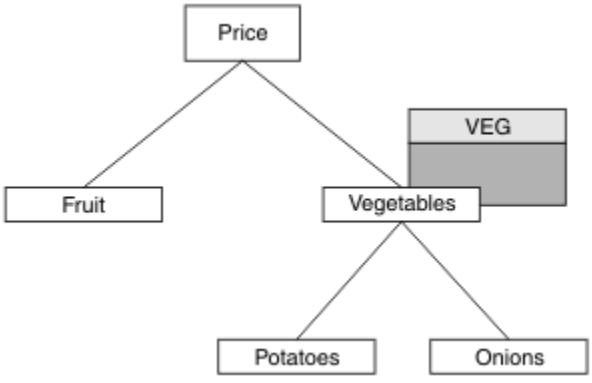


Figura 28. Concedendo acesso de publicação em um tópico em uma árvore de tópicos

Tabela 86. Exemplo de requisitos de acesso de publicação

Tópico	Acesso de assinatura necessário	Objeto do Tópico
Preço (Real R$)	Nenhum usuário	Nenhum
Preço/Vegetais	USER1	VEG
Preço/Vegetais/Batatas	USER1	
Preço/Vegetais/Cebolas	USER1	

Na tarefa anterior USER1 recebeu acesso para publicar o tópico `"Price/Vegetables/Potatoes"` concedendo acesso ao perfil `hlq.PUBLISH.VEG` no z/OS ou acesso de publicação ao perfil `VEG` em outras plataformas. Esse único perfil também concede acesso USER1 para publicação em `"Price/Vegetables/Onions"`.

Quando USER1 tenta publicar no tópico `"Price/Vegetables/Potatoes"` o resultado é sucesso; essa chamada MQOPEN será bem-sucedida.

Quando USER2 tenta assinar o tópico `"Price/Vegetables/Potatoes"` o resultado é uma falha; ou seja, a chamada MQOPEN falhará com uma mensagem `MQRC_NOT_AUTHORIZED`, juntamente com:

- No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Em outras plataformas, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables/Potatoes"
```

Observe o seguinte :

- As mensagens que você recebe no z/OS são idênticas àquelas recebidas na tarefa anterior como os mesmos objetos e perfis de objeto estão controlando o acesso.
- A mensagem do evento que você recebe em outras plataformas é semelhante à recebida na tarefa anterior, mas a sequência de tópicos real é diferente.

Conceder acesso para publicação e assinatura

Este tópico é o último em uma lista de tarefas que informam como conceder acesso para publicar e assinar tópicos por mais de um usuário.

Antes de começar

Este tópico usa a configuração descrita em “Conceder acesso a um usuário para publicar em um tópico dentro da árvore” na página 487.

Sobre esta tarefa

Em uma tarefa anterior USER1 foi fornecido acesso para assinar o tópico `"Price/Fruit"`. Este tópico informa como conceder acesso ao usuário para publicar para o tópico.

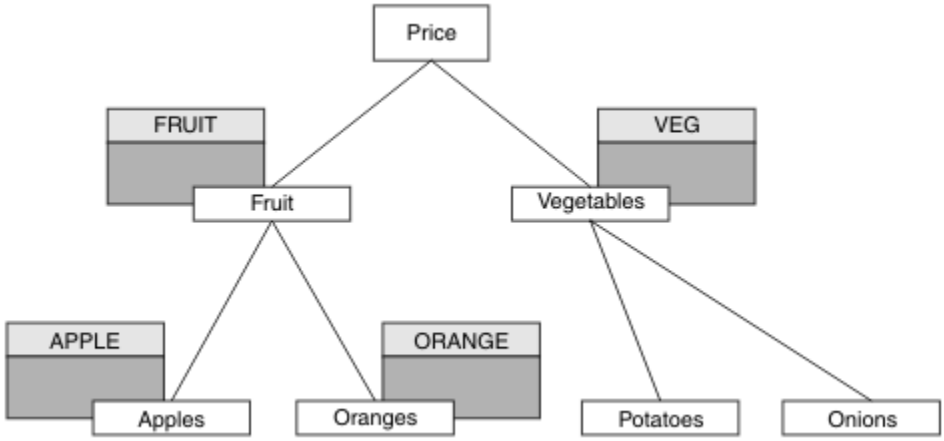


Figura 29. Concedendo acesso para publicação e assinatura

Tabela 87. Exemplo de requisitos de acesso de publicação e assinatura

Tópico	Acesso de assinatura necessário	Acesso de publicação necessário	Objeto do Tópico
Preço (Real R$)	Nenhum usuário	Nenhum usuário	Nenhum
Preço/Fruta	USER1	USER1	FRUTA
Preço/Fruta/ Maçãs	USER1 e USER2		APPLE
Preço/Fruta/ Laranjas	USER1		LARANJA

Procedimento

Conceda acesso como a seguir:

- z/OS **z/OS** :

  Em uma tarefa anterior USER1 recebeu acesso para assinar o tópico `"Price/Fruit"`, concedendo o acesso do usuário ao perfil `hlq.SUBSCRIBE.FRUIT`.

  Para publicar o tópico `"Price/Fruit"` conceda acesso ao USER1 para o perfil `hlq.PUBLISH.FRUIT`. Faça isso usando os comandos RACF a seguir:

  ```
  RDEFINE MXTOPIC hlq.PUBLISH.FRUIT UACC(NONE)
  PERMIT hlq.PUBLISH.FRUIT CLASS(MXTOPIC) ID(USER1) ACCESS(ALTER)
  ```

- Em outras plataformas:

  Conceda acesso para USER1 para publicar no tópico `"Price/Fruit"` por conceder o acesso de publicação do usuário para o perfil FRUIT. Faça isso usando o comando de autorização para a plataforma:

Sistemas Windows, UNIX and Linux

```
setmqaut -t topic -n FRUIT -p USER1 +pub
```

IBM i

```
GRTMQAUT OBJ(FRUIT) OBJTYPE(*TOPIC) USER(USER1) AUT(*PUB)
```

Resultados

No z/OS, quando USER1 tentar de publicar no tópico `"Price/Fruit"` a verificação de segurança na chamada MQOPEN aprova.

Quando USER2 tentar publicar no tópico `"Price/Fruit"`, o resultado será uma falha com uma mensagem `MQRC_NOT_AUTHORIZED`, juntamente com:

- No z/OS, as mensagens a seguir vistas no console que mostram o caminho de segurança completo através da árvore de tópicos que foi tentada:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- No Windows, UNIX e plataformas Linux o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

- No IBMi, o evento de autorização a seguir:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Seguindo o conjunto completo dessas tarefas, fornece USER1 e USER2 as seguintes autoridades de acesso para publicar e subscrever-se nos tópicos listados:

Tabela 88. Conclua lista de autoridades de acesso resultante de exemplos de segurança

Tópico	Acesso de assinatura necessário	Acesso de publicação necessário	Objeto do Tópico
Preço (Real R$)	Nenhum usuário	Nenhum usuário	Nenhum
Preço/Fruta	USER1	USER1	FRUTA
Preço/Fruta/Maçãs	USER1 e USER2		APPLE
Preço/Fruta/Laranjas	USER1		LARANJA

Tabela 88. Conclua lista de autoridades de acesso resultante de exemplos de segurança (continuação)			
Tópico	**Acesso de assinatura necessário**	**Acesso de publicação necessário**	**Objeto do Tópico**
Preço/ Vegetais		USER1	VEG
Preço/ Vegetais/ Batatas			
Preço/ Vegetais/ Cebolas			

Onde houver requisitos diferentes para acesso de segurança em níveis diferentes dentro da árvore de tópicos, o planejamento cuidadoso assegura que você não receberá avisos de segurança externos no log do console do z/OS. Configurando a segurança no nível correto na árvore evita mensagens de segurança enganosas.

Segurança de assinatura

MQSO_ALTERNATE_USER_AUTHORITY

O campo AlternateUserId contém um identificador de usuário a ser usado para validar esta chamada MQSUB. A chamada pode ser bem-sucedida somente se este AlternateUserId estiver autorizado a assinar o tópico com opções de acesso especificadas, independentemente de se o ID do usuário sob o qual o aplicativo estiver em execução está autorizado para tanto.

MQSO_SET_IDENTITY_CONTEXT

A assinatura deve usar o token de conta e os dados de identificação do aplicativo fornecidos nos campos PubAccountingToken e PubApplIdentityData.

Se esta opção for especificada, a mesma verificação de autorização será executada como se a fila de destino tivesse sido acessada usando uma chamada MQOPEN com MQOO_SET_IDENTITY_CONTEXT, exceto no caso em que a opção MQSO_MANAGED também é usada; neste caso, não há nenhuma verificação de autorização na fila de destino.

Se esta opção não for especificada, as publicações enviadas a este assinante terão informações de contexto padrão associadas a elas da seguinte maneira:

Tabela 89. Informações de contexto de publicação padrão	
Campo no MQMD	**Valor Usado**
UserIdentifier	O ID do usuário associado à assinatura (consulte o campo SUBUSER em DISPLAY SBSTATUS) no momento em que a publicação é feita.
AccountingToken	Determinado a partir do ambiente, se possível; caso contrário, configure como MQACT_NONE.
ApplIdentityData	Configure como em branco.

Esta opção é válida apenas com MQSO_CREATE e MQSO_ALTER. Se usada com MQSO_RESUME, os campos PubAccountingToken e PubApplIdentityData são ignorados, portanto, esta opção não tem efeito.

Se uma assinatura é alterada sem o uso dessa opção na qual a opção forneceu informações de contexto anteriormente, as informações de contexto padrão são geradas para assinatura alterada.

Se uma assinatura permitindo que diferentes IDs de usuário a usem com a opção MQSO_ANY_USERID for continuada por um ID do usuário diferente, o contexto de identidade padrão será gerado para o novo ID do usuário que agora possui a assinatura e todas as publicações subsequentes serão entregues contendo o novo contexto de identidade.

AlternateSecurityId

Este é um identificador de segurança que é transmitido com o AlternateUserId para o serviço de autorização para permitir que verificações de autorização apropriadas sejam executadas. AlternateSecurityId é usado somente se MQSO_ALTERNATE_USER_AUTHORITY for especificado e o campo AlternateUserId não estiver completamente em branco até o primeiro caractere nulo ou no final do campo.

Opção de Assinatura MQSO_ANY_USERID

Quando MQSO_ANY_USERID é especificado, a identidade do assinante não é restrita a um único ID do usuário. Isso permite que qualquer usuário altere ou continue a assinatura quando tem autoridade adequada. Apenas um único usuário pode ter a assinatura a qualquer momento. Uma tentativa de continuar o uso de uma assinatura atualmente em uso por outro aplicativo irá fazer com que a chamada falhe com MQRC_SUBSCRIPTION_IN_USE.

Para incluir essa opção a uma assinatura existente a chamada MQSUB (utilizando MQSO_ALTER) deve vir do mesmo ID do usuário da assinatura original.

Se uma chamada MQSUB se referir a uma assinatura existente com MQSO_ANY_USERID configurado e o ID do usuário for diferente da assinatura original, a chamada será bem-sucedida apenas se o novo ID do usuário tiver autoridade para assinar o tópico. Após concluir com sucesso, publicações futuras a este assinante serão colocadas na fila do assinante com o novo ID do usuário configurado na publicação.

MQSO_FIXED_USERID

Quando MQSO_FIXED_USERID é especificado, a assinatura somente pode ser alterada ou retomada por um único ID do usuário proprietário. Este ID do usuário é o último ID do usuário a alterar a assinatura que configura esta opção, removendo a opção MQSO_ANY_USERID ou se nenhuma alteração ocorreu, é o ID do usuário que criou a assinatura.

Se um verbo MQSUB se referir a uma assinatura existente com MQSO_ANY_USERID configurado e altera a assinatura (usando MQSO_ALTER) para usar a opção MQSO_FIXED_USERID, o ID do usuário da assinatura agora será fixo nesse novo ID do usuário. A chamada será bem-sucedida apenas se o novo ID do usuário tiver autoridade para assinar o tópico.

Se um ID do usuário diferente do registrado como pertencente a uma assinatura tenta continuar ou alterar uma assinatura MQSO_FIXED_USERID, a chamada falhará com MQRC_IDENTITY_MISMATCH. O ID do usuário proprietário de uma assinatura pode ser visualizado usando o comando DISPLAY SBSTATUS.

Se nem MQSO_ANY_USERID ou MQSO_FIXED_USERID forem especificados, o padrão será MQSO_FIXED_USERID.

Segurança de Publicação/Assinatura entre os Gerenciadores de Filas

Mensagens internas de publicação/assinatura, como assinaturas de proxy e publicações são colocadas em filas do sistema de publicação/assinatura usando as regras de segurança de canal normal. As informações e diagramas neste tópico destacam os vários processos e IDs de usuário envolvidos na entrega dessas mensagens.

Controle de Acesso Local

O acesso aos tópicos para publicação e assinaturas é controlado pelas definições de segurança local e regras que são descritas em Segurança de Publicação/Assinatura. No z/OS, nenhum objeto do tópico local é necessário para estabelecer o controle de acesso. Nenhum tópico local é necessário para controle de acesso em outras plataformas. Os administradores podem optar por aplicar o controle de acesso aos objetos do tópico em cluster, independentemente se eles existirem no cluster ainda.

Os administradores do sistema são responsáveis pelo controle de acesso em seu sistema local. Eles devem confiar nos administradores de outros membros da hierarquia ou dos coletivos do cluster para serem responsáveis pela política de controle de acesso. Como o controle de acesso é definido para cada máquina separada, é provável que seja oneroso se o controle de nível bom for necessário. Pode não ser necessário impor qualquer controle de acesso ou o controle de acesso pode ser definido nos objetos de alto nível na árvore de tópicos. O controle de acesso de nível de multa pode ser definido para cada subdivisão do espaço de nomes de tópico.

Fazendo uma Assinatura de Proxy

Confie em uma organização para conectar seu gerenciador de filas em seu gerenciador de filas é confirmado por meio de autenticação de canal normal. Se essa organização de confiança também for permitida para fazer publicação/assinatura distribuída, uma verificação de autoridade será feita. A verificação é feita quando o canal coloca uma mensagem em uma fila de publicação/assinatura distribuída. Por exemplo, se uma mensagem for colocada para a fila `SYSTEM.INTER.QMGR.CONTROL`. O ID do usuário para a verificação de autoridade da fila depende dos valores `PUTAUT` do canal de recebimento. Por exemplo, o ID do usuário do canal, `MCAUSER`, o contexto da mensagem, dependendo do valor e da plataforma. Para obter mais informações sobre a segurança do canal, consulte Segurança de Canal.

As assinaturas de proxy são feitas com o ID do usuário do agente de publicação/assinatura distribuída no gerenciador de filas remotas. Por exemplo, `QM2` em Figura 30 na página 493. Ao usuário é, então, facilmente concedido acesso aos perfis do objeto do tópico local, porque esse ID do usuário é definido no sistema e, portanto, não haverá nenhum conflito de domínio.

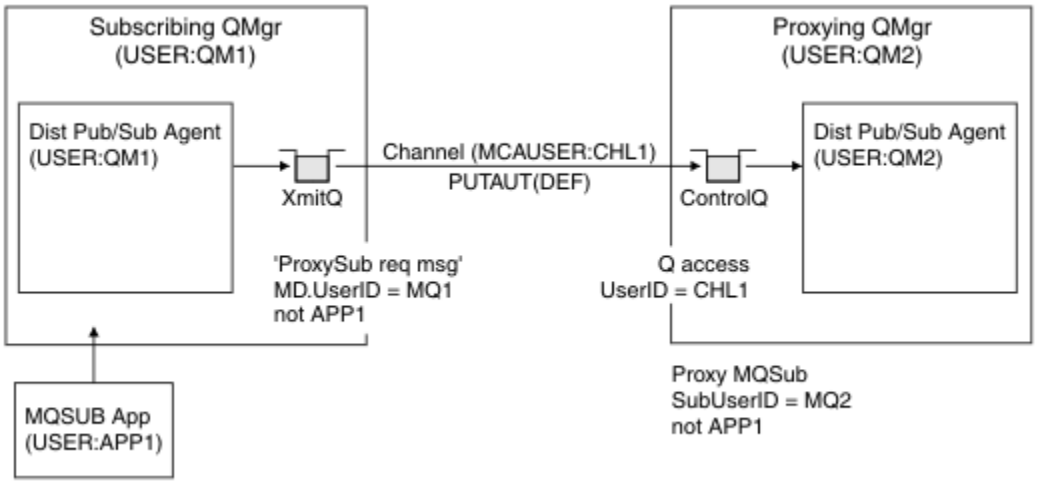


Figura 30. Segurança de Assinatura de Proxy Criando uma Assinatura

Enviando de Volta Publicações Remotas

Quando uma publicação é criada no gerenciador de filas de publicação, uma cópia da publicação é criada para qualquer assinatura de proxy. O contexto da publicação copiada contém o contexto do ID do usuário que fez a assinatura; `QM2` em Figura 31 na página 494. A assinatura de proxy é criada com uma fila de destino que é uma fila remota, portanto, a mensagem de publicação é resolvida em uma fila de transmissão.

A confiança para uma organização para conectar seu gerenciador de filas, QM2, para outro gerenciador de filas, QM1, é confirmada por meios normais de autenticação de canais. Se essa organização confiável tiver permissão para fazer publicação/assinatura distribuída, uma verificação de autoridade será feita quando o canal colocar a mensagem de publicação na fila de publicação de publicação/assinatura distribuída SYSTEM.INTER.QMGR.PUBS. O ID do usuário para a verificação de autoridade da fila depende do valor PUTAUT do canal de recebimento (por exemplo, o ID do usuário do canal, MCAUSER, o contexto da mensagem e outros, dependendo do valor e da plataforma). Para obter mais informações sobre a segurança do canal, consulte Segurança de Canal.

Quando a mensagem de publicação alcançar o gerenciador de filas de assinatura, outro MQPUT para o tópico é feito sob a autoridade desse gerenciador de filas e o contexto com a mensagem é substituído pelo contexto de cada um dos assinantes locais, conforme eles são dados a cada mensagem.

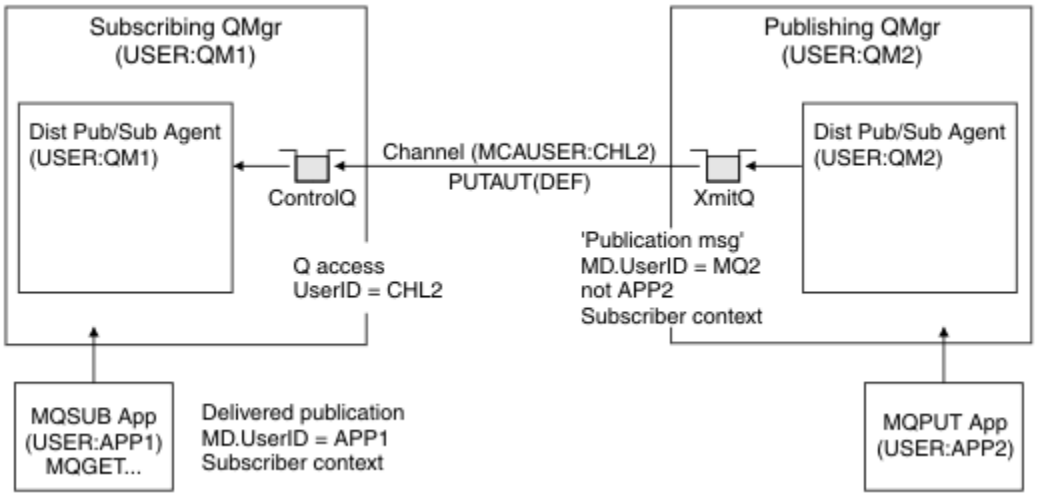


Figura 31. Segurança de Assinatura de Proxy, Publicações de Redirecionamento

Em um sistema em que pouco foi considerado em relação à segurança, os processos de publicação/assinatura distribuídos provavelmente serão executados sob um ID de usuário no grupo mqm, o parâmetro MCAUSER em um canal está em branco (o padrão) e as mensagens são entregues ao várias filas do sistema conforme necessário. O sistema descoberto torna mais fácil de configurar uma prova de conceito para demonstrar a publicação/assinatura distribuída.

Em um sistema no qual a segurança é mais seriamente considerada, essas mensagens internas estão sujeitas aos mesmos controles de segurança que qualquer mensagem vai através do canal.

Se o canal for configurado com um MCAUSER não em branco e um valor PUTAUT especificando que MCAUSER deve ser verificado, então, o MCAUSER em questão deve receber acesso às filas SYSTEM.INTER.QMGR.*. Se houver vários gerenciadores de filas remotas diferentes, com canais em execução em diferentes IDs MCAUSER, todos esses IDs de usuário precisam ter acesso concedido às filas SYSTEM.INTER.QMGR.*. Os canais em execução sob diferentes IDs de MCAUSER pode ocorrer, por exemplo, quando várias conexões hierárquicas forem configuradas em um único gerenciador de filas.

Se o canal estiver configurado com um valor PUTAUT especificando que o contexto da mensagem é usado, o acesso às filas SYSTEM.INTER.QMGR.* será verificado com base no ID do usuário dentro da mensagem interna. Como todas estas mensagens são colocadas com o ID do usuário do agente de publicação/assinatura distribuída a partir do gerenciador de filas que está enviando a mensagem interna ou mensagem de publicação (consulte Figura 31 na página 494), ele não é um conjunto muito grande de IDs do usuário para os quais conceder acesso às diversas filas do sistema (um por gerenciador de filas remotas), se você desejar configurar a segurança de sua publicação/assinatura distribuída desta maneira. Ele ainda tem todos os mesmos problemas que a segurança de contexto de canal sempre possui; a dos domínios de ID do usuário diferente e o fato de que o ID do usuário na mensagem não pode ser definido no sistema receptor. No entanto, é uma maneira perfeitamente aceitável para execução se necessário.

z/OS A Segurança da fila do sistema fornece uma lista de filas e o acesso que é necessário para configurar com segurança do seu ambiente de publicação/assinatura distribuída. Se as mensagens

internas ou quaisquer publicações falharem ao serem colocadas devido a violações de segurança, o canal gravará uma mensagem para o log da maneira normal e as mensagens poderão ser enviadas para a fila de devoluções de acordo com o processamento de erro de canal normal.

Todos os gerenciadores de filas de mensagens para fins de publicação/assinatura distribuída são executados usando a segurança de canal normal.

Para obter informações sobre a restrição de publicações e assinaturas de proxy no nível de tópico, consulte Segurança de publicação/assinatura.

Usando os IDs de Usuário Padrão com uma Hierarquia do Gerenciador de Filas

Se você tiver uma hierarquia de gerenciadores de filas em execução em diferentes plataformas e estiver usando IDs de usuário padrão, observe que esses IDs de usuário padrão diferem entre as plataformas e podem não ser conhecidos na plataforma de destino. Como resultado, um gerenciador de filas em execução em uma plataforma rejeita mensagens recebidas de gerenciadores de filas em outras plataformas com o código de razão `MQRC_NOT_AUTHORIZED`.

Para evitar mensagens sendo rejeitadas, no mínimo, as seguintes autoridades precisam ser incluídas nos IDs de usuário padrão usados em outras plataformas:

- Autoridade *GET *PUT nas filas do SYSTEM.BROKER. filas
- Autoridade *SUB *PUB nos tópicos do SYSTEM.BROKER. tópicos
- Autoridade *ADMCHG *ADMDLT *ADMCRT na fila do SYSTEM.BROKER.CONTROL.QUEUE.

Os IDs de usuário padrão com uma hierarquia do Gerenciador de Filas são os seguintes:

Plataforma	**ID do usuário padrão**
Windows	`MUSR_MQADMIN`
Sistemas UNIX and Linux	`mqm`
IBM i	`QMQM`
z/OS	O ID de usuário do espaço de endereço inicializador de canais

Crie e conceda acesso ao ID do usuário 'qmqm' se hierarquicamente conectado a um gerenciador de filas no IBM i para os Gerenciadores de Filas nas plataformas Windows, UNIX, Linux e z/OS.

Crie e conceda acesso ao ID do usuário 'mqm' se hierarquicamente conectado a um gerenciador de filas no Windows, UNIX ou Linux para Gerenciadores de Filas nas plataformas IBM i e z/OS.

Crie e conceda acesso de usuário para o ID do usuário do espaço de endereço do inicializador de canais do z/OS se hierarquicamente conectado a um gerenciador de filas no z/OS para Gerenciadores de Filas nas plataformas Windows,UNIX, Linux e IBM i.

Os IDs de usuário podem ter distinção entre maiúsculas e minúsculas. O gerenciador de filas originário (se sistemas IBM i, Windows, UNIX ou Linux) força o ID do usuário para estar todo em letras maiúsculas. O gerenciador de filas de recebimento (se sistemas Windows, UNIX ou Linux) força o ID do usuário para estar todo em letras minúsculas. Portanto, todos os IDs do usuário criados em sistemas UNIX and Linux devem ser criados em sua forma minúscula. Se uma saída de mensagem tiver sido instalada, forçando o ID do usuário em maiúsculas ou minúsculas não ocorrerá. É preciso ter cuidado para entender como a saída de mensagem processa o ID do usuário.

Para evitar problemas em potencial com a conversão de IDs de usuário:

- Nos sistemas UNIX, Linux, and Windows, assegure-se de que os IDs do usuário sejam especificados em letra minúscula.
- No IBM i e no z/OS, certifique-se de que os IDs de usuários sejam especificados em maiúsculas.

V 9.1.0 IBM MQ Console e a segurança do REST API

A segurança para o IBM MQ Console e o REST API é configurada por meio da edição da configuração do servidor mqweb no arquivo `mqwebuser.xml`.

Sobre esta tarefa

É possível rastrear as ações do usuário e auditar o uso do IBM MQ Console e da REST API examinando os arquivos de log do servidor mqweb.

Os usuários do IBM MQ Console e da REST API podem ser autenticados usando:

- Registro Básico
- registro LDAP
- Registro do S.O. local
- SAF no z/OS
- Qualquer outro tipo de registro suportado pelo WebSphere Liberty

As funções podem ser designadas aos usuários do IBM MQ Console e aos usuários da REST API para determinar qual nível de acesso é concedido a eles para os objetos do IBM MQ. Por exemplo, para executar o sistema de mensagens, os usuários devem ser designados à função `MQWebUser`. Para obter mais informações sobre as funções disponíveis, veja “Funções no IBM MQ Console e na REST API” na página 507.

Depois que um usuário é designado a uma função, há vários métodos que podem ser usados para autenticar o usuário. Com o IBM MQ Console, os usuários podem efetuar login com um nome de usuário e uma senha ou podem usar autenticação por certificado de cliente. Com a REST API, os usuários podem usar a autenticação básica de HTTP, a autenticação baseada em token ou a autenticação por certificado de cliente.

Procedimento

1. Defina o registro do usuário para autenticar usuários e designe a cada usuário ou grupo uma função para autorizar os usuários e grupos a usar o IBM MQ Console ou a REST API. Para obter mais informações, consulte “Configurando usuários e funções” na página 497
2. Escolha como os usuários do IBM MQ Console são autenticados com o servidor mqweb. Você não precisa usar o mesmo método para todos os usuários:
   - Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o tempo de validade para o token LTPA. Para obter mais informações, veja Configurando o intervalo de validação de token LTPA.
   - Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte “Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console” na página 509.
3. Escolha como os usuários do REST API são autenticados com o servidor mqweb. Você não precisa usar o mesmo método para todos os usuários:
   - Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte “Usando autenticação básica HTTP com a REST API” na página 512.

- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte "Usando autenticação baseada em token com a API de REST" na página 514.

  Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. No entanto, se você tiver ativado conexões HTTP, será possível permitir que um token LTPA emitido para uma conexão HTTPS seja usado para uma conexão HTTP. Para obter mais informações, consulte Configurando o token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

4. Opcional: Configure o Cross Origin Resource Sharing para a REST API.

   Por padrão, um navegador da web não permite scripts, como JavaScript, para chamar a REST API quando o script não é da mesma origem que a REST API. Ou seja, as solicitações de origem cruzada não estão ativadas. É possível configurar o Cross Origin Resource Sharing (CORS) para permitir solicitações de origem cruzada de URLs especificadas. Para obter informações adicionais, consulte "Configurando o CORS para a REST API" na página 516.
5. Opcional: Configure a validação do cabeçalho do host para o IBM MQ Console e a REST API.

   É possível configurar a validação do cabeçalho do host e criar uma lista de permissões de nomes do host e portas para garantir que somente as solicitações que contêm cabeçalhos de host específicos sejam processadas pelo IBM MQ Console e pela REST API. Para obter informações adicionais, consulte "Configurando a validação do cabeçalho do host para o IBM MQ Console e a REST API" na página 517.

V 9.1.0 Configurando usuários e funções

Para usar o IBM MQ Console ou a REST API, os usuários precisam autenticar-se em um registro do usuário, definido para o servidor mqweb.

Sobre esta tarefa

Os usuários autenticados precisam ser membros de um dos grupos que autorizam o acesso aos recursos do IBM MQ Console e da REST API. Por padrão, o registro do usuário não contém nenhum usuário; estes precisam ser incluindo por meio da edição do arquivo `mqwebuser.xml`.

Ao configurar usuários e grupos, você configura primeiro um registro do usuário para autenticar usuários e grupos. Esse registro do usuário é compartilhado entre o IBM MQ Console e a REST API. É possível controlar se os usuários e grupos têm acesso ao IBM MQ Console, REST API, ou a ambos, ao configurar funções para seus usuários e grupos.

Depois de configurar o registro do usuário, você configura funções para os usuários e grupos para conceder autorização a eles. Há várias funções disponíveis, incluindo funções específicas para usar a REST API para Managed File Transfer. Cada função concede um nível diferente de acesso. Para obter informações adicionais, consulte "Funções no IBM MQ Console e na REST API" na página 507.

Vários arquivos XML de amostra são fornecidos com o servidor mqweb para tornar a configuração de usuários e grupos mais simples. Os usuários que estão familiarizados com a configuração de segurança no WebSphere Liberty (WLP) podem preferir não usar as amostras. O WLP fornece outros recursos de autorização, além daqueles documentados aqui.

Procedimento

- Configure usuários e grupos com um registro básico usando o arquivo `basic_registry.xml`.

Os nomes e as senhas do usuário no registro são utilizados para autenticar e autorizar usuários do IBM MQ Console e da REST API.

Para configurar um registro básico usando o arquivo de amostra `basic_registry.xml`, veja “Configurando um registro básico para o IBM MQ Console e a REST API” na página 499.

- Configure usuários e grupos com um registro LDAP usando o arquivo `ldap_registry.xml`.

  Os nomes de usuário e senhas no registro LDAP são usados para autenticar e autorizar o uso do IBM MQ Console e da REST API.

  Para configurar um registro LDAP usando o arquivo de amostra `ldap_registry.xml`, veja “Configurando um registro LDAP para o IBM MQ Console e a REST API” na página 503.

- ULW

  Configure usuários e grupos com um registro do sistema operacional local usando o arquivo `local_os_registry.xml`.

  Os nomes de usuário e senhas no registro do sistema operacional são usados para autenticar e autorizar os usuários do IBM MQ Console e da REST API.

  Para configurar um registro do S.O. local usando o arquivo de amostra `local_os_registry.xml`, veja “Configurando um registro de S.O. local para o IBM MQ Console e a REST API” na página 501.

- z/OS

  Configure usuários e grupos com a interface System Authorization Facility (SAF) no z/OS usando o arquivo `zos_saf_registry.xml`.

  Os perfis do RACF, ou de outro produto de segurança, são usados para conceder aos usuários e grupos acesso a funções. Os nomes de usuário e senhas no banco de dados RACF são usados para autenticar e autorizar os usuários do IBM MQ Console e da REST API.

  Para configurar a interface SAF usando o arquivo de amostra `zos_saf_registry.xml`, veja “Configurando um registro SAF para o IBM MQ Console e a REST API” na página 505.

- Desative a segurança, incluindo a capacidade de acessar o IBM MQ Console ou a REST API usando HTTPS, usando o arquivo `no_security.xml`.

Como proceder a seguir

Escolha como os usuários se autenticam:

Opções de autenticação do IBM MQ Console

- Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o intervalo de expiração do token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte “Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console” na página 509.

Opções de autenticação do REST API

- Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte “Usando autenticação básica HTTP com a REST API” na página 512.

- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte "Usando autenticação baseada em token com a API de REST" na página 514. É possível configurar o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

V 9.1.0 Configurando um registro básico para o IBM MQ Console e a REST API

É possível configurar um registro básico dentro do arquivo `mqwebuser.xml`. Os nomes de usuário, senhas e funções no arquivo xml são usados para autenticar e autorizar usuários do IBM MQ Console e da REST API.

Antes de começar

- Ao configurar usuários dentro do registro básico, deve-se designar uma função a cada usuário. Cada função fornece diferentes níveis de privilégio para acessar o IBM MQ Console e a REST API, além de determinar o contexto de segurança que será usado quando uma operação permitida for tentada. É necessário entender essas funções antes de configurar o registro básico. Para obter mais informações sobre cada uma das funções, consulte "Funções no IBM MQ Console e na REST API" na página 507.
- Para completar esta tarefa, você deve ser um usuário com privilégios suficientes para editar o arquivo `mqwebuser.xml`:
  - z/OS No z/OS, você deve ter acesso de gravação ao arquivo `mqwebuser.xml`.
  - Multi Em todos os outros sistemas operacionais, deve-se ser um usuário privilegiado.

Procedimento

1. Copie o arquivo XML de amostra `basic_registry.xml` de um dos caminhos a seguir:
   - ULW No UNIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS No z/OS: `PathPrefix /web/mq/samp/configuration`

   em que `PathPrefix` é o caminho de instalação do Unix System Services Components do IBM MQ.
2. Coloque o arquivo de amostra no diretório apropriado:
   - ULW

     No UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     No z/OS: *WLP_user_directory*`/servers/mqweb`

     em que *WLP_user_directory* é o diretório que foi especificado quando o script **crtmqweb** foi executado para criar a definição do servidor do mqweb.
3. Opcional: Se você mudou as definições de configuração em `mqwebuser.xml`, copie-as para o arquivo de amostra.
4. Exclua o arquivo `mqwebuser.xml` existente e renomeie o arquivo de amostra para `mqwebuser.xml`.

5. Edite o novo arquivo `mqwebuser.xml` para incluir usuários e grupos dentro das tags **basicRegistry**.

   Esteja ciente de que qualquer usuário com a função `MQWebUser` pode executar somente as operações que o ID do usuário pode executar no gerenciador de filas. Portanto, o ID do usuário definido no registro deve ter um ID do usuário idêntico no sistema no qual o IBM MQ está instalado. Esses IDs de usuários devem estar no mesmo caso ou o mapeamento entre os IDs de usuários pode falhar.

   Para obter mais informações sobre como configurar registros do usuário básico, veja Configurando um registro do usuário básico para o Liberty na documentação do WebSphere Liberty.
6. Designe funções a usuários e grupos editando o arquivo `mqwebuser.xml`:

   Há várias funções disponíveis que autorizam usuários e grupos a usarem o IBM MQ Console e o REST API. Cada função concede um nível diferente de acesso. Para obter informações adicionais, consulte "Funções no IBM MQ Console e na REST API" na página 507.

   - Para designar funções e conceder acesso ao IBM MQ Console, inclua seus usuários e grupos entre as tags **security-role** apropriadas dentro das tags **<enterpriseApplication id="com.ibm.mq.console">**.
   - Para designar funções e conceder acesso ao REST API, inclua seus usuários e grupos entre as tags **security-role** apropriadas dentro das tags **<enterpriseApplication id="com.ibm.mq.rest">**.

   Para ajudar com o formato das informações sobre o usuário e grupo dentro das tags **security-role**, veja os exemplos.
7. Se você tiver fornecido senhas aos usuários no `mqwebuser.xml`, será necessário codificá-las para torná-las mais seguras usando o comando **securityUtility encoding** fornecido pelo WebSphere Liberty. Para obter mais informações, consulte Liberty: comandosecurityUtility na documentação do produto WebSphere Liberty .

Exemplo

No exemplo a seguir, é concedido ao grupo `MQWebAdminGroup` acesso ao IBM MQ Console com a função `MQWebAdmin`. O usuário `reader` recebe acesso à função `MQWebAdminRO` e o usuário `guest` recebe acesso à função `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>
```

No exemplo a seguir, os usuários `reader` e `guest` recebem acesso ao IBM MQ Console. O usuário `user` tem acesso concedido à REST API e quaisquer usuários dentro do grupo `MQAdmin` têm acesso concedido ao IBM MQ Console e à REST API. O usuário `mftadmin` tem acesso concedido à REST API para 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>
```

Como proceder a seguir

Escolha como os usuários se autenticam:

Opções de autenticação do IBM MQ Console

- Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o intervalo de expiração do token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte “Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console” na página 509.

Opções de autenticação do REST API

- Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte “Usando autenticação básica HTTP com a REST API” na página 512.
- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte “Usando autenticação baseada em token com a API de REST” na página 514. É possível configurar o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte “Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console” na página 509.

ULW V 9.1.0 Configurando um registro de S.O. local para o IBM MQ Console e a REST API

É possível configurar um registro do sistema operacional local dentro do arquivo `mqwebuser.xml`. Os nomes de usuário e senhas no sistema operacional local são usados para autenticar e autorizar usuários do IBM MQ Console e da REST API.

Antes de começar

- Para a autenticação por certificado de cliente com o recurso de autenticação do S.O. local, a identidade do usuário é o nome comum (CN) do nome distinto (DN) do certificado de cliente. Se a identidade do

usuário não existir como um usuário do sistema operacional, o login de certificado de cliente falhará e efetuará fallback para autenticação baseada em senha.

- Para concluir essa tarefa, deve-se ser um usuário privilegiado.

Sobre esta tarefa

Com um registro do sistema operacional local, os usuários e grupos são designados automaticamente a uma função:

- Qualquer usuário que faz parte do grupo 'mqm' ou do grupo 'QMQMADM' no IBM i tem as funções MQWebAdmin e MFTWebAdmin concedidas.
- Todos os outros usuários têm a função MQWebUser concedida.

Para obter informações adicionais sobre essas funções, consulte "Funções no IBM MQ Console e na REST API" na página 507.

Um registro do sistema operacional local pode ser usado somente no UNIX, Linux, and Windows. A função equivalente é fornecida no z/OS, configurando um registro do SAF. Para obter informações adicionais, consulte "Configurando um registro SAF para o IBM MQ Console e a REST API" na página 505.

Procedimento

1. Copie o arquivo XML de amostra `local_os_registry.xml` do caminho a seguir:
   MQ_INSTALLATION_PATH`/web/mq/samp/configuration`
2. Coloque o arquivo de amostra no diretório a seguir:
   MQ_DATA_PATH`/web/installations/`*installationName*`/servers/mqweb`
3. Opcional: Se você mudou as definições de configuração em `mqwebuser.xml`, copie-as para o arquivo de amostra.
4. Exclua o arquivo `mqwebuser.xml` existente e renomeie o arquivo de amostra para `mqwebuser.xml`.

Como proceder a seguir

Escolha como os usuários se autenticam:

Opções de autenticação do IBM MQ Console

- Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o intervalo de expiração do token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

Opções de autenticação do REST API

- Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte "Usando autenticação básica HTTP com a REST API" na página 512.
- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte

"Usando autenticação baseada em token com a API de REST" na página 514. É possível configurar o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o token LTPA.

- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

V 9.1.0 Configurando um registro LDAP para o IBM MQ Console e a REST API

É possível configurar um registro LDAP dentro do arquivo `mqwebuser.xml`. Os nomes de usuário e senhas no registro LDAP são usados para autenticar e autorizar usuários do IBM MQ Console e da REST API.

Antes de começar

- Ao configurar um registro LDAP, deve-se designar uma função a cada usuário. Cada função fornece diferentes níveis de privilégio para acessar o IBM MQ Console e a REST API, além de determinar o contexto de segurança que será usado quando uma operação permitida for tentada. É necessário entender essas funções antes de configurar o registro. Para obter mais informações sobre cada uma das funções, consulte "Funções no IBM MQ Console e na REST API" na página 507.

  Esteja ciente de que qualquer usuário com a função `MQWebUser` pode executar somente as operações que o ID do usuário pode executar no gerenciador de filas. Portanto, o ID do usuário definido no servidor LDAP deve ter um ID do usuário idêntico no sistema no qual o IBM MQ está instalado. Esses IDs de usuários devem estar no mesmo caso ou o mapeamento entre os IDs de usuários pode falhar.
- Para completar esta tarefa, você deve ser um usuário com privilégios suficientes para editar o arquivo `mqwebuser.xml`:
  - z/OS No z/OS, você deve ter acesso de gravação ao arquivo `mqwebuser.xml`.
  - Multi Em todos os outros sistemas operacionais, deve-se ser um usuário privilegiado.

Procedimento

1. Copie o arquivo XML de amostra `ldap_registry.xml` de um dos caminhos a seguir:
   - ULW No UNIX, Linux, and Windows: *MQ_INSTALLATION_PATH* `/web/mq/samp/configuration`
   - z/OS No z/OS: `PathPrefix /web/mq/samp/configuration`

   em que `PathPrefix` é o caminho de instalação do Unix System Services Components do IBM MQ.
2. Coloque o arquivo de amostra no diretório apropriado:
   - ULW

     No UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     No z/OS: *WLP_user_directory*`/servers/mqweb`

     em que *WLP_user_directory* é o diretório que foi especificado quando o script **crtmqweb** foi executado para criar a definição do servidor do mqweb.
3. Opcional: Se você mudou as definições de configuração em `mqwebuser.xml`, copie-as para o arquivo de amostra.

4. Exclua o arquivo `mqwebuser.xml` existente e renomeie o arquivo de amostra para `mqwebuser.xml`.
5. Edite o novo arquivo `mqwebuser.xml` para mudar as configurações de registro LDAP dentro das tags **`ldapRegistry`** e **`idsLdapFilterProperties`**.

   Para obter mais informações sobre como configurar registros LDAP, veja Configurando registros do usuário LDAP no Liberty na documentação do WebSphere Liberty.
6. Designe funções a usuários e grupos editando o arquivo `mqwebuser.xml`:

   Há várias funções disponíveis que autorizam usuários e grupos a usarem o IBM MQ Console e o REST API. Cada função concede um nível diferente de acesso. Para obter informações adicionais, consulte "Funções no IBM MQ Console e na REST API" na página 507.

   - Para designar funções e conceder acesso ao IBM MQ Console, inclua seus usuários e grupos entre as tags **`security-role`** apropriadas dentro das tags **`<enterpriseApplication id="com.ibm.mq.console">`**.
   - Para designar funções e conceder acesso ao REST API, inclua seus usuários e grupos entre as tags **`security-role`** apropriadas dentro das tags **`<enterpriseApplication id="com.ibm.mq.rest">`**.

Como proceder a seguir

Escolha como os usuários se autenticam:

Opções de autenticação do IBM MQ Console

- Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o intervalo de expiração do token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

Opções de autenticação do REST API

- Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte "Usando autenticação básica HTTP com a REST API" na página 512.
- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte "Usando autenticação baseada em token com a API de REST" na página 514. É possível configurar o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

z/OS V 9.1.0 Configurando um registro SAF para o IBM MQ Console e a REST API

A interface System Authorization Facility (SAF) permite que o servidor mqweb chame o gerenciador de segurança externa para verificação de autenticação e autorização. Um usuário pode então efetuar login no IBM MQ Console e na REST API com um ID do usuário e senha do z/OS.

Antes de começar

- Ao configurar um registro do SAF, deve-se designar uma função aos usuários. Cada função fornece diferentes níveis de privilégio para acessar o IBM MQ Console e a REST API, além de determinar o contexto de segurança que será usado quando uma operação permitida for tentada. É necessário entender essas funções antes de configurar o registro. Para obter mais informações sobre cada uma das funções, consulte "Funções no IBM MQ Console e na REST API" na página 507.
- É necessário que o processo Angel do WebSphere Liberty esteja em execução para usar a interface autorizada para o SAF. Consulte Ativando z/OS serviços autorizados no Liberty para z/OS para obter mais informações.
- Para completar esta tarefa, deve-se ter acesso de gravação ao arquivo `mqwebuser.xml` e autoridade para definir perfis do gerenciador de segurança.

Nota: V 9.1.0.20 A partir de IBM MQ 9.1.0 Fix Pack 20, o arquivo de configuração de amostra `zos_saf_registry.xml` foi atualizado para remover uma entrada safAuthorization duplicada

Esta atualização corrige um problema no qual um erro ICH408I pode ocorrer quando o MQ Console on z/OS é atualizado para um nível que envia WebSphere Liberty Profile 22.0.0.12 ou posterior: ou seja, de IBM MQ 9.1.0 Fix Pack 15. Ter mais de uma instrução safAuthorization não é suportado e pode causar um erro ICH408I quando os usuários que não estão nas funções MQWebAdmin ou MQWebAdminRO, na classe EBJROLE, tentarem acessar um gerenciador de filas do z/OS por meio do MQ Console

O padrão para **racRouteLog**, que especifica os tipos de tentativas de acesso a serem registradas, é NONE Se você precisar de um relatório ou registro adicional para auditoria de segurança, consulte Autorização SAF (safAuthorization) para obter mais informações.

Sobre esta tarefa

A interface SAF permite que o servidor mqweb chame o gerenciador de segurança externa para a verificação de autenticação e autorização para o IBM MQ Console e a REST API.

Procedimento

1. Siga as etapas em Ativando os serviços autorizados z/OS no Liberty for z/OS para dar ao seu servidor mqweb acesso para usar os serviços autorizados do z/OS.

   Amostra de JCL para iniciar o processo angel no USS_ROOT/`web/templates/zos/procs/bbgzangl.jcl`, em que USS_ROOT é o caminho no Unix System Services no qual os componentes USS do IBM MQ for z/OS são instalados.

   Em `bbgzangl.jcl`, altere a instrução SET ROOT para apontar para USS_ROOT/`web`, por exemplo, `/usr/lpp/mqm/V9R1M0/web`

   Consulte Administrando o Liberty on z/OS para obter mais informações sobre como parar e iniciar o processo angel.
2. Siga as etapas em Liberty: Configurando o usuário não autenticado pelo System Authorization Facility (SAF) para criar o usuário não autenticado que o Liberty precisa.
3. Copie o arquivo `zos_saf_registry.xml` do caminho a seguir: `PathPrefix /web/mq/samp/configuration` em que `PathPrefix` é o caminho da instalação do IBM MQ Unix System Services Components.

4. Coloque o arquivo de amostra no diretório *WLP_user_directory*/servers/mqweb, em que *WLP_user_directory* é o diretório que foi especificado quando o script **crtmqweb** foi executado para criar a definição do servidor mqweb.
5. Opcional: Se você mudou anteriormente quaisquer definições de configuração em mqwebuser.xml, copie-as para o arquivo de amostra.
6. Exclua o arquivo mqwebuser.xml existente e renomeie o arquivo de amostra para mqwebuser.xml.
7. Customize o elemento **safCredentials** em mqwebuser.xml.
   a. Configure **profilePrefix** para um nome que seja exclusivo do seu servidor Liberty. Se você tiver mais de um servidor mqweb em execução em um único sistema, será necessário escolher um nome diferente para cada servidor; por exemplo, MQWEB910 e MQWEB905.
   b. Configure **unauthenticatedUser** para o nome do usuário não autenticado criado na etapa "2" na página 505.
8. Defina o APPLID do servidor mqweb como RACF.

   O nome do recurso APPLID é o valor especificado no atributo **profilePrefix** na etapa "7" na página 506. O exemplo a seguir define o APPLID do servidor mqweb no RACF:

```
RDEFINE APPL profilePrefix UACC(NONE)
```

9. Conceda a todos os usuários ou grupos a serem autenticados no MQ Console ou na REST API o acesso READ ao servidor mqweb APPLID na classe APPL.

   Também deve-se fazer isso para o usuário não autenticado definido na etapa "2" na página 505. O exemplo a seguir concede a um usuário acesso READ para o APPLID do servidor mqweb no RACF:

```
PERMIT profilePrefix CLASS(APPL) ACCESS(READ) ID(userID)
```

10. Defina os perfis na classe EJBROLE necessária para dar aos usuários acesso às funções no MQ Console e na REST API.

    O exemplo a seguir define os perfis no RACF, em que **profilePrefix** é o valor especificado para o atributo **profilePrefix** na etapa "7" na página 506.

```
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.console.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebAdminRO UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MQWebUser UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdmin UACC(NONE)
RDEFINE EJBROLE profilePrefix.com.ibm.mq.rest.MFTWebAdminRO UACC(NONE)
```

11. Conceda aos usuários o acesso a funções no MQ Console e na REST API.

    Para fazer isso, dê aos usuários ou grupos o acesso READ a um ou mais perfis na classe EBJROLE criada na etapa "10" na página 506. Para obter informações adicionais sobre as funções, consulte "Funções no IBM MQ Console e na REST API" na página 507.

    O exemplo a seguir fornece a um usuário acesso à função MQWebAdmin para a REST API no RACF, em que **profilePrefix** é o valor especificado para o atributo **profilePrefix** na etapa "7" na página 506.

```
PERMIT profilePrefix.com.ibm.mq.rest.MQWebAdmin CLASS(EJBROLE) ACCESS(READ) ID(userID)
```

Resultados

Você configurou a autenticação SAF para o IBM MQ Console e a REST API.

Como proceder a seguir

Escolha como os usuários se autenticam:

Opções de autenticação do IBM MQ Console

- Permitir que os usuários se autentifiquem usando a autenticação do token. Neste caso, um usuário insere um ID do usuário e senha no log do IBM MQ Console na tela. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Nenhuma configuração adicional é necessária para usar essa opção de autenticação, mas é possível configurar opcionalmente o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o intervalo de expiração do token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no IBM MQ Console, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

Opções de autenticação do REST API

- Permitir que os usuários se autentifiquem usando a autenticação de HTTP básica. Nesse caso, um nome de usuário e uma senha são codificados, mas não criptografados, e enviados com cada solicitação de REST API para autenticar e autorizar o usuário para essa solicitação. Para que essa autenticação seja segura, deve-se usar uma conexão segura. Ou seja, deve-se usar HTTPS. Para obter mais informações, consulte "Usando autenticação básica HTTP com a REST API" na página 512.
- Permitir que os usuários se autentifiquem usando a autenticação do token. Nesse caso, um usuário fornece um ID de usuário e uma senha para o recurso REST API `login` com o método HTTP POST. É gerado um token LTPA que permite que o usuário permaneça com login efetuado e autorizado por um período de tempo configurado. Para obter informações adicionais, consulte "Usando autenticação baseada em token com a API de REST" na página 514. É possível configurar o intervalo de validação para o token LTPA. Para obter mais informações, consulte Configurando o token LTPA.
- Permitir que os usuários se autentifiquem usando certificados de cliente. Nesse caso, o usuário não usa um ID do usuário ou senha para efetuar login no REST API, mas usa o certificado de cliente. Para obter mais informações, consulte "Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console" na página 509.

V 9.1.0 Funções no IBM MQ Console e na REST API

Ao autorizar usuários e grupos a usar IBM MQ Console ou REST API, deve-se atribuir aos usuários e grupos uma das funções disponíveis: **MQWebAdmin**, **MQWebAdminRO**, **MQWebUser**, **MFTWebAdmin** e **MFTWebAdminRO**. Cada função fornece diferentes níveis de privilégio para acessar o IBM MQ Console e a REST API, além de determinar o contexto de segurança que será usado quando uma operação permitida for tentada.

Nota: Com exceção da função **MQWebUser**, o ID do usuário não faz distinção entre maiúsculas de minúsculas. Consulte "MQWebUser" na página 508 para os requisitos específicos para esta função.

MQWebAdmin
Um usuário ou grupo que é designado a essa função pode executar todas as operações administrativas e opera sob o contexto de segurança do ID do usuário do sistema operacional que é usado para iniciar o servidor mqweb.

Um usuário ou grupo com essa função não tem acesso aos serviços REST a seguir:

- O REST API para MFT. Para utilizar esses serviços, o usuário ou grupo também deve ser designado a função **MFTWebAdmin** ou **MFTWebAdminRO**.
- O messaging REST API. Para usar o messaging REST API, o usuário deve ser designado à função **MQWebUser**.

MQWebAdminRO
Essa função fornece acesso somente leitura para o IBM MQ Console ou a REST API. Um usuário ou um grupo ao qual essa função está designada pode executar as operações a seguir:

- Exibir e consultar operações nos objetos do IBM MQ, como filas e canais.

- Procurar mensagens em filas.

Um usuário ou um grupo ao qual essa função está designada opera no contexto de segurança do ID de usuário do sistema operacional usado para iniciar o servidor mqweb.

Um usuário ou grupo com essa função não tem acesso aos serviços REST a seguir:

- O REST API para MFT. Para utilizar esses serviços, o usuário ou grupo também deve ser designado a função **MFTWebAdmin** ou **MFTWebAdminRO**.
- O messaging REST API. Para usar o messaging REST API, o usuário deve ser designado à função **MQWebUser**.

MQWebUser
Um usuário ou grupo que é designado a essa função pode executar qualquer operação que o ID do usuário pode executar no gerenciador de filas. Por exemplo:

- Operações de início e parada em objetos IBM MQ , tais como canais.
- Definir e configurar operações nos objetos do IBM MQ, como filas e canais.
- Exibir e consultar operações nos objetos do IBM MQ, como filas e canais.
- Colocar e obter mensagens usando o messaging REST API.

Um usuário ou um grupo ao qual essa função está designada opera no contexto de segurança do principal e pode executar somente as operações que o ID do usuário pode executar no gerenciador de filas.

Portanto, o usuário ou grupo que está definido no registro do usuário mqweb deve receber autoridade dentro do IBM MQ para que esse usuário possa executar quaisquer operações. Ao utilizar esta função, é possível controlar precisamente quais usuários possuem qual tipo de acesso a recursos específicos do IBM MQ quando eles usam o IBM MQ Console e o REST API.

Nota:

- O comprimento máximo de um ID do usuário que é designado a essa função é 12 caracteres.
- O caso do ID do usuário deve ser o mesmo no registro do usuário mqweb e no sistema IBM MQ. Se as maiúsculas e minúsculas do ID do usuário forem diferentes, o usuário poderá ser autenticado pelo IBM MQ Console e pelo REST API, mas não autorizado a usar os recursos do IBM MQ.

Um usuário ou grupo com essa função não tem acesso a nenhum dos serviços da REST API para MFT. Para utilizar esses serviços, o usuário ou grupo também deve ser designado a função **MFTWebAdmin** ou **MFTWebAdminRO**.

MFTWebAdmin
Um usuário ou grupo atribuído a essa função pode executar todas as operações MFT de REST e opera sob o contexto de segurança do ID do usuário do sistema operacional usado para iniciar o servidor mqweb.

Um usuário ou grupo com essa função não tem acesso a nenhum dos serviços do IBM MQ REST API. Para utilizar esses serviços, o usuário ou grupo também deve ser designado à função **MQWebAdmin**, **MQWebAdminRO** ou **MQWebUser**.

MFTWebAdminRO
Essa função fornece acesso somente leitura à REST API para MFT. Um usuário ou grupo ao qual foi designada essa função pode executar operações somente leitura (solicitações GET) como transferência e agentes de lista.

Um usuário ou um grupo ao qual essa função está designada opera no contexto de segurança do ID de usuário do sistema operacional usado para iniciar o servidor mqweb.

Um usuário ou grupo com essa função não tem acesso a nenhum dos serviços do IBM MQ REST API. Para utilizar esses serviços, o usuário ou grupo também deve ser designado à função **MQWebAdmin**, **MQWebAdminRO** ou **MQWebUser**.

Para obter mais informações sobre como configurar usuários e grupos para usar essas funções, veja “Configurando usuários e funções” na página 497.

Funções de sobreposição

Mais de uma função pode ser designada a um usuário ou a um grupo. Quando um usuário executa uma operação nessa situação, a função com privilégio mais alto que for aplicável à operação será usada. Por exemplo, se um usuário com as funções **MQWebAdminRO** e **MQWebUser** executa uma operação de fila de consulta, a função **MQWebAdminRO** é usada e a operação é tentada no contexto do ID do usuário do sistema que iniciou o servidor web. Se esse mesmo usuário executar uma operação de definição, a função **MQWebUser** será usada e a operação será tentada no contexto do principal.

ULW V 9.1.0 Usando a autenticação por certificado de cliente com a REST API e o IBM MQ Console

É possível mapear certificados de cliente para principais para autenticar usuários do IBM MQ Console e da REST API.

Antes de começar

- Configure usuários, grupos e funções para que sejam autorizados a usar o IBM MQ Console e a REST API. Para obter informações adicionais, consulte “Configurando usuários e funções” na página 497.
- Quando você usa a REST API, é possível consultar as credenciais do usuário atual utilizando o método HTTP GET no recurso `login`, fornecendo o certificado de cliente para autenticar a solicitação. Esta solicitação retorna informações sobre o nome do usuário e as funções designadas ao usuário. Para obter mais informações, consulte GET `/login`
- Ao mapear certificados de cliente para principais para autenticar usuários, o nome distinto do certificado de cliente é usado para corresponder a usuários no registro de usuário configurado:
  - Para um registro básico, o Nome Comum (CN) é correspondido ao usuário. Por exemplo, `CN=Fred, O=IBM, C=GB` é correspondida a um nome de usuário de `Fred`.
  - Para um registro LDAP, por padrão, o nome distinto completo é correspondido ao LDAP. É possível configurar filtros e mapeamento para customizar a correspondência. Para obter mais informações, consulte Liberty: modo de mapa de certificado LDAP na WebSphere Liberty documentação.

Sobre esta tarefa

Quando um usuário é autenticado usando um certificado de cliente, o certificado é usado no lugar de um nome do usuário e uma senha. Para a REST API, o certificado de cliente é fornecido com cada solicitação REST para autenticar o usuário. Para o IBM MQ Console, quando um usuário efetua login com um certificado, não é possível efetuar seu logout em seguida.

O procedimento presume as informações a seguir:

- Que seu arquivo `mqwebuser.xml` é baseado em uma das amostras a seguir:
  - `basic_registry.xml`
  - `local_os_registry.xml`
  - `ldap_registry.xml`
- Que você está usando um sistema UNIX, Linux ou Windows.
- Você é um usuário privilegiado .

Para configurar a autenticação por certificado de cliente com um conjunto de chaves do RACF no z/OS, siga o procedimento em “Configurando o TLS para a REST API e o IBM MQ Console no z/OS” na página 521.

Nota: O procedimento a seguir descreve as etapas necessárias para usar certificados de cliente com o IBM MQ Console e a REST API. Para conveniência do desenvolvedor, as etapas detalham como criar e usar certificados autoassinados. No entanto, para produção, use certificados que são obtidos de uma autoridade de certificação.

Procedimento

1. Inicie o servidor mqweb inserindo o comando **strmqweb** na linha de comandos.
2. Crie um certificado de cliente:
   a) Crie um keystore PKCS#12:
      i) Abra a ferramenta IBM Key Management inserindo o comando **strmqikm** na linha de comandos.
      ii) No menu **Arquivo do banco de dados de chave** na ferramenta IBM Key Management, clique em **Novo**.
      iii) Selecione **PKCS12** na lista **Tipo de banco de dados de chaves**.
      iv) Selecione um local para salvar o keystore e insira um nome apropriado no campo **Nome do arquivo**. Por exemplo, `user.p12`
      v) Configure uma senha quando solicitado.
   b) Crie o certificado, criando um certificado autoassinado ou obtendo um certificado de uma autoridade de certificação:
      - Crie um certificado autoassinado:
        i) Clique em **Novo Auto-assinado**.
        ii) Insira `user` no campo **Rótulo chave**.
        iii) Se você estiver usando um registro do usuário básico, insira o nome de um usuário de seu registro do usuário no campo **Nome comum**. Por exemplo, `mqadmin`. Para um registro do usuário LDAP, certifique-se de que o nome distinto para o certificado corresponda ao nome distinto no registro LDAP.
        iv) Clique em **OK**.
      - Obtenha um certificado de uma autoridade de certificação. O certificado de CA deve incluir o nome do usuário apropriado dentro do nome comum (CN) do campo de nome distinto (DN):
        i) Solicite um novo certificado. No menu **Criar** clique em **Novo Pedido de Certificado**.
        ii) No campo **Rótulo chave**, insira o rótulo certificado.
        iii) Se você estiver usando um registro do usuário básico, no campo **Nome comum**, insira o nome do usuário do usuário para o qual se destina o certificado.

        Se você estiver usando um registro de S. O. local, o campo **Nome comum** deverá corresponder ao ID do usuário do S.O. local.

        Para um registro do usuário LDAP, certifique-se de que o nome distinto para o certificado corresponda ao nome distinto no registro LDAP.
        iv) Digite ou selecione valores para os campos restantes, conforme aplicável.
        v) Escolha onde salvar a solicitação de certificado e o nome do arquivo para a solicitação de certificado, em seguida, clique em **OK**.
        vi) Envie o arquivo de solicitação de certificado para uma autoridade de certificação (CA).
        vii) Quando você tiver o certificado da CA, abra a ferramenta IBM Key Management inserindo o comando **strmqikm** na linha de comandos.
        viii) No menu **Arquivo do banco de dados de chave** na ferramenta IBM Key Management, clique em **Abrir**.
        ix) Selecione o keystore PKCS#12 que retém o certificado de cliente. Por exemplo,`user.p12`
        x) Clique em **Receber**, selecione o certificado apropriado e clique em **OK**.
3. Extraia a parte pública do certificado de cliente:
   a) Abra a ferramenta IBM Key Management inserindo o comando **strmqikm** na linha de comandos.
   b) No menu **Arquivo do banco de dados de chave** na ferramenta IBM Key Management, clique em **Abrir**.

c) Selecione o keystore PKCS#12 que retém o certificado de cliente. Por exemplo,`user.p12`

d) Selecione o certificado de cliente por meio da lista de certificados na ferramenta IBM Key Management.

e) Clique **Extrair Certificado**.

f) Selecione um local para salvar o certificado e insira um nome de arquivo apropriado no campo **Nome do arquivo de certificado**. Por exemplo, `user.arm`.

4. Importe a parte pública do certificado de cliente para o keystore confiável do servidor mqweb como um certificado de assinante para que o servidor possa validar o certificado de cliente:

a) Crie um keystore `trust.jks` para uso pelo servidor mqweb, se um ainda não existir:

i) No menu **Arquivo do banco de dados de chave** na ferramenta IBM Key Management, clique em **Novo**.

ii) Selecione **JKS** na lista **Tipo de banco de dados de chaves**.

iii) Clique em **Procurar** e navegue até: `MQ_DATA_DIRECTORY/web/installations/installationName/servers/mqweb/resources/security`.

Esse diretório já deverá conter um arquivo `key.jks`. Se um arquivo `trust.jks` já existir, abra o existente em vez de sobrescrevê-lo.

iv) Insira `trust.jks` no campo **Nome do arquivo**.

v) Configure uma senha quando solicitado.

b) No menu suspenso, selecione **Certificados de Assinante**.

c) Clique em **Incluir**.

d) Selecione o arquivo arm apropriado e clique em **OK**. Por exemplo, selecione `user.arm`.

e) Insira um rótulo para o certificado.

5. Mude a senha do keystore do servidor mqweb:

a) A partir do menu **Arquivo de Banco de Dados de Chave**, clique em **Abrir**.

b) Selecione **JKS** na lista **Tipo de banco de dados de chaves**.

c) Clique em **Procurar** e navegue até *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb/resources/security`

d) Selecione o keystore `key.jks` e clique em **Abrir**.

e) Insira a senha quando solicitado. A senha padrão é `password`.

f) No menu **Arquivo do banco de dados de chave**, clique em **Mudar senha**.

g) Insira uma nova senha para o keystore.

6. Ative a autenticação de certificado de cliente no arquivo `mqwebuser.xml`:

O arquivo `mqwebuser.xml` pode ser localizado no caminho a seguir: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`

a) Descomente a seção no arquivo `mqwebuser.xml` que ativa a autenticação de certificado de cliente. A seção contém o texto a seguir:

```
<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) Verifique se o valor **serverKeyAlias** corresponde ao nome do certificado do servidor. Se você estiver usando o certificado do servidor padrão, o valor estará correto.

c) Mude o valor de **password** para o `defaultKeyStore` para uma versão codificada da senha para o keystore `key.jks`:

i) No diretório *MQ_INSTALLATION_PATH*/web/bin, insira o comando a seguir na linha de comandos:

```
securityUtility encode password
```

ii) Coloque a saída desse comando no campo **password** para o defaultKeyStore.

d) Mude o valor de **password** para o defaultTrustStore para corresponder à senha do keystore trust.jks:

i) No diretório *MQ_INSTALLATION_PATH*/web/bin, insira o comando a seguir na linha de comandos:

```
securityUtility encode password
```

ii) Coloque a saída desse comando no campo **password** para o defaultTrustStore.

e) Remova, ou comente, a linha a seguir no arquivo mqwebuser.xml:

```
<sslDefault sslRef="mqDefaultSSLConfig"/>
```

7. Pare o servidor mqweb inserindo o comando **endmqweb** na linha de comandos.
8. Inicie o servidor mqweb inserindo o comando **strmqweb** na linha de comandos.
9. Use o certificado de cliente para autenticar:
   - Para usar o certificado de cliente com o IBM MQ Console, instale o certificado de cliente no navegador da web que é usado para acessar o IBM MQ Console. Por exemplo, instale o certificado de cliente user.p12 como um certificado pessoal.
   - Para usar o certificado de cliente com a REST API, forneça o certificado de cliente com cada solicitação REST. Ao usar os métodos HTTP POST, PATCH ou DELETE, deve-se fornecer autenticação extra com o certificado de cliente para evitar ataques de falsificação de solicitação entre sites. Ou seja, a autenticação extra é usada para confirmar que as credenciais que estão sendo usadas para autenticar a solicitação estão sendo usadas pelo proprietário das credenciais.

     Essa autenticação extra é fornecida pelo cabeçalho HTTP ibm-mq-rest-csrf-token. Configure o valor do cabeçalho ibm-mq-csrf-token para qualquer coisa, incluindo em branco, em seguida, envie a solicitação.

Exemplo

Importante: No exemplo, nem todas as implementações de cURL suportam certificados autoassinados, portanto, deve-se usar uma implementação de cURL que suporte isso.

O exemplo de cURL a seguir mostra como criar uma nova fila Q1, no gerenciador de filas QM1, com a autenticação por certificado de cliente. A configuração exata desse comando cURL depende das bibliotecas com relação às quais o cURL foi construído. O exemplo é baseado em um sistema Windows, com cURL construído com relação ao OpenSSL.

- Use o método HTTP POST com o recurso de fila, autenticando com o certificado de cliente e incluindo o cabeçalho de HTTP ibm-mq-rest-csrf-token com um valor arbitrário. Esse valor pode ser qualquer coisa, incluindo em branco. A sinalização --cert-type especifica que o certificado é um certificado PKCS#12. A sinalização --cert especifica o local do certificado, seguido por dois-pontos, : , em seguida, a senha para o certificado:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -
-cert-type P12 --cert c:\user.p12:password
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 Usando autenticação básica HTTP com a REST API

Os usuários da REST API podem se autenticar fornecendo seus IDs e senhas em um cabeçalho de HTTP. Para usar esse método de autenticação com métodos de HTTP, como POST, PATCH e DELETE, o

cabeçalho de HTTP `ibm-mq-rest-csrf-token` também deve ser fornecido, bem como o ID do usuário e a senha.

Antes de começar

- Configure os usuários, os grupos e as funções para que sejam autorizados a usar a REST API. Para obter mais informações, consulte “Configurando usuários e funções” na página 497.
- Assegure-se de que a autenticação básica HTTP esteja ativada. Verifique se o XML a seguir está presente e não está comentado no arquivo `mqwebuser.xml`. Este XML deve estar dentro das tags `<featureManager>`:

  ```
  <feature>basicAuthenticationMQ-1.0</feature>
  ```

  z/OS No z/OS, deve-se ser um usuário que tenha acesso de gravação ao `mqwebuser.xml` para editar este arquivo.

  Multi Em todos os outros sistemas operacionais, você deve ser um usuário privilegiado para editar o arquivo `mqwebuser.xml`.
- Assegure-se de que você esteja usando uma conexão segura ao enviar solicitações REST. Como a combinação de nome de usuário e senha é codificada, mas não criptografada, deve-se usar uma conexão segura (HTTPS) ao utilizar a autenticação básica HTTP com a REST API.
- É possível consultar as credenciais do usuário atual usando o método HTTP GET no recurso `login`, fornecendo as informações básicas sobre autenticação para autenticar a solicitação. Esta solicitação retorna informações sobre o nome do usuário e as funções designadas ao usuário. Para obter mais informações, consulte GET `/login`

Procedimento

1. Concatene o nome do usuário com dois-pontos e a senha. Observe que o nome do usuário faz distinção entre maiúsculas e minúsculas.

   Por exemplo, um nome de usuário de administrador e uma senha de administrador tornam-se a sequência a seguir:

   ```
   admin:admin
   ```
2. Codifique essa sequência de nome do usuário e senha na codificação base64.
3. Inclua esse nome do usuário e senha codificados em um cabeçalho de HTTP `Authorization: Basic`.

   Por exemplo, com um nome de usuário codificado de administrador e uma senha de administrador, o cabeçalho a seguir é criado:

   ```
   Authorization: Basic YWRtaW46YWRtaW4=
   ```
4. Quando você usa os métodos de HTTP POST, PATCH ou DELETE, deve-se fornecer autenticação extra, bem como um nome de usuário e uma senha.

   Essa autenticação extra é fornecida pelo cabeçalho HTTP `ibm-mq-rest-csrf-token`. O cabeçalho de HTTP `ibm-mq-rest-csrf-token` deve estar presente na solicitação, mas seu valor pode ser qualquer coisa, incluindo em branco.
5. Envie sua solicitação REST para o IBM MQ com os cabeçalhos apropriados.

Exemplo

O exemplo a seguir mostra como criar uma nova fila Q1, no gerenciador de filas QM1, com autenticação básica em sistemas Windows. O exemplo usa o cURL:

- Use o método de HTTP POST com o recurso de fila, autenticando com a autenticação básica e incluindo o cabeçalho de HTTP `ibm-mq-rest-csrf-token` com um valor arbitrário. Esse valor pode ser qualquer coisa, incluindo em branco:

```
curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST
-u mqadmin:mqadmin
-H "ibm-mq-rest-csrf-token: value"
-H "Content-Type: application/json" --data "{\"name\":\"Q1\"}"
```

V 9.1.0 Usando autenticação baseada em token com a API de REST

Os usuários do REST API podem autenticar fornecendo um ID do usuário e uma senha para o recurso REST API `login` com o método HTTP POST. Um token LTPA é gerado, que permite que o usuário autentique solicitações futuras. Esse token LTPA tem o prefixo `LtpaToken2`. O usuário pode efetuar logout usando o método HTTP DELETE e pode consultar as informações de login do usuário atual com o método HTTP GET.

Antes de começar

- Configure os usuários, os grupos e as funções para que sejam autorizados a usar a REST API. Para obter mais informações, consulte “Configurando usuários e funções” na página 497.
- Por padrão, o nome do cookie que inclui o token LTPA inicia com `LtpaToken2` e inclui um sufixo que pode ser mudado quando o servidor mqweb é reiniciado. Esse nome de cookie escolhido a esmo permite que mais de um servidor do mqweb seja executado no mesmo sistema. No entanto, se você desejar que o nome do cookie permaneça um valor consistente, será possível especificar o nome dele usando o comando **setmqweb**. Para obter mais informações, consulte Configurando o token LTPA.
- Por padrão, o cookie do token LTPA expira após 120 minutos. É possível configurar o tempo de validade do cookie de token LTPA usando o comando **setmqweb**. Para obter mais informações, consulte Configurando o token LTPA.
- Assegure-se de que você esteja usando uma conexão segura ao enviar solicitações REST. Quando você usa o método HTTP POST no recurso `login`, a combinação de nome do usuário e senha enviada com a solicitação não é criptografada. Portanto, deve-se usar uma conexão segura (HTTPS) ao usar a autenticação baseada em token com a REST API. Por padrão, não é possível usar HTTP com a autenticação do token LTPA. É possível ativar o token LTPA para ser usado por conexões HTTP não seguras, configurando **secureLTPA** como `False`. Para obter mais informações, consulte Configurando o token LTPA.
- É possível consultar as credenciais do usuário atual usando o método de HTTP GET no recurso `login`, fornecendo o token LTPA para autenticar a solicitação. Esta solicitação retorna informações sobre o nome do usuário e as funções designadas ao usuário. Para obter mais informações, consulte GET / login.

Procedimento

1. Efetue login de um usuário:
   a) Use o método HTTP POST no recurso `login`:

   ```
   https://host:port/ibmmq/rest/v1/login
   ```

   Inclua o nome do usuário e a senha no corpo da solicitação JSON, no formato a seguir:

   ```
   {
       "username" : name,
       "password" : password
   }
   ```

   b) Armazene o token LTPA que é retornado da solicitação no armazenamento de cookie local. Por padrão, esse token LTPA tem um prefixo `LtpaToken2`.
2. Autentique as solicitações REST com o token LTPA armazenado como um cookie com cada solicitação.

Para solicitações que usam os métodos de HTTP PUT, PATCH ou DELETE, inclua um cabeçalho `ibm-mq-rest-csrf-token`. O valor desse cabeçalho pode ser qualquer coisa, inclusive em branco.

3. Efetue logout de um usuário:
   a) Use o método HTTP DELETE no recurso `login`:

   ```
   https://host:9443/ibmmq/rest/v1/login
   ```

   Deve-se fornecer o token LTPA como um cookie para autenticar a solicitação e incluir um cabeçalho `ibm-mq-rest-csrf-token`. O valor desse cabeçalho pode ser qualquer coisa, inclusive em branco

   b) Processe a instrução para excluir o token LTPA do armazenamento de cookie local.

   Nota: Se a instrução não for processada e o token LTPA permanecer no armazenamento de cookie local, o token LTPA poderá ser usado para autenticar solicitações REST futuras. Ou seja, quando o usuário tenta autenticar com o token LTPA após a sessão ser encerrada, uma nova sessão é criada usando o token existente.

Exemplo

O exemplo de cURL a seguir mostra como criar uma nova fila Q1, no gerenciador de filas QM1, com autenticação baseada em token em sistemas Windows:

- Efetue login e inclua o token LTPA com o prefixo `LtpaToken2` no armazenamento de cookie local. As informações sobre nome do usuário e senha são incluídas no corpo JSON. A sinalização `-c` especifica o local do arquivo para armazenar o token em:

  ```
  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
  ```

- Crie uma fila. Use o método de HTTP POST com o recurso de fila, autenticando com o token LTPA. O token LTPA com o prefixo `LtpaToken2` é recuperado do arquivo `cookiejar.txt` usando a sinalização `-b`. A proteção de CSRF é fornecida pela presença do cabeçalho de HTTP `ibm-mq-rest-csrf-token`:

  ```
  curl -k https://localhost:9443/ibmmq/rest/v1/admin/qmgr/QM1/queue -X POST -b
  c:\cookiejar.txt -H "ibm-mq-rest-csrf-token: value" -H "Content-Type: application/json"
  --data "{\"name\":\"Q1\"}"
  ```

- Efetue logout e exclua o token LTPA do armazenamento de cookie local. O token LTPA é recuperado do arquivo `cookiejar.txt` usando a sinalização `-b`. A proteção de CSRF é fornecida pela presença do cabeçalho de HTTP `ibm-mq-rest-csrf-token`. O local do arquivo `cookiejar.txt` é especificado pela sinalização `-c` para que o token LTPA seja excluído do arquivo:

  ```
  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
  ```

Referências relacionadas

POST /login
GET /login
Excluir /login

V 9.1.3 Integrando o IBM MQ Console a um IFrame

O elemento HTML < iframe> pode ser usado para integrar uma página da web em outra usando um Quadro Sequencial (IFrame). Por razões de segurança, o IBM MQ Console não pode ser integrado em um IFrame por padrão. No entanto, é possível ativar um IFrame usando a propriedade de configuração **`mqConsoleFrameAncestors`** no servidor mqweb.

Sobre esta tarefa

O servidor mqweb mantém uma lista de permissões de origens de páginas da Web que podem integrar o IBM MQ Console usando um IFrame Uma origem é uma combinação de um esquema de URL, domínio e porta, por exemplo, `https://example.com:1234`.

É possível usar a propriedade de configuração **mqConsoleFrameAncestors** no servidor mqweb para especificar as entradas na lista.

Por padrão, **mqConsoleFrameAncestors** está em branco, o que significa que o IBM MQ Console não pode ser integrado em um IFrame.

Procedimento

Especifique uma lista de origens de páginas da web, que podem integrar o IBM MQ Console em um IFrame, inserindo o comando a seguir:

```
setmqweb properties -k mqConsoleFrameAncestors -v allowedOrigins
```

em que *allowedOrigins* é uma lista de origens separada por vírgulas. Cada origem deve consistir em:

- Um nome do host ou endereço IP
- Um esquema de URL opcional
- Um número de porta opcional

Observe que o nome do host pode começar com o caractere curinga (*) e o número da porta também pode usar o caractere curinga curinga (*).

As origens de exemplo são:

```
https://example.com:1234
```

que permite que qualquer página da web seja entregue a partir de `https://example.com:1234` para integrar o IBM MQ Console em um IFrame.

```
https://*.example.com:*
```

que permite qualquer página da web HTTPS com um nome do host que termina com `example.com`, e usando qualquer porta, para integrar o IBM MQ Console em um IFrame.

Exemplo

O exemplo a seguir permite que o IBM MQ Console seja integrado a um IFrame a partir de páginas da web servidas a partir de `https://site2.example.com:1234` ou `https://site2.example.com:1235`:

```
setmqweb properties -k mqConsoleFrameAncestors -v
https://site2.example.com:1234,https://site2.example.com:1235
```

V 9.1.0 Configurando o CORS para a REST API

Por padrão, um navegador da web não permite scripts, como JavaScript, para chamar a REST API quando o script não é da mesma origem que a REST API. Ou seja, as solicitações de origem cruzada não estão ativadas. É possível configurar o Cross Origin Resource Sharing (CORS) para permitir solicitações de origem cruzada de origens especificadas.

Sobre esta tarefa

É possível acessar a REST API por meio de um navegador da web, por exemplo, por um script. Como essas solicitações são de uma origem diferente para a REST API, o navegador da web recusa a solicitação por se tratar de uma solicitação de origem cruzada. A origem será diferente se o domínio, porta ou esquema não for o mesmo.

Por exemplo, se você tiver um script hospedado em `http://localhost:1999/`, fará uma solicitação de origem cruzada se você emitir um HTTP GET em um website hospedado em `https://localhost:9443/`. Essa solicitação é uma solicitação de origem cruzada porque os números de porta e esquema (HTTP) são diferentes.

É possível ativar solicitações de origem cruzada configurando o CORS e especificando as origens que têm permissão para acessar a REST API.

Para obter mais informações sobre o CORS, consulte https://www.w3.org/TR/cors/ e https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS.

Procedimento

1. Visualize a configuração atual inserindo o comando a seguir:

   ```
   dspmqweb properties -a
   ```

   A entrada `mqRestCorsAllowedOrigins` especifica as origens permitidas. A entrada `mqRestCorsMaxAgeInSeconds` especifica o tempo, em segundos, que o navegador da web pode armazenar em cache os resultados de quaisquer verificações de simulação do CORS.
2. Especifique as origens que têm permissão para acessar a REST API inserindo o comando a seguir:

   ```
   setmqweb properties -k mqRestCorsAllowedOrigins -v allowedOrigins
   ```

   em que *allowedOrigins* especifica a origem da qual você deseja permitir solicitações de origem cruzada. É possível usar um asterisco entre aspas duplas, "*", para permitir todas as solicitações de origem cruzada. É possível inserir mais de uma origem em uma lista separada por vírgula, circundada por aspas duplas. Para permitir solicitações que não sejam de origem cruzada, insira aspas vazias como o valor para *allowedOrigins*.
3. Especifique o tempo, em segundos, que você deseja permitir que um navegador da web armazene em cache os resultados de quaisquer verificações prévias do CORS, inserindo o comando a seguir.

   ```
   setmqweb properties -k mqRestCorsMaxAgeInSeconds -v time
   ```

Exemplo

O exemplo a seguir mostra as solicitações de origem cruzada ativadas para `http://localhost:9883`, `https://localhost:1999` e `https://localhost:9663`. A idade máxima dos resultados em cache de quaisquer verificações prévias do CORS é configurada como 90 segundos:

```
setmqweb properties -k mqRestCorsAllowedOrigins -v "http://localhost:9883,https://
localhost:1999,https://localhost:9663"
setmqweb properties -k mqRestCorsMaxAgeInSeconds -v 90
```

Configurando a validação do cabeçalho do host para o IBM MQ Console e a REST API

É possível configurar o servidor mqweb para restringir o acesso ao IBM MQ Console e à REST API de modo que somente as solicitações enviadas com um cabeçalho do host que corresponda a uma lista de permissões especificada sejam processadas. Um erro será retornado se um valor de cabeçalho do host que não esteja na lista de permissões for usado.

Sobre esta tarefa

O servidor mqweb usa hosts virtuais para definir a lista de permissões de cabeçalhos do host aceitáveis. Para obter mais informações sobre os hosts virtuais, consulte a documentação do WebSphere Liberty: https://www.ibm.com/docs/SSEQTP_liberty/com.ibm.websphere.wlp.doc/ae/cwlp_virtual_hosts.html

Para completar esta tarefa, você deve ser um usuário com privilégios suficientes para editar o arquivo `mqwebuser.xml`:

- z/OS No z/OS, você deve ter acesso de gravação ao arquivo `mqwebuser.xml`.

- Multi Em todos os outros sistemas operacionais, deve-se ser um usuário privilegiado.

Procedimento

1. Abra o arquivo `mqwebuser.xml`. Esse arquivo está em um dos locais a seguir:
   - ULW

     No UNIX, Linux, and Windows: *MQ_DATA_PATH*`/web/installations/`*installationName*`/servers/mqweb`
   - z/OS

     No z/OS: *WLP_user_directory*`/servers/mqweb`

     em que *WLP_user_directory* é o diretório que foi especificado quando o script **crtmqweb** foi executado para criar a definição do servidor do mqweb.
2. Inclua ou descomente o código a seguir no arquivo `mqwebuser.xml`:

```
<virtualHost allowFromEndpointRef="defaultHttpEndpoint" id="default_host">
        <hostAlias>localhost:9080</hostAlias>
</virtualHost>
```

3. Edite o campo **<hostAlias>**, inserindo a combinação de nome de host e porta que você deseja permitir.

   Essa combinação pode ser o nome do host e o nome da porta que você usou na configuração do servidor mqweb. Por exemplo, se você usar a configuração padrão do `localhost:9443`, você pode querer usar `localhost:9443` no campo **<hostAlias>**.

   Se necessário, é possível incluir vários campos **<hostAlias>** dentro das tags **<virtualHost>** para permitir mais combinações de nome de host e porta. Por exemplo, para permitir cabeçalhos do host que usam uma porta HTTP, bem como cabeçalhos do host que usam a porta HTTPS.

V 9.1.0 Auditing

Os registros de auditoria de operações executadas no IBM MQ Console e no REST API podem ser produzidos ativando eventos de configuração e comando do gerenciador de filas e, no UNIX, Linux, and Windows, mudanças de estado significativo são registradas nos arquivos de log do servidor mqweb.

Mudanças de Estado Significativas

ULW

No UNIX, Linux, and Windows, o IBM MQ Console registra mudanças de estado significativas, como mensagens nos logs do servidor mqweb. Cada mensagem indica o nome do principal autenticado que solicitou a operação.

Mudanças de estado significativas, como quando os gerenciadores de filas são criados, iniciados, terminados ou excluídos, são registradas nos arquivos `messages.log` e `console.log` do servidor mqweb no nível de criação de log [AUDIT]. Cada entrada de log indica o nome do principal autenticado que solicitou a operação.

Os arquivos `messages.log` e `console.log` podem ser localizados no local a seguir:

- ULW No UNIX, Linux, and Windows: *MQ_DATA_PATH*`\web\installations\`*installationName*`\servers\mqweb\logs`

Para obter mais informações sobre como configurar os níveis de criação de log do servidor mqweb, consulte Configurando a criação de log.

Eventos de comando e configuração

É possível, opcionalmente, ativar eventos de comando e configuração no gerenciador de filas para fornecer informações sobre a maioria das atividades do IBM MQ Console e do REST API. Por exemplo, a criação de canais e a consulta de filas geram eventos de comando e de configuração. Para obter mais informações sobre como ativar eventos de comando e configuração, veja Controlando os eventos de configuração, de comando e de criador de logs.

Para essas mensagens de evento de comando e de configuração, o campo MQIACF_EVENT_ORIGIN é configurado como MQEVO_REST e o campo MQCACF_EVENT_APPL_IDENTITY relata os primeiros 32 caracteres do nome do principal autenticado. Se um usuário tem a função **MQWebAdmin** ou **MQWebAdminRO**, o campo MQCACF_EVENT_USER_ID relata o ID do usuário do servidor mqweb, não o nome de usuário do proprietário que emitiu o comando. No entanto, se o usuário tiver a função **MQWebUser**, o MQCACF_EVENT_USER_ID relatará o nome do usuário do principal que emitiu o comando.

Conceitos relacionados

"Auditing" na página 463

É possível procurar por intrusões de segurança ou tentativas de intrusão usando mensagens do evento. Também é possível verificar a segurança do seu sistema usando o IBM MQ Explorer.

Considerações de segurança para o IBM MQ Console e para a REST API em z/OS

O IBM MQ Console e a REST API possuem recursos de segurança que controlam se um usuário pode emitir, exibir ou alterar comandos. Os comandos são então passados para o gerenciador de filas e o gerenciador de filas é então usado para controlar se o usuário tem permissão para emitir o comando para esse gerenciador de filas específico.

Procedimento

1. Assegure-se de que o ID do usuário da tarefa iniciada do servidor mqweb tenha autoridades apropriadas para emitir determinados comandos PCF e acessar determinadas filas. Para obter informações adicionais, consulte "Autoridade requerida pelo ID do usuário da tarefa iniciada do servidor mqweb" na página 519.
2. Assegure-se de que quaisquer usuários para os quais a função `MQWebUser` foi concedida tenham autoridades apropriadas.

   Os usuários do IBM MQ Console e da REST API aos quais é designada a função `MQWebUser` operam sob o contexto de segurança do principal. Esses IDs de usuário podem executar somente operações que o ID do usuário possa executar no gerenciador de filas e precisam receber acesso às mesmas filas do sistema que o espaço de endereço do servidor mqweb.

   O ID do usuário da tarefa iniciada do servidor mqweb deve ter o acesso de usuário alternativo concedido para todos os usuários designados à função `MQWebUser`.

   Para obter mais informações sobre como conceder autoridades apropriadas para usuários com a função `MQWebUser`, veja "Acesso aos recursos do IBM MQ requeridos para usar o MQ Console ou a REST API" na página 520.
3. Opcional: Configure o TLS para o IBM MQ Console e a REST API. Para obter informações adicionais, consulte "Configurando o TLS para a REST API e o IBM MQ Console no z/OS" na página 521.

z/OS Autoridade requerida pelo ID do usuário da tarefa iniciada do servidor mqweb

No z/OS, o ID do usuário da tarefa iniciada do servidor mqweb requer que determinadas autoridades emitam comandos PCF e acessem recursos do sistema.

O ID do usuário da tarefa iniciada do servidor mqweb precisa de:

- Um identificador de usuários (UID) do z/OS UNIX para poder usar o z/OS UNIX System Services.

- Acesso aos conjuntos de dados `hlq.SCSQAUTH` e `hlq.SCSQANL*` na instalação do IBM MQ.
- Acesso de leitura para os arquivos de instalação do IBM MQ no z/OS UNIX System Services.
- Acesso de leitura e gravação para o diretório do usuário do Liberty criado pelo script **crtmqweb**.
- Autoridade para se conectar ao gerenciador de filas. Conceder ao ID do usuário de tarefa iniciada do servidor mqweb acesso de *LEITURA* ao perfil `hlq.BATCH` na classe MQCONN.
- Autoridade para emitir comandos do IBM MQ e acessar determinadas filas. Esses detalhes são descritos em "IBM MQ Console - perfis de segurança de comando necessários" na página 230, "Segurança da Fila do Sistema" na página 207 e "Perfis para Segurança de Contexto" na página 218.
- Autoridade para assinar o tópico SYSTEM.FTE , para usar o REST API para MFT. Conceder ao ID do usuário de tarefa iniciada do servidor mqweb acesso de *ALTERAÇÃO* ao perfil `hlq.SUBSCRIBE.SYSTEM.FTE` na classe MXTOPIC.
- Se você estiver configurando um registro SAF, acesso a vários perfis de segurança. Veja "Configurando um registro SAF para o IBM MQ Console e a REST API" na página 505 para obter mais informações.

Autenticação de conexão

Se o seu Gerenciador de Filas foi configurado para exigir que todos os aplicativos em lote fornecessem um ID de usuário e senha válidos, ao configurar CHKLOCL (REQUERIDO), deve-se conceder ao ID do usuário de tarefa iniciada do servidor mqweb acesso de *ATUALIZAÇÃO* ao perfil `hlq.BATCH` na classe MQCONN.

Essa autoridade faz com que a autenticação de conexão opere no modo CHKLOCL(OPTIONAL) para o ID do usuário da tarefa iniciada do servidor mqweb.

Se você não configurou o Gerenciador de Filas para exigir que todos os aplicativos em lote forneçam um ID de usuário e senha válidos, será suficiente conceder ao ID do usuário que inicia a tarefa do servidor mqweb acesso de *LEITURA* ao perfil `hlq.BATCH` na classe MQCONN.

Para obter mais informações sobre CHCKLOCL, veja "Usando o CHCKLOCL em aplicativos de limite local" na página 197.

Acesso aos recursos do IBM MQ requeridos para usar o MQ Console ou a REST API

As operações executadas no MQ Console ou na REST API por um usuário na função `MQWebUser` ocorrem sob o contexto de segurança do usuário.

Sobre esta tarefa

Consulte "Funções no IBM MQ Console e na REST API" na página 507 para obter mais informações sobre as funções no MQ Console e na REST API.

Use o procedimento a seguir para conceder a um usuário, na função `MQWebUser`, o acesso aos recursos do gerenciador de filas necessários para usar o MQ Console ou a REST API.

Procedimento

1. Conceda acesso de usuário alternativo ao ID do usuário `mqweb server started task` a cada ID do usuário na função `MQWebUser`.

   Faça isso em cada gerenciador de filas que os usuários administrarão por meio do MQ Console ou da REST API.

   É possível usar os comandos RACF de amostra a seguir para conceder ao usuário alternativo do ID do usuário `mqweb server started task` acesso a um usuário na função `MQWebUser` :

   ```
   RDEFINE MQADMIN hlq.ALTERNATE.USER.userId UACC(NONE)
   PERMIT hlq.ALTERNATE.USER.userId CLASS(MQADMIN) ACCESS(UPDATE) ID(mqwebUserId)
   SETROPTS RACLIST(MQADMIN) REFRESH
   ```

em que:

hlq
É o prefixo do perfil, que pode ser o nome do gerenciador de filas ou o nome do grupo de filas compartilhadas

userId
É o usuário na função `MQWebUser`

mqwebUserId
É o ID do usuário `mqweb server started task`

Nota: Se você estiver usando segurança composta por letras maiúsculas e minúsculas, use a classe MXADMIN em vez da classe MQADMIN.

2. Conceda a cada usuário na função `MQWebUser` o acesso a filas do sistema que são necessárias para usar o MQ Console e a REST API.

   Para fazer isso, para SYSTEM.ADMIN.COMMAND.QUEUE e SYSTEM.REST.REPLY.QUEUE, dê a cada usuário acesso UPDATE às classes MQQUEUE ou MXQUEUE, dependendo se a segurança composta por letras maiúsculas e minúsculas está ou não em uso.

   É necessário fazer isso em cada gerenciador de filas que o usuário administrará por meio do REST API, incluindo gerenciadores de filas remotas administrados por meio do gateway doadministrative REST API.
3. Para permitir que um usuário na função `MQWebUser` administre gerenciadores de filas remotas, conceda ao usuário acesso UPDATE ao perfil na classe MQQUEUE ou MXQUEUE, protegendo a fila de transmissão usada para enviar comandos ao gerenciador de filas remotas. Observe que é necessário fornecer ao usuário acesso UPDATE no gerenciador de filas de gateway.

   No gerenciador de filas remotas, conceda o acesso do mesmo usuário, para colocar na fila de transmissão usada para enviar mensagens de resposta do comando de volta para o gerenciador de filas de gateway.
4. Conceda aos usuários na função `MQWebUser` o acesso a quaisquer outros recursos necessários para executar as operações suportadas pelo MQ Console e pela REST API.

   O acesso necessário para:

   - Executar operações no REST API, é descrito nas seções *Requisitos de segurança* dos recursosREST API individuais
   - Emitir comandos pelo MQ Console, é descrito em “IBM MQ Console - perfis de segurança de comando necessários” na página 230

V 9.1.0 Configurando o TLS para a REST API e o IBM MQ Console no z/OS

No z/OS, é possível configurar o servidor mqweb para usar um conjunto de chaves do RACF para armazenar certificados para conexões seguras com TLS e autenticação por certificado de cliente.

Antes de começar

Deve-se ser um usuário que tenha acesso de gravação no arquivo `mqwebuser.xml` e autoridade para trabalhar com conjuntos de chaves SAF, para concluir esse procedimento.

Sobre esta tarefa

A configuração do servidor mqweb padrão usa os keystores do Java para os certificados confiáveis e do servidor. No z/OS, é possível configurar o servidor mqweb para usar um conjunto de chaves do RACF, em vez dos keystores do Java. O servidor também pode ser configurado para permitir que os usuários se autentiquem usando um certificado de cliente.

Veja Liberty: keystores para obter informações sobre como usar conjuntos de chaves do RACF no Liberty.

Siga este procedimento para configurar o servidor mqweb para usar um conjunto de chaves do RACF e, opcionalmente, configurar a autenticação por certificado de cliente.

Procedimento

1. Crie um certificado de autoridade de certificação (CA), que será usado para assinar o certificado do servidor. Por exemplo, insira o comando RACF a seguir:

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb Certification Authority')
    O('IBM')
    OU('MQ'))
  SIZE(2048)
  WITHLABEL('mqwebCertauth')
```

2. Crie um certificado do servidor, assinado com o certificado de CA criado na etapa 1, inserindo o comando a seguir:

```
RACDCERT ID(mqwebUserId) GENCERT
  SUBJECTSDN(CN('hostname')
   O('IBM')
   OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebCertauth'))
  WITHLABEL('mqwebServerCert')
```

   em que *mqwebUserId* é o ID do usuário da tarefa iniciada do servidor mqweb e *hostname* é o nome do host do servidor mqweb.

3. Conecte o certificado de CA e o certificado do servidor a um conjunto de chaves do SAF, inserindo os comandos a seguir:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebCertauth') CERTAUTH)
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebServerCert'))
```

   em que *mqwebUserId* é o ID do usuário da tarefa iniciada pelo servidor do mqweb e *keyring* é o nome do anel de chaves que você deseja usar.

4. Exporte o certificado de CA para um arquivo CER, inserindo o comando a seguir:

```
RACDCERT CERTAUTH EXPORT(LABEL('mqwebCertauth'))
        DSN('hlq.CERT.MQWEBCA')
        FORMAT(CERTDER)
        PASSWORD('password')
```

5. Transfira por FTP o certificado de CA exportado em binário para sua estação de trabalho e importe-o em seu navegador como um certificado de autoridade de certificação.

6. Opcional: Se você desejar configurar a autenticação por certificado de cliente, crie e exporte um certificado de cliente.

   a) Crie um certificado de autoridade de certificação (CA), que será usado para assinar o certificado de cliente. Por exemplo, insira o comando RACF a seguir:

```
RACDCERT GENCERT
  CERTAUTH
  SUBJECTSDN(CN('mqweb User CA')
   O('IBM')
   OU('MQ'))
   SIZE(2048)
  WITHLABEL('mqwebUserCertauth')
```

   b) Conecte o certificado de CA a um conjunto de chaves do SAF, inserindo o comando a seguir:

```
RACDCERT ID(mqwebUserId) CONNECT(RING(keyring) LABEL('mqwebUserCertauth') CERTAUTH)
```

   em que *mqwebUserId* é o ID do usuário da tarefa iniciada pelo servidor do mqweb e *keyring* é o nome do anel de chaves que você deseja usar.

c) Crie um certificado de cliente, assinado com o certificado de CA. Por exemplo, insira o comando a seguir:

```
RACDCERT ID(clientUserId) GENCERT
  SUBJECTSDN(CN('clientUserId')
     O('IBM')
     OU('MQ'))
   SIZE(2048)
   SIGNWITH (CERTAUTH LABEL('mqwebUserCertauth'))
  WITHLABEL('userCertLabel')
```

em que *clientUserId* é o nome do usuário.

O método usado para mapear um certificado para um principal depende do tipo de registro do usuário configurado:

- Se você estiver usando um registro básico, o campo Nome comum no certificado será correspondido com relação ao usuário no registro.
- Se você estiver usando um registro SAF e o certificado estiver no banco de dados do RACF, o proprietário do certificado, especificado com o parâmetro **ID** ao criar o certificado, será usado.
- Se você estiver usando um registro LDAP, o nome distinto completo no certificado será correspondido com relação ao registro LDAP.

d) Exporte o certificado de cliente para um arquivo PKCS #12, inserindo o comando a seguir:

```
RACDCERT ID(mqwebUserId) EXPORT(LABEL('userCertLabel')) PASSWORD('password')
DSN('hlq.USER.CERT')
```

e) Transfira por FTP o certificado exportado em binário para sua estação de trabalho. Para usar o certificado de cliente com o IBM MQ Console, importe-o para o navegador da web usado para acessar o IBM MQ Console como um certificado pessoal.

7. Edite o arquivo *WLP_user_directory*/servers/mqweb/mqwebuser.xml, em que *WLP_user_directory* é o diretório que foi especificado quando o script **crtmqweb** foi executado para criar a definição do servidor mqweb.

   Faça as mudanças a seguir para configurar o servidor mqweb para usar um conjunto de chaves do RACF:

   a) Remova ou comente a linha a seguir:

   ```
   <sslDefault sslRef="mqDefaultSSLConfig"/>
   ```

   b) Inclua as instruções a seguir:

   ```
   <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"/>
   ```

   em que:

   - *mqwebUserId* é o ID do usuário da tarefa iniciada do servidor mqweb.
   - *keyring* é o nome do conjunto de chaves do RACF.
   - *mqwebServerCert* é o rótulo do certificado do servidor mqweb.

   Notes: O valor de **keyStore password** é ignorado.

8. Reinicie o servidor mqweb parando e reiniciando a tarefa iniciada do servidor mqweb.
9. Opcional: Use o certificado de cliente para autenticar:

   - Para usar o certificado de cliente com o IBM MQ Console, insira a URL para o MQ Console no navegador da web em que você instalou o certificado de cliente.

- Para usar o certificado de cliente com a API de REST, forneça o certificado de cliente com cada solicitação REST.

Notes:

a. Se você estiver usando somente certificados para autenticação no IBM MQ Console, o navegador poderá exibir uma lista de certificados dentre os quais será possível selecionar.

b. Se você desejar usar um certificado diferente, pode ser necessário fechar e reiniciar o navegador.

c. Se você estiver usando certificados de cliente que não estão no banco de dados do RACF, será possível usar a filtragem de nomes de certificado do RACF para mapear atributos de certificado para um ID do usuário. Por exemplo:

```
RACDCERT ID(DEPT3USR) MAP SDNFILTER(OU=DEPT1.C=US)
```

mapeia certificados com um nome distinto de assunto contendo OU=DEPT1 e C=US para o ID do usuário DEPT3USR.

Resultados

Você configurou uma interface TLS para o IBM MQ Console e a REST API.

ULW Gerenciando chaves e certificados no UNIX, Linux, and Windows

Use o comando `runmqckm` (UNIX e Windows) e o comando `runmqakm` (UNIX, Linux, and Windows) para gerenciar chaves, certificados e solicitações de certificado.

O comando runmqckm

O comandeo **runmqckm** está disponível no UNIX e no Windows.

O comando **runmqckm** fornece funções que são semelhantes àquelas do iKeyman, descritas em “ProtegendoIBM MQ” na página 5.

Para usar o comando **runmqckm** , certifique-se de que as variáveis de ambiente do sistema estejam configuradas corretamente executando o comando **setmqenv**

V 9.1.0 O comando **runmqckm** requer que o componente JRE do IBM MQ seja instalado. Se esse componente não for instalado, será possível usar o comando **runmqackm** em substituição

O comando runmqakm

O comando **runmqakm** está disponível no UNIX, Linux e Windows.

Para usar o comando **runmqaqm** , certifique-se de que as variáveis de ambiente do sistema estejam configuradas corretamente executando o comando **setmqenv**

Se for preciso gerenciar certificados TLS de um modo compatível com FIPS, use o comando **runmqakm** em vez dos comandos **runmqckm**. Isso ocorre porque o comando **runmqakm** suporta criptografia mais avançada.

Use os comandos `runmqckm` e `runmqakm` para executar o seguinte:

- Criar o tipo de arquivo do banco de dados de chave CMS que o IBM MQ requer
- Criar pedidos de certificado
- Importar certificados pessoais
- Importar certificados de CA
- Gerenciar certificados autoassinados

Informações relacionadas

Keytool

ULW runmqckm e comandos runmqakm em UNIX, Linux, and Windows

Esta seção descreve os comandos runmqckm e runmqakm de acordo com o objeto do comando.

As principais diferenças entre os dois comandos são as seguintes:

- ULW **runmqakm**
  - Está disponível no UNIX, Linux e Windows.
  - Suporta a criação de certificados e pedidos de certificados com chaves públicas Elliptic Curve, o comando **runmqckm** não.
  - Suporta mais forte de criptografia do arquivo de repositório de chaves que o comando **runmqckm** por meio do parâmetro **-strong** .
  - Foram certificados como compatíveis com FIPS 140-2, e pode ser configurado para operar em um modo compatível com FIPS, utilizando o parâmetro **-fips** , ao contrário do comando **runmqckm** .
- Windows UNIX **runmqckm**
  - Está disponível no UNIX e no Windows.
  - Suporta os formatos de arquivo de repositório de chaves JKS e JCEKS, enquanto o comando **runmqakm** não suporta.

Atenção: V 9.1.0 O comando **runmqckm** requer a instalação do recurso IBM MQ Java runtime environment (JRE).

Cada comando especifica pelo menos um *objeto*. Comandos para operações de dispositivo PKCS #11 podem especificar objetos adicionais. Comandos para objetos de banco de dados de chaves, certificado e solicitação de certificado especificam uma *ação*. O objeto pode ser um dos seguintes:

-keydb
Ações se aplicam a um banco de dados de chaves

-cert
Ações se aplicam a um certificado

-certreq
Ações se aplicam a uma solicitação de certificado

-help
Exibe a ajuda

-versão
Exibe informações da versão

Os subtópicos a seguir descrevem as ações que você pode tomar sobre objetos de banco de dados de chaves, certificado e solicitação de certificado; consulte “Opções runmqckm e runmqakm em UNIX, Linux, and Windows” na página 535 para obter uma descrição das opções desses comandos.

ULW Comandos para um banco de dados de chaves CMS somente no UNIX, Linux, and Windows

É possível usar os comandos **runmqckm** e **runmqakm** para gerenciar chaves e certificados para um banco de dados de chaves CMS.

-keydb -changepw
Mude a senha para um banco de dados de chaves CMS:

```
-keydb -changepw -db filename -pw password -new_pw new_password


-stash
```

-keydb -create
Crie um banco de dados de chaves CMS:

```
-keydb -create -db filename
-pw password -type cms -expire days -stash
```

-keydb -stashpw
Armazene em arquivo stash a senha de um banco de dados de chaves CMS em um arquivo:

```
-keydb -stashpw -db filename
-pw password
```

-cert -getdefault

Nota: O certificado padrão não é suportado pelo IBM MQ 8.0. É necessário usar a configuração do rótulo de certificado conforme descrito em "Rótulos de Certificados Digitais, Entendendo os Requisitos" na página 26.

Obtenha o certificado pessoal padrão:

```
-cert -getdefault -db filename
-pw password
```

-cert -modify
Modifica um certificado.

Nota: Atualmente, o único campo que pode ser modificado é o campo Certificado de Confiança.

```
-cert -modify -db filename
-pw password -label label
-trust enable|disable
```

-cert -setdefault

Nota: O certificado padrão não é suportado pelo IBM MQ 8.0 ou mais recente. É necessário usar a configuração do rótulo de certificado conforme descrito em "Rótulos de Certificados Digitais, Entendendo os Requisitos" na página 26.

Configure o certificado pessoal padrão:

```
-cert -setdefault -db filename
-pw password -label label
```

ULW Comando para bancos de dados de chaves CMS ou PKCS #12 no UNIX, Linux, and Windows

É possível usar os comandos runmqckm e runmqakm para gerenciar chaves e certificados para um banco de dados de chaves CMS ou banco de dados de chaves PKCS #12.

Nota: O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.

Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.

-keydb -changepw
Mude a senha para um banco de dados de chaves:

```
-keydb -changepw -db filename -pw password -new_pw
new_password -expire days
```

-keydb -convert
converta o banco de dados de chaves de um formato para outro:

```
-keydb -convert -db filename -pw password
-old_format cms | pkcs12 -new_format cms
```

-keydb -create
Crie um banco de dados de chaves:

```
-keydb -create -db filename -pw password -type cms
| pkcs12
```

-keydb -delete
Exclua um banco de dados de chaves:

```
-keydb -delete -db filename -pw password
```

-keydb -list
Listar os tipos de banco de dados de chaves suportados atualmente:

```
-keydb -list
```

-cert -add
Inclua um certificado de um arquivo em um banco de dados de chaves:

```
-cert -add -db filename -pw password -label label
-file filename
-format ascii | binary
```

-cert -create
Crie um certificado autoassinado:

```
-cert -create -db filename -pw password -label label
-dn distinguished_name
-size 1024 | 512 -x509version 3 | 1
| 2
-expire days -sig_alg MD2_WITH_RSA | MD2WithRSA
|
MD5_WITH_RSA | MD5WithRSA
|
SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA
|
SHA2WithRSA | SHA384_WITH_RSA
|
SHA384WithRSA | SHA512_WITH_RSA
|
SHA512WithRSA | SHA_WITH_DSA
|
SHA_WITH_RSA | SHAWithDSA
|
SHAWithRSA
```

-cert -delete
Exclua um certificado:

```
-cert -delete -db filename -pw password -label label
```

-cert -details
Liste as informações detalhadas para um certificado específico:

```
-cert -details -db filename -pw password -label label
```

-cert -export
Exporte um certificado pessoal e sua chave privada associada de um banco de dados de chaves para um arquivo PKCS #12 ou para outro banco de dados de chaves:

```
-cert -export -db filename -pw password -label label
-type cms | pkcs12
-target filename -target_pw password -target_type
cms | pkcs12
```

-cert -extract
Extraia um certificado de um banco de dados de chaves:

```
-cert -extract -db filename -pw password -label label
-target filename
-format ascii | binary
```

-cert -import
Importe um certificado pessoal de um banco de dados de chaves:

```
-cert -import -file filename -pw password -type
pkcs12 -target filename
-target_pw password -target_type cms -label
label
```

A opção `-label` é necessária e especifica o rótulo do certificado que deve ser importado do banco de dados de chaves de origem.

A opção `-new_label` é opcional e permite que o certificado importado receba um rótulo no banco de dados de chaves de destino diferente do rótulo no banco de dados de origem.

-cert -list
Liste todos os certificados em um banco de dados de chaves:

```
-cert -list all | personal | CA
-db filename -pw password
```

-cert -receive
Receba um certificado de um arquivo:

```
-cert -receive -file filename -db filename -pw password

-format ascii | binary -default_cert yes |
no
```

-cert -sign
Assine um certificado:

```
-cert -sign -db filename -file filename -pw password
-label label -target filename
-format ascii | binary -expire days
-sig_alg MD2_WITH_RSA | MD2WithRSA | MD5_WITH_RSA
|
MD5WithRSA | SHA1WithDSA | SHA1WithRSA
|
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

-certreq -create
Crie uma solicitação de certificado:

```
-certreq -create -db filename -pw password
-label label -dn distinguished_name
-size 1024 | 512 -file filename
-sig_alg MD2_WITH_RSA | MD2WithRSA |
MD5_WITH_RSA | MD5WithRSA |
SHA1WithDSA | SHA1WithRSA |
SHA256_WITH_RSA | SHA256WithRSA |
SHA2WithRSA | SHA384_WITH_RSA |
SHA384WithRSA | SHA512_WITH_RSA |
SHA512WithRSA | SHA_WITH_DSA |
SHA_WITH_RSA | SHAWithDSA |
SHAWithRSA
```

-certreq -delete
Exclua uma solicitação de certificado:

```
-certreq -delete -db filename -pw password -label
label
```

-certreq -details
Liste as informações detalhadas de uma solicitação de certificado específica:

```
-certreq -details -db filename -pw password -label
label
```

Liste as informações detalhadas sobre uma solicitação de certificado e mostre a solicitação de certificado integral:

```
-certreq -details -showOID -db filename
-pw password -label label
```

-certreq -extract
Extraia uma solicitação de certificado de um banco de dados de solicitações de certificado em um arquivo:

```
-certreq -extract -db filename -pw password
-label label -target filename
```

-certreq -list
Liste todas as solicitações de certificado no banco de dados de solicitações de certificado:

```
-certreq -list -db filename -pw password
```

-certreq -recreate
Recrie uma solicitação de certificado:

```
-certreq -recreate -db filename -pw password
-label label -target filename
```

ULW Comandos para operações de dispositivo de criptografia no UNIX, Linux, and Windows

É possível usar os comandos runmqckm e runmqakm para gerenciar chaves e certificados para operações de dispositivo criptográfico.

Nota: O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.

Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.

-keydb -changepw
Mude a senha para um dispositivo criptográfico:

```
-keydb -changepw -crypto module_name -tokenlabel token_label
-pw password -new_pw new_password
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-keydb -list
Listar os tipos de banco de dados de chaves suportados atualmente:

```
-keydb -list
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -add
Inclua um certificado de um arquivo em um dispositivo criptográfico:

```
-cert -add -crypto module_name -tokenlabel token_label
-pw password -label label -file filename -format
ascii | binary
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -create
Crie um certificado autoassinado em um dispositivo criptográfico:

```
-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
```

Nota: Não é possível importar um certificado que contenha vários atributos de OU (unidade organizacional) no nome distinto.

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -delete
Exclua um certificado em um dispositivo criptográfico:

```
-cert -delete -crypto module_name -tokenlabel token_label
-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -details
Liste as informações detalhadas para um certificado específico em um dispositivo criptográfico:

```
-cert -details -crypto module_name -tokenlabel token_label

-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

Liste as informações detalhadas e mostre o certificado integral para um certificado específico em um dispositivo criptográfico:

```
-cert -details -showOID -crypto module_name -tokenlabel
token_label
-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -extract
Extraia um certificado de um banco de dados de chaves:

```
-cert -extract -crypto module_name -tokenlabel token_label
-pw password -label label -target filename
-format ascii | binary
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -import

Importe um certificado para um dispositivo criptográfico com suporte do banco de dados de chaves secundário:

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

```
-cert -import -db filename -pw password -label label
-type cms
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Importe um certificado PKCS #12 para um dispositivo criptográfico com suporte do banco de dados de chaves secundário:

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

```
-cert -import -file filename -pw password -type pkcs12
-crypto module_name -tokenlabel token_label -pw
password
-secondaryDB filename -secondaryDBpw password -fips
```

Nota: Não é possível importar um certificado que contenha vários atributos de OU (unidade organizacional) no nome distinto.

-cert -list

Liste todos os certificados em um dispositivo criptográfico:

```
-cert -list all | personal | CA
-crypto module_name -tokenlabel token_label -pw
password
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-cert -receive
Receba um certificado de um arquivo para um dispositivo criptográfico com suporte do banco de dados de chaves secundário:

```
-cert -receive -file filename -crypto module_name -tokenlabel
token_label
-pw password -default_cert yes | no
-secondaryDB filename -secondaryDBpw password -format
ascii | binary
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

Usando o comando **runmqakm**:

-certreq -create
Crie uma solicitação de certificado em um dispositivo criptográfico:

```
-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
```

Nota: Não é possível importar um certificado que contenha vários atributos de OU (unidade organizacional) no nome distinto.

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-certreq -delete
Exclua uma solicitação de certificado de um dispositivo criptográfico:

```
-certreq -delete -crypto module_name -tokenlabel token_label

-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As

plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-certreq -details
Liste as informações detalhadas de uma solicitação de certificado específica em um dispositivo criptográfico:

```
-certreq -details -crypto module_name -tokenlabel token_label

-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

Liste as informações detalhadas sobre uma solicitação de certificado e mostrar a solicitação de certificado integral em um dispositivo criptográfico:

```
-certreq -details -showOID -crypto module_name -tokenlabel
token_label
-pw password -label label
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-certreq -extract
Extraia uma solicitação de certificado de um banco de dados de solicitações de certificado em um dispositivo criptográfico para um arquivo:

```
-certreq -extract -crypto module_name -tokenlabel token_label

-pw password -label label -target filename
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

-certreq -list
Liste todas as solicitações de certificado no banco de dados de solicitações de certificado em um dispositivo criptográfico:

```
-certreq -list -crypto module_name -tokenlabel token_label

-pw password
```

Se você estiver usando certificados ou chaves armazenadas no hardware de criptografia PKCS n.º 11, observe que **runmqckm** e **strmqikm** são programas de 64 bits. Módulos externos necessários para o suporte do PKCS #11 serão carregados em um processo de 64 bits, portanto, você deverá ter uma biblioteca do PKCS #11 de 64 bits instalada para a administração do hardware de criptografia. As

plataformas Windows e Linux x86 de 32 bits são as únicas exceções, uma vez que os programas **strmqikm** e **runmqckm** são de 32 bits nessas plataformas.

ULW Opções runmqckm e runmqakm em UNIX, Linux, and Windows

É possível usar as opções da linha de comandos **runmqckm** (iKeycmd) e **runmqakm** para gerenciar chaves, certificados e solicitações de certificado.

ULW O comando `runmqakm` está disponível no UNIX, Linux, and Windows.

Windows UNIX O comandeo `runmqckm` está disponível no UNIX e no Windows.

Nota: O IBM MQ não suporta algoritmos SHA-3 ou SHA-5. É possível usar os nomes de algoritmos de assinatura digital SHA384WithRSA e SHA512WithRSA porque ambos os algoritmos são membros da família do SHA-2.

Os nomes dos algoritmos de assinatura digital SHA3WithRSA e SHA5WithRSA são descontinuados porque eles são uma forma abreviada do SHA384WithRSA e do SHA512WithRSA, respectivamente.

O significado de uma opção pode depender do objeto e da ação especificados no comando.

*Tabela 90. Opções que podem ser usadas com **runmqckm** e **runmqakm***

Parâmetro	Descrição
`-create`	Opção para criar um banco de dados de chaves.
`-crypto`	Nome do módulo para gerenciar um dispositivo criptográfico PKCS #11. Um valor após **-crypto** será opcional se você especificar o nome do módulo no arquivo de propriedades. Se você estiver usando certificados ou chaves armazenadas no hardware criptográfico PKCS #11 , observe que **runmqckm** e **strmqikm** são executados usando a máquina virtual Java (JVM) fornecida com a instalação do IBM MQ. Os módulos externos necessários para o suporte do PKCS #11 serão carregados no processo da JVM, portanto, deve-se ter uma biblioteca do PKCS #11 instalada para a administração de hardware de criptografia que corresponda à quantidade de bits da JVM e essa biblioteca deve ser especificada para **runmqckm** ou **strmqikm**.
-db	Nome do caminho completo de um banco de dados de chaves.
-default_cert	Configura um certificado como padrão. O valor pode ser `yes` ou `no`. O padrão é `no`.
-dn	nome distinto X.500. O valor é uma sequência entre aspas duplas, por exemplo, `"CN=John Smith,O=IBM,OU=Test,C=GB"`. Observe que apenas os atributos O e C são obrigatórios. Especificar um nome comum (CN) é opcional.
-encryption	Força da criptografia usada no comando de exportação de certificado. O valor pode ser `strong` ou `weak`. O padrão é `strong`.
-expire	Prazo de expiração em dias de uma senha de certificado ou de banco de dados. O padrão são 365 dias para uma senha de certificado. Não há nenhum tempo padrão para uma senha do banco de dados: utilize o parâmetro **-expire** para configurar um tempo de expiração da senha do banco de dados explicitamente.
-file	Nome do arquivo de um certificado ou solicitação de certificado.

*Tabela 90. Opções que podem ser usadas com **runmqckm** e **runmqakm** (continuação)*	
Parâmetro	**Descrição**
-fips	Especifica que o comando é executado no modo FIPS. Quando estiver no modo FIPS, o componente ICC usará os algoritmos que foram validados pelo FIPS 140-2. Se o componente ICC não for inicializado no modo FIPS, o comando **runmqakm** falhará.
-format	Formato de um certificado. O valor pode ser `ascii` para ASCII codificado como Base64 ou `binário` para dados DER binários. O padrão é `ascii`.
-label	Rótulo conectado a um certificado ou a um pedido de certificado. Se o certificado for um certificado pessoal usado para identificar um aplicativo cliente ou gerenciador de filas do IBM MQ, o rótulo deverá corresponder à configuração do rótulo de certificado (CERTLABL) do IBM MQ. Para obter mais informações, consulte "Rótulos de Certificados Digitais, Entendendo os Requisitos" na página 26.
-new_format	Novo formato do banco de dados de chaves.
-new_label	Usada em um comando de importação de certificado, esta opção permite que um certificado seja importado com um rótulo diferente do que ele tinha no banco de dados de chaves de origem. Se o certificado for um certificado pessoal usado para identificar um aplicativo cliente ou gerenciador de filas do IBM MQ, o rótulo deverá corresponder à configuração do rótulo de certificado (CERTLABL) do IBM MQ. Para obter mais informações, consulte "Rótulos de Certificados Digitais, Entendendo os Requisitos" na página 26.
-new_pw	Nova senha do banco de dados.
-old_format	Antigo formato do banco de dados de chaves.
-pw	A senha para o banco de dados de chaves ou arquivo PKCS #12.
-secondaryDB	Nome de um banco de dados de chaves secundário para operações de dispositivo PKCS #11.
-secondaryDBpw	Senha para o banco de dados de chaves secundário para operações de dispositivo PKCS #11.
-showOID	Exibe o certificado ou a solicitação de certificado integrais.

*Tabela 90. Opções que podem ser usadas com **runmqckm** e **runmqakm** (continuação)*	
Parâmetro	**Descrição**
-sig_alg	O algoritmo hash utilizado durante a criação de um pedido de certificado, um certificado auto-assinado ou a assinatura de um certificado. Esse algoritmo hash é usado para criar a assinatura associada ao certificado ou à solicitação de certificado recém-criados. Para **runmqckm**, o valor pode ser 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. O valor padrão é SHA1WithRSA. Para **runmqakm**, o valor pode ser md5, MD5_WITH_RSA, MD5WithRSA, SHA_WITH_DSA, SHA_WITH_RSA, sha1, SHA1WithDSA, SHA1WithECDSA, SHA1WithRSA, sha224, SHA224_WITH_RSA, SHA224WithDSA, SHA224WithECDSA, SHA224WithRSA, sha256, SHA256_WITH_RSA, SHA256WithDSA, SHA256WithECDSA, SHA256WithRSA, SHA2WithRSA, sha384, SHA384_WITH_RSA, SHA384WithECDSA, SHA384WithRSA, sha512, SHA512_WITH_RSA, SHA512WithECDSA, SHA512WithRSA, SHAWithDSA, SHAWithRSA, EC_ecdsa_with_SHA1, EC_ecdsa_with_SHA224, EC_ecdsa_with_SHA256, EC_ecdsa_with_SHA384 ou EC_ecdsa_with_SHA512. O valor padrão é SHA1WithRSA.
-size	Tamanho da chave. Para **runmqckm**, o valor pode ser 512, 1024 ou 2048. O valor padrão é 1024 bits. Para **runmqakm**, o valor depende do algoritmo de assinatura: • Para algoritmos de assinatura RSA (o algoritmo padrão usado se nenhum **-sig_alg** for especificado), o valor poderá ser 512, 1024, 2048 ou 4096. Um tamanho de chave RSA de 512 bits não será permitido se o parâmetro **-fips** estiver ativado. O tamanho de chave RSA padrão é de 1024 bits. • Para algoritmos de Curva Elíptica, o valor pode ser 256, 384 ou 512. O tamanho de chave de Curva Elíptica padrão depende do algoritmo de assinatura. Para SHA256, ele é 256; para SHA384, ele é 384; e para SHA512, ele é 512.
-stash	Armazene em arquivo stash a senha do banco de dados de chaves para um arquivo. Apenas aplicável a bancos de dados do tipo CMS e PKCS12. **Nota: -stash** é válido em **-keydb** -create comandos para informar **runmqckm**/ **runmqakm** para criar um arquivo stash que contém a senha A emissão do comando $ runmqakm -help lista apenas os parâmetros de ajuda de alto nível

*Tabela 90. Opções que podem ser usadas com **runmqckm** e **runmqakm** (continuação)*	
Parâmetro	**Descrição**
-stashed	Indica que a senha para o banco de dados de chaves ou o arquivo PKCS #12 está em um arquivo stash **Nota:** A opção **-stashed** é válida em chamadas, além dos comandos **-keydb** -create Se você não especificar essa opção, será necessário fornecer a senha usando **-pw** Além disso, somente quando você instrui o comando que tipo de ação você está executando a ajuda detalhada mostrando **-stashed** aparece.
-target	Arquivo ou banco de dados de destino.
-target_pw	Senha para o banco de dados de chaves se **-target** especificar um banco de dados de chaves.
-target_type	Tipo do banco de dados especificado pelo operando **-target**. Consulte o parâmetro **-type** para obter os valores permitidos.
-tokenLabel	Rótulo de um dispositivo criptográfico PKCS #11.
-trust	Status de confiança de um certificado de CA. O valor pode ser `ativar` ou `desativar`. O padrão é `enable`.
-type	O tipo do banco de dados. O valor pode ser qualquer um dos seguintes valores: • `cms` para um banco de dados de chaves CMS • `pkcs12` para um arquivo PKCS #12.
-x509version	Versão do certificado X.509 a ser criado. O valor pode ser de 1, 2 ou 3. O padrão é 3.

-rfc3339	Use esse parâmetro para exibir a data no formato RFC 3339 para o comando `runmqakm -cert -details`, que é um dos formatos a seguir:
	`Not Before : 2015-08-26T08:53:37Z`
	`Not After : 2016-08-26T08:53:37Z`
	Observe que o parâmetro **-rfc3339** tem que aparecer no comando após os parâmetros adicionais:
	`runmqakm -cert -details -db exampleDB -stashed -label certficateLabel -rfc3339`

Nota: As propriedades fornecidas com o IBM Global Security Kit (GSKit) relacionadas ao parâmetro **-seckey** de criptografia de chave simétrica no utilitário **runmqckm** são ignoradas e não suportadas pelo IBM MQ.

ULW Códigos de erro runmqakm em UNIX, Linux, and Windows

Uma tabela dos códigos numéricos de erro emitidos por runmqakm e o que eles significam.

código de erro	mensagem de erro
0	Sucesso
1	Erro desconhecido ocorrido

código de erro	mensagem de erro
2	Ocorreu um erro de codificação/decodificação ASN.1.
3	Ocorreu um erro ao inicializar o codificador/ decodificador ASN.1.
4	Ocorreu um erro de codificação/decodificação ASN.1 devido a um índice fora do intervalo ou a um campo opcional não existente.
5	Ocorreu um erro de banco de dados.
6	Ocorreu um erro ao abrir o arquivo de banco de dados, verifique a existência e a permissão do arquivo.
7	Ocorreu um erro ao reabrir o arquivo de banco de dados.
8	Falha na criação do banco de dados.
9	O banco de dados já existe.
10	Ocorreu um erro ao excluir o arquivo de banco de dados.
11	O banco de dados não pôde ser aberto.
12	Ocorreu um erro ao ler o arquivo de banco de dados.
13	Ocorreu um erro ao ler os dados para o arquivo de banco de dados.
14	Ocorreu um erro de validação de banco de dados.
15	Foi encontrada uma versão inválida do banco de dados.
16	Foi encontrada um senha do banco de dados inválida.
17	Foi encontrado um tipo de arquivo inválido do banco de dados.
18	O banco de dados especificado foi corrompido.
19	Uma senha inválida foi fornecida ou o banco de dados de chaves foi corrompido.
20	Ocorreu um erro de integridade de entrada de chave do banco de dados.
21	Já existe um certificado duplicado no banco de dados.
22	Uma chave duplicada já existe no banco de dados (ID de Registro).
23	Um certificado com o mesmo rótulo já existia no banco de dados de chaves.
24	Uma chave duplicada já existe no banco de dados (Assinatura).

código de erro	mensagem de erro
25	Uma chave duplicada já existe no banco de dados (Certificado não Assinado).
26	Uma chave duplicada já existe no banco de dados (Emissor e Número de Série).
27	Uma chave duplicada já existe no banco de dados (Informações de Chave Pública de Assunto).
28	Uma chave duplicada já existe no banco de dados (CRL não Assinado).
29	O rótulo foi utilizado no banco de dados.
30	Ocorreu um erro de criptografia de senha.
31	Ocorreu um erro relacionando ao LDAP. (LDAP não é suportado por este programa)
32	Ocorreu um erro criptográfico.
33	Ocorreu um erro de criptografia/decriptografia.
34	Foi encontrado um erro de criptografia inválido.
35	Ocorreu um erro ao assinar dados.
36	Ocorreu um erro durante a verificação de dados.
37	Ocorreu um erro durante o cálculo de classificação de dados.
38	Foi encontrado um parâmetro criptográfico inválido.
39	Foi encontrado um algoritmo criptográfico não suportado.
40	O tamanho da entrada especificada é maior que o tamanho do módulo suportado.
41	Foi localizado um tamanho de módulo não suportado.
42	Ocorreu um erro de validação de banco de dados.
43	A validação de entrada de chave falhou.
44	Existe um campo de extensão duplicado.
45	A versão da chave está incorreta.
46	Um campo de extensão obrigatório não existe.
47	O período de validade não inclui hoje ou não cai dentro do período de validade de seu emissor
48	O período de validade não inclui hoje ou não cai dentro do período de validade de seu emissor.
49	Ocorreu um erro durante a validação da extensão de utilização da chave privativa.
50	O emissor da chave não foi localizado.

código de erro	mensagem de erro
51	Uma extensão de certificado requerida está ausente.
52	Foi localizada uma extensão de restrição básica inválida.
53	A validação de assinatura da chave falhou.
54	A chave raiz da chave não é confiável.
55	A chave foi anulada.
56	Ocorreu um erro durante a validação da extensão do identificador da chave de autoridade.
57	Ocorreu um erro durante a validação da extensão de utilização da chave privativa.
58	Ocorreu um erro durante a validação da extensão do nome alternativo do assunto.
59	Ocorreu um erro durante a validação da extensão do nome alternativo do emissor.
60	Ocorreu um erro durante a validação da extensão de utilização da chave.
61	Uma extensão crítica desconhecida foi localizada.
62	Ocorreu um erro durante a validação de entradas de pares de chaves.
63	Ocorreu um erro ao validar a CRL.
64	Ocorreu um erro de exclusão mútua.
65	Um parâmetro inválido foi localizado.
66	Foi encontrado um parâmetro nulo ou erro de alocação de memória.
67	O número ou tamanho é muito grande ou muito pequeno.
68	A senha antiga é inválida.
69	A nova senha é inválida.
70	A senha expirou.
71	Ocorreu um erro relacionado ao encadeamento.
72	Ocorreu um erro durante a criação de subtarefas.
73	Ocorreu um erro enquanto um encadeamento aguardava para sair.
74	Ocorreu um erro de E/S.
75	Ocorreu um erro ao carregar o CMS.
76	Ocorreu um erro relacionado ao hardware de criptografia.
77	A rotina de inicialização da biblioteca não foi chamada com êxito.

código de erro	mensagem de erro
78	A tabela do identificador do banco de dados interno está danificado.
79	Ocorreu um erro de alocação de memória.
80	Uma opção não reconhecida foi localizada.
81	Ocorreu um erro ao obter informações de tempo.
82	Ocorreu um erro de criação de exclusão mútua.
83	Ocorreu um erro ao abrir o catálogo de mensagens.
84	Ocorreu um erro ao abrir o catálogo de mensagens de erro
85	Um nome de campo nulo foi localizado.
86	Ocorreu um erro durante a abertura de arquivos, verifique a existência do arquivo e as permissões.
87	Ocorreu um erro ao abrir arquivos para leitura.
88	Ocorreu um erro ao abrir arquivos para gravação.
89	Não existe esse arquivo.
90	O arquivo não pode ser aberto devido a sua definição de permissão.
91	Ocorreu um erro ao gravar dados em arquivos.
92	Ocorreu um erro ao excluir arquivos.
93	Foram encontrados dados codificados Base64 inválidos.
94	Foi encontrado um tipo de mensagem Base64 inválida.
95	Ocorreu um erro ao codificar dados com a regra de codificação Base64.
96	Ocorreu um erro ao decodificar dados codificados pelo Base64.
97	Ocorreu um erro durante a obtenção de uma marcação de nome exclusivo.
98	O campo de nome comum necessário está vazio.
99	O campo requerido de nome do país ou região está vazio.
100	Uma manipulação de banco de dados inválida foi localizada.
101	O banco de dados de chave não existe.
102	O banco de dados do par de chaves do pedido não existe.
103	O arquivo de senha não existe.
104	A nova senha é idêntica à antiga.

código de erro	mensagem de erro
105	Nenhuma chave foi encontrada no banco de dados chave.
106	Nenhuma chave de pedido foi encontrada.
107	Nenhuma CA confiável foi localizada.
108	Nenhuma chave de pedido foi encontrada para o certificado.
109	Não há nenhuma chave privada no banco de dados de chaves.
110	Não há chave padrão no banco de dados chave
111	Não há nenhuma chave privativa no registro de chaves.
112	Não há certificado no registro de chave.
113	Não há entrada de CRL.
114	Foi encontrado um nome de arquivo de banco de dados inválido.
115	Foi encontrado um tipo de chave privativa não reconhecida.
116	Foi encontrada uma entrada de nome distinto inválida.
117	Não foi encontrada nenhuma entrada de chave que tenha o rótulo de chave especificada.
118	A lista de etiquetas de chaves foi danificada.
119	Os dados de entrada não são dados PKCS12 válidos.
120	A senha é inválida ou os dados do PKCS12 foram corrompidos ou criados com uma versão mais recente do PKCS12
121	Um tipo de exportação de chave não reconhecido foi localizado.
122	Foi encontrado um algoritmo de criptografia com base na senha não suportado.
123	Ocorreu um erro ao converter o arquivo do conjunto de chaves em um banco de dados de chaves CMS.
124	Ocorreu um erro ao converter o banco de dados de chaves CMS em um arquivo do conjunto de chaves.
125	Ocorreu um erro durante a criação de um certificado para o pedido de certificado.
126	Impossível construir uma cadeia completa de emissores.
127	Dados WEBDB inválidos foram localizados.

código de erro	mensagem de erro
128	Não há dados para serem gravados no arquivo do conjunto de chaves.
129	O número de dias que você inseriu estende além do período de validade permitido.
130	A senha é muito pequena, ela deve consitir em, pelo menos, {0} caracteres.
131	A senha deve conter, pelo menos, um dígito numérico.
132	Todos os caracteres na senha são caracteres alfanuméricos ou numéricos.
133	Foi especificado um algoritmo de assinatura não reconhecido e não suportado.
134	Um tipo de banco de dados inválido foi encontrado.
135	O banco de dados de chaves secundário especificado está em uso por outro dispositivo PKCS#11.
136	Nenhum banco de dados de chaves secundário foi especificado.
137	O rótulo não existe no dispositivo PKCS#11.
138	Senha necessária para acessar o dispositivo PKCS#11.
139	Senha não necessária para acessar o dispositivo PKCS#11.
140	Impossível carregar a biblioteca criptográfica.
141	PKCS#11 não é suportado para esta operação.
142	Uma operação em um dispositivo PKCS#11 falhou.
143	O usuário LDAP não é um usuário válido. (LDAP não é suportado por este programa)
144	O usuário LDAP não é um usuário válido. (LDAP não é suportado por este programa)
145	A consulta de LDAP falhou. (LDAP não é suportado por este programa)
146	Uma cadeia de certificados inválida foi localizada.
147	O certificado raiz não é confiável.
148	Um certificado revogado foi encontrado.
149	Uma função de objeto criptográfico falhou.
150	Não há uma origem de dados da lista de revogação de certificado disponível.
151	Não há um token criptográfico disponível.
152	O modo FIPS não está disponível.

código de erro	mensagem de erro
153	Há um conflito com as configurações do modo FIPS.
154	A senha inserida não atende à força mínima necessária.
200	Houve uma falha durante a inicialização do programa.
201	A tokenização dos argumentos passados para o Programa runmqakm falhou.
202	O objeto identificado no comando não é um objeto reconhecido.
203	A ação passada não é uma ação -keydb conhecida.
204	A ação passada não é uma ação -cert conhecida.
205	A ação passada não é uma ação -certreq conhecida.
206	Há uma tag ausente para o comando solicitado.
207	O valor passado com a tag -version não é um valor reconhecido.
208	O valor passado com a tag -size não é um valor reconhecido.
209	O valor passado com a tag -dn não está no formato correto.
210	O valor passado com a tag -format não é um valor reconhecido.
211	Houve um erro associado à abertura do arquivo.
212	PKCS12 não é suportado neste estágio.
213	O token criptográfico para o qual você está tentando alterar a senha não é protegido por senha.
214	PKCS12 não é suportado neste estágio.
215	A senha inserida não atende à força mínima necessária.
216	O modo FIPS não está disponível.
217	O número de dias que você inseriu como a data de expiração está fora do intervalo permitido.
218	A força da senha falhou quanto aos requisitos mínimos.
219	Nenhum certificado padrão foi localizado no banco de dados de chaves solicitado.
220	Um status de confiança inválido foi encontrado.
221	Um algoritmo de assinatura não suportado foi encontrado. Neste estágio, apenas MD5 e SHA1 são suportados.

código de erro	mensagem de erro
222	PCKS11 não suportado para essa operação específica.
223	A ação passada não é uma ação -random conhecida.
224	Um comprimento menor que zero não é permitido.
225	Ao usar a tag -strong, a senha de comprimento mínimo é 14 caracteres.
226	Ao usar a tag -strong, a senha de comprimento máximo será 300 caracteres.
227	O algoritmo MD5 não é suportado quando no modo FIPS.
228	A tag de site não é suportada para o comando -cert -list. Esse atributo é incluído para compatibilidade com versões anteriores e potencial aprimoramento futuro.
229	O valor associado à tag -ca não é reconhecido. O valor deve ser 'true' ou 'false'.
230	O valor passado com a tag -type não é válido.
231	O valor passado com a tag -expire está abaixo do intervalo permitido.
232	O algoritmo de criptografia usado ou solicitado não é suportado.
233	O destino já existe.

Proteção de detalhes de autenticação do banco de dados

Se você estiver usando a autenticação de nome de usuário e senha para se conectar ao gerenciador do banco de dados, poderá armazená-los no armazenamento de credenciais do MQ XA para evitar armazenar a senha em texto sem formatação no arquivo `qm.ini`.

Atualize XAOpenString para o gerenciador de recursos

Para usar o armazenamento de credenciais, deve-se modificar o XAOpenString no arquivo `qm.ini`. A sequência é usada para se conectar ao gerenciador do banco de dados. É possível especificar campos substituíveis para identificar onde o nome de usuário e a senha são substituídos dentro da sequência XAOpenString.

- O campo +USER+ é substituído pelo valor do nome de usuário armazenado no armazenamento de XACredentials.
- O campo +PASSWORD+ é substituído pelo valor de senha armazenado no armazenamento de XACredentials..

Os exemplos a seguir mostram como modificar um XAOpenString para usar o arquivo de credenciais para se conectar ao banco de dados.

Conectando-se a um banco de dados Db2

```
XAResourceManager:
  Name=mydb2
  SwitchFile=db2swit
```

```
  XAOpenString=db=mydbname,uid=+USER+,pwd=+PASSWORD+,toc=t
  ThreadOfControl=THREAD
```

Conectando-se a um banco de dados Oracle

```
XAResourceManager:
  Name=myoracle
  SwitchFile=oraswit
  XAOpenString=Oracle_XA+Acc=P/+USER+/+PASSWORD++SesTm=35
            +LogDir=/tmp+threads=true
  ThreadOfControl=THREAD
```

Trabalhe com as credenciais para o banco de dados para o armazenamento das credenciais de MQ XA

Depois de atualizar o arquivo `qm.ini` com as sequências de credenciais substituíveis, você deve incluir o nome do usuário e a senha no armazenamento de credenciais do MQ usando o comando **setmqxacred** . Também é possível usar **setmqxacred** para modificar as credenciais existentes, excluir credenciais ou listar as credenciais. Os exemplos a seguir fornecem alguns casos de uso típico:

Incluindo Credenciais

O comando a seguir salva com segurança o nome do usuário e a senha para o gerenciador de filas `QM1` para o recurso `mqdb2`.

```
setmqxacred -m QM1 -x mydb2 -u user1 -p Password2
```

Atualizando credenciais

Para atualizar o nome do usuário e a senha usados para conectar a um banco de dados, emita novamente o comando **setmqxacred** com o novo nome do usuário e a senha:

```
setmqxacred -m QM1 -x mydb2 -u user3 -p Password4
```

Deve-se reiniciar o gerenciador de filas para que as mudanças entrem em vigor.

Excluindo credenciais

O seguinte comando exclui as credenciais:

```
setmqxacred -m QM1 -x mydb2 -d
```

Listando as credenciais

O seguinte comando lista as credenciais:

```
setmqxacred -m QM1 -l
```

Referências relacionadas

setmqxacred

Segurança do Managed File Transfer

Diretamente após a instalação e sem nenhuma modificação, o Managed File Transfer terá um nível de segurança que pode ser apropriado para propósitos de teste ou avaliação em um ambiente protegido. Entretanto, em um ambiente de produção, deve-se considerar o controle apropriado de quem pode iniciar as operações de transferência de arquivos, quem pode ler e gravar os arquivos que estão sendo transferidos e como proteger a integridade dos arquivos.

Tarefas relacionadas

Restringindo autoridades grupo para recursos específicos do MFT

Gerenciando autoridades para recursos específicos do MFT

“Usando o Advanced Message Security com o Managed File Transfer” na página 611
Este cenário explica como configurar o Advanced Message Security para fornecer privacidade de mensagem para dados que estão sendo enviados por meio de um Managed File Transfer.

Referências relacionadas

Autoridades para MFT para acessar sistemas de arquivos

Propriedade commandPath do MFT

Autoridade para publicar mensagens de log e de status dos agentes MFT

Autenticação de conexão do MFT e IBM MQ

A autenticação de conexão permite que um gerenciador de filas seja configurado para autenticar aplicativos usando um ID do usuário e uma senha fornecidos. Se o gerenciador de filas associado tiver a segurança ativada e requerer detalhes da credencial (ID do usuário e senha), o recurso de autenticação de conexão deverá ser ativado antes que uma conexão bem-sucedida com um gerenciador de filas possa ser feita. A autenticação de conexão pode ser executada no modo de compatibilidade ou no modo de autenticação MQCSP.

Métodos de Fornecer Detalhes da Credencial

Muitos comandos Managed File Transfer suportam os seguintes métodos de fornecimento de detalhes de credencial:

Detalhes fornecidos por argumentos da linha de comandos.
Os detalhes da credencial podem ser especificados usando os parâmetros **-mquserid** e **-mqpassword** . Se o **-mqpassword** não for fornecido, então, o usuário será solicitado a fornecer a senha em que a entrada não é exibida.

Detalhes fornecidos por meio de um arquivo de credenciais: `MQMFTCredentials.xml`.
Os detalhes da credencial podem ser predefinidos em um arquivo `MQMFTCredentials.xml` como texto não criptografado ou texto ofuscado.

Para obter informações sobre como configurar um arquivo MQMFTCredentials.xml em IBM MQ for Multiplatforms consulte “Configurando MQMFTCredentials.xml em multiplataformas” na página 549.

Para obter informações sobre como configurar um arquivo MQMFTCredentials.xml em IBM MQ for z/OS consulte “Configurando o MQMFTCredentials.xml no z/OS” na página 550.

Precedência

A precedência de determinar os detalhes de credencial é:

1. Argumento da linha de comandos.
2. Índice do `MQMFTCredentials.xml` por Gerenciador de Filas associado e usuário executando o comando.
3. Índice do `MQMFTCredentials.xml` por Gerenciador de Filas associado.
4. Modo de compatibilidade com versões anteriores padrão em que nenhum detalhe de credencial é fornecido para permitir compatibilidade com liberações anteriores do IBM MQou IBM WebSphere MQ

Notas:

- Os comandos **`fteStartAgent`** e **`fteStartLogger`** não suportam o argumento de linha de comandos **-mquserid**, ou **-mqpassword**e os detalhes de credencial só podem ser especificados com o arquivo `MQMFTCredentials.xml`.
- z/OS

  No z/OS, a senha deve ser maiúscula, mesmo se a senha do usuário tiver letras minúsculas. Por exemplo, se a senha do usuário foi "senha", terá que ser inserida como "SENHA".

Referências relacionadas

Qual Comando do MFT se Conecta a qual Gerenciador de Filas

Configurando `MQMFTCredentials.xml` em multiplataformas

Se o Managed File Transfer (MFT) for configurado com a segurança ativada, a autenticação de conexão requererá todos os comandos do MFT que se conectam a um gerenciador de filas para fornecer credenciais de ID do usuário e senha Da mesma forma, os criadores de logs do MFT podem ser necessários para especificar um ID do usuário e senha ao se conectar a um banco de dados. Essas informações de credenciais podem ser armazenadas no arquivo de credenciais MFT .

Sobre esta tarefa

Os elementos no arquivo `MQMFTCredentials.xml` devem estar em conformidade com o esquema `MQMFTCredentials.xsd`. Para obter informações sobre o formato de `MQMFTCredentials.xml`, consulte Formato de arquivo de credenciais do MFT.

É possível localizar um arquivo de credenciais de amostra no diretório `MQ_INSTALLATION_PATH/mqft/samples/credentials` .

Você pode ter um MFT arquivo de credenciais para o gerenciador de filas de coordenação, um para o gerenciador de filas de comando, um para cada agente e um para cada logger. Como alternativa, é possível ter um arquivo que seja usado por tudo em sua topologia

O local padrão do arquivo de credenciais MFT é o seguinte:

Linux UNIX **UNIX and Linux**

`$HOME`

Windows **Windows**

`%USERPROFILE%` ou `%HOMEDRIVE%%HOMEPATH%`

Se o arquivo de credenciais estiver armazenado em um local diferente, será possível usar as propriedades a seguir para especificar onde os comandos devem procurá-lo:

Tabela 91. : Propriedades que definem o local do arquivo MQMFTCredentials.xml para vários comandos.

Tipo de comando	Arquivo de Propriedades	Nome da Propriedade
Comando que se conecta ao gerenciador de filas de coordenação	coordination.properties	coordinationQMgrAuthenticationCredentialsFile
Comando que se conecta ao gerenciador de fila de comandos	connection.properties	connectionQMgrAuthenticationCredentialsFile
Comando que se conecta a um processo do agente	agent.properties	agentQMgrAuthenticationCredentialsFile
Comando que se conecta a um processo do criador de logs	logger.properties	loggerQMgrAuthenticationCredentialsFile

Tabela 92. : Propriedades que definem o local do arquivo MQMFTCredentials.xml para agentes e processos do criador de logs..

Tipo de comando	Arquivo de Propriedades	Nome da Propriedade
Agentes do MFT	agent.properties	agentQMgrAuthenticationCredentialsFile

Tabela 92. : Propriedades que definem o local do arquivo MQMFTCredentials.xml para agentes e processos do criador de logs.. (continuação)		
Tipo de comando	**Arquivo de Propriedades**	**Nome da Propriedade**
MFT criadores de logs	logger.properties	loggerQMgrAuthenticationCredentialsFile

Para obter detalhes sobre quais comandos e processos se conectam a qual gerenciador de filas, consulte Quais MFT Comandos e Processos se Conectam a Qual Gerenciador de Filas

Como o arquivo de credenciais contém informações de ID do usuário e senha, ele requer permissões especiais para evitar o acesso não autorizado a ele:

Linux UNIX **UNIX and Linux**

```
chown <agent owner userid>
chmod 600
```

Windows **Windows**

Assegure-se de que a herança não esteja ativada e, em seguida, remova todos os IDs do usuário, exceto aqueles que estão executando o agente ou criador de logs que estarão usando o arquivo de credenciais.

Os detalhes da credencial usados para se conectar a um gerenciador de filas de coordenação do MFT , no plug-in do IBM MQ Explorer Managed File Transfer , dependem do tipo de configuração:

Global (configuração no disco local)

Uma configuração global usa o arquivo de credenciais especificado nas propriedades de coordenação e de comando.

Local (definido em IBM MQ Explorer):

Uma configuração local usa as propriedades dos detalhes de conexão do gerenciador de filas associado no IBM MQ Explorer.

Tarefas relacionadas

“Ativando a autenticação de conexão para o MFT” na página 552

A autenticação de conexão do Plug-in do IBM MQ Explorer MFT conectando-se a um gerenciador de filas de coordenação ou a um gerenciador de filas de comando e a autenticação de conexão para um agente do Managed File Transfer conectando-se a um gerenciador de filas de coordenação ou a um gerenciador de filas de comando podem ser executadas no modo de compatibilidade ou no modo de autenticação do MQCSP.

Referências relacionadas

Formato de arquivo de credenciais do MFT

`fteObfuscate`: criptografar dados sensíveis

z/OS Configurando o `MQMFTCredentials.xml` no z/OS

Se o Managed File Transfer (MFT) for configurado com a segurança ativada, a autenticação de conexão exigirá todos os agentes do MFT e comandos que se conectam a um gerenciador de fila para fornecer credenciais de ID do usuário e senha

Da mesma forma, os criadores de logs do MFT podem ser necessários para especificar um ID do usuário e senha ao se conectar a um banco de dados.

Essas informações de credenciais podem ser armazenadas no arquivo de credenciais MFT . Observe que os arquivos de credenciais são opcionais, no entanto, é mais fácil definir o arquivo ou os arquivos necessários antes de customizar o ambiente.

Além disso, se você tiver arquivos de credenciais, você receberá menos mensagens de aviso. As mensagens de aviso informará que o MFT considera que a segurança do gerenciador de filas está desligado e, portanto, você não está fornecendo detalhes de autenticação.

É possível localizar um arquivo de credenciais de amostra no diretório `MQ_INSTALLATION_PATH/mqft/samples/credentials`.

Aqui está um exemplo de um arquivo `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>
```

Quando uma tarefa com o ID precisa para se conectar ao gerenciador de filas ADMIN MQPH, ele transmite o ID do usuário *JOHNDOEH* e utiliza a senha *cXXXX*.

Se o job for executado por qualquer outro ID de usuário e conecta-se MQPH, essa tarefa ID do usuário do *NONEH* e senha *yXXXX*.

O local padrão para o arquivo `MQMFTCredentials.xml` é o diretório inicial do usuário em z/OS UNIX System Services (USS) Também é possível armazenar o arquivo em um local diferente no USS ou em um membro em um conjunto de dados particionados.

Se o arquivo de credenciais estiver armazenado em um local diferente, será possível usar as propriedades a seguir para especificar onde os comandos devem procurá-lo:

Tabela 93. : Propriedades que definem o local do arquivo MQMFTCredentials.xml para vários comandos.

Tipo de comando	**Arquivo de Propriedades**	**Nome da Propriedade**
Comando que se conecta ao gerenciador de filas de coordenação	coordination.properties	coordinationQMgrAuthenticationCredentialsFile
Comando que se conecta ao gerenciador de fila de comandos	connection.properties	connectionQMgrAuthenticationCredentialsFile
Comando que se conecta a um processo do agente	agent.properties	agentQMgrAuthenticationCredentialsFile
Comando que se conecta a um processo do criador de logs	logger.properties	loggerQMgrAuthenticationCredentialsFile

Tabela 94. : Propriedades que definem o local do arquivo MQMFTCredentials.xml para agentes e processos do criador de logs..

Tipo de comando	**Arquivo de Propriedades**	**Nome da Propriedade**
Agentes do MFT	agent.properties	agentQMgrAuthenticationCredentialsFile
MFT criadores de logs	logger.properties	loggerQMgrAuthenticationCredentialsFile

Para obter detalhes sobre quais comandos e processos se conectam a qual gerenciador de filas, consulte Quais MFT Comandos e Processos se Conectam a Qual Gerenciador de Filas

Para criar o arquivo de credenciais dentro de um conjunto de dados particionados, execute as etapas a seguir:

- Crie um PDSE com o formato VB e comprimento de registro lógico (Lrecl) 200.
- Crie um membro dentro do conjunto de dados, tome nota do conjunto de dados e membro e inclua o seguinte código para o membro:

```
<?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>
```

É possível proteger o arquivo de credenciais usando um produto de segurança, por exemplo, RACF, mas os IDs do usuário executando os comandos Managed File Transfer e administrando os processos do agente e do criador de logs precisam de acesso de leitura a esse arquivo.

é possível ocultar as informações nesse arquivo utilizando a JCL no membro BFGCROBS. Isso o leva o arquivo e criptografa a IBM MQ do ID de usuário e senha. Por exemplo membro BFGCROBS segue a linha

```
<tns:qmgr name="MQPI" user="JOHNDOE2" mqUserId="JOHNDOE1" mqPassword="yXXXX" />
```

e cria

```
<tns:qmgr mqPasswordCipher="e977c61e9b9c363c" mqUserIdCipher="c394c5887867157c"
name="MQPI" user="JOHNDOE2"/>
```

Se desejar manter o ID do usuário para IBM MQ de mapeamento de ID de usuário, você pode incluir comentários no arquivo. Por exemplo:

```
<!--      name="MQPI" user="ADMIN"    mqUserId="JOHNDOE1 -->
```

Esses comentários são mudados pelo processo obscurecimento.

Observe que o conteúdo está obscurecida, não altamente criptografada. É necessário limitar quais IDs do usuário possuem acesso ao arquivo.

Tarefas relacionadas

“Configurando MQMFTCredentials.xml em multiplataformas” na página 549
Se o Managed File Transfer (MFT) for configurado com a segurança ativada, a autenticação de conexão requererá todos os comandos do MFT que se conectam a um gerenciador de filas para fornecer credenciais de ID do usuário e senha Da mesma forma, os criadores de logs do MFT podem ser necessários para especificar um ID do usuário e senha ao se conectar a um banco de dados. Essas informações de credenciais podem ser armazenadas no arquivo de credenciais MFT .

Ativando a autenticação de conexão para o MFT

A autenticação de conexão do Plug-in do IBM MQ Explorer MFT conectando-se a um gerenciador de filas de coordenação ou a um gerenciador de filas de comando e a autenticação de conexão para um agente do Managed File Transfer conectando-se a um gerenciador de filas de coordenação ou a um gerenciador de filas de comando podem ser executadas no modo de compatibilidade ou no modo de autenticação do MQCSP.

Sobre esta tarefa

Antes do IBM MQ 9.1.1, o modo de compatibilidade é a configuração padrão para a autenticação de conexão. No entanto, é possível desativar o modo de compatibilidade padrão e ativar o modo de autenticação do MQCSP.

V 9.1.1 A partir da IBM MQ 9.1.1, o modo de autenticação MQCSP é o padrão.

Para a autenticação de conexão para o plug-in do IBM MQ Explorer Managed File Transfer ou para os agentes do Managed File Transfer que se conectam a um gerenciador de filas usando o transporte CLIENT, as senhas com mais de 12 caracteres são suportadas somente para o modo de autenticação do MQCSP. Se você especificar uma senha com mais de 12 caracteres de comprimento ao autorizar o uso do modo de compatibilidade, ocorrerá um erro e o agente não será autenticado com o gerenciador de filas. Veja a mensagem BFGAG0187E em Mensagens de diagnóstico: BFGAG0001 - BFGAG9999.

Procedimento

- Para selecionar o modo de autenticação de conexão para um gerenciador de filas de coordenação ou para um gerenciador de filas de comandos no IBM MQ Explorer, conclua as etapas a seguir:
  a) Selecione o gerenciador de filas ao qual você deseja se conectar.
  b) Clique com o botão direito do mouse e selecione **Detalhes da Conexão-> Propriedades** no menu pop-up.
  c) Clique na guia **ID do usuário**.
  d) Certifique-se de que a caixa de seleção para o modo de autenticação de conexão que você deseja usar esteja selecionada:
     - V 9.1.0 No IBM MQ 9.1.0, por padrão, a caixa de seleção **Modo de compatibilidade de identificação de usuário** está desmarcada. Isso significa que se a caixa de seleção **Ativar identificação de usuário** for selecionada, o IBM MQ Explorer usará a autenticação do MQCSP ao conectar-se ao gerenciador de filas. Se o IBM MQ Explorer precisar se conectar ao gerenciador de filas usando o modo de compatibilidade ao invés da autenticação do MQCSP, você deverá assegure-se de que as duas caixas de seleção **Ativar identificação de usuário** e **Modo de compatibilidade de identificação de usuário** estejam selecionadas.
     - Antes do IBM MQ 9.1.0, por padrão, a caixa de seleção **Modo de compatibilidade de identificação do usuário** estava selecionada. Isso significa que, se a caixa de seleção **Ativar identificação de usuário** for selecionada, o IBM MQ Explorer usará o modo de compatibilidade ao conectar-se ao gerenciador de filas. Se o IBM MQ Explorer precisar se conectar ao gerenciador de filas usando a autenticação do MQCSP, você deverá assegurar-se de que a caixa de seleção **Ativar identificação de usuário** esteja selecionada e que a caixa de seleção **Modo de compatibilidade de identificação do usuário** não esteja selecionada.
- Para ativar ou desativar o modo de autenticação do MQCSP para um agente do Managed File Transfer usando o arquivo `MQMFTCredentials.xml`, inclua o parâmetro **useMQCSPAuthentication** no arquivo `MQMFTCredentials.xml` para o usuário relevante.

  O parâmetro **useMQCSPAuthentication** tem os valores a seguir:

  true
  O modo de autenticação do MQCSP é usado para autenticar o usuário com o gerenciador de filas.

  V 9.1.1 No IBM MQ 9.1.1, `true` é o valor padrão. Se o parâmetro **useMQCSPAuthentication** não for especificado, ele será, por padrão, configurado como `true` e o modo de autenticação do MQCSP será usado para autenticar o usuário com o gerenciador de filas.

  false
  O modo de compatibilidade é usado para autenticar o usuário com o gerenciador de filas.

  Antes do IBM MQ 9.1.1, caso o parâmetro **useMQCSPAuthentication** não fosse especificado, ele era, por padrão, configurado como `false` e o modo de compatibilidade era usado para autenticar o usuário com o gerenciador de filas.

  O exemplo a seguir mostra como configurar o parâmetro **useMQCSPAuthentication** no arquivo `MQMFTCredentials.xml`:

```
<tns:qmgr name="CoordQueueMgr" user="ernest" mqUserId="ernest"
    mqPassword="AveryL0ngPassw0rd2135" useMQCSPAuthentication="true"/>
```

Conceitos relacionados

"Proteção de senha do MQCSP" na página 30
A partir do IBM MQ 8.0, é possível enviar as senhas que estão incluídas na estrutura MQCSP protegida, usando a funcionalidade do IBM MQ, ou criptografada, usando a criptografia TLS.

Referências relacionadas

"Autenticação de conexão do MFT e IBM MQ" na página 548
A autenticação de conexão permite que um gerenciador de filas seja configurado para autenticar aplicativos usando um ID do usuário e uma senha fornecidos. Se o gerenciador de filas associado tiver a segurança ativada e requerer detalhes da credencial (ID do usuário e senha), o recurso de autenticação de conexão deverá ser ativado antes que uma conexão bem-sucedida com um gerenciador de filas possa ser feita. A autenticação de conexão pode ser executada no modo de compatibilidade ou no modo de autenticação MQCSP.

Formato de arquivo de credenciais do MFT

Ambientes de simulação do MFT

É possível restringir a área do sistema de arquivos que o agente pode acessar como parte de uma transferência. A área à qual o agente está restrito é chamada de ambiente de simulação. É possível aplicar restrições ao agente ou ao usuário que solicitar uma transferência.

Os ambientes de simulação não são suportados quando o agente é um agente de ponte de protocolo ou um agente de ponte Connect:Direct. Não é possível usar a criação de ambiente de simulação de agente para agentes que precisam transferir para ou a partir de filas do IBM MQ.

Referências relacionadas

"Trabalhando com ambientes de simulação do agente MFT" na página 554
Para incluir um nível de segurança adicional no Managed File Transfer, é possível restringir a área de um sistema de arquivos que um agente pode acessar.

"Trabalhando com ambientes de simulação do usuário do MFT" na página 556
É possível restringir a área do sistema de arquivos à qual os arquivos podem ser transferidos para/de com base no nome de usuário MQMD do usuário que solicita a transferência.

Trabalhando com ambientes de simulação do agente MFT

Para incluir um nível de segurança adicional no Managed File Transfer, é possível restringir a área de um sistema de arquivos que um agente pode acessar.

Não é possível usar a criação de ambiente de simulação de agente para os agentes que transferem para ou a partir de filas do IBM MQ. A restrição de acesso às filas do IBM MQ com a criação de ambiente de simulação pode ser implementada em vez de usar a criação de ambiente de simulação do usuário, que é a solução recomendada para quaisquer requisitos de criação de ambiente de simulação. Para obter mais informações sobre a criação de ambiente de simulação do usuário, consulte "Trabalhando com ambientes de simulação do usuário do MFT" na página 556

Para ativar a criação de ambiente de simulação do agente, inclua a propriedade a seguir no arquivo `agent.properties` para o agente que deseja restringir:

```
sandboxRoot=[!]restricted_directory_nameseparator...separator[!]restricted_directory_name
```

em que:

- *`restricted_directory_name`* é um caminho de diretório a ser permitido ou negado.
- `!` é opcional e especifica que o valor a seguir para *`restricted_directory_name`* é negado (excluído). Se `!` não for especificado, *`restricted_directory_name`* será um caminho permitido (incluído).
- *`separator`* é o separador específico da plataforma.

Por exemplo, se você deseja restringir o acesso que AGENT1 tem apenas ao diretório `/tmp`, mas não permitir que o subdiretório `private` seja acessado, configure a propriedade da seguinte forma no arquivo `agent.properties` pertencente a AGENT1: `sandboxRoot=/tmp:!/tmp/private`.

A propriedade sandboxRoot é descrita em Propriedades Avançadas do Agente

Ambas as criações de ambiente de simulação, do agente e do usuário, não são suportadas em agentes de ponte de protocolo ou em agentes de ponte do Connect:Direct.

Trabalhando em um ambiente de simulação nas plataformas UNIX, Linux e Windows

ULW Nas plataformas UNIX, Linux e Windows, a criação de ambiente de simulação restringe de quais diretórios um Managed File Transfer Agent pode ler e nos quais pode gravar. Quando a criação de ambiente de simulação está ativada, o Managed File Transfer Agent pode ler e gravar nos diretórios especificados, conforme o permitido, e nos subdiretórios contidos nos diretórios especificados, a menos que os subdiretórios estejam especificados como negados no sandboxRoot. A criação de ambiente de simulação do Managed File Transfer não tem precedência sobre a segurança do sistema operacional. O usuário que iniciou o Managed File Transfer Agent deve ter o acesso apropriado no nível do sistema operacional a qualquer diretório para poder ler do diretório ou gravar nele. Um link simbólico para um diretório não será seguido se o diretório vinculado estiver fora dos diretórios sandboxRoot especificados (e subdiretórios).

Trabalhando em um Ambiente de Simulação no z/OS

z/OS No z/OS, a criação de ambiente de simulação restringe de quais qualificadores de nome do conjunto de dados o Managed File Transfer Agent pode ler e nos quais pode gravar. O usuário que iniciou o Managed File Transfer Agent deve ter as autoridades corretas do sistema operacional para quaisquer conjuntos de dados envolvidos. Se você colocar um valor do qualificador de nome do conjunto de dados sandboxRoot entre aspas duplas, o valor seguirá a convenção normal do z/OS e será tratado como completo. Se você omitir as aspas duplas, sandboxRoot será prefixado com o ID do usuário atual. Por exemplo, se você configurar a propriedade sandboxRoot para o seguinte: `sandboxRoot=//test`, o agente poderá acessar os seguintes conjuntos de dados (em notação z/OS padrão) `//`*`username`*`.test.**` No tempo de execução, se os níveis iniciais do nome do conjunto de dados totalmente resolvido não corresponderem a sandboxRoot, a solicitação de transferência será rejeitada.

Trabalhando em um Ambiente de Simulação em Sistemas IBM i

IBM i Para arquivos no sistema de arquivos integrado em sistemas IBM i, a criação de ambiente de simulação restringe de quais diretórios um Managed File Transfer Agent pode ler e nos quais pode gravar. Quando a criação de ambiente de simulação está ativada, o Managed File Transfer Agent pode ler e gravar nos diretórios especificados, conforme o permitido, e nos subdiretórios contidos nos diretórios especificados, a menos que os subdiretórios estejam especificados como negados no sandboxRoot. A criação de ambiente de simulação do Managed File Transfer não tem precedência sobre a segurança do sistema operacional. O usuário que iniciou o Managed File Transfer Agent deve ter o acesso apropriado no nível do sistema operacional a qualquer diretório para poder ler do diretório ou gravar nele. Um link simbólico para um diretório não será seguido se o diretório vinculado estiver fora dos diretórios sandboxRoot especificados (e subdiretórios).

Referências relacionadas

“Verificações adicionais para transferências curingas” na página 559
Se um agente tiver sido configurado com um ambiente de simulação do usuário ou do agente para restringir os locais para os quais e dos quais o agente pode transferir arquivos, é possível especificar se verificações adicionais devem ser feitas em transferências curingas para esse agente.

“Trabalhando com ambientes de simulação do agente MFT” na página 554
Para incluir um nível de segurança adicional no Managed File Transfer, é possível restringir a área de um sistema de arquivos que um agente pode acessar.

O arquivo MFT `agent.properties`

Trabalhando com ambientes de simulação do usuário do MFT

É possível restringir a área do sistema de arquivos à qual os arquivos podem ser transferidos para/de com base no nome de usuário MQMD do usuário que solicita a transferência.

Os ambientes de simulação não serão suportados quando o agente for um agente de ponte de protocolo ou um agente de ponte Connect:Direct.

Para ativar a criação de ambiente de simulação do agente, inclua a propriedade a seguir no arquivo `agent.properties` para o agente que deseja restringir:

```
userSandboxes=true
```

Quando esta propriedade está presente e configurada como true, o agente usa as informações no arquivo *MQ_DATA_PATH*`/mqft/config/`*coordination_qmgr_name*`/agents/`*agent_name*`/UserSandboxes.xml` para determinar quais partes do sistema de arquivos podem ser acessadas pelo usuário que solicita a transferência.

O XML `UserSandboxes.xml` é composto de um elemento `<agent>` que contém zero ou mais elementos `<sandbox>`. Esses elementos descrevem quais regras são aplicadas a quais usuários. O atributo `user` do elemento `<sandbox>` é um padrão usado para correspondência com o usuário MQMD da solicitação.

O arquivo `UserSandboxes.xml` é recarregado periodicamente pelo agente e quaisquer mudanças válidas no arquivo afetarão o comportamento do agente. O intervalo de recarregamento padrão é de 30 segundos. Este intervalo pode ser alterado especificando a propriedade do agente xmlConfigReloadInterval no arquivo `agent.properties`.

Se você especificar o atributo ou valor `userPattern="regex"`, o atributo `user` será interpretado como uma expressão regular Java. Para obter mais informações, consulte Expressões regulares usadas pelo MFT.

Se você não especificar o atributo `userPattern="regex"` ou o valor, o atributo `user` será interpretado como um padrão com os seguintes caracteres curinga:

- asterisco (*), que representa zero ou mais caracteres
- ponto de interrogação (?), que representa exatamente um caractere

As correspondências são realizadas na ordem em que os elementos `<sandbox>` estão listados no arquivo. Apenas a primeira correspondência é usada, todas as possíveis correspondências seguintes no arquivo são ignoradas. Se nenhum dos elementos `<sandbox>` especificados no arquivo corresponder ao usuário MQMD associado à mensagem de solicitação de transferência, a transferência não poderá acessar o sistema de arquivos. Quando uma correspondência foi encontrada entre o nome de usuário MQMD e um atributo `user`, a correspondência identifica um conjunto de regras dentro de um elemento `<sandbox>` que são aplicadas na transferência. Este conjunto de regras é usado para determinar quais arquivos ou conjuntos de dados, pode ser lido ou gravado como parte da transferência.

Cada conjunto de regras pode especificar um elemento `<read>`, que identifica quais arquivos podem ser lidos, e um elemento `<write>` que identifica quais arquivos podem ser gravados. Se você omitir os elementos `<read>` ou `<write>` de um conjunto de regras, presume-se que o usuário associado a esse conjunto de regras não tenha permissão para realizar leituras ou gravações, conforme apropriado.

Nota: O elemento `<read>` deve estar antes do elemento `<write>` e o elemento `<include>` deve estar antes do elemento `<exclude>` no arquivo `UserSandboxes.xml`.

Cada elemento `<read>` ou `<write>` contém um ou mais padrões que são usados para determinar se um arquivo está no ambiente de simulação e pode ser transferido. Especifique esses padrões usando os elementos `<include>` e `<exclude>`. O atributo `name` do elemento `<include>` ou `<exclude>` especifica o padrão a ser correspondido. Um atributo `type` opcional especifica se o valor do nome é um padrão de arquivo ou de fila. Se o atributo `type` não for especificado, o agente tratará o padrão como um padrão de caminho de arquivo ou diretório. Por exemplo:

```
<tns:read>
    <tns:include name="/home/user/**"/>
```

```
    <tns:include name="USER.**" type="queue"/>
    <tns:exclude name="/home/user/private/**"/>
</tns:read>
```

Os padrões <include> e <exclude> name são usados pelo agente para determinar se os arquivos, conjuntos de dados ou filas podem ser lidos ou gravados. Uma operação é permitida se o caminho de arquivo canônico, conjunto de dados ou nome da fila corresponder a pelo menos um dos padrões incluídos e exatamente zero dos padrões excluídos. Os padrões especificados usando o atributo name dos elementos <include> e <exclude> usam os separadores de caminho e as convenções apropriadas para a plataforma na qual o agente está em execução Se você especificou caminhos de arquivo relativos, os caminhos serão resolvidos em relação à propriedade transferRoot do agente.

Quando você especificar uma restrição de fila, uma sintaxe de QUEUE@QUEUEMANAGER será suportada com as seguintes regras:

- Se o caractere (@) estiver ausente da entrada, o padrão será tratado como um nome da fila que pode ser acessado em qualquer gerenciador de filas. Por exemplo, se o padrão for name, ele será tratado da mesma forma que name@**.
- Se o caractere (@) for o primeiro caractere na entrada, o padrão será tratado como um nome do gerenciador de filas e todas as filas no gerenciador de filas poderão ser acessadas. Por exemplo, se o padrão for @name, ele será tratado da mesma forma que **@name.

Os seguintes caracteres curinga têm significado especial quando você os especifica como parte do atributo name dos elementos <include> e <exclude> :

*****
: Um único asterisco corresponde a zero ou mais caracteres em um nome de diretório ou em um qualificador de um nome do conjunto de dados ou nome da fila .

?
: Um ponto de interrogação corresponde exatamente a um caractere em um nome de diretório ou em um qualificador de um nome do conjunto de dados ou nome da fila .

******
: Dois caracteres de asterisco correspondem a zero ou mais nomes de diretórios ou zero ou mais qualificadores em um nome do conjunto de dados ou nome da fila. Além disso, os caminhos que terminam com um separador de caminhos possuem um "**" implícito incluído no final do caminho. Assim, /home/user/ é o mesmo que /home/user/**.

Por exemplo:

- O /**/test/** corresponde a qualquer arquivo que tenha um diretório test em seu caminho
- O /test/file? corresponde a qualquer arquivo dentro do diretório /test que começa com a sequência file seguida por qualquer caractere único
- O c:\test*.txt corresponde a qualquer arquivo dentro do diretório c:\test com uma extensão .txt
- O c:\test***.txt corresponde a qualquer arquivo dentro do diretório 'c:\test ou um de seus subdiretórios que tem uma extensão .txt
- z/OS O //'TEST.*.DATA' corresponde a qualquer conjunto de dados que tenha o primeiro qualificador de TEST, qualquer segundo qualificador e um terceiro qualificador de DATA.
- *@QM1 corresponde a qualquer fila no gerenciador de filas QM1 que possui um único qualificador...
- O TEST.*.QUEUE@QM1 corresponde a qualquer fila no Gerenciador de Filas QM1 que tem o primeiro qualificador de TEST, qualquer segundo qualificador e um terceiro qualificador de QUEUE.
- **@QM1 corresponde a qualquer fila no gerenciador de filas QM1.

Links Simbólicos

Deve-se resolver completamente qualquer link simbólico que você usa nos caminhos de arquivo no arquivo UserSandboxes.xml especificando os links de disco rígido nos elementos <include> e

<exclude>. Por exemplo, se você tiver um link simbólico no qual /var é mapeado para /SYSTEM/var, deverá especificar esse caminho como <tns:include name="/SYSTEM/var"/>, caso contrário, a transferência desejada falhará com um erro de segurança do ambiente de simulação do usuário.

exemplo

Este exemplo mostra como permitir que o usuário com o nome de usuário do MQMD guest transfira qualquer arquivo do diretório /home/user/public ou qualquer um de seus subdiretórios no sistema no qual o agente AGENT_JUPITER está em execução, incluindo o elemento <sandbox> a seguir no arquivo UserSandboxes.xml no diretório de configuração do 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>
```

exemplo

Este exemplo mostra como permitir que qualquer usuário com o nome do usuário do MQMD account seguido por um único dígito, por exemplo, account4, conclua as ações a seguir:

- Transfira qualquer arquivo do diretório /home/account ou de qualquer um de seus subdiretórios, excluindo o diretório /home/account/private no sistema em que o agente AGENT_SATURN está em execução
- Transfira qualquer arquivo para o diretório /home/account/output ou qualquer um de seus subdiretórios no sistema em que o agente AGENT_SATURN está em execução
- Leia mensagens de filas no Gerenciador de Filas locais começando com o prefixo ACCOUNT. a menos que ele comece com ACCOUNT.PRIVATE. (ou seja, tenha PRIVATE no segundo nível).
- Transfira dados nas filas começando com o prefixo ACCOUNT.OUTPUT. em qualquer gerenciador de filas.

Para permitir que um usuário com o nome do usuário MQMD account conclua essas ações, inclua o elemento <sandbox> a seguir no arquivo UserSandboxes.xml, no diretório de configuração do 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>
```

Referências relacionadas

“Verificações adicionais para transferências curingas” na página 559
Se um agente tiver sido configurado com um ambiente de simulação do usuário ou do agente para restringir os locais para os quais e dos quais o agente pode transferir arquivos, é possível especificar se verificações adicionais devem ser feitas em transferências curingas para esse agente.

O arquivo MFT `agent.properties`

Verificações adicionais para transferências curingas

Se um agente tiver sido configurado com um ambiente de simulação do usuário ou do agente para restringir os locais para os quais e dos quais o agente pode transferir arquivos, é possível especificar se verificações adicionais devem ser feitas em transferências curingas para esse agente.

Propriedade additionalWildcardSandboxChecking

Para ativar a verificação adicional para transferências curingas, inclua a propriedade a seguir no arquivo `agent.properties` para o agente que você deseja verificar.

```
additionalWildcardSandboxChecking=true
```

Quando essa propriedade estiver configurada como true e o agente fizer uma solicitação de transferência que tente ler um local que estiver fora do ambiente de simulação definido para correspondência de arquivos do curinga, a transferência falhará. Se houver múltiplas transferências dentro de uma solicitação de transferência e uma dessas solicitações falhar devido à tentativa de ler um local fora do ambiente de simulação, a transferência inteira falhará. Se a verificação falhar, a razão para a falha será fornecida em uma mensagem de erro.

Se a propriedade adiciontionalWildcardSandboxChecking for omitida do arquivo `agent.properties` de um agente ou for configurada como false, nenhuma verificação adicional será feita em transferências curingas para esse agente.

Mensagens de erro para verificação de curinga

As mensagens que são relatadas quando uma solicitação de transferência curinga é feita em um local fora de um local do ambiente de simulação configurado são conforme a seguir.

A mensagem a seguir ocorrerá quando um caminho de arquivo curinga em uma solicitação de transferência estiver localizado fora do ambiente de simulação restrito:

```
BFGSS0077E: A tentativa de ler o caminho de arquivo: path foi negada.
O caminho do arquivo foi localizado fora do ambiente restrito de simulação de transferência.
```

A mensagem a seguir ocorrerá quando uma transferência dentro de uma solicitação de múltiplas transferências contiver uma solicitação de transferência curinga no local em que o caminho estiver localizado fora do ambiente de simulação restrito:

```
BFGSS0078E: A tentativa de ler o caminho de arquivo: path foi ignorada porque outro item de
transferência na transferência gerenciada tentou ler fora do ambiente restrito de simulação de
transferência.
```

A mensagem a seguir ocorrerá quando um arquivo estiver localizado fora do ambiente de simulação restrito:

```
BFGSS0079E: A tentativa de ler o arquivo file path foi negada.
O arquivo está localizado fora da sandbox de transferência restrita.
```

A mensagem a seguir ocorrerá em uma solicitação de múltiplas transferências na qual outra solicitação de transferência curinga fez essa ser ignorada:

```
BFGSS0080E: A tentativa de ler o arquivo: file path foi ignorada pois outro item de
transferência na transferência gerenciada tentou ler fora do ambiente restrito de simulação de
transferência.
```

No caso de transferências de arquivos simples que não incluem curingas, a mensagem que é relatada quando a transferência envolve um arquivo que está localizado fora do ambiente de simulação é inalterada desde as liberações anteriores:

```
Falha com BFGIO0056E: A tentativa de ler o arquivo "FILE" foi negada.
O arquivo está localizado fora da sandbox de transferência restrita.
```

Referências relacionadas

“Trabalhando com ambientes de simulação do usuário do MFT” na página 556
É possível restringir a área do sistema de arquivos à qual os arquivos podem ser transferidos para/de com base no nome de usuário MQMD do usuário que solicita a transferência.

“Trabalhando com ambientes de simulação do agente MFT” na página 554
Para incluir um nível de segurança adicional no Managed File Transfer, é possível restringir a área de um sistema de arquivos que um agente pode acessar.

O arquivo MFT `agent.properties`

Configurando a criptografia SSL ou TLS para o MFT

É possível usar SSL ou TLS que podem ser usados com o IBM MQ Managed File Transfer para proteger a comunicação entre os agentes e seus gerenciadores de fila de agentes, comandos e os gerenciadores de filas aos quais eles estão se conectando e os vários gerenciadores de filas para conexões do gerenciador de filas dentro de sua topologia

Antes de começar

É possível usar a criptografia SSL ou TLS para criptografar mensagens que estão fluindo por uma topologia do IBM MQ Managed File Transfer . Isso inclui:

- Mensagens que são transmitidas entre um agente e seu gerenciador de filas do agente
- Mensagens para comandos e gerenciadores de filas aos quais eles estão se conectando.
- Mensagens internas que fluem entre os gerenciadores de fila do agente, gerenciadores de fila de comandos e gerenciador de fila de coordenação dentro da topologia.

Sobre esta tarefa

Para obter informações gerais sobre como usar SSL com o IBM MQ, veja “Trabalhando com SSL/TLS” na página 276. Nos termos do IBM MQ, o Managed File Transfer é um aplicativo de cliente Java padrão.

Siga estas etapas para usar o SSL com o Managed File Transfer:

Procedimento

1. Crie um arquivo truststore e, opcionalmente, um arquivo keystore (estes arquivos podem ser o mesmo arquivo). Se você não precisar de uma autenticação de cliente (ou seja, SSLCAUTH=OPTIONAL em canais), não será necessário fornecer um keystore. Você precisa de um armazenamento confiável apenas para autenticar o certificado do gerenciador de fila

   O algoritmo de chave usado para criar certificados para o armazenamento confiável e keystores deve ser RSA para trabalhar com o IBM MQ.
2. Configure o gerenciador de filas do IBM MQ para usar o SSL.

   Para obter informações sobre configuração de um gerenciador de filas para usar SSL usando o IBM MQ Explorer, por exemplo, veja Configurando SSL em gerenciadores de filas.
3. Salve os arquivos truststore e keystore (se houver um) em um local apropriado. Um local sugerido é o diretório *config_directory*/*coordination_qmgr*/agents/*agent_name*.
4. Configure as propriedades de SSL conforme necessário para cada gerenciador de filas ativado para SSL no arquivo de propriedades do Managed File Transfer apropriado. Cada conjunto de propriedades faz referência a um gerenciador de filas separado (agente, coordenação e comando), embora um gerenciador de fila possa executar duas ou mais funções.

Uma das propriedades **CipherSpec** ou **CipherSuite** é necessária, caso contrário, o cliente tentará se conectar sem o SSL. Ambas as propriedades, **CipherSpec** ou **CipherSuite**, são fornecidas devido às diferenças de terminologia entre o IBM MQ e o Java. O Managed File Transfer aceita uma das propriedades e faz a conversão necessária, para que você não precise configurar ambas as propriedades. Se você especificar as propriedades **CipherSpec** ou **CipherSuite**, **CipherSpec** terá precedência.

A propriedade **PeerName** é opcional. É possível configurar a propriedade como o Nome Distinto do gerenciador de filas ao qual quer se conectar. O Managed File Transfer rejeita conexões com um servidor SSL incorreto com um Nome Distinto que não corresponde.

Configure as propriedades **SslTrustStore** e **SslKeyStore** como nomes de arquivos que apontam para os arquivos truststore e keystore. Se estiver configurando essas propriedades para um agente já em execução, pare e reinicie o agente a fim de se reconectar no modo SSL.

Os arquivos de propriedades contêm senhas de texto simples, assim considere configurar as permissões do sistema de arquivos apropriadas.

Para obter mais informações sobre propriedades SSL, veja Propriedades SSL para MFT.

5. Se um gerenciador de filas do agente usar SSL, não será possível fornecer os detalhes necessários ao criar o agente. Use as etapas a seguir para criar o agente:
   a) Crie o agente usando o comando **fteCreateAgent**. Você recebe um aviso sobre não ser possível publicar a existência do agente no gerenciador de filas de coordenação.
   b) Edite o arquivo `agent.properties` que foi criado pela etapa anterior para incluir as informações de SSL. Quando o agente é iniciado com êxito, a publicação é tentada novamente.
6. Se agentes ou instâncias do IBM MQ Explorer estiverem em execução enquanto as propriedades de SSL no arquivo `agent.properties` ou arquivo no `coordination.properties` forem mudadas, o agente ou o IBM MQ Explorer deverá ser reiniciado.

Referências relacionadas

O arquivo MFT `agent.properties`

Conectando-se a um gerenciador de filas no modo cliente com autenticação de canal

O IBM WebSphere MQ 7.1 introduziu registros de autenticação de canal para controlar mais precisamente o acesso a um nível de canal. Essa mudança no comportamento significa que, por padrão, gerenciadores de filas recém-criados do IBM WebSphere MQ 7.1 ou posterior rejeitam conexões do cliente do componente Managed File Transfer.

Para obter mais informações sobre autenticação de canal, veja “Registros de Autenticação de Canal” na página 49.

Se a configuração de autenticação de canal para o SVRCONN usada pelo Managed File Transfer especifica um ID de MCAUSER não privilegiado, deve-se conceder registros de autoridade específicos para o gerenciador de filas, filas e tópicos, para permitir que o Managed File Transfer Agent e os comandos funcionem corretamente. Use o comando do MQSC SET CHLAUTH ou o comando do PCF Configurar Registro de Autenticação de Canal para criar, modificar ou remover registros de autenticação de canal. Para todos os agentes do Managed File Transfer que você deseja conectar ao gerenciador de filas do IBM WebSphere MQ 7.1 ou posterior, é possível configurar um ID MCAUSER a ser usado para todos os seus agentes ou configurar um ID MCAUSER separado para cada agente.

Conceda a cada ID de MCAUSER as permissões a seguir:

- Registros de autoridade necessários para o gerenciador de filas:
  - connect
  - setid
  - inq
- Registros de autoridade necessários para filas.

Para todas as filas específicas do agente, ou seja, nomes de filas que terminam em *agent_name* na lista a seguir, deve-se criar esses registros de autoridade de fila para cada agente que você deseja conectar ao gerenciador de filas do IBM WebSphere MQ 7.1 ou posterior usando uma conexão do cliente.

  - put, get, dsp (SYSTEM.DEFAULT.MODEL.QUEUE)
  - put, get, setid, browse (SYSTEM.FTE.COMMAND.*agent_name*)
  - put, get (SYSTEM.FTE.DATA.*agent_name*)
  - put, get (SYSTEM.FTE.REPLY.*agent_name*)
  - put, get, inq, browse (SYSTEM.FTE.STATE.*agent_name*)
  - put, get, browse (SYSTEM.FTE.EVENT.*agent_name*)
  - put, get (SYSTEM.FTE)

- Registros de autoridade necessários para tópicos:
  - sub, pub (SYSTEM.FTE)
- Registros de autoridade necessários para transferências de arquivos.

  Se você tiver IDs de MCAUSER separados para o agente de origem e de destino, crie os registros de autoridade nas filas dos agentes na origem e no destino.

  Por exemplo, se o ID do MCAUSER do agente de origem for **user1** e o ID do MCAUSER do agente de destino for **user2**, configure as autoridades a seguir para os usuários do agente:

Usuário agente	Fila	Autoridade necessária
user1	SYSTEM.FTE.DATA.*destination_agent_name*	put
user1	SYSTEM.FTE.COMMAND.*destination_agent_name*	put
user2	SYSTEM.FTE.REPLY.*source_agent_name*	put
user2	SYSTEM.FTE.COMMAND.*source_agent_name*	put

Configurando SSL ou TLS entre o agente de ponte Connect:Direct e o nó Connect:Direct

Configure o agente ponte Connect:Direct e o nó Connect:Direct para conectar um ao outro por meio do protocolo SSL criando um keystore e um truststore configurando propriedades no arquivo de propriedades do agente ponte Connect:Direct.

Sobre esta tarefa

Estas etapas incluem instruções para obter suas chaves designadas por uma autoridade de certificação. Se você não usar uma autoridade de certificação, poderá gerar um certificado autoassinado. Para obter mais informações sobre como gerar um certificado autoassinado, veja “Trabalhando com SSL/TLS no UNIX, Linux, and Windows” na página 288.

Estas etapas incluem instruções para criar um novo keystore e truststore para o agente ponte Connect:Direct. Se o agente de ponte do Connect:Direct já tiver um keystore e um armazenamento confiável que ele usa para conectar-se com segurança aos gerenciadores de filas do IBM MQ, será possível usar o keystore e o armazenamento confiável existentes quando conectar-se com segurança ao nó do Connect:Direct. Para obter mais informações, consulte “Configurando a criptografia SSL ou TLS para o MFT” na página 560.

Procedimento

Para o nó Connect:Direct, complete as seguintes etapas:

1. Gere um certificado assinado e chave para o nó Connect:Direct.

É possível fazer isso usando a ferramenta de Gerenciamento de Chaves do IBM que é fornecida com o IBM MQ. Para obter informações adicionais, consulte "Trabalhando com SSL/TLS" na página 276.

2. Envie um pedido para uma autoridade de certificação para obter a chave assinada. Você recebe um certificado como resposta.
3. Crie um arquivo de texto; por exemplo, `/test/ssl/certs/CAcert`, que contenha a chave pública de sua autoridade de certificação.
4. Instale a opção Secure + no nó Connect:Direct .

   Se o nó já existe, você pode instalar a Opção Secure+ executando o instalador novamente, especificando o local da instalação existentee escolhendo instalar somente a Opção Secure+.
5. Crie um novo arquivo de texto; por exemplo, `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt`.
6. Copie o certificado que você recebeu de sua autoridade de certificação e a chave privada, localizada no `/test/ssl/cd/privateKeys/`*`node_name`*`.key`, no arquivo de texto.

   O conteúdo de `/test/ssl/cd/keyCertFile/`*`node_name`*`.txt` deve estar no formato a seguir:

```
-----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. Inicie o Secure+ Admin Tool.
   - Em sistemas Linux ou UNIX, execute o comando **spadmin.sh**.
   - Em sistemas Windows, clique em **Iniciar** > **Programas** > **Sterling Commerce Connect:Direct** > **CD Secure+ Admin Tool**

   O CD Secure+ Admin Tool inicia.
8. No CD Secure+ Admin Tool, dê um clique duplo na linha **.Local** para editar as configurações SSL ou TLS principais.
   a) Selecione **Ativar Protocolo SSL** ou **Ativar Protocolo TLS**, dependendo de qual protocolo você está usando.
   b) Selecione **Desativar Substituição**.
   c) Selecione pelo menos um Conjunto de códigos
   d) Se desejar autenticação bidirecional, altere o valor de **Ativar Autenticação de Cliente** para Yes.

e) No campo **Certificado raiz confiável**, insira o caminho para o arquivo de certificado público de sua autoridade de certificação, `/test/ssl/certs/CAcert`.

f) No campo **Arquivo de certificado de chave**, insira o caminho para o arquivo que você criou, `/test/ssl/cd/keyCertFile/`*node_name*`.txt`.

9. Dê um clique duplo na linha **.Client** para editar as configurações SSL ou TLS principais.

a) Selecione **Ativar Protocolo SSL** ou **Ativar Protocolo TLS**, dependendo de qual protocolo você está usando.

b) Selecione **Desativar Substituição**.

Para o agente ponte Connect:Direct, execute as seguintes etapas:

10. Crie um truststore. É possível fazer isso criando uma chave simulada e então excluindo a chave simulada.

    É possível usar os seguintes comandos:

```
keytool -genkey -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

```
keytool -delete -alias dummy -keystore /test/ssl/fte/stores/truststore.jks
```

11. Importe o certificado público da autoridade de certificação dentro do truststore.

    É possível usar o seguinte comando:

```
keytool -import -trustcacerts -alias myCA
        -file /test/ssl/certs/CAcert
        -keystore /test/ssl/fte/stores/truststore.jks
```

12. Edite o arquivo de propriedades do agente ponte Connect:Direct.

    Inclua as seguintes linha em qualquer parte do arquivo:

```
cdNodeProtocol=protocol
cdNodeTruststore=/test/ssl/fte/stores/truststore.jks
cdNodeTruststorePassword=password
```

    No exemplo nesta etapa, *protocol* é o protocolo que está usando, SSL ou TLSe *password* é a senha que especificou quando criou o armazenamento confiável.

13. Se deseja autenticação de duas vias, crie uma chave e certificado para o agente ponte Connect:Direct.

a) Crie um keystore e chave.

    É possível usar o seguinte comando:

```
keytool -genkey -keyalg RSA -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -validity 365
```

b) Gere uma solicitação de sinal.

    É possível usar o seguinte comando:

```
keytool -certreq -v -alias agent_name
        -keystore /test/ssl/fte/stores/keystore.jks -storepass password
        -file /test/ssl/fte/requests/agent_name.request
```

c) Importe o certificado que você recebe da etapa precedente no keystore. O certificado deve estar no formato x.509.

    É possível usar o seguinte comando:

```
keytool -import -keystore /test/ssl/fte/stores/keystore.jks
        -storepass password -file certificate_file_path
```

d) Edite o arquivo de propriedades do agente ponte Connect:Direct.

Inclua as seguintes linha em qualquer parte do arquivo:

```
cdNodeKeystore=/test/ssl/fte/stores/keystore.jks
cdNodeKeystorePassword=password
```

No exemplo nesta etapa, *password* é a senha que especificou quando criou o keystore.

Tarefas relacionadas

Configurando a Ponte Connect:Direct

ULW Protegendo clientes AMQP

Você usa um intervalo de mecanismos de segurança para proteger conexões de clientes AMQP e assegurar que os dados sejam convenientemente protegidos na rede. É possível construir segurança em seus aplicativos MQ Light. Também é possível usar os recursos de segurança existentes do IBM MQ com clientes AMQP, da mesma maneira que os recursos são usados para outros aplicativos.

Regras de autenticação de canal (CHLAUTH)

É possível usar as regras de autenticação de canal para restringir as conexões TCP para um gerenciador de filas. Os canais AMQP suportam o uso de regras de autenticação de canal configurados para seu gerenciador de filas. Se as regras de autenticação de canal forem definidas com um perfil que corresponda a quaisquer canais AMQP em seu gerenciador de filas, essas regras serão aplicadas a esses canais. Por padrão, a autenticação de canal é ativada nos novos gerenciadores de filas do IBM® MQ, então você deverá concluir pelo menos alguma configuração antes de poder usar um canal AMQP.

Para obter mais informações sobre como configurar as regras de autenticação de canal para permitir conexões AMQP para o seu gerenciador de filas, consulte Criando e usando canais AMQP.

Autenticação de conexão (CONNAUTH)

É possível usar a autenticação de conexão para autenticar conexões com um gerenciador de filas. Os canais AMQP suportam o uso de autenticação de conexão para controlar o acesso ao gerenciador de filas a partir de aplicativos AMQP.

O protocolo AMQP usa a estrutura SASL (Camada de Segurança e Autenticação Simples) para especificar como uma conexão é autenticada. Há vários mecanismos de SASL e o IBM MQ suporta dois mecanismos de SASL : ANONYMOUS e PLAIN.

No caso de ANONYMOUS, nenhuma credencial é transmitida do cliente para o gerenciador de filas para autenticação. Se o objeto MQ AUTHINFO especificado no atributo CONNAUTH possuir um valor CHCKCLNT de REQUIRED ou REQDADM (se conectar como um usuário administrativo), a conexão será recusada. Se o valor de CHCKCLNT for NONE ou OPTIONAL, a conexão será aceita.

No caso de PLAIN, uma senha e um nome do usuário são transmitidos do cliente para o gerenciador de filas para autenticação. Se o objeto MQ AUTHINFO especificado no atributo CONNAUTH possuir um valor CHCKCLNT de NONE, a conexão será recusada. Se o valor de CHCKCLNT for OPTIONAL, REQUIRED ou REQDADM (se conectar como um usuário administrativo), a senha e o nome do usuário serão verificados pelo gerenciador de filas. O gerenciador de filas verifica o sistema operacional (se o objeto AUTHINFO for do tipo IDPWOS) ou um repositório LDAP (se o objeto AUTHINFO for do tipo IDPWLDAP).

A tabela a seguir resume esse comportamento de autenticação:

Tabela 95. Resumo dos mecanismos do SASL e da autenticação de conexão		
Mecanismo SASL	**Credenciais que foram transmitidas do cliente para o gerenciador de filas?**	**Valor CHKCLNT**
ANONYMOUS	NÃO	REQUIRED ou REQDADM - conexão recusada NONE ou OPTIONAL - conexão aceita
PLAIN	Sim, nome do usuário e senha	REQUIRED, REQDADM ou OPTIONAL - nome do usuário e senha conferidos pelo gerenciador de filas NONE - conexão recusada

Se você estiver usando um cliente do MQ Light, será possível especificar as credenciais incluindo-as no endereço AMQP conectado, por exemplo:

```
amqp://mwhitehead:mYp4ssw0rd@localhost:5672/sports/football
```

Configurando MCAUSER em um canal

Os canais AMQP têm um atributo MCAUSER, que é possível ser usado para configurar o ID do usuário do IBM MQ que todas as conexões a esse canal estão autorizadas. Todas as conexões dos clientes AMQP a este canal adotam o ID MCAUSER, se você as tiver configurado. Esse ID do usuário é utilizado para autorização de mensagens em tópicos diferentes.

É recomendável usar a autenticação de canal (CHLAUTH) para proteger as conexões para os gerenciadores de filas. Se você estiver usando a autenticação de canal, será recomendável configurar o valor de MCAUSER para um usuário não privilegiado. Isso assegura que se uma conexão com um canal não for correspondida por uma regra CHLAUTH, a conexão não estará autorizada a executar nenhuma mensagem no gerenciador de filas.

Nota: Windows No Windows, antes do IBM MQ 9.1.1, a configuração do ID do usuário MCAUSER é suportada apenas para IDs de usuário com até 12 caracteres de comprimento.

V 9.1.1 No IBM MQ 9.1.1, o limite de 12 caracteres é removido.

Suporte SSL/TLS

Os canais AMQP suportam a criptografia de SSL/TLS usando as chaves a partir do repositório de chaves configurado para seu gerenciador de filas. As opções de configuração do canal AMQP para a criptografia de SSL/TLS suportam as mesmas opções que outros tipos de canal do MQ; é possível determinar uma especificação de cifra e se o gerenciador de filas requer certificados a partir de conexões do cliente AMQP.

Ao usar os atributos do FIPS do gerenciador de filas será possível controlar os conjuntos de cifras SSL/TLS, que será possível usar para proteger as conexões de clientes AMQP.

Para obter informações sobre como configurar um repositório de chaves para o gerenciador de filas, consulte Trabalhando com SSL ou TLS em sistemas UNIX, Linux e Windows.

Para obter informações sobre como configurar o suporte SSL/TLS para uma conexão do cliente AMQP, consulte Criando e usando canais AMQP.

Java Authentication and Authorization Service (JAAS)

É possível, opcionalmente, configurar os canais AMQP com um módulo de login JAAS, que pode verificar o nome do usuário e a senha fornecidos por um cliente AMQP. Consulte o “Configurando o JAAS para canais AMQP” na página 568.

Tarefas relacionadas

Desenvolvendo aplicativos clientes AMQP

Criando e utilizando canais AMQP

ULW Restringindo o controle do cliente AMQP

Quando uma conexão do cliente é feita AMQP que possui o mesmo identificador de cliente como uma conexão do cliente AMQP existente, a conexão do cliente existente está desconectado por padrão. Entretanto, será possível configurar o gerenciador de filas para restringir o comportamento de controle do cliente para que o controle seja possível apenas quando determinados critérios forem atendidos.

Por exemplo, desconectar a conexão de um cliente existente pode não ser apropriado se houver aplicativos AMQP em desenvolvimento por equipes diferentes que possam estar usando o mesmo identificador de cliente. Para abordar esse problema, você pode restringir o controle do cliente com base no nome do canal AMQP que está sendo utilizado, o endereço IP do cliente, e ID do Usuário do cliente (quando a autenticação de SASL é ativado).

Use as configurações dos atributos do gerenciador de filas **AdoptNewMCA** e **AdoptNewMCACheck** para especificar o nível necessário de restrição de controle do cliente, conforme detalhado na tabela a seguir:

*Tabela 96. Configurações **AdoptNewMCA** e **AdoptNewMCACheck** para restringir o controle do cliente*

AdoptNewMCA	AdoptNewMCACheck	Critérios verificados antes do controle de cliente ser permitido
NO ou indefinido	Não-aplicável	Nenhum. O controle do cliente é permitido para todas as conexões do cliente autenticadas e transmite todas as regras CHLAUTH.
TODOS (ou valor diferente de NO)	QM ou indefinido	Nenhum. O controle do cliente é permitido para todas as conexões do cliente autenticadas e transmite todas as regras CHLAUTH.
TODOS (ou valor diferente de NO)	NOME	ID do usuário (quando SASL ativado) Nome do canal
TODOS (ou valor diferente de NO)	ADDRESS	ID do usuário (quando SASL ativado) Endereço IP
TODOS (ou valor diferente de NO)	ALL	ID do usuário (quando SASL ativado) Nome do canal Endereço IP

Os atributos do gerenciador de filas **AdoptNewMCA** e **AdoptNewMCACheck** fazem parte da configuração do gerenciador de filas, que está definida na sub-rotina CANAIS. Nos sistemas IBM MQ for Windows e

IBM MQ for Linux x86-64, modifique as informações de configuração usando o IBM MQ Explorer. Em outros sistemas, modifique as informações editando o arquivo de configuração `qm.ini` . Para obter informações sobre como modificar as informações de canais do gerenciador de filas, consulte Atributos de canais.

Tarefas relacionadas

Desenvolvendo aplicativos clientes AMQP

Criando e utilizando canais AMQP

ULW Configurando o JAAS para canais AMQP

Os módulos customizados do Java Authentication and Authorization Service (JAAS) podem ser usados para autenticar credenciais de nome do usuário e senha passados para um canal AMQP por um cliente AMQP quando ele se conecta.

Sobre esta tarefa

Você poderá desejar usar um módulo JAAS customizado se já usar módulos JAAS para autenticação em outros sistemas baseados em Java e desejar reutilizar esses módulos para autenticar conexões AMQP para MQ. Como alternativa, você poderá desejar gravar um módulo JAAS customizado se os recursos de autenticação construídos no MQ não suportarem o mecanismo de autenticação que você deseja usar.

A configuração de módulos JAAS para canais AMQP é feita em um nível do gerenciador de filas. Isso significa que, se você configurar um módulo JAAS para autenticar conexões AMQP para o gerenciador de filas, esse módulo se aplicará a todos os canais AMQP. O nome do canal que chamou o módulo JAAS é passado para o módulo, permitindo codificar um log JAAS diferente em comportamento para diferentes canais.

Outras informações também são passadas para o módulo JAAS:

- O identificador de cliente do cliente AMQP que está tentando autenticar.
- O endereço de rede do cliente AMQP.
- O nome do canal que chamou o módulo JAAS.

Procedimento

Defina um módulo de configuração JAAS para canais AMQP concluindo as etapas a seguir:

1. Defina um arquivo `jaas.config` contendo uma ou mais sub-rotinas de configuração do módulo JAAS. A sub-rotina deve especificar o nome completo da classe Java que implementa a interface `javax.security.auth.spi.LoginModule` do JAAS.
   - Um arquivo padrão `jaas.config` é enviado com o produto e está localizado em *QM_data_directory*`/amqp/jaas.config`.
   - Uma sub-rotina pré-configurada denominada `MQXRConfig` já está definida no arquivo padrão `jaas.config`.
2. Especifique o nome da sub-rotina a usar para canais AMQP.
   - UNIX Inclua uma propriedade no arquivo `amqp_unix.properties`.
   - Windows Inclua uma propriedade no arquivo `amqp_win.properties`.

   A propriedade tem a forma a seguir:

   ```
   com.ibm.mq.MQXR.JAASConfig=JAAS_stanza_name
   ```

   Por exemplo:

   ```
   com.ibm.mq.MQXR.JAASConfig=MQXRConfig
   ```

3. Configure o ambiente do gerenciador de filas para incluir a classe do módulo customizado. O serviço AMQP deve ter acesso à classe Java configurada na sub-rotina de configuração do JAAS.

   Você faz isso incluindo o caminho para a classe JAAS para o arquivo MQ `service.env`. Edite o arquivo `service.env` no diretório de configuração MQ (*MQ_config_directory*) ou o diretório de configuração do Gerenciador de Filas (*QM_config_directory*) para configurar a variável CLASSPATH para a localização da classe de módulo JAAS.

Como proceder a seguir

Um módulo de login de amostra JAAS é enviado com o produto no diretório *mq_installation_directory*`/amqp/samples`. O módulo de login do JAAS de amostra autentica todas as conexões do cliente, independentemente do nome do usuário ou senha com o qual o cliente se conecta.

É possível modificar o código-fonte da amostra e recompilá-lo para tentar a autenticação de somente usuários específicos com uma senha particular. Para configurar o canal AMQP em um sistema UNIX para usar o módulo de login do JAAS de amostra enviado com o produto:

1. Edite o arquivo `/var/mqm/qmgrs/QMNAME/amqp/amqp_unix.properties` e configure a propriedade `com.ibm.mq.MQXR.JAASConfig=MQXRConfig`.
2. Edite o arquivo /var/mqm/service.env e configure a propriedade `CLASSPATH=`*mq_installation_location*`/amqp/samples`

O arquivo `jaas.config` já contém uma sub-rotina nomeada `MQXRConfig` que especifica a classe de amostra `samples.JAASLoginModule` como a classe do módulo de login. Nenhuma mudança é necessária para `jaas.config` antes de você tentar o módulo de amostra.

Tarefas relacionadas

Desenvolvendo aplicativos clientes AMQP

Criando e utilizando canais AMQP

Advanced Message Security

O Advanced Message Security (AMS) é um componente do IBM MQ que fornece um alto nível de proteção para dados sensíveis que fluem por meio da rede do IBM MQ, ao mesmo tempo em que não impacta os aplicativos finais.

Visão geral do Advanced Message Security

Os aplicativos do IBM MQ podem usar Advanced Message Security para enviar dados confidenciais, como transações financeiras de valor alto e informações pessoais, com níveis diferentes de proteção usando um modelo de criptografia de chave pública.

Referências relacionadas

Códigos de retorno do GSKit usados em mensagens do AMS

Recursos e Funções do Advanced Message Security

O Advanced Message Security expande serviços de segurança do IBM MQ para fornecer dados de assinatura e criptografia no nível de mensagem. Os serviços expandidos garantem que os dados da mensagem não foram modificados entre quando eles foram originalmente colocados em uma fila e quando são recuperados. Além disso, o AMS verifica se um emissor de dados da mensagem está autorizado a colocar mensagens assinadas em uma fila de destino.

O AMS oferece as seguintes funções:

- Protege transações sensíveis ou de valor alto processadas pelo IBM MQ.
- Detecta e remove mensagens prejudiciais ou não autorizadas antes de serem processadas por uma aplicação de recepção.
- Verifica se as mensagens não foram modificadas durante a passagem de uma fila para outra.

- Protege os dados não só à medida que eles fluem através da rede, mas também quando são colocados em uma fila.
- Assegura as aplicações proprietárias e gravadas pelo cliente para IBM MQ.
- V 9.1.3 z/OS No IBM MQ 9.1.3, o IBM MQ for z/OS fornece a capacidade de, opcionalmente, remover e incluir a proteção do AMS de ou para mensagens que fluem pela rede, respectivamente. Isso é conhecido como *Intercepção do Agente do canal de mensagens (MCA) de servidor para servidor*.
- ULW V 9.1.4 V 9.1.0.4 No IBM MQ 9.1.4 e IBM MQ 9.1.0 Fix Pack 4, foi incluída uma verificação no código de biblioteca do IBM MQ que é executado no programa de aplicativo cliente. A verificação é executada no início de sua inicialização para ler o valor da variável de ambiente *AMQ_AMS_FIPS_OFF* e, se for configurado como qualquer valor, então, o código do GSKit será executado no modo não FIPS nesse aplicativo.

Qualidades de proteção disponíveis com AMS

Existem três qualidades de proteção para Advanced Message Security, `Integrity`, `Privacy` e `Confidentiality`.

A proteção `Integrity` é fornecida por assinatura digital, que garante quem criou a mensagem e que a mensagem não foi alterada ou adulterada.

A proteção `Privacy` é fornecida por uma combinação de assinatura digital e criptografia. A criptografia assegura que os dados da mensagem estejam visíveis somente ao destinatário-alvo ou destinatários. Mesmo que destinatários desautorizados obtenham uma cópia dos dados da mensagem criptografada, eles não poderão visualizar os dados da mensagem real em si.

A proteção `Confidentiality` é fornecida por criptografia apenas com reutilização de chave opcional.

Efeito sobre o Desempenho

O AMS usa uma combinação de rotinas criptográficas simétricas e assimétricas para fornecer a assinatura digital e a criptografia. Como as operações de chave simétrica são muito rápidas em comparação com operações de chave assimétrica, que são de CPU intensiva, isso pode ter um impacto significativo nos custos da proteção de grandes números de mensagens com o AMS.

Rotinas criptográficas assimétricas

Por exemplo, ao colocar uma mensagem assinada, o hash de mensagem é assinado usando uma operação de chave assimétrica.

Ao colocar uma mensagem assinada, uma operação de chave assimétrica adicional é usada para verificar o hash assinado.

Portanto, um mínimo de duas operações de chave assimétrica é necessário por mensagem para assinar e verificar os dados da mensagem.

Rotinas criptográficas assimétricas e simétricas

Ao colocar uma mensagem criptografada, uma chave simétrica é gerada e depois criptografada usando uma operação de chave assimétrica para cada destinatário-alvo da mensagem.

Os dados da mensagem são criptografados com a chave simétrica. Ao colocar a mensagem criptografada, o destinatário-alvo precisa usar uma operação de chave assimétrica para descobrir a chave simétrica em uso para a mensagem.

Todas as três qualidades de proteção, portanto, contêm vários elementos de operações de chave assimétrica de CPU intensiva, que impactarão significativamente a taxa máxima do sistema de mensagens acessível para aplicativos que estejam colocando e obtendo mensagens.

As políticas `Confidentiality`, no entanto, permitem a reutilização de chave simétrica em uma sequência de mensagens. Economias significativas de custo de CPU podem ser feitas com políticas `Confidentiality` por meio da reutilização de chave simétrica. Esse modo de operação continua usando o formato PKCS#7 para compartilhar uma chave de criptografia simétrica. Entretanto, não há assinatura digital, o que elimina algumas das operações de chave assimétrica por mensagem. A chave

simétrica ainda precisa ser criptografada com operações de chave assimétrica para cada destinatário, mas a chave simétrica pode ser reutilizada opcionalmente em diversas mensagens destinada aos mesmos destinatários. Se a reutilização de chave for permitida pela política, somente a primeira mensagem requererá operações de chave assimétrica. As mensagens subsequentes só precisam usar operações de chave simétrica.

Reutilização da chave

Com políticas do `Confidentiality` , é possível usar a abordagem de reutilização de chave simétrica para reduzir significativamente os custos envolvidos na criptografia de várias mensagens que são colocadas na mesma fila e destinadas ao mesmo destinatário ou destinatários.

Por exemplo, ao colocar 10 mensagens criptografadas no mesmo conjunto de destinatários, uma chave simétrica é gerada e, em seguida, criptografada para a primeira mensagem, usando uma operação de chave assimétrica para cada destinatário-alvo da mensagem.

Com base nos limites controlados de políticas, a chave simétrica criptografada pode ser reutilizada pelas mensagens subsequentes destinadas para os mesmos destinatários. Um aplicativo que está obtendo mensagens criptografadas pode aplicar a mesma otimização, no sentido de que o aplicativo pode detectar quando uma chave simétrica não foi mudada e evitar a despesa de recuperá-la.

Neste exemplo, 90% das operações de chave assimétrica podem ser evitadas tanto colocando quanto obtendo aplicativos pela reutilização da mesma chave.

Para obter mais informações sobre como usar a reutilização de chave, consulte:

- Comando MQSC SET POLICY
- Comando de controle setmqspl
- IBM i Comando IBM i SETMQMSPL

Conceitos chave no AMS

Aprenda sobre os conceitos chave no Advanced Message Security para entender como a ferramenta funciona e como gerenciar de forma efetiva.

Infraestrutura de chave pública e Advanced Message Security

A infraestrutura de chave pública (PKI) é um sistema de recursos, políticas e serviços que suportam o uso de criptografia de chave pública para obter comunicação segura.

Não há um padrão que defina os componentes de uma infraestrutura de chave pública, mas um PKI geralmente envolve o uso de certificados de chave pública e inclui autoridades de certificação (CA) e outras autoridades de registro (RA) que fornecem os serviços a seguir:

- Emissão de certificados digitais
- Validação de certificados digitais
- Revogação de certificados digitais
- Distribuindo Certificados

A identidade de usuários e aplicativos é representada pelo campo **nome distinto (DN)** em um certificado associado às mensagens assinadas ou criptografadas. O Advanced Message Security usa essa identidade para representar um usuário ou um aplicativo Para autenticar essa identidade, o usuário ou aplicativo deve ter acesso ao armazenamento de chaves no qual o certificado e a chave privada associada são armazenados. Cada certificado é representado por um rótulo no keystore.

Conceitos relacionados

“Usando keystores e certificados” na página 614
Para fornecer proteção criptográfica transparente para aplicativos IBM MQ, o Advanced Message Security usa o arquivo keystore, em que certificados de chave pública e uma chave privada são armazenados. No z/OS, um anel de chaves SAF é usado em vez de um arquivo keystore.

Certificados digitais no AMS

O Advanced Message Security associa usuários e aplicativos com certificados digitais padrão X.509. Certificados X.509 são geralmente assinados por uma autoridade de certificação (CA) confiável e envolvem as chaves públicas e privadas que são usadas para criptografia e decriptografia.

Os certificados digitais fornecem proteção contra identidades pela ligação de uma chave pública a seu proprietário, se esse for um indivíduo, um gerenciador de filas ou alguma outra entidade. Certificados digitais também são conhecidos como certificados de chave pública, porque eles oferecem a garantia sobre a propriedade de uma chave pública quando você usa um esquema de chave assimétrica. Este esquema requer que uma chave pública e uma chave privada sejam geradas para um aplicativo. Os dados criptografados com a chave pública só podem ser decriptografados usando a chave privada correspondente enquanto os dados criptografados com a chave privada só podem ser decriptografados usando a chave pública correspondente. A chave privada é armazenada em um arquivo do banco de dados de chaves protegido por senha. Apenas o proprietário tem acesso à chave privada usada para decriptografar mensagens que foram criptografadas usando a chave pública correspondente.

Se chaves públicas forem enviadas diretamente por seu proprietário a outra entidade, há um risco de que a mensagem possa ser interceptada e a chave pública ser substituída por outra. Isso é conhecido como um ataque "man-in-the-middle". A solução é trocar chaves públicas por meio de terceiros confiáveis, fornecendo ao usuário uma garantia segura de que a chave pública pertence à entidade com a qual você está se comunicando. Em vez de enviar sua chave pública diretamente, peça aos terceiros confiáveis para incorporá-la a um certificado digital. Os terceiros confiáveis que emitem certificados digitais são chamados de autoridade de certificação (CA).

Para obter mais informações sobre certificados digitais, consulte O que é um certificado digital.

Um certificado digital contém a chave pública de uma entidade e afirma que a chave pública pertence àquela entidade:

- quando um certificado for para uma entidade individual, ele será chamado de *certificado pessoal* ou *certificado de usuário*.
- quando um certificado for para uma autoridade de certificação, ele será chamado de *certificado CA* ou *certificado de assinante*.

Nota: O Advanced Message Security suporta certificados autoassinados em ambos o Java e aplicativos nativos

Conceitos relacionados

“Criptografia” na página 7
Criptografia é o processo de conversão entre texto legível, chamado *texto simples*, e uma forma ilegível, chamada *texto cifrado*.

Multi *Gerenciador de autoridade de objeto*

Em multiplataformas, o gerenciador de autoridade de objeto (OAM) é o componente de serviço de autorização fornecido com os produtos IBM MQ.

O acesso às entidades Advanced Message Security é controlado por meio de grupos de IBM MQ do usuário e do OAM. Os administradores podem usar a interface da linha de comandos para conceder ou revogar as autorizações, conforme necessário. Diferentes grupos de usuários podem ter diferentes tipos de autoridade de acesso para os mesmos objetos. Por exemplo, um grupo pode executar ambas as operações PUT e GET para uma fila específica enquanto outro grupo pode ter permissão somente para navegar na fila. Da mesma forma, alguns grupos podem ter a autoridade GET e PUT a para uma fila, mas não têm permissão para alterar ou excluir a fila.

Através do OAM, é possível controlar:

- Acesso a objetos Advanced Message Security por meio da Message Queue Interface (MQI). Quando um programa de aplicativo tenta acessar objetos, o OAM verifica se o perfil do usuário fazendo a solicitação tem a autorização para a operação solicitada. Isso significa que as filas e as mensagens nas filas podem ser protegidas contra acesso não autorizado.
- Permissão de usar comandos PCF e MQSC.

Conceitos relacionados

Gerenciador de autoridade de objeto

Visão geral da Message Queue Interface

Tecnologia suportada pelo Advanced Message Security

O Advanced Message Security depende de vários componentes de tecnologia para fornecer uma infraestrutura de segurança.

O Advanced Message Security suporta as interfaces de programação de aplicativos (APIs) do IBM MQ a seguir:

- MQI (Message Queue Interface)
- IBM MQ Java Message Service (JMS) 1.0.2 e 1.1.
- IBM MQ Classes base para o Java
- Classes do IBM MQ para .Net em um modo não gerenciado

Nota: O Advanced Message Security suporta autoridades de certificado compatíveis com X.509.

Limitações conhecidas de AMS

Há várias opções do IBM MQ que não são suportadas ou têm limitações para o Advanced Message Security.

- As opções do IBM MQ a seguir não são suportadas ou têm limitações:

  Publicação/assinatura
  Um dos principais benefícios de um modelo de sistema de mensagens de publicação/assinatura sobre ponto a ponto é que os aplicativos de envio e de recebimento não precisam saber nada um do outro para que os dados sejam enviados e recebidos. Esse benefício é negado pelo uso de políticas do Advanced Message Security que devem definir destinatários-alvo ou assinantes autorizados. É possível para um aplicativo publicar em um tópico por meio de uma definição de fila de alias que é protegida por uma política, também é possível para um aplicativo de assinatura obter mensagens de uma fila protegida por política. Não é possível designar uma política diretamente a uma sequência de tópicos, as políticas podem ser designadas somente a definições de filas.

  Conversão de dados do canal
  A carga útil protegida de uma mensagem protegida Advanced Message Security é transmitida usando formato binário, isso assegura que a conversão de dados em um canal entre aplicativos não invalide o trecho da mensagem. Os aplicativos que recuperam mensagens de uma fila protegida por política devem solicitar a conversão de dados, a conversão da carga útil protegida será tentada após as mensagens terem sido verificadas e desprotegidas com sucesso.

  Listas de distribuição
  As políticas Advanced Message Security podem ser usadas ao proteger os aplicativos que colocam mensagens em listas de distribuição, desde que cada fila de destino na lista tenha uma política idêntica definida. Se políticas inconsistentes forem identificadas quando um aplicativo abrir uma lista de distribuição, a operação aberta falhará e um erro de segurança retornado para o aplicativo.

  Segmentação da mensagem do aplicativo
  O tamanho das mensagens protegidas por política aumentará e não será possível para os aplicativos especificarem com precisão os limites de segmento de uma mensagem.

  Aplicativos que usam o IBM MQ classes for .NET em um modo gerenciado (conexões do cliente)
  Os aplicativos que usam o IBM MQ classes for .NET em um modo gerenciado (conexões do cliente) não são suportados.

  Nota: A intercepção de MCA pode ser usada para permitir que clientes não suportados usem o AMS.

  O cliente do serviço de mensagens para aplicativos .NET (XMS) em um modo gerenciado
  O cliente do serviço de mensagens para aplicativos .NET (XMS) em um modo gerenciado não é suportado.

  Nota: A intercepção de MCA pode ser usada para permitir que clientes não suportados usem AMS.

Filas do IBM MQ processadas pela ponte do IMS
As filas do IBM MQ processadas pela ponte do IMS não são suportadas.

Nota: O AMS é suportado nas filas de ponte do CICS. É necessário usar o mesmo ID do usuário para MQPUT (criptografia) e MQGET (decriptografia) nas filas de ponte do CICS.

Colocar em espera de getter
Colocar em getter getter não é suportado para aplicativos getter com relação a filas que possuem políticas AMS definidas para eles.

V 9.1.3 **Intercepção do servidor para servidor MCA**
No IBM MQ 9.1.3, no IBM MQ for z/OS, a intercepção do MCA de servidor para servidor é suportada apenas para tipos de canais emissor, servidor, receptor e solicitante.

- Os usuários devem evitar colocar mais de um certificado com o mesmo Nome distinto em um único arquivo keystore, porque a opção de qual certificado usar ao proteger uma mensagem é indefinida.
- O AMS não será suportado no JMS se a propriedade **WMQ_PROVIDER_VERSION** estiver configurada como 6.
- O interceptor do AMS não é suportado para canais AMQP ou MQTT.

V 9.1.3 z/OS Visão geral da intercepção Advanced Message Security nos canais de mensagens

Na z/OS, a interceptação Advanced Message Security (AMS) aprimora a oferta existente incluindo uma opção adicional de proteção de política de segurança (SPLPROT) para canais do emissor, do servidor, do receptor e do solicitante.

Atualmente, usando o exemplo de uma câmara de compensação que se comunica com um banco, ambos os lados do sistema precisam suportar AMS, conforme mostrado na Figura 1.

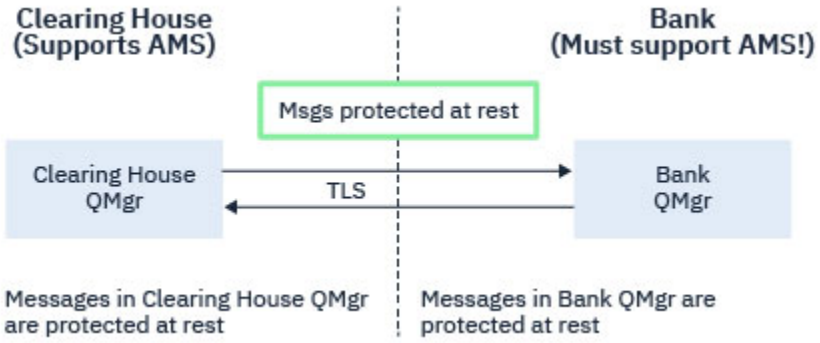


Figura 32. Uso atual do AMS

Um benefício chave da opção adicional é que, se sua empresa tiver AMS configurado, e nem todos os seus parceiros de negócios suportem AMS, é possível remover a proteção de mensagens de saída e proteger mensagens de entrada em canais para e a partir desses parceiros de negócios que não suportam AMS.

Usando o exemplo de uma câmara de compensação e de bancos, esse cenário é mostrado na Figura 2, em que há um fluxo de mensagens entre a câmara de compensação, os bancos e os parceiros de negócios em que algumas instituições têm AMSe outras não.

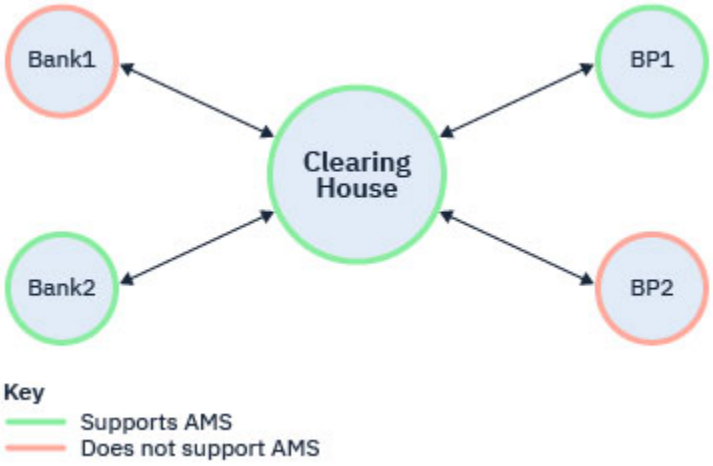


Figura 33. Alguns parceiros suportam AMS e alguns não

Geralmente, os canais são ativados para TLS.

No entanto, pode haver um caso em que alguns bancos e parceiros de negócios não suportam AMS, e há um requisito para ser capaz de trocar mensagens entre todos os bancos e parceiros de negócios. Este cenário é mostrado na Figura 3

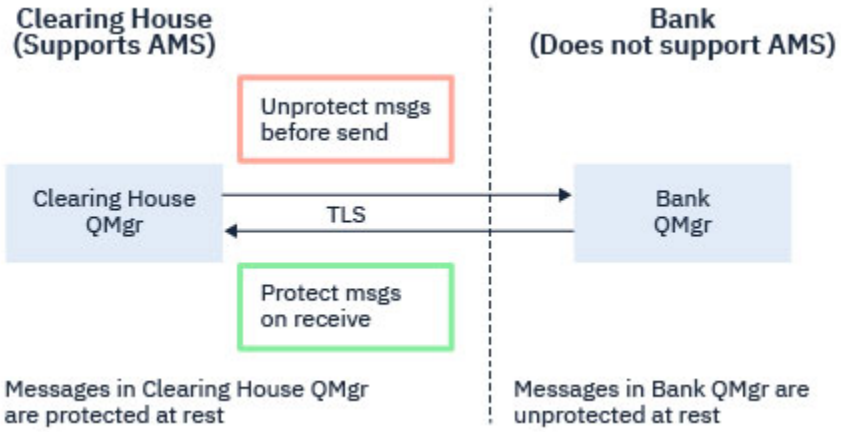


Figura 34. Fluxo de mensagens entre parceiros de negócios

Tarefas relacionadas

Configurações de exemplo de intercepção de canal de mensagem do servidor para servidor

V 9.1.3 z/OS

Interceptação do AMS em canais de mensagens servidor a servidor

A interceptação de canal de mensagens do servidor para servidor fornece um meio para controlar se as mensagens devem ter quaisquer políticas aplicáveis Advanced Message Security (AMS) aplicadas a elas, quando os agentes do canal de mensagens do tipo emissor de mensagens recebem mensagens de filas de transmissão, e os agentes do canal de mensagens do tipo receptor colocam mensagens para filas de destino.

Isso permite que a proteção AMS seja ativada em um gerenciador de filas ao se comunicar, usando canais de mensagens do servidor para servidor do tipo remetente, servidor, receptor e solicitante, com um gerenciador de filas que não possui AMS ativado.

Ou seja, as mensagens protegidas por AMS em gerenciadores de filas ativados por AMS podem ser desprotegidas antes de serem enviadas para gerenciadores de filas não ativadas para AMS e as mensagens desprotegidas recebidas de gerenciadores de filas não ativados por AMS podem ser protegidas, por políticas aplicáveis por AMS nos gerenciadores de filas ativados por AMS.

Configurando a Interceptação do Canal de Mensagem do Servidor para o Servidor

A intercepção do canal de mensagem do servidor para servidor é configurada com o atributo SPLPROT em canais com um tipo de canal de emissor, servidor, receptor ou solicitante. As opções disponíveis para configurar o comportamento são dependentes do tipo de canal especificado:

PASSTHRU
Transmita, de maneira inalterada, quaisquer mensagens enviadas ou recebidas pelo agente do canal de mensagens para esse canal.

Este valor é válido para canais com um tipo de canal (**CHLTYPE**) de SDR, SVR, RCVR ou RQSTR, e é o valor padrão.

REMOVE
Remova qualquer proteção do AMS das mensagens recuperadas da fila de transmissão pelo agente do canal de mensagens e envie as mensagens para o parceiro.

Quando o agente do canal de mensagens recebe uma mensagem da fila de transmissão, se uma política do AMS for definida para a fila de transmissão, ela será aplicada para remover qualquer proteção do AMS da mensagem antes de enviar a mensagem pelo canal. Se uma política do AMS não estiver definida para a fila de transmissão, a mensagem será enviada no estado em que se encontra.

Esse valor é válido apenas para canais com um tipo de canal de SDR ou SVR.

ASPOLICY
Com base na política definida para a fila de destino, aplique a proteção do AMS nas mensagens de entrada antes de colocá-las na fila de destino.

Quando o agente do canal de mensagens recebe uma mensagem de entrada, se uma política do AMS estiver definida para a fila de destino, a proteção do AMS será aplicada à mensagem antes de a mensagem ser colocada na fila de destino. Se uma política do AMS não estiver definida para a fila de destino, a mensagem será colocada na fila de destino no estado em que se encontra.

Esse valor é válido apenas para canais com um tipo de canal de RCVR ou RQSTR.

ID do usuário para intercepção do canal de mensagens

O requisito para IDs de usuário usados com a intercepção do canal de mensagens servidor para servidor é o mesmo daqueles para aplicativos ativados existentes do AMS. Para um canal em execução, o agente do canal de mensagens de envio recebe mensagens de uma fila de transmissão e o agente do canal de mensagens de recebimento coloca mensagens nas filas de destino. O campo do ID do usuário do agente do canal de mensagens (MCAUSER), configurado no servidor para os canais do servidor, define o ID do usuário sob o qual os agentes do canal de mensagens executam solicitações put e get.

Com a intercepção do canal de mensagem do servidor para servidor, as funções AMS são executadas durante as solicitações get e put, como com outros aplicativos ativados por AMS . Portanto, os IDs do usuário do agente do canal de mensagens têm os mesmos requisitos que aqueles para os IDs de usuário do aplicativo AMS .

O MCAUSER usado para executar a put e get é configurável e depende de se ele é um canal de saída ou de entrada. Consulte MCAUSER para obter detalhes de como o ID do usuário escolhido executa ações no agente do canal de mensagens. Como tal, o ID do usuário sob o qual o inicializador de canais está sendo executado é o ID do usuário que deve ser usado para funções AMS executadas durante a intercepção do canal de mensagem servidor a servidor. Portanto, esses IDs de usuário têm os mesmos requisitos que aqueles para IDs de usuário do aplicativo AMS .

A autenticação é executada usando as regras existentes para o canal detalhado para os canais com a configuração PUTAUT. Consulte IDs de usuário usados pelo inicializador de canais para obter mais informações.

Nota: A intercepção do canal de mensagens servidor para servidor não considera o valor do atributo de canal PUTAUT.

Tamanho da mensagem e MAXMSGL

Devido à proteção AMS , o tamanho da mensagem de mensagens protegidas será maior do que o tamanho da mensagem original.

As mensagens protegidas são maiores do que as mensagens não protegidas. Portanto, o valor do atributo **MAXMSGL** , em ambas as filas e canais, pode precisar ser alterado para levar em conta o tamanho das mensagens protegidas.

Referências relacionadas

Configurações de exemplo de intercepção de canal de mensagem do servidor para servidor

Manipulação de Erros

O IBM MQ Advanced Message Security define uma fila de manipulação de erros para gerenciar mensagens que contêm erros ou mensagens que não podem ser desprotegidas.

As mensagens defeituosas são tratadas como casos excepcionais. Se uma mensagem recebida não atender aos requisitos de segurança para a fila em que ela está, por exemplo, se a mensagem estiver assinada quando deveria estar criptografada ou a decriptografia ou verificação de assinatura falhar, a mensagem será enviada para a fila de manipulação de erros. Uma mensagem pode ser enviada para a fila de manipulação de erros pelas razões a seguir:

- Incompatibilidade de quality of protection - uma incompatibilidade de quality of protection (QOP) existe entre a mensagem recebida e a definição de QOP na política de segurança.
- Erro de decriptografia - a mensagem não pode ser decriptografada.
- Erro de cabeçalho PDMQ - o cabeçalho da mensagem do Advanced Message Security (AMS) não pode ser acessado.
- Incompatibilidade de tamanho - comprimento de uma mensagem após a decriptografia ser diferente daquela esperada.
- Incompatibilidade de intensidade de algoritmo de criptografia - o algoritmo de criptografia de mensagem é mais fraco do que o necessário.
- Erro desconhecido - ocorreu um erro inesperado.

AMS usa o sistema SYSTEM.PROTECTION.ERROR.QUEUE como sua fila de manipulação de erros.. Todas as mensagens colocadas pelo IBM MQ AMS no sistema SYSTEM.PROTECTION.ERROR.QUEUE são precedidos por um cabeçalho MQDLH..

O administrador do IBM MQ também pode definir o SYSTEM SYSTEM.PROTECTION.ERROR.QUEUE como uma fila de alias apontando para outra fila.

V 9.1.3 z/OS No IBM MQ 9.1.3, no IBM MQ for z/OS, se a intercepção do Agente do canal de mensagens (MCA) de servidor para servidor estiver em uso:

- Se, por um dos motivos mencionados anteriormente, o IBM MQ AMS mover mensagens da fila de transmissão para a fila de manipulação de erros, o MCA do remetente simplesmente continuará processando a próxima mensagem disponível na fila de transmissão.
- Em geral, as regras de canal existentes se aplicam a:
  - colocar mensagens na Fila de mensagens não entregues e
  - as ações executadas se inclusões na Fila de mensagens não entregues falharem.

Consulte “Mensagens não entregues para AMS on z/OS” na página 577 para obter informações adicionais sobre cenários específicos.

V 9.1.3 z/OS *Mensagens não entregues para AMS on z/OS*

Cenários específicos relacionados à intercepção do Agente do canal de mensagens de servidor para servidor no IBM MQ for z/OS.

No IBM MQ 9.1.3, no IBM MQ for z/OS, se a intercepção do Agente do canal de mensagens (MCA) de servidor para servidor estiver em uso:

- Se, após ter desprotegido e desprotegido uma mensagem, o MCA do emissor não entregar uma mensagem por algum motivo, por exemplo, porque a mensagem é muito grande para o canal, se o atributo do canal emissor USEDLQ estiver configurado como YES, o MCA do emissor moverá a mensagem para a Fila de Devoluções (DLQ) local.

  Se o SYSTEM.DEAD.LETTER.QUEUE estiver sendo usado como a DLQ local, a mensagem será colocada desprotegida.

  Nota: O IBM MQ AMS não suporta a proteção de mensagens colocadas em filas do sistema.

  Se um DLQ nomeado estiver sendo usado como o DLQ local, a mensagem será colocada como protegida, se você tiver definido uma política do IBM MQ AMS com o mesmo nome que o DLQ nomeado, e desprotegida, se você não definiu uma política adequada.
- Se uma mensagem não puder ser colocada na DLQ local por algum motivo e se o NPMSPEED do canal estiver configurado como NORMAL, ou a mensagem for uma mensagem persistente, o lote atual de mensagens será restaurado e o canal será colocado no estado RETRY. Caso contrário, a mensagem será descartada e o MCA do emissor continuará processando a próxima mensagem na fila de transmissão.
- Como as políticas de segurança não têm efeito sobre a SYSTEM.DEAD.LETTER.QUEUE ou as outras filas SYSTEM listadas em “Proteção da fila do sistema no AMS” na página 650, se o SYSTEM.DEAD.LETTER.QUEUE estiver em uso, as mensagens colocadas nesta fila por MCAs serão colocadas como estão. Ou seja, se as mensagens foram protegidas anteriormente, elas serão protegidas; caso contrário, elas serão colocadas desprotegidas.

  Se o atributo DEADQ do gerenciador de filas tiver sido configurado para o nome de uma fila de mensagens não entregues alternativa (não do sistema) e uma política do AMS com o mesmo nome não existir, as mensagens colocadas nessa fila pelos MCAs serão colocadas no estado em que se encontram. Ou seja, se as mensagens foram protegidas anteriormente, elas serão protegidas; caso contrário, elas serão colocadas desprotegidas.

  Se o atributo DEADQ do gerenciador de filas tiver sido configurado para o nome de uma fila de mensagens não entregues alternativa (não sistema) e uma política do AMS com o mesmo nome que a DLQ existir, a política será usada para proteger mensagens colocadas nessa fila por MCAs. Se a mensagem já tiver sido protegida anteriormente, ela não será protegida novamente; isso é para evitar a proteção dupla. Se uma política AMS com o mesmo nome não existir, as mensagens serão colocadas no estado em que se encontram.
- Se houver uma política para a DLQ com a opção de tolerância no comando setmqspl configurada como desativada, isto é, '**-t** O', a colocação na DLQ falhará se a mensagem não for protegida pelo AMS e, portanto, não tiver um cabeçalho PDMQ. Isso acontece se a mensagem chegar ao receptor sem um cabeçalho PDMQ. Esse é o putter original da mensagem não tinha uma política para o destino, e o O receptor não possui SPLPROT (ASPOLICY) configurado.
- Um MCA poderá falhar ao enviar uma mensagem ao DLQ se a política do AMS definida para o DLQ não permitir o ID do usuário no qual o iniciador do canal está sendo executado para proteger a mensagem.
- Os canais receptores geralmente colocam mensagens não entregues na DLQ local, enquanto canais emissores geralmente colocam mensagens que não podem ser processadas por algum motivo, por exemplo, mensagens muito grandes para fila ou cabeçalho MQXQH inválido e assim por diante para a DLQ local.
- Os manipuladores DLQ geralmente só olham para o cabeçalho DLQ (DLH) e não a carga útil da mensagem em si. Assim, o fato de que a carga útil da mensagem pode ser protegida não impede os manipuladores de determinarem a razão pela qual a mensagem foi colocada na DLQ.
- Se uma DLQ não estiver definida, o canal:
  - se encerrará anormalmente (e irá para o estado de nova tentativa) se uma mensagem persistente não puder ser entregue;
  - descartará uma mensagem não entregue não persistente e continuará a execução.

Conceitos relacionados

"Manipulação de Erros" na página 577
O IBM MQ Advanced Message Security define uma fila de manipulação de erros para gerenciar mensagens que contêm erros ou mensagens que não podem ser desprotegidas.

Cenários do usuário

Familiarize-se com cenários possíveis para entender quais metas de negócios é possível obter com o Advanced Message Security.

Windows *Guia de iniciação rápida para o AMS em plataformas Windows*

Use este guia para configurar rapidamente o Advanced Message Security para fornecer segurança de mensagens em plataformas Windows. No momento em que você concluir, você terá criado um banco de dados de chaves para verificar identidades do usuário e definido políticas de assinatura/criptografia para o seu gerenciador de filas.

Antes de começar

É necessário ter pelo menos os recursos a seguir instalados em seu sistema:

- Servidor
- Kit de ferramentas de desenvolvimento (para os programas de amostra)
- Advanced Message Security

Consulte os recursos do IBM MQ para os sistemas Windows para obter detalhes.

Para obter informações sobre como usar o comando **setmqenv** para inicializar o ambiente atual para que os comandos IBM MQ apropriados possam ser localizados e executados pelo sistema operacional, consulte setmqenv (configurar ambiente IBM MQ).

1. Criando um gerenciador de filas e uma fila

Sobre esta tarefa

Todos os exemplos a seguir usam uma fila nomeada `TEST.Q` para passar mensagens entre aplicativos. Advanced Message Security usa interceptores para assinar e criptografar mensagens no ponto em que elas entram na estrutura IBM MQ através da interface padrão do IBM MQ. A configuração básica é feita no IBM MQ e é configurada nas etapas a seguir.

É possível usar o IBM MQ Explorer para criar o gerenciador de filas QM_VERIFY_AMS e sua fila local chamada `TEST.Q` usando todas as configurações do assistente padrão ou é possível usar os comandos localizados em `C:\Program Files\IBM\MQ\bin` Lembre-se de que deve-se ser um membro do grupo de usuários `mqm` para executar os comandos administrativos a seguir.

Procedimento

1. Crie um gerenciador de filas

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Iniciar o Gerenciador de Filas

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Crie uma fila chamada `TEST.Q` inserindo o comando a seguir em **runmqsc** para o gerenciador de filas QM_VERIFY_AMS

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Resultados

Se o procedimento for concluído, o comando inserido em **runmqsc** irá exibir detalhes sobre TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Criando e autorizando usuários

Sobre esta tarefa

Há dois usuários que aparecem neste exemplo: alice, o emissor e bob, o receptor. Para usar a fila do aplicativo, esses usuários precisam receber autoridade para usá-la. Além disso, para usar com sucesso as políticas de proteção que vamos definir estes usuários devem ser concedidos acesso a algumas filas do sistema. Para obter mais informações sobre o comando **setmqaut**, consulte **setmqaut**.

Procedimento

1. Crie os dois usuários e assegure que HOMEPATH e HOMEDRIVE estejam configurados para ambos esses usuários.
2. Autorize os usuários para se conectarem ao gerenciador de filas e para trabalhar com a fila

```
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. É necessário também permitir que os dois usuários naveguem na fila de políticas do sistema e coloquem mensagens na fila de erros.

```
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
```

Atenção: O IBM MQ otimiza o desempenho armazenando em cache políticas para que você não tenha que procurar registros para obter detalhes da política no SYSTEM.PROTECTION.POLICY.QUEUE em todos os casos..

O IBM MQ não armazena em cache todas as políticas disponíveis. Se houver um grande número de políticas, o IBM MQ armazenará em cache um número limitado de políticas. Portanto, se o gerenciador de filas tiver um número baixo de políticas definidas, não haverá a necessidade de fornecer a opção de navegação para o SYSTEM.PROTECTION.POLICY.QUEUE.

No entanto, é necessário dar autoridade de navegação a essa fila nos casos em que há um grande número de políticas definidas ou quando você está usando clientes antigos. O SYSTEM.PROTECTION.ERROR.QUEUE é usado para colocar mensagens de erro geradas pelo código AMS. A autoridade put para essa fila é verificada apenas quando você tenta colocar uma mensagem de erro na fila. Sua autoridade put em relação à fila não é verificada quando você tenta colocar ou obter mensagens de uma fila protegida por AMS.

Resultados

Os usuários agora são criados e as autoridades necessárias concedidas a eles.

Como proceder a seguir

Para verificar se as etapas foram executadas corretamente, use as amostras amqsput e amqsget , conforme descrito na seção “7. Testando a configuração” na página 583

3. Criando banco de dados de chaves e certificados

Sobre esta tarefa

O interceptor requer a chave pública dos usuários de envio para criptografar a mensagem. Portanto, o banco de dados de chaves das identidades do usuário mapeado para chaves pública e privada deve ser criado. No sistema real, no qual os usuários e aplicativos são dispersos por meio de vários computadores, cada usuário teria seu próprio keystore privado. Da mesma forma, nesse guia, criamos banco de dados de chaves para `alice` e bob e compartilhamos os certificados de usuário entre eles.

Nota: Neste guia, usamos os aplicativos de amostra escritos em C conectando usando ligações locais. Se você planeja usar aplicativos Java usando as ligações de cliente, deve-se criar um keystore e certificados JKS usando o comando **`keytool`**, que é parte do JRE (consulte "Guia de iniciação rápida para o AMS com os clientes Java" na página 602 para obter mais detalhes). Para todas as outras linguagens e para os aplicativos Java usar ligações locais as etapas deste guia estão corretas.

Procedimento

1. Use o IBM Key Management GUI (`strmqikm.exe`) para criar um novo banco de dados de chaves para o usuário `alice`.

   ```
   Type:       CMS
   Filename:   alicekey.kdb
   Location:   C:/Documents and Settings/alice/AMS
   ```

   Nota:

   - É aconselhável usar uma senha forte para proteger o banco de dados.
   - Certifique-se de que a caixa de seleção **armazenar a senha em arquivo stash** foi selecionada.
2. Mude a visualização de conteúdo do banco de dados chave para **Certificados pessoais**.
3. Selecione **Novo autoassinado** ; certificados autoassinados são usados nesse cenário.
4. Crie um certificado identificando o usuário `alice` para uso na criptografia usando estes campos:

   ```
   Key label: Alice_Cert
   Common Name: alice
   Organisation: IBM
   Country: GB
   ```

   Nota:

   - Para o propósito desse guia, estamos usando certificado autoassinado que pode ser criado sem o uso de uma Autoridade de Certificação. Para sistemas de produção, é aconselhável não usar certificados autoassinados, mas em vez disso contar com certificados assinados por uma Autoridade de certificação.
   - O parâmetro **`Key label`** especifica o nome para o certificado, que os interceptores procurarão para receber informações necessárias.
   - O **`Common Name`** e parâmetros opcionais especificam os detalhes do **Nome distinto** (DN), que deve ser exclusivo para cada usuário.
5. Repita as etapas 1-4 para o usuário bob

Resultados

Os dois usuários `alice` e bob agora possuem cada um certificado autoassinado.

4. Criando keystore.conf

Sobre esta tarefa

Deve-se apontar os interceptores do Advanced Message Security para o diretório no qual os bancos de dados de chaves e os certificados estão located.This é feito por meio do arquivo `keystore.conf` ,

que contém essas informações em formato de texto simples Cada usuário deve ter um arquivo `keystore.conf` separado na pasta `.mqs`. Esta etapa deve ser feita para ambos, `alice` e bob.

O conteúdo de `keystore.conf` deve ser dessa forma:

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

Exemplo

Para este cenário, o conteúdo do `keystore.conf` será o seguinte:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

Nota:

- O caminho para o arquivo keystore deve ser fornecido sem extensão de arquivo.
- O rótulo certificado pode incluir espaços, portanto "Alice_Cert" e "Alice_Cert " (com um espaço no final), por exemplo, são reconhecidos como rótulos de dois certificados diferentes. No entanto, para evitar confusão, é melhor não usar espaços no nome do rótulo.
- Existem os formatos de keystore a seguir: CMS (Cryptographic Message Sintaxe), JKS (Java Keystore) e JCEKS (Java Cryptographic Extension Keystore). Para obter informações adicionais, consulte “Estrutura do arquivo de configuração do keystore (keystore.conf) para AMS” na página 615.
- *%HOMEDRIVE%\%HOMEPATH%*\`.mqs\keystore.conf` (por exemplo, C:\Documents and Settings\alice\.mqs\keystore.conf) é o local padrão em que Advanced Message Security procura pelo arquivo `keystore.conf`. Para obter informações sobre como usar um local não padrão para o `keystore.conf`, consulte “Usando keystores e certificados” na página 614.
- Para criar o diretório `.mqs`, deve-se usar o prompt de comando.

5. Compartilhando os certificados

Sobre esta tarefa

Compartilhe os certificados entre os dois bancos de dados de chaves para que cada usuário possa identificar com sucesso o outro. Isso é feito extraindo cada certificado público do usuário para um arquivo, que é, então, incluído no banco de dados de chaves do outro usuário.

Nota: Tome cuidado para usar a opção *extract* e não a opção *export*. *Extract* obtém a chave pública do usuário, enquanto *export* obtém a chave pública e a privada. Usar *export* por engano comprometeria completamente o seu aplicativo, transmitindo a sua chave privada.

Procedimento

1. Extraia o certificado identificando `alice` para um arquivo externo:

   ```
   runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
   -label Alice_Cert -target alice_public.arm
   ```

2. Inclua o certificado para o keystore bob's:

   ```
   runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
   Alice_Cert -file alice_public.arm
   ```

3. Repita as etapas para 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
```

Resultados

Os dois usuários, `alice` e bob, agora podem identificar um ao outro com êxito como tendo criado e compartilhado certificados autoassinados.

Como proceder a seguir

Verifique se um certificado está no keystore procurando por ele usando a GUI ou executando os comandos a seguir que imprimem seus detalhes:

```
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. Definindo a política de filas

Sobre esta tarefa

Com o gerenciador de filas criado e os interceptores preparados para interceptar mensagens e acessar chaves de criptografia, podemos começar a definir políticas de proteção no `QM_VERIFY_AMS` usado o comando `setmqspl`. Consulte setmqspl para obter mais informações sobre este comando. Cada nome da política deve ser o mesmo que o nome da fila para a qual ela deve ser aplicada.

Exemplo

Este é um exemplo de uma política definida para a fila `TEST.Q`. No exemplo, as mensagens são assinadas com o algoritmo SHA1 e criptografados com o algoritmo AES256. `alice` é o único emissor válido e bob é o único receptor das mensagens nesta fila:

```
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"
```

Nota: Os DNs correspondem exatamente aos especificados no respectivo certificado do usuário do banco de dados de chaves.

Como proceder a seguir

Para verificar a política que você definiu, emita o comando a seguir:

```
dspmqspl -m QM_VERIFY_AMS
```

Para imprimir os detalhes da política como um conjunto de comandos `setmqspl`, use a sinalização `-export`. Isso permite armazenar políticas já definidas:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testando a configuração

Sobre esta tarefa

Ao executar programas diferentes em diferentes usuários é possível verificar se o aplicativo foi configurado corretamente.

Procedimento

1. Alterne o usuário para ser executado como `alice`

   Clique com o botão direito em `cmd.exe` e selecione **Executar como ...**. Quando solicitado, efetue login como o usuário `alice`.
2. Como o usuário `alice` coloque uma mensagem usando um aplicativo de amostra:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. Digite o texto da mensagem e em seguida pressione Enter.
4. Alterne o usuário para ser executado como bob

   Abra outra janela clicando com o botão direito em `cmd.exe` e selecionando **Executar como...**. Quando solicitado, efetue login como o usuário bob.
5. Como o usuário bob obtenha uma mensagem usando um aplicativo de amostra:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Resultados

Se o aplicativo foi configurado corretamente para ambos os usuários, a mensagem do usuário `alice` será exibida quando o bob executar o aplicativo de obtenção.

8. Testando a criptografia

Sobre esta tarefa

Para verificar se a criptografia está ocorrendo conforme o esperado, crie uma fila de alias que faça referência à fila original `TEST.Q`. Esta fila de alias não terá uma política de segurança e, portanto, nenhum usuário terá as informações para decriptografar a mensagem e, portanto, os dados criptografados serão mostrados.

Procedimento

1. Usando o comando **runmqsc** no gerenciador de filas QM_VERIFY_AMS, crie uma fila de alias.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```
2. Conceda a bob acesso para procurar da fila de alias

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```
3. Como o usuário `alice`, coloque outra mensagem usando um aplicativo de amostra como antes:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
4. Como o usuário bob, procure a mensagem usando um aplicativo de amostra por meio da fila de alias dessa vez:

   ```
   amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```
5. Como o usuário bob, obtenha a mensagem usando um aplicativo de amostra a partir da fila local:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Resultados

A saída do aplicativo `amqsbcg` mostra os dados criptografados que estão na fila, provando que a mensagem foi criptografada.

UNIX *Guia de iniciação rápida para o AMS no UNIX*

Use este guia para configurar rapidamente o Advanced Message Security para fornecer segurança de mensagens no UNIX. No momento em que você concluir, você terá criado um banco de dados de chaves para verificar identidades do usuário e definido políticas de assinatura/criptografia para o seu gerenciador de filas.

Antes de começar

É necessário ter pelo menos os componentes a seguir instalados em seu sistema:

- tempo de execução
- Servidor
- Programas de Amostra
- IBM Global Security Kit
- Advanced Message Security

Consulte os tópicos a seguir para os nomes dos componentes em cada plataforma específica:

- Linux IBM MQ componentes para Linux sistemas
- AIX IBM MQ componentes para AIX sistemas
- Solaris IBM MQ componentes para Solaris sistemas

1. Criando um gerenciador de filas e uma fila

Sobre esta tarefa

Todos os exemplos a seguir usam uma fila nomeada `TEST.Q` para passar mensagens entre aplicativos. Advanced Message Security usa interceptores para assinar e criptografar mensagens no ponto em que elas entram na estrutura IBM MQ através da interface padrão do IBM MQ. A configuração básica é feita no IBM MQ e é configurada nas etapas a seguir.

É possível usar o IBM MQ Explorer para criar o gerenciador de filas QM_VERIFY_AMS e sua fila local chamada `TEST.Q` usando todas as configurações padrão do assistente ou é possível usar os comandos localizados em *MQ_INSTALLATION_PATH*`/bin`. Lembre-se de que deve-se ser um membro do grupo de usuários `mqm` para executar os comandos administrativos a seguir.

Procedimento

1. Crie um gerenciador de filas

```
crtmqm QM_VERIFY_AMS
```

2. Iniciar o Gerenciador de Filas

```
strmqm QM_VERIFY_AMS
```

3. Crie uma fila chamada `TEST.Q` inserindo o comando a seguir em **runmqsc** para o gerenciador de filas QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Resultados

Se o procedimento foi concluído com sucesso, o comando a seguir inserido em **runmqsc** irá exibir detalhes sobre TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Criando e autorizando usuários

Sobre esta tarefa

Há dois usuários que aparecem neste exemplo: `alice`, o emissor e `bob`, o receptor. Para usar a fila do aplicativo, esses usuários precisam receber autoridade para usá-la. Além disso, para usar com sucesso as políticas de proteção que vamos definir estes usuários devem ser concedidos acesso a algumas filas do sistema. Para obter mais informações sobre o comando **setmqaut**, consulte **setmqaut**.

Procedimento

1. Crie os dois usuários

   ```
   useradd alice
   useradd bob
   ```

2. Autorize os usuários para se conectarem ao gerenciador de filas e para trabalhar com a fila

   ```
   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. É necessário também permitir que os dois usuários naveguem na fila de políticas do sistema e coloquem mensagens na fila de erros.

   ```
   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
   ```

   Atenção: O IBM MQ otimiza o desempenho armazenando em cache políticas para que você não tenha que procurar registros para obter detalhes da política no SYSTEM.PROTECTION.POLICY.QUEUE em todos os casos..

   O IBM MQ não armazena em cache todas as políticas disponíveis. Se houver um grande número de políticas, o IBM MQ armazenará em cache um número limitado de políticas. Portanto, se o gerenciador de filas tiver um número baixo de políticas definidas, não haverá a necessidade de fornecer a opção de navegação para o SYSTEM.PROTECTION.POLICY.QUEUE.

   No entanto, é necessário dar autoridade de navegação a essa fila nos casos em que há um grande número de políticas definidas ou quando você está usando clientes antigos. O SYSTEM.PROTECTION.ERROR.QUEUE é usado para colocar mensagens de erro geradas pelo código AMS. A autoridade put para essa fila é verificada apenas quando você tenta colocar uma mensagem de erro na fila. Sua autoridade put em relação à fila não é verificada quando você tenta colocar ou obter mensagens de uma fila protegida por AMS.

Resultados

Agora os grupos de usuários são criados e as autoridades requeridas concedidas a eles. Desse modo os usuários que estiverem designados a esses grupos também terão permissão para se conectar ao gerenciador de filas e colocar e obter da fila.

Como proceder a seguir

Para verificar se as etapas foram executadas corretamente, use as amostras `amqsput` e `amqsget` , conforme descrito na seção “8. Testando a criptografia” na página 590

3. Criando banco de dados de chaves e certificados

Sobre esta tarefa

Para criptografar a mensagem, o interceptor requer a chave privada do usuário de envio e a chave pública(s) do destinatário(s). Portanto, o banco de dados de chaves das identidades do usuário mapeado para chaves pública e privada deve ser criado. No sistema real, no qual os usuários e aplicativos são dispersos por meio de vários computadores, cada usuário teria seu próprio keystore privado. Da mesma forma, nesse guia, criamos banco de dados de chaves para `alice` e bob e compartilhamos os certificados de usuário entre eles.

Nota: Neste guia, usamos os aplicativos de amostra escritos em C conectando usando ligações locais. Se você planeja usar aplicativos Java usando as ligações de cliente, deve-se criar um keystore e certificados JKS usando o comando **keytool**, que é parte do JRE (consulte "Guia de iniciação rápida para o AMS com os clientes Java" na página 602 para obter mais detalhes). Para todas as outras linguagens e para os aplicativos Java usar ligações locais as etapas deste guia estão corretas.

Procedimento

1. Crie um novo banco de dados de chaves para o usuário `alice`

   ```
   mkdir /home/alice/.mqs -p
   runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
   ```

   Nota:

   - É aconselhável usar uma senha forte para proteger o banco de dados.
   - O parâmetro **stash** armazena a senha no arquivo `key.sth`, que interceptores podem usar para abrir o banco de dados.
2. Assegure que o banco de dados chave é legível

   ```
   chmod +r /home/alice/.mqs/alicekey.kdb
   ```

3. Crie um certificado que identifica o usuário `alice` para uso na criptografia

   ```
   runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd
   -label Alice_Cert -dn "cn=alice,O=IBM,c=GB" -default_cert yes
   ```

   Nota:

   - Para o propósito desse guia, estamos usando certificado autoassinado que pode ser criado sem o uso de uma Autoridade de Certificação. Para sistemas de produção, é aconselhável não usar certificados autoassinados, mas em vez disso contar com certificados assinados por uma Autoridade de certificação.
   - O parâmetro **label** especifica o nome para o certificado, que os interceptores consultarão para receber as informações necessárias.
   - O parâmetro **DN** especifica os detalhes do **Nome Distinto** (DN), que deve ser exclusivo para cada usuário.
4. Agora criamos o banco de dados de chaves, é necessário configurar a propriedade dele e verificar se ele está ilegível para todos os outros usuários.

   ```
   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. Repita as etapas 1-4 para o usuário bob

Resultados

Os dois usuários `alice` e bob agora possuem cada um certificado autoassinado.

4. Criando keystore.conf

Sobre esta tarefa

Deve-se apontar os interceptores do Advanced Message Security para o diretório no qual os bancos de dados de chave e certificados estão localizados. Isso é feito por meio do arquivo `keystore.conf`, que mantém essas informações em texto sem formatação. Cada usuário deve ter um arquivo `keystore.conf` separado na pasta `.mqs`. Esta etapa deve ser feita para ambos, `alice` e bob.

O conteúdo de `keystore.conf` deve ser dessa forma:

```
cms.keystore = dir/keystore_file
cms.certificate = certificate_label
```

Exemplo

Para este cenário, o conteúdo do `keystore.conf` será o seguinte:

```
cms.keystore = /home/alice/.mqs/alicekey
cms.certificate = Alice_Cert
```

Nota:

- O caminho para o arquivo keystore deve ser fornecido sem extensão de arquivo.
- Existem os formatos de keystore a seguir: CMS (Cryptographic Message Sintaxe), JKS (Java Keystore) e JCEKS (Java Cryptographic Extension Keystore). Para obter informações adicionais, consulte “Estrutura do arquivo de configuração do keystore (keystore.conf) para AMS” na página 615.
- `HOME/.mqs/keystore.conf` é o local padrão em que o Advanced Message Security procura o arquivo `keystore.conf`. Para obter informações sobre como usar um local não padrão para o `keystore.conf`, consulte “Usando keystores e certificados” na página 614.

5. Compartilhando os certificados

Sobre esta tarefa

Compartilhe os certificados entre os dois bancos de dados de chaves para que cada usuário possa identificar com sucesso o outro. Isso é feito extraindo cada certificado público do usuário para um arquivo, que é, então, incluído no banco de dados de chaves do outro usuário.

Nota: Tome cuidado para usar a opção *extract* e não a opção *export*. *Extract* obtém a chave pública do usuário, enquanto *export* obtém a chave pública e a privada. Usar *export* por engano comprometeria completamente o seu aplicativo, transmitindo a sua chave privada.

Procedimento

1. Extraia o certificado identificando `alice` para um arquivo externo:

   ```
   runmqakm -cert -extract -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert
   -target alice_public.arm
   ```

2. Inclua o certificado para o keystore bob ' s:

   ```
   runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
   alice_public.arm
   ```

3. Repita a etapa para bob:

```
runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
bob_public.arm
```

4. Inclua o certificado para bob para o keystore `alice's`:

```
runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert -file
bob_public.arm
```

Resultados

Os dois usuários, `alice` e bob, agora podem identificar um ao outro com êxito como tendo criado e compartilhado certificados autoassinados.

Como proceder a seguir

Verifique se o certificado está no keystore executando os comandos a seguir que imprimem seus detalhes:

```
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. Definindo a política de filas

Sobre esta tarefa

Com o gerenciador de filas criado e os interceptores preparados para interceptar mensagens e acessar chaves de criptografia, podemos começar a definir políticas de proteção no `QM_VERIFY_AMS` usado o comando `setmqspl`. Consulte setmqspl para obter mais informações sobre este comando. Cada nome da política deve ser o mesmo que o nome da fila para a qual ela deve ser aplicada.

Exemplo

Este é um exemplo de uma política definida para a fila `TEST.Q`. Neste exemplo, as mensagens são assinadas pelo usuário `alice` usando o algoritmo SHA1 algoritmo e criptografados usando o algoritmo 256-bit AES. `alice` é o único emissor válido e bob é o único receptor das mensagens nesta fila:

```
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"
```

Nota: Os DNs correspondem exatamente aos especificados no respectivo certificado do usuário do banco de dados de chaves.

Como proceder a seguir

Para verificar a política que você definiu, emita o comando a seguir:

```
dspmqspl -m QM_VERIFY_AMS
```

Para imprimir os detalhes da política como um conjunto de comandos `setmqspl`, use a sinalização `-export`. Isso permite armazenar políticas já definidas:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testando a configuração

Sobre esta tarefa

Ao executar programas diferentes em diferentes usuários é possível verificar se o aplicativo foi configurado corretamente.

Procedimento

1. Mude para o diretório que contém as amostras. Se o MQ estiver instalado em um local não padrão, este poderá estar em um local diferente.

```
cd /opt/mqm/samp/bin
```

2. Alterne o usuário para ser executado como `alice`

```
su alice
```

3. Como o usuário `alice`, coloque uma mensagem usando um aplicativo de amostra:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Digite o texto da mensagem e em seguida pressione Enter.
5. Pare de executar como o usuário `alice`

```
exit
```

6. Alterne o usuário para ser executado como bob

```
su bob
```

7. Como o usuário bob, obtenha uma mensagem usando um aplicativo de amostra:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Resultados

Se o aplicativo foi configurado corretamente para ambos os usuários, a mensagem do usuário `alice` será exibida quando o bob executar o aplicativo de obtenção.

8. Testando a criptografia

Sobre esta tarefa

Para verificar se a criptografia está ocorrendo conforme o esperado, crie uma fila de alias que faça referência à fila original TEST.Q. Esta fila de alias não terá uma política de segurança e, portanto, nenhum usuário terá as informações para decriptografar a mensagem e, portanto, os dados criptografados serão mostrados.

Procedimento

1. Usando o comando **runmqsc** no gerenciador de filas QM_VERIFY_AMS, crie uma fila de alias.

```
DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
```

2. Conceda a bob acesso para procurar da fila de alias

```
setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
```

3. Como o usuário `alice`, coloque outra mensagem usando um aplicativo de amostra como antes:

```
./amqsput TEST.Q QM_VERIFY_AMS
```

4. Como o usuário bob, procure a mensagem usando um aplicativo de amostra por meio da fila de alias dessa vez:

```
./amqsbcg TEST.ALIAS QM_VERIFY_AMS
```

5. Como o usuário bob, obtenha a mensagem usando um aplicativo de amostra a partir da fila local:

```
./amqsget TEST.Q QM_VERIFY_AMS
```

Resultados

A saída do aplicativo `amqsbcg` mostrará os dados criptografados que estão na fila, provando que a mensagem foi criptografada.

z/OS *Exemplo de configurações no z/OS*

Essa seção fornece configurações de exemplo de políticas e certificados para cenários de enfileiramento do Advanced Message Security no z/OS.

Consulte Configurando o Advanced Message Security for z/OS para obter detalhes sobre como configurar o Advanced Message Security.

Os exemplos cobrir as políticas do Advanced Message Security necessárias e os certificados digitais que devem existir em relação a usuários e conjuntos de chave. Os exemplos supõem que os usuários envolvidos nos cenários foram configurados seguindo as instruções fornecidas em Conceder permissões de recursos de usuários para o Advanced Message Security.

V 9.1.3 Além disso, do IBM MQ 9.1.3 em diante, consulte os exemplos de interceptação de canal de mensagens de servidor para servidor.

z/OS *Enfileiramento local de mensagens de integridade protegida no z/OS*

Este exemplo detalha as políticas e certificados do Advanced Message Security necessários para enviar e recuperar mensagens de integridade protegida para e a partir de uma fila local para os aplicativos de envio e recebimento.

O gerenciador de filas e a fila de exemplo são:

```
BNK6        - Queue manager
FIN.XFER.Q7 - Local queue
```

Esses usuários são usados:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

Criar os certificados de usuário

Nesse exemplo, somente um certificado de usuário é necessário. Este é o certificado de usuário de envio, que é necessário para assinar as mensagens de integridade protegida. O usuário de envio é 'TELLER5'.

O certificado da autoridade de certificação (CA) também é necessário. O certificado de autoridade de certificação é o certificado da autoridade que emitiu o certificado de usuário. Isso pode ser uma cadeia de certificados. Se assim for, todos os certificados na cadeia são necessários no conjunto de chaves do usuário da tarefa do Advanced Message Security, neste caso o usuário WMQBNK6.

Um certificado de autoridade de certificação pode ser criado usando o comando RACDCERT do RACF. Este certificado é usado para emitir certificados de usuário. Por exemplo:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Este comando RACDCERT cria um certificado de autoridade de certificação que pode então ser usado para emitir um certificado de usuário para o usuário 'TELLER5'. Por exemplo:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

A instalação terá procedimentos para escolher ou criar um certificado de autoridade de certificação, bem como os procedimentos para emitir certificados e distribuí-los para sistemas relevantes.

Ao exportar e importar esses certificados, o Advanced Message Security requer:

- O certificado de autoridade de certificação (cadeia).
- O certificado de usuário e sua chave privada.

Se você estiver usando o RACF, o comando RACDCERT EXPORT pode ser usado para exportar certificados para um conjunto de dados e o comando RACDCERT ADD pode ser usado para importar certificados do conjunto de dados. Para obter informações adicionais sobre estes e outros comandos RACDCERT, consulte *Referência de linguagem de comandos do z/OS: Security Server RACF*.

Os certificados, neste caso, são necessários no sistema z/OS que está executando o gerenciador de filas BNK6.

Quando os certificados forem importados no sistema z/OS que está executando BNK6, o certificado de usuário irá requer o atributo TRUST. O comando RACDCERT ALTER pode ser usado para incluir o atributo TRUST ao certificado. Por exemplo:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Neste exemplo, nenhum certificado será necessário para o usuário destinatário.

Conectar os certificados aos conjuntos de chaves relevantes

Quando os certificados necessários forem criados ou importados e definidos como confiáveis, eles devem ser conectados aos conjuntos de chaves apropriados do usuário no sistema z/OS que estiver executando o BNK6. Para criar os conjuntos de chave use os comandos RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário da tarefa do Advanced Message Security, WMQBNK6 e um conjunto de chaves para o usuário de envio, 'TELLER5'. Observe que o nome do conjunto de chaves drq.ams.keyring é obrigatório e o nome faz distinção entre maiúsculas e minúsculas.

Quando os conjuntos de chave foram criados, os certificados relevantes podem ser conectados:

```
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))
```

O certificado de usuário de envio deve estar conectado como DEFAULT. Se o usuário de envio possui mais de um certificado em seu drq.ams.keyring, o certificado padrão é usado para fins de assinatura.

A criação e modificação de certificados não é reconhecida pelo Advanced Message Security até que o gerenciador de filas seja parado e reiniciado ou o comando do z/OS **MODIFY** seja usado para atualizar a configuração de certificado do Advanced Message Security. Por exemplo:

```
F BNK6AMSM,REFRESH KEYRING
```

Criar a política do Advanced Message Security

Neste exemplo, as mensagens de integridade protegida são colocadas na fila FIN.XFER.Q7 por um aplicativo em execução como o usuário 'TELLER5' e recuperadas da mesma fila por um aplicativo em execução como o usuário 'FINADM2', portanto, apenas uma política do Advanced Message Security é necessária.

As políticas do Advanced Message Security são criadas usando o utilitário CSQ0UTIL, que está documentado em O utilitário de política de segurança da mensagem (CSQ0UTIL).

Use o utilitário CSQ0UTIL para executar o comando a seguir:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Nesta política, o gerenciador de filas é identificado como BNK6. O nome da política e da fila associada é FIN.XFER.Q7. O algoritmo que é usado para gerar a assinatura do emissor é MD5 e o nome distinto (DN) do usuário de envio é 'CN=Teller5,O=BCO,C=US'.

Depois de definir a política, reinicie o gerenciador de filas BNK6 ou use o comando do z/OS **MODIFY** para atualizar a configuração de política do Advanced Message Security. Por exemplo:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Enfileiramento local de mensagens de privacidade protegida no z/OS*

Este exemplo detalha as políticas e os certificados do Advanced Message Security necessários para enviar e recuperar mensagens protegidas por privacidade para/de uma fila local para os aplicativos de colocação e obtenção. As mensagens de privacidade protegida são assinadas e criptografadas.

O exemplo do gerenciador de filas e a fila local são os seguintes:

```
BNK6        - Queue manager
FIN.XFER.Q8 - Local queue
```

Esses usuários são usados:

```
WMQBNK6  - AMS task user
TELLER5  - Sending user
FINADM2  - Recipient user
```

As etapas para configurar esse cenário são:

Criar os certificados de usuário

Nesse exemplo, dois certificados de usuário são necessários. Esses são certificados de usuário de envio que é necessário para assinar mensagens e o certificado de usuário destinatário, que é necessário

para criptografar e decriptografar os dados da mensagem. O usuário de envio é 'TELLER5' e o usuário destinatário é 'FINADM2'.

O certificado da autoridade de certificação (CA) também é necessário.O certificado de autoridade de certificação é o certificado da autoridade que emitiu o certificado de usuário. Isso pode ser uma cadeia de certificados. Se assim for, todos os certificados na cadeia são necessários no conjunto de chaves do usuário da tarefa do Advanced Message Security, neste caso o usuário WMQBNK6.

Um certificado de autoridade de certificação pode ser criado usando o comando RACDCERT do RACF. Este certificado é usado para emitir certificados de usuário. Por exemplo:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Este comando RACDCERT cria um certificado de autoridade de certificação que pode então ser usado para emitir certificados de usuário para os usuários TELLER5' e 'FINADM2'. Por exemplo:

```
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)
```

A instalação terá procedimentos para escolher ou criar um certificado de autoridade de certificação, bem como os procedimentos para emitir certificados e distribuí-los para sistemas relevantes.

Ao exportar e importar esses certificados, o Advanced Message Security requer:

- O certificado de autoridade de certificação (cadeia).
- O certificado de usuário de envio e sua chave privada.
- O certificado de usuário destinatário e sua chave privada.

Se você estiver usando o RACF, o comando RACDCERT EXPORT pode ser usado para exportar certificados para um conjunto de dados e o comando RACDCERT ADD pode ser usado para importar certificados do conjunto de dados. Para obter mais informações sobre esses e outros comandos RACDCERT, consulte RACDCERT (Gerenciar certificados digitais RACF) no *z/OS: Security Server RACF Command Language Reference*.

Os certificados nesse caso são necessários no sistema z/OS que está executando o gerenciador de filas BNK6.

Quando os certificados forem importados no sistema z/OS que estiver executando BNK6, os certificados de usuário irão requerer o atributo TRUST. O comando RACDCERT ALTER pode ser usado para incluir o atributo TRUST ao certificado. Por exemplo:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Conectar os certificados aos conjuntos de chaves relevantes

Quando os certificados necessários forem criados ou importados e definidos como confiáveis, eles devem ser conectados aos conjuntos de chaves apropriados do usuário no sistema z/OS que estiver executando o BNK6. Para criar os conjuntos de chaves use o comando RACDCERT ADDRING:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário da tarefa do Advanced Message Security e conjuntos de chaves para os usuários de envio e destinatário. Observe que o nome do conjunto de chaves drq.ams.keyring é obrigatório e o nome faz distinção entre maiúsculas e minúsculas.

Quando os conjuntos de chave forem criados, os certificados relevantes poderão ser conectados.

```
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))
```

Os certificados de usuário de envio e destinatário devem estar conectados como DEFAULT. Se qualquer usuário possuir mais de um certificado em seu drq.ams.keyring, o certificado padrão será usado para propósitos de assinatura e decriptografia.

O certificado de usuário destinatário deve também estar conectado ao conjunto de chaves do usuário de tarefa do Advanced Message Security com USAGE(SITE). Isso ocorre porque a tarefa Advanced Message Security precisa da chave pública do destinatário ao criptografar os dados da mensagem. O USAGE(SITE) impede a chave privada de ser acessível no conjunto de chaves.

A criação e modificação de certificados não é reconhecida pelo Advanced Message Security até que o gerenciador de filas seja parado e reiniciado ou o comando do z/OS **MODIFY** seja usado para atualizar a configuração de certificado do Advanced Message Security. Por exemplo:

```
F BNK6AMSM,REFRESH KEYRING
```

Criar a política do Advanced Message Security

Neste exemplo, as mensagens de privacidade protegida são colocadas na fila FIN.XFER.Q8 por um aplicativo em execução como o usuário 'TELLER5' e recuperadas a partir da mesma fila por um aplicativo em execução como o usuário 'FINADM2', portanto, apenas uma política do Advanced Message Security é necessária.

As políticas do Advanced Message Security são criadas usando o utilitário CSQ0UTIL, que está documentado em O utilitário de política de segurança da mensagem (CSQ0UTIL).

Use o utilitário CSQ0UTIL para executar o comando a seguir:

```
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
```

Nesta política, o gerenciador de filas é identificado como BNK6. O nome da política e a fila associada é FIN.XFER.Q8. O algoritmo que é usado para gerar a assinatura do emissor é SHA1, o nome distinto (DN) do usuário de envio é 'CN=Teller5,O=BCO,C=US' e o usuário do destinatário é 'CN=FinAdm2,O=BCO,C=US'. O algoritmo que é usado para criptografar os dados da mensagem é o 3DES.

Depois de definir a política, reinicie o gerenciador de filas BNK6 ou use o comando do z/OS **MODIFY** para atualizar a configuração de política do Advanced Message Security. Por exemplo:

```
F BNK6AMSM,REFRESH POLICY
```

z/OS *Enfileiramento remoto de mensagens de integridade protegida no z/OS*

Este exemplo detalha as políticas e certificados do Advanced Message Security necessários para enviar e recuperar mensagens de integridade protegida para e a partir de filas gerenciadas por dois gerenciadores

de filas diferentes. Os dois gerenciadores de filas podem estar em execução no mesmo sistema z/OS ou em diferentes sistemas z/OS ou um gerenciador de filas pode estar em um sistema distribuído executando o Advanced Message Security.

Os gerenciadores de filas e filas de exemplo são:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Nota: Para este exemplo, BNK6 e BNK7 são gerenciadores de filas em execução em diferentes sistemas z/OS.

Esses usuários são usados:

```
WMQBNK6  - AMS task user on BNK6
WMQBNK7  - AMStask user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

As etapas para configurar esse cenário são as seguintes:

Criar os certificados de usuário

Nesse exemplo, somente um certificado de usuário é necessário. Este é o certificado de usuário de envio que é necessário para assinar a mensagem de integridade protegida. O usuário de envio é 'TELLER5'.

O certificado da autoridade de certificação (CA) também é necessário.O certificado de autoridade de certificação é o certificado da autoridade que emitiu o certificado de usuário. Isso pode ser uma cadeia de certificados. Se assim for todos os certificados na cadeia são necessários no conjunto de chaves do usuário da tarefa do Advanced Message Security, neste caso o usuário WMQBNK7.

Um certificado de autoridade de certificação pode ser criado usando o comando RACDCERT do RACF. Este certificado é usado para emitir certificados de usuário. Por exemplo:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Este comando RACDCERT cria um certificado de autoridade de certificação que pode então ser usado para emitir certificados de usuário para o usuário 'TELLER5'. Por exemplo:

```
RACDCERT ID(TELLER5) GENCERT SUBJECTSDN(CN('Teller5') O('BCO') C('US'))
WITHLABEL('Teller5') SIGNWITH(CERTAUTH LABEL('BCOCA'))
KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)
```

A instalação terá procedimentos para escolher ou criar um certificado de autoridade de certificação, bem como os procedimentos para emitir certificados e distribuí-los para sistemas relevantes.

Ao exportar e importar esses certificados, o Advanced Message Security requer:

- O certificado de autoridade de certificação (cadeia).
- O certificado de usuário de envio e sua chave privada.

Se você estiver usando o RACF, o comando RACDCERT EXPORT pode ser usado para exportar certificados para um conjunto de dados e o comando RACDCERT ADD pode ser usado para importar certificados do conjunto de dados. Para obter mais informações sobre esses e outros comandos RACDCERT, consulte RACDCERT (Gerenciar certificados digitais RACF) no *z/OS: Security Server RACF Command Language Reference*.

Os certificados, neste caso, são necessários no sistema z/OS que está executando o gerenciador de filas BNK6 e BNK7.

Neste exemplo, o certificado de envio deve ser importado para o sistema z/OS que está executando o BNK6 e o certificado CA deve ser importado para o sistema z/OS que está executando o BNK7. Quando os certificados forem importados, o certificado de usuário irá requer o atributo TRUST. O comando RACDCERT ALTER pode ser usado para incluir o atributo TRUST ao certificado. Por exemplo, no BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
```

Conectar os certificados aos conjuntos de chaves relevantes

Quando os certificados necessários foram criados ou importados e definidos como confiáveis, eles devem ser conectados aos conjuntos de chaves apropriados do usuário no sistema z/OS que está executando BNK6 e BNK7.

Para criar os conjuntos de chaves use o comando RACDCERT ADDRING, no BNK6:

```
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário de envio no BNK6. Observe que o nome do conjunto de chaves drq.ams.keyring é obrigatório e o nome faz distinção entre maiúsculas e minúsculas.

No BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário da tarefa do Advanced Message Security no BNK7. Nenhum conjunto de chaves do usuário é necessário para 'TELLER5' no BNK7.

Quando os conjuntos de chave forem criados, os certificados relevantes poderão ser conectados.

No BNK6:

```
RACDCERT ID(TELLER5) CONNECT(ID(TELLER5) LABEL('Teller5')
RING(drq.ams.keyring) DEFAULT USAGE(PERSONAL))
```

No BNK7:

```
RACDCERT ID(WMQBNK7) CONNECT(CERTAUTH LABEL('BCOCA')
RING(drq.ams.keyring))
```

O certificado de usuário de envio deve estar conectado como DEFAULT. Se o usuário de envio possui mais de um certificado em seu drq.ams.keyring, o certificado padrão é usado para fins de assinatura.

A criação e modificação de certificados não é reconhecida pelo Advanced Message Security até que o gerenciador de filas seja parado e reiniciado ou o comando do z/OS **MODIFY** seja usado para atualizar a configuração de certificado do Advanced Message Security. Por exemplo:

No BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

No BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Criar as políticas do Advanced Message Security

Neste exemplo, as mensagens de integridade protegida são colocadas na fila remota FIN.XFER.Q7 no BNK6 por um aplicativo em execução como o usuário 'TELLER5' e recuperadas a partir da fila local FIN.RCPT.Q7 no BNK7 por um aplicativo em execução como o usuário 'FINADM2', portanto, duas políticas do Advanced Message Security são necessárias.

As políticas do Advanced Message Security são criadas usando o utilitário CSQ0UTIL, que está documentado em O utilitário de política de segurança da mensagem (CSQ0UTIL).

Use o utilitário CSQ0UTIL para executar o comando a seguir para definir uma política de integridade para a fila remota no BNK6:

```
setmqspl -m BNK6 -p FIN.XFER.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Nesta política, o gerenciador de filas é identificado como BNK6. O nome da política e da fila associada é FIN.XFER.Q7. O algoritmo que é usado para gerar a assinatura do emissor é MD5 e o nome distinto (DN) do usuário de envio é 'CN=Teller5,O=BCO,C=US'.

Além disso, use o utilitário CSQ0UTIL para executar o comando a seguir para definir uma política de integridade para a fila local no BNK7:

```
setmqspl -m BNK7 -p FIN.RCPT.Q7 -s MD5 -a CN=Teller5,O=BCO,C=US
```

Nesta política, o gerenciador de filas é identificado como BNK7. O nome da política e da fila associada é FIN.RCPT.Q7. O algoritmo esperado para a assinatura do emissor é MD5 e é esperado que o nome distinto (DN) do usuário de envio seja 'CN=Teller5,O=BCO,C=US'.

Depois de definir as duas políticas, reinicie os gerenciadores de filas BNK6 e BNK7 ou use o comando do z/OS **MODIFY** para atualizar as configurações de política do Advanced Message Security. Por exemplo:

No BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

No BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

z/OS *Enfileiramento remoto de mensagens de privacidade protegida no z/OS*

Este exemplo detalha as políticas e certificados do Advanced Message Security necessários para enviar e recuperar mensagens de privacidade protegida para e a partir de filas gerenciadas por dois gerenciadores de filas diferentes. Os dois gerenciadores de filas podem estar em execução no mesmo sistema z/OS ou em diferentes sistemas z/OS ou um gerenciador de filas pode estar em um sistema distribuído executando o Advanced Message Security.

Os gerenciadores de filas e filas de exemplo são:

```
BNK6        - Sending queue manager
BNK7        - Recipient queue manager
FIN.XFER.Q7 - Remote queue on BNK6
FIN.RCPT.Q7 - Local queue on BNK7
```

Nota: Para este exemplo, BNK6 e BNK7 são gerenciadores de filas em execução em diferentes sistemas z/OS com o mesmo nome.

Esses usuários são usados:

```
WMQBNK6  - AMS task user on BNK6
```

```
WMQBNK7  - AMS task user on BNK7
TELLER5  - Sending user on BNK6
FINADM2  - Recipient user on BNK7
```

As etapas para configurar esse cenário são as seguintes:

Criar os certificados de usuário

Nesse exemplo, dois certificados de usuário são necessários. Esses são certificados de usuário de envio que é necessário para assinar mensagens e o certificado de usuário destinatário, que é necessário para criptografar e decriptografar os dados da mensagem. O usuário de envio é 'TELLER5' e o usuário destinatário é 'FINADM2'.

O certificado da autoridade de certificação (CA) também é necessário.O certificado de autoridade de certificação é o certificado da autoridade que emitiu o certificado de usuário. Isso pode ser uma cadeia de certificados. Se assim for todos os certificados na cadeia são necessários no conjunto de chaves do usuário da tarefa do Advanced Message Security, neste caso o usuário WMQBNK7.

Um certificado de autoridade de certificação pode ser criado usando o comando RACDCERT do RACF. Este certificado é usado para emitir certificados de usuário. Por exemplo:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('BCOCA') O('BCO') C('US'))
KEYUSAGE(CERTSIGN) WITHLABEL('BCOCA')
```

Este comando RACDCERT cria um certificado de autoridade de certificação que pode então ser usado para emitir certificados de usuário para os usuários TELLER5' e 'FINADM2'. Por exemplo:

```
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)
```

A instalação terá procedimentos para escolher ou criar um certificado de autoridade de certificação, bem como os procedimentos para emitir certificados e distribuí-los para sistemas relevantes.

Ao exportar e importar esses certificados, o Advanced Message Security requer:

- O certificado de autoridade de certificação (cadeia).
- O certificado de usuário de envio e sua chave privada.
- O certificado de usuário destinatário e sua chave privada.

Se você estiver usando o RACF, o comando RACDCERT EXPORT pode ser usado para exportar certificados para um conjunto de dados e o comando RACDCERT ADD pode ser usado para importar certificados do conjunto de dados.

Para obter mais informações sobre esses e outros comandos RACDCERT, consulte RACDCERT (Gerenciar certificados digitais RACF) no *z/OS: Security Server RACF Command Language Reference*.

Os certificados, neste caso, são necessários no sistema z/OS que está executando o gerenciador de filas BNK6 e BNK7.

Neste exemplo, os certificados de envio e destinatário devem ser importados no sistema z/OS que está executando o BNK6 e os certificados de CA e destinatário devem ser importados no sistema z/OS que está executando o BNK7. Quando os certificados forem importados, os certificados de usuário irão requerer o atributo TRUST. O comando RACDCERT ALTER pode ser usado para incluir o atributo TRUST ao certificado. Por exemplo:

No BNK6:

```
RACDCERT ID(TELLER5) ALTER (LABEL('Teller5')) TRUST
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

No BNK7:

```
RACDCERT ID(FINADM2) ALTER (LABEL('FinAdm2')) TRUST
```

Conectar os certificados aos conjuntos de chaves relevantes

Quando os certificados necessários forem criados ou importados e definidos como confiáveis, eles devem ser conectados aos conjuntos de chaves apropriados do usuário nos sistemas z/OS que estão executando BNK6 e BNK7.

Para criar os conjuntos de chaves use o comando RACDCERT ADDRING:

No BNK6:

```
RACDCERT ID(WMQBNK6) ADDRING(drq.ams.keyring)
RACDCERT ID(TELLER5) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário da tarefa do Advanced Message Security e um conjunto de chaves para o usuário de envio no BNK6. Observe que o nome do conjunto de chaves drq.ams.keyring é obrigatório e o nome faz distinção entre maiúsculas e minúsculas.

No BNK7:

```
RACDCERT ID(WMQBNK7) ADDRING(drq.ams.keyring)
RACDCERT ID(FINADM2) ADDRING(drq.ams.keyring)
```

Isso cria um conjunto de chaves para o usuário da tarefa do Advanced Message Security e um conjunto de chaves para o destinatário do usuário no BNK7.

Quando os conjuntos de chave forem criados, os certificados relevantes poderão ser conectados.

No 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))
```

No 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))
```

Os certificados de usuário de envio e destinatário devem estar conectados como DEFAULT. Se qualquer usuário possui mais de um certificado em seu drq.ams.keyring, o certificado padrão é usado para propósitos de assinatura e criptografia/decriptografia.

No BNK6, o certificado de usuário destinatário também deve estar conectado ao conjunto de chaves do usuário da tarefa do Advanced Message Security com USAGE(SITE). Isso ocorre porque a tarefa Advanced Message Security precisa da chave pública do destinatário ao criptografar os dados da mensagem. O USAGE(SITE) impede a chave privada de ser acessível no conjunto de chaves.

A criação e modificação de certificados não é reconhecida pelo Advanced Message Security até que o gerenciador de filas seja parado e reiniciado ou o comando do z/OS **MODIFY** seja usado para atualizar a configuração de certificado do Advanced Message Security. Por exemplo:

No BNK6:

```
F BNK6AMSM,REFRESH,KEYRING
```

No BNK7:

```
F BNK7AMSM,REFRESH,KEYRING
```

Criar as políticas do Advanced Message Security

Neste exemplo, as mensagens de privacidade protegida são colocadas na fila remota FIN.XFER.Q7 no BNK6 por um aplicativo em execução como usuário o 'TELLER5' e recuperadas da fila local FIN.RCPT.Q7 no BNK7 por um aplicativo em execução como o usuário 'FINADM2', portanto, duas políticas do Advanced Message Security são necessárias.

As políticas do Advanced Message Security são criadas usando o utilitário CSQ0UTIL, que está documentado em O utilitário de política de segurança da mensagem (CSQ0UTIL).

Use o utilitário CSQ0UTIL para executar o comando a seguir para definir uma política de privacidade para a fila remota no 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
```

Nesta política, o gerenciador de filas é identificado como BNK6. O nome da política e da fila associada é FIN.XFER.Q7. O algoritmo que é usado para gerar a assinatura do emissor é SHA1, o nome distinto (DN) do usuário de envio é 'CN=Teller5,O=BCO,C=US' e o usuário destinatário é 'CN=FinAdm2,O=BCO,C=US'. O algoritmo que é usado para criptografar os dados da mensagem é o 3DES.

Além disso, use o utilitário CSQ0UTIL para executar o comando a seguir para definir uma política de privacidade para a fila local no 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
```

Nesta política, o gerenciador de filas é identificado como BNK7. O nome da política e da fila associada é FIN.RCPT.Q7. O algoritmo esperado para a assinatura do emissor é SHA1, é esperado que o nome distinto (DN) do usuário de envio seja 'CN=Teller5,O=BCO,C=US' e o usuário destinatário é 'CN=FinAdm2,O=BCO,C=US'. O algoritmo que é usado para decriptografar os dados da mensagem é o 3DES.

Depois de definir as duas políticas, reinicie os gerenciadores de filas BNK6 e BNK7 ou use o comando do z/OS **MODIFY** para atualizar a configuração de política do Advanced Message Security. Por exemplo:

No BNK6:

```
F BNK6AMSM,REFRESH,POLICY
```

No BNK7:

```
F BNK7AMSM,REFRESH,POLICY
```

Guia de iniciação rápida para o AMS com os clientes Java

Use este guia para configurar rapidamente o Advanced Message Security para fornecer segurança de mensagens para aplicativos do Java conectando usando ligações do cliente. No momento em que você concluir, você terá criado um armazenamento de chaves para verificar identidades do usuário e definido políticas de assinatura/criptografia para o seu gerenciador de filas.

Antes de começar

Assegure-se de que você tenha os componentes apropriados instalados conforme descrito no **Guia de Iniciação Rápida** (Windows ou UNIX).

1. Criando um gerenciador de filas e uma fila

Sobre esta tarefa

Todos os exemplos a seguir usam uma fila nomeada TEST.Q para passar mensagens entre aplicativos. Advanced Message Security usa interceptores para assinar e criptografar mensagens no ponto em que elas entram na estrutura IBM MQ através da interface padrão do IBM MQ. A configuração básica é feita no IBM MQ e é configurada nas etapas a seguir.

Procedimento

1. Crie um gerenciador de filas

```
crtmqm QM_VERIFY_AMS
```

2. Iniciar o Gerenciador de Filas

```
strmqm QM_VERIFY_AMS
```

3. Crie e inicie um listener inserindo os comandos a seguir no **runmqsc** para o gerenciador de filas QM_VERIFY_AMS

```
DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
START LISTENER(AMS.LSTR)
```

4. Crie um canal para os nossos aplicativos para se conectar inserindo o comando a seguir em **runmqsc** para o gerenciador de filas QM_VERIFY_AMS

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. Crie uma fila chamada TEST.Q inserindo o comando a seguir em **runmqsc** para o gerenciador de filas QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Resultados

Se o procedimento concluiu com sucesso, o comando a seguir inserido em **runmqsc** exibe detalhes sobre TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Criando e autorizando usuários

Sobre esta tarefa

Há dois usuários que aparecem neste cenário: `alice`, o emissor e bob, o receptor. Para usar a fila do aplicativo, esses usuários precisam receber autoridade para usá-la. Além disso, para usar com sucesso as políticas de proteção definidas neste cenário, esses usuários devem ser concedidos acesso a algumas filas do sistema. Para obter mais informações sobre o comando **setmqaut**, consulte **setmqaut**.

Procedimento

1. Crie os dois usuários conforme descrito no **Guia de iniciação rápida** (Windows ou UNIX) para sua plataforma.
2. Autorize os usuários para se conectarem ao gerenciador de filas e para trabalhar com a fila

```
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. É necessário também permitir que os dois usuários naveguem na fila de políticas do sistema e coloquem mensagens na fila de erros.

```
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
```

Atenção: O IBM MQ otimiza o desempenho armazenando em cache políticas para que você não tenha que procurar registros para obter detalhes da política no SYSTEM.PROTECTION.POLICY.QUEUE em todos os casos..

O IBM MQ não armazena em cache todas as políticas disponíveis. Se houver um grande número de políticas, o IBM MQ armazenará em cache um número limitado de políticas. Portanto, se o gerenciador de filas tiver um número baixo de políticas definidas, não haverá a necessidade de fornecer a opção de navegação para o SYSTEM.PROTECTION.POLICY.QUEUE.

No entanto, é necessário dar autoridade de navegação a essa fila nos casos em que há um grande número de políticas definidas ou quando você está usando clientes antigos. O SYSTEM.PROTECTION.ERROR.QUEUE é usado para colocar mensagens de erro geradas pelo código AMS. A autoridade put para essa fila é verificada apenas quando você tenta colocar uma mensagem de erro na fila. Sua autoridade put em relação à fila não é verificada quando você tenta colocar ou obter mensagens de uma fila protegida por AMS.

Resultados

Os usuários agora são criados e as autoridades necessárias concedidas a eles.

Como proceder a seguir

Para verificar se as etapas foram realizadas corretamente, use as amostras `JmsProducer` e `JmsConsumer` conforme descrito na seção “7. Testando a configuração” na página 606.

3. Criando banco de dados de chaves e certificados

Sobre esta tarefa

Para criptografar a mensagem para o interceptor requer a chave pública dos usuários de envio. Portanto, o banco de dados de chaves das identidades do usuário mapeado para chaves pública e privada deve ser criado. No sistema real, no qual os usuários e aplicativos são dispersos por meio de vários computadores, cada usuário teria seu próprio keystore. Da mesma forma, nesse guia, criamos banco de dados de chaves para `alice` e bob e compartilhamos os certificados de usuário entre eles.

Nota: Neste guia, podemos usar os aplicativos de amostra escritos em Java conectando usando as ligações de cliente. Se você planeja usar os aplicativos Java usando ligações locais ou aplicativos C, deve-se criar um keystore CMS e certificados usando o comando **runmqakm**. Isso é mostrado no **Guia de iniciação rápida** (Windows ou UNIX).

Procedimento

1. Crie um diretório no qual criar seu keystore, por exemplo `/home/alice/.mqs`. Você pode desejar criá-lo no mesmo diretório usado pelo **Guia de iniciação rápida** (Windows ou UNIX) para a sua plataforma.

   Nota: Esse diretório é referido como *keystore-dir* nas etapas a seguir
2. Crie um novo keystore e o certificado que identifica o usuário `alice` para uso na criptografia

   Nota: O comando **keytool** é parte do 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
   ```

   Nota:

   - Se o *keystore-dir* contiver espaços, deve-se colocar entre aspas ao redor o nome completo de seu keystore
   - É aconselhável usar uma senha forte para proteger o keystore.
   - Para o propósito desse guia, estamos usando certificado autoassinado que pode ser criado sem o uso de uma Autoridade de Certificação. Para sistemas de produção, é aconselhável não usar certificados autoassinados, mas em vez disso contar com certificados assinados por uma Autoridade de certificação.
   - O parâmetro **alias** especifica o nome para o certificado, que os interceptores consultarão para receber as informações necessárias.
   - O parâmetro **dname** especifica os detalhes do **Nome Distinto** (DN), que deve ser exclusivos para cada usuário.
3. No UNIX, assegure-se de que o keystore esteja legível

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Repita as etapas 1-4 para o usuário bob

Resultados

Os dois usuários `alice` e bob agora possuem cada um certificado autoassinado.

4. Criando keystore.conf

Sobre esta tarefa

Deve-se apontar os interceptores do Advanced Message Security para o diretório no qual os bancos de dados de chave e certificados estão localizados. Isso é feito por meio do arquivo `keystore.conf`, que retém essas informações em texto sem formatação. Cada usuário deve ter um arquivo `keystore.conf` separado. Esta etapa deve ser feita para ambos `alice` e bob.

Exemplo

Para este cenário, os conteúdos do `keystore.conf` para `alice` são os seguintes:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
```

```
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Para este cenário, os conteúdos do `keystore.conf` para bob são os seguintes:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Nota:

- O caminho para o arquivo keystore deve ser fornecido sem extensão de arquivo.
- Se você já tiver um arquivo `keystore.conf` porque seguiu as instruções no Guia de iniciação rápida (Windows ou UNIX), será possível editar o arquivo existente para incluir essas linhas.
- Para obter informações adicionais, consulte "Estrutura do arquivo de configuração do keystore (keystore.conf) para AMS" na página 615.

5. Compartilhando os certificados

Sobre esta tarefa

Compartilhe os certificados entre os dois keystores para que cada usuário pode identificar com sucesso o outro. Isso é feito extraindo cada certificado do usuário e importando-o para o keystore do outro usuário.

Nota: Os termos *extract* e *export* são usados de forma diferente por ferramentas de certificado diferentes. Por exemplo, a ferramenta de comando IBM GSKit **strmqikm** (ikeyman) faz uma distinção entre *extrair* certificados (chaves públicas) e *exportar* chaves privadas. Essa distinção é extremamente importante para ferramentas que oferecem ambas as opções, pois usar *export* por engano comprometeria completamente o seu aplicativo, transmitindo a sua chave privada. Como a distinção é tão importante, a documentação do IBM MQ esforça-se para usar esses termos de forma consistente. No entanto, a keytool do Java fornece uma opção da linha de comandos denominada *exportcert* que extrai apenas a chave pública. Por esses motivos, o procedimento a seguir refere-se a *extrair* certificados usando a opção *exportcert*.

Procedimento

1. Extraia o certificado que identifica `alice`.

   ```
   keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
   -alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
   ```

2. Importe o certificado identificando `alice` no keystore que bob usará. Quando solicitado indique que você irá confiar nesse certificado.

   ```
   keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
   -keystore bob-keystore-dir/keystore.jks -storepass passw0rd
   ```

3. Repita as etapas para bob

Resultados

Os dois usuários, `alice` e bob, agora podem identificar um ao outro com êxito como tendo criado e compartilhado certificados autoassinados.

Como proceder a seguir

Verifique se o certificado está no keystore executando os comandos a seguir que imprimem seus detalhes:

```
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. Definindo a política de filas

Sobre esta tarefa

Com o gerenciador de filas criado e os interceptores preparados para interceptar mensagens e acessar chaves de criptografia, podemos começar a definir políticas de proteção no QM_VERIFY_AMS usado o comando `setmqspl`. Consulte setmqspl para obter mais informações sobre este comando. Cada nome da política deve ser o mesmo que o nome da fila para a qual ela deve ser aplicada.

Exemplo

Este é um exemplo de uma política definida na fila TEST.Q, assinada pelo usuário `alice` usando o algoritmo SHA1 e criptografada usando o algoritmo 256-bit AES para o usuário 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"
```

Nota: Os DNs correspondem exatamente aos especificados no respectivo certificado do usuário do banco de dados de chaves.

Como proceder a seguir

Para verificar a política que você definiu, emita o comando a seguir:

```
dspmqspl -m QM_VERIFY_AMS
```

Para imprimir os detalhes da política como um conjunto de comandos `setmqspl`, o sinalizador `-export`. Isso permite armazenar políticas já definidas:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Testando a configuração

Antes de começar

Assegure-se de que a versão do Java que você está usando possui os arquivos de políticas JCE sem restrição instalados.

Nota: A versão do Java fornecida na instalação do IBM MQ já possui esses arquivos de políticas. Ela pode ser localizada em *MQ_INSTALLATION_PATH*`/java/bin`.

Sobre esta tarefa

Ao executar programas diferentes em diferentes usuários é possível verificar se o aplicativo foi configurado corretamente. Consulte o **Guia de iniciação rápida** (Windows ou UNIX) para sua plataforma, para obter detalhes sobre execução de programas sob diferentes usuários.

Procedimento

1. Para executar estes aplicativos de amostra do JMS, use a configuração de CLASSPATH para sua plataforma conforme mostrado em Variáveis de ambiente usadas pelo IBM MQ classes for JMS para assegurar que o diretório de amostras está incluído.
2. Como o usuário `alice`, coloque uma mensagem usando um aplicativo de amostra, se conectando como um cliente:

```
java JmsProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

3. Como o usuário bob, obtenha uma mensagem usando um aplicativo de amostra, se conectando como um cliente:

```
java JmsConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
```

Resultados

Se o aplicativo foi configurado corretamente para ambos os usuários, a mensagem do usuário `alice` será exibida quando o bob executar o aplicativo de obtenção.

Protegendo filas remotas

Para proteger completamente as filas remotas, as políticas devem ser configuradas na fila remota e na fila local para a qual as mensagens são transmitidas.

Quando uma mensagem é colocada em uma fila remota, o Advanced Message Security intercepta a operação e processa a mensagem de acordo com a política configurada para a fila remota. Por exemplo, para uma política de criptografia a mensagem é criptografada antes de ser transmitida para que o IBM MQ a manuseie. Depois que Advanced Message Security tiver processado a mensagem colocada em uma fila remota, o IBM MQ a colocará em uma fila de transmissão associada e a redirecionará para o gerenciador de filas de destino e para a fila de destino.

Quando uma operação GET for executada na fila local, o Advanced Message Security tentará decodificar a mensagem de acordo com a política configurada na fila local. Para que a operação seja bem-sucedida, a política usada para decriptografar a mensagem deve ser idêntica à que foi usada para criptografá-la. Qualquer discrepância fará com que a mensagem seja rejeitada.

Se, por algum motivo ambas as políticas não puderem ser configuradas ao mesmo tempo, um suporte ao lançamento em estágios será fornecido. A política pode ser configurada em uma fila local com o sinalizador de tolerância ligado, o que indica que uma política associada a uma fila pode ser ignorada quando uma tentativa de recuperar uma mensagem da fila envolve uma mensagem que não possui o conjunto de política de segurança. Neste caso, GET tentará decriptografar a mensagem, mas permitirá que as mensagens não criptografadas sejam entregues. Dessa maneira as políticas em filas remotas podem ser configuradas após a filas locais terem sido protegidas (e testadas).

Não se esqueça: Remova o sinalizador de tolerância quando a apresentação do Advanced Message Security for concluída.

Referências relacionadas

setmqspl (configurar política de segurança)

Roteando as mensagens protegidas usando o IBM Integration Bus

O Advanced Message Security pode proteger mensagens em uma infraestrutura na qual o IBM Integration Bus ou WebSphere Message Broker 8.0.0.1 (ou mais recente) é instalado. É necessário entender a natureza de ambos os produtos antes de aplicar a segurança no ambiente do IBM Integration Bus.

Sobre esta tarefa

O Advanced Message Security fornece segurança de ponta a ponta da carga útil da mensagem. Isso significa que apenas as partes especificadas como emissores e destinatários válidos de uma mensagem são capazes de produzir ou recebê-la. Isto significa que, a fim de proteger as mensagens que fluem por meio do IBM Integration Bus, é possível permitir que o IBM Integration Bus processe mensagens sem saber seu conteúdo (Cenário 1) ou torná-lo um usuário autorizado capaz de receber e enviar mensagens (Cenário 2).

Antes de começar

É necessário ter seu IBM Integration Bus conectado a um gerenciador de filas existente. Substitua *QMgrName* com esse nome do gerenciador de filas existente nos comandos a seguir.

Sobre esta tarefa

Neste cenário, Alice coloca uma mensagem protegida em uma fila de entrada `QIN`. Com base na propriedade da mensagem `routeTo`, a mensagem é roteada para *bob's* (`QBOB`),[1](`QCECIL`), ou a fila padrão (`QDEF`). O roteamento é possível porque o Advanced Message Security protege apenas a carga útil da mensagem e não seus cabeçalhos e propriedades, que permanecem desprotegidos e podem ser lidos pelo IBM Integration Bus. O Advanced Message Security é usado somente por *alice*, *bob* e *cecil*. Não é necessário instalar ou configurar para o IBM Integration Bus.

O IBM Integration Bus recebe a mensagem protegida da fila de alias não protegido para evitar qualquer tentativa de decriptografar a mensagem. Se fosse usar a fila protegida diretamente a mensagem seria colocada na fila DEAD LETTER como impossível de decriptografar. A mensagem é roteada pelo IBM Integration Bus e chega na fila de destino inalterada. Portanto, ela continua assinada pelo autor original (ambos *bob* e *cecil* aceitam somente mensagens enviadas por *alice*) e protegida como antes (somente *bob* e *cecil* pode lê-la). O IBM Integration Bus coloca a mensagem roteada em um alias desprotegido. Os destinatários recuperam a mensagem a partir de uma fila de saída protegida em que AMS decriptografará a mensagem de modo transparente.

Procedimento

1. Configure *alice*, *bob* e *cecil* para usar o Advanced Message Security conforme descrito no **Guia de iniciação rápida** (Windows ou UNIX).

   Assegure-se de que as etapas a seguir sejam concluídas:

   - Criando e autorizando usuários
   - Criando banco de dados de chaves e certificados
   - Criando keystore.conf

2. Forneça o certificado da *alice* para *bob* e *cecil* para que *alice* possa ser identificada por eles ao verificarem assinaturas digitais em mensagens.

   Faça isso extraindo o certificado que identifica *alice* em um arquivo externo e, em seguida, incluindo o certificado extraído nos keystores *do bob* e *da cecil*. É importante que você use o método descrito na **Tarefa 5. Compartilhando certificados** no **Guia de Iniciação Rápida** (Windows ou UNIX).

3. Forneça os certificados de *bob* e *do cecil* para *alice*, para que *alice* possa enviar mensagens criptografadas para *bob* e *cecil*.

   Faça isso usando o método especificado na etapa anterior.

4. Em seu gerenciador de filas, defina as filas locais chamadas `QIN`, `QBOB`, `QCECIL` e `QDEF`.

   ```
   DEFINE QLOCAL(QIN)
   ```

5. Configure a política de segurança para a fila `QIN` para uma configuração elegível. Use a configuração idêntica para as filas `QBOB`, `QCECIL` e `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"
   ```

   Este cenário supõe a política de segurança na qual *alice* é o único emissor autorizado e *bob* e *cecil* são os destinatários.

[1] cecil's

6. Defina as filas de alias AIN, ABOB e ACECIL fazendo referência à filas locais QIN, QBOB e QCECIL respectivamente.

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. Verifique se a configuração de segurança para o alias especificado na etapa anterior não está presente; caso contrário, defina sua política para NONE.

```
dspmqspl -m QMgrName -p AIN
```

8. No IBM Integration Bus crie um fluxo de mensagens para rotear as mensagens que chegam na fila de alias AIN para os nós BOB, CECIL ou DEF, dependendo da propriedade routeTo da mensagem. Para fazê-lo:
   a) Crie um nó MQInput chamado IN e designe o alias AIN como seu nome da fila.
   b) Crie nós MQOutput chamados BOB, CECIL e DEF e designe filas de alias ABOB, ACECIL e ADEF como seus respectivos nomes de filas.
   c) Crie um nó de rota e chame-o TEST.
   d) Conecte o nó IN ao terminal de entrada do nó TEST.
   e) Crie os terminais de saída bob e cecil para o nó TEST.
   f) Conecte o terminal de saída bob ao nó BOB.
   g) Conecte o terminal de saída cecil ao nó CECIL.
   h) Conecte o nó DEF para o terminal de saída padrão.
   i) Aplique as regras a seguir:

```
$Root/MQRFH2/usr/routeTo/text()="bob"
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. Implemente o fluxo de mensagens para o componente de tempo de execução do IBM Integration Bus.
10. Executando como o usuário Alice, coloque uma mensagem que também contém uma propriedade de mensagem chamada routeTo com um valor de bob ou cecil. Executar o aplicativo de amostra **amqsstm** permitirá que você faça isso.

```
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. Executando como o usuário *bob*, recupere a mensagem da fila QBOB usando o aplicativo de amostra **amqsget**.

Resultados

Quando *alice* colocar uma mensagem na fila QIN a mensagem será protegida. Ela é recuperada em forma protegida pelo IBM Integration Bus a partir da fila de alias AIN. O IBM Integration Bus decide para onde rotear a mensagem ao ler a propriedade routeTo que é, como todas as propriedades, não criptografada. O IBM Integration Bus coloca a mensagem no alias desprotegido, evitando sua proteção adicional. Quando recebida por *bob* ou *cecil* da fila, a mensagem será decriptografada e a assinatura digital será verificada.

Cenário 2 - O Integration Bus pode ver o conteúdo da mensagem

Sobre esta tarefa

Neste cenário, um grupo de indivíduos têm permissão para enviar mensagens para o IBM Integration Bus. Outro grupo está autorizado a receber mensagens que são criadas pelo IBM Integration Bus. A transmissão entre as partes e o IBM Integration Bus não pode ser espionada do tráfego de rede.

Lembre-se de que o IBM Integration Bus lê as políticas de proteção e certificados somente quando uma fila for aberta, portanto deve-se recarregar o grupo de execução após fazer quaisquer atualizações para as políticas de proteção para que as mudanças entrem em vigor.

```
mqsireload execution-group-name
```

Se o IBM Integration Bus for considerado uma parte autorizada com permissão para ler ou assinar a carga útil da mensagem, deve-se configurar o Advanced Message Security para o usuário que inicia o serviço do IBM Integration Bus. Esteja ciente de que ele não é necessariamente o mesmo usuário que coloca/obtém as mensagens nas filas nem o usuário que cria e implementa os aplicativos do IBM Integration Bus.

Procedimento

1. Configure *alice*, *bob*, *cecil* e *dave* e o usuário do serviço IBM Integration Bus para usar o Advanced Message Security conforme descrito no **Guia de iniciação rápida** (Windows ou UNIX).

   Assegure-se de que as etapas a seguir sejam concluídas:

   - Criando e autorizando usuários
   - Criando banco de dados de chaves e certificados
   - Criando keystore.conf
2. Forneça os certificados de *alice*, *bob*, *cecil* e *dave* ao usuário do serviço do IBM Integration Bus.

   Faça isso extraindo cada um dos certificados que identificam *alice*, *bob*, *cecil* e *dave* em arquivos externos e, em seguida, incluindo os certificados extraídos no keystore do IBM Integration Bus. É importante que você use o método descrito na **Tarefa 5. Compartilhando certificados** no **Guia de Iniciação Rápida** (Windows ou UNIX).
3. Forneça certificado de usuário de serviço do IBM Integration Bus para *alice*, *bob*, *cecil* e *dave*.

   Faça isso usando o método especificado na etapa anterior.

   Nota: *alice* e *bob* precisam do certificado de usuário do serviço do IBM Integration Bus para criptografar as mensagens corretamente. O usuário do serviço do IBM Integration Bus precisa dos certificados de *alice* e *bob* para verificar os autores das mensagens. O usuário do serviço do IBM Integration Bus precisa dos certificados de *cecil* e *dave* para criptografar as mensagens para eles. *cecil* e *dave* precisam do certificado de usuário do serviço do IBM Integration Bus para verificar se a mensagem vem do IBM Integration Bus.
4. Defina uma fila local denominada `IN` e defina a política de segurança com *alice* e *bob* especificados como autores e o usuário do serviço para o IBM Integration Bus especificado como destinatário:

   ```
   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. Defina uma fila local denominada `OUT` e defina a política de segurança com o usuário do serviço para o IBM Integration Bus especificado como autor e *cecil* e *dave* especificados como destinatários:

   ```
   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. No IBM Integration Bus crie um fluxo de mensagens com um nó `MQInput` e `MQOutput`. Configure o nó `MQInput` para usar a fila `IN` e o nó `MQOutput` para usar a fila `OUT`.
7. Implemente o fluxo de mensagens para o componente de tempo de execução do IBM Integration Bus.

8. Executando como os usuários *alice* ou *bob*, coloque uma mensagem na fila `IN` usando o aplicativo de amostra **amqsput**.
9. Executando como os usuários *cecil* ou *dave*, recupere a mensagem da fila `OUT` usando o aplicativo de amostra **amqsget**.

Resultados

As mensagens enviadas por *alice* ou *bob* para a fila de entrada `IN` são criptografadas, permitindo que somente o IBM Integration Bus as leia. O IBM Integration Bus aceita somente mensagens de *alice* e *bob* e rejeita quaisquer outras. As mensagens aceitas são processadas adequadamente e, em seguida, assinadas e criptografadas com as chaves de *cecil* e *dave* antes de serem colocadas na fila de saída `OUT`. Somente *cecil* e *dave* são capazes de ler, as mensagens não assinadas pelo IBM Integration Bus são rejeitadas.

Usando o Advanced Message Security com o Managed File Transfer

Este cenário explica como configurar o Advanced Message Security para fornecer privacidade de mensagem para dados que estão sendo enviados por meio de um Managed File Transfer.

Antes de começar

Assegure-se de que você tenha o componente Advanced Message Security instalado na instalação do IBM MQ que hospeda as filas usadas pelo Managed File Transfer que deseja proteger.

Se os agentes do Managed File Transfer estiverem se conectando no modo de ligações, assegure-se de ter o componente GSKit instalado em sua instalação local.

Sobre esta tarefa

Quando a transferência de dados entre dois agentes do Managed File Transfer for interrompida, dados possivelmente confidenciais poderão permanecer desprotegido nas filas do IBM MQ subjacentes usadas para gerenciar a transferência. Este cenário explica como configurar e usar o Advanced Message Security para proteger tais dados no Managed File Transfer.

Nesse cenário, consideramos uma topologia simples composta por uma máquina com duas Managed File Transfer filas e dois agentes, `AGENT1` e `AGENT2`, compartilhando um único gerenciador de filas, conforme descrito no cenário Visão geral do cenário. Ambos os agentes se conectam da mesma maneira, no modo de ligações ou no modo cliente.

1. Criando certificados

Antes de começar

Este cenário usa um modelo simples em que um usuário `ftagent` em um grupo FTAGENTS é usado para executar os processos do Managed File Transfer Agent. Se você estiver usando os seus próprios nomes do usuário e do grupo, mude os comandos de modo correspondente.

Sobre esta tarefa

O Advanced Message Security usa a criptografia de chave pública para assinar e/ou criptografar mensagens em filas protegidas.

Nota:

- Se os seus agentes do Managed File Transfer estiverem em execução em modo de ligações, os comandos que você usar para criar um keystore do CMS (Cryptographic Message Syntax) serão detalhados no **Guia de iniciação rápida** (Windows ou UNIX) para a sua plataforma.
- Se os agentes do Managed File Transfer estiverem em execução no modo cliente, os comandos que você precisará para criar um JKS (Java Keystore) são detalhadas no “Guia de iniciação rápida para o AMS com os clientes Java” na página 602.

Procedimento

1. Crie um certificado autoassinado para identificar o usuário `ftagent` conforme detalhado no Guia de iniciação rápida apropriado.
   Use um Nome distinto (DN) conforme a seguir:

```
CN=ftagent, OU=MFT, O=<organisation>, L=<location>, ST=<state>, C=<country>
```

2. Crie um arquivo `keystore.conf` para identificar a localização do keystore e o certificado dentro dele conforme detalhado no Guia de iniciação rápida apropriado.

2. Configurando a proteção de mensagens

Sobre esta tarefa

É necessário definir uma política de segurança para a fila de dados usada pelo AGENT2 usando o comando **setmqspl**. Nesse cenário, o mesmo usuário é usado para iniciar ambos os agentes, e, portanto, o signatário e o destinatário DN são iguais e corresponderem ao certificado gerado.

Procedimento

1. Encerre os agentes do Managed File Transfer em preparação para a proteção usando o comando **fteStopAgent**.
2. Crie uma política de segurança para proteger a fila 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. Assegure-se de que o usuário que está executando o processo do Managed File Transfer Agent tenha acesso para procurar a fila de política do sistema e colocar mensagens na fila de erros.

```
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. Reinicie os agentes do Managed File Transfer usando o comando **fteStartAgent**.
5. Confirme se seus agentes foram reiniciados com sucesso usando o comando **fteListAgents** e verifique se os agentes estão em status READY.

Resultados

Você agora é capaz de enviar transferências do AGENT1 para AGENT2 e o conteúdo do arquivo será transmitido de forma segura entre os dois agentes.

Visão Geral de Instalação do Advanced Message Security

Instale o componente Advanced Message Security em várias plataformas.

Sobre esta tarefa

Para obter informações sobre os procedimentos de instalação, veja Instalando o Advanced Message Security em multiplataformas e Instalando o Advanced Message Security no z/OS.

Tarefas relacionadas

Desinstalando o Advanced Message Security

z/OS A auditoria no z/OS

O Advanced Message Security (AMS) for z/OS fornece um meio para a auditoria opcional de operações por aplicativos nas filas protegidas por política. Quando ativado, os registros de auditoria do IBM System

Management Facility (SMF) são gerados para o sucesso e a falha dessas operações em filas protegidas por política. As operações auditadas incluem MQPUT, MQPUT1 e MQGET.

A auditoria está desativada por padrão, no entanto, é possível ativar a auditoria definindo _AMS_SMF_TYPE e _AMS_SMF_AUDIT no arquivo _CEE_ENVFILE do Language Environment® configurado para o espaço de endereço do AMS. Para obter mais informações, consulte Criar procedimentos para o Advanced Message Security. A variável de _AMS_SMF_TYPE é usada para designar o tipo de registro SMF e é um número entre 128 e 255. Um tipo de registro SMF de 180 é habitual, no entanto não é obrigatório. A auditoria é desativada especificando um valor de 0. A variável _AMS_SMF_AUDIT configura se os registros de auditoria são criados para operações que são bem-sucedidas, operações que falham, ou ambas. As opções de auditoria também podem ser mudadas dinamicamente enquanto o AMS está ativo usando comandos do operador. Para obter mais informações, consulte Operando o Advanced Message Security.

O registro SMF é definido usando subtipos, com o subtipo 1 sendo um evento de auditoria geral. O registro SMF contém todos os dados relevantes para a solicitação que está sendo processada.

O registro SMF é mapeado pela macro CSQ0KSMF (observe o zero no nome da macro), que é fornecida na biblioteca de destino SCSQMACS. Se você estiver gravando programas de redução de dados para dados SMF, é possível incluir essa macro de mapeamento para auxiliar no desenvolvimento e customização do pós-processamento de rotinas do SMF.

Nos registros SMF produzidos pelo Advanced Message Security para z/OS, os dados são organizados em seções. O registro consiste em:

- um cabeçalho SMF padrão
- uma extensão de cabeçalho definida pelo Advanced Message Security for z/OS
- uma seção do produto
- uma seção de dados

A seção do produto do registro SMF está sempre presente nos registros produzidos pelo Advanced Message Security para z/OS. A seção de dados varia com base no subtipo. Atualmente, um subtipo é definido e, portanto, uma única seção de dados é usada.

O SMF é descrito no Manual z/OS System Management Facilities (SA22-7630). Os tipos de registro válidos são descritos no membro SMFPRMxx do conjunto de dados PARMLIB do sistema. Consulte a documentação do SMF para obter mais informações.

Gerador do relatório de auditoria do Advanced Message Security (CSQ0USMF)

O Advanced Message Security for z/OS fornece uma ferramenta de gerador de relatório de auditoria chamada CSQ0USMF, que é fornecida na biblioteca SCSQAUTH da instalação. A JCL de amostra para executar o utilitário CSQ0USMF chamado CSQ40RSM é fornecida na biblioteca SCSQPROC de instalação.

Antes de executar o utilitário CSQ0USMF, deve-se efetuar dump dos registros SMF do tipo 180 dos conjuntos de dados SMF do sistema para um conjunto de dados sequenciais. Como um exemplo, esse JCL efetua dump de registros SMF do tipo 180 de um conjunto de dados SMF e os transfere para um conjunto de dados de destino:

```
//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))
/*
```

Deve-se verificar os nomes reais do conjunto de dados SMF usados por sua instalação. O conjunto de dados de destino para os registros realizados dump deve ter um formato de registro de VBS e um comprimento de registro de 32760.

Nota: Se os fluxos de logs SMF estão sendo usados, o programa IFASMFDL deve ser usado para efetuar dump de um fluxo de logs para um conjunto de dados sequenciais. Consulte Processando registros SMF tipo 116 para um exemplo da JCL utilizada.

O conjunto de dados de destino pode, então, ser usado como entrada para o utilitário CSQ0USMF para produzir um relatório de auditoria do AMS. Por exemplo:

```
//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
//
```

O programa CSQ0USMF aceita dois parâmetros opcionais, que são listados em Tabela 97 na página 614:

Tabela 97. Parâmetros opcionais do CSQ0USMF

Parâmetro	Value	Descrição
SMFTYPE	nnn	O tipo de registro SMF aplicável ao relatório de auditoria. O programa CSQ0USMF usa apenas os registros SMF que correspondem ao valor SMFTYPE ao gerar o relatório. Se você não especificar SMFTYPE, um valor padrão de 180 será usado.
M	qmgr	O nome do gerenciador de filas do IBM MQ aplicável ao relatório de auditoria. Se você não especificar o parâmetro -M, o relatório de auditoria incluirá todos os registros de auditoria para todos os gerenciadores de filas representado no conjunto de dados SMFIN.

Usando keystores e certificados

Para fornecer proteção criptográfica transparente para aplicativos IBM MQ, o Advanced Message Security usa o arquivo keystore, em que certificados de chave pública e uma chave privada são armazenados. No z/OS, um anel de chaves SAF é usado em vez de um arquivo keystore.

No Advanced Message Security, usuários e aplicativos são representados por identidades de infraestrutura de chave pública (PKI). Esse tipo de identidade é usado para assinar e criptografar mensagens. A identidade PKI é representada pelo campo **nome distinto (DN)** do sujeito em um certificado que está associado com mensagens assinadas e criptografadas. Para um usuário ou aplicativo criptografar suas mensagens eles requerem acesso ao arquivo keystore no qual os certificados e chaves privadas e públicas associadas são armazenados.

No Windows e UNIX o local do keystore é fornecido no arquivo de configuração keystore, que é `keystore.conf` por padrão. Cada usuário do Advanced Message Security deve ter o arquivo de configuração keystore que aponta para um arquivo keystore. O Advanced Message Security aceita o formato a seguir de arquivos keystore: `.kdb`, `.jceks`, `.jks`.

O local padrão do arquivo `keystore.conf` é:

- IBM i UNIX Em UNIX e IBM i: `$HOME/.mqs/keystore.conf`
- Windows No Windows: *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Nota: O caminho em Windows pode e deve especificar a letra da unidade se mais de uma letra de unidade estiver disponível.

Se você estiver usando um nome do arquivo keystore e local especificados, é necessário usar os comandos a seguir

- Para Java: `java -DMQS_KEYSTORE_CONF=path/filename app_name`
- Para C Client e Servidor:
  - No UNIX and Linux: `export MQS_KEYSTORE_CONF=path/filename`
  - No Windows: `set MQS_KEYSTORE_CONF=path\filename`

Conceitos relacionados

"Nomes distintos do remetente no AMS" na página 641
Os nomes distintos (DNs) do emissor identificam usuários que estão autorizados a colocar mensagens em uma fila. Um emissor usa seu certificado para assinar uma mensagem antes de colocar a mensagem em uma fila.

"Nomes distintos do destinatário no AMS" na página 642
Os nomes distintos (DN) do destinatário identificam usuários que estão autorizados a recuperar mensagens em uma fila.

Estrutura do arquivo de configuração do keystore (keystore.conf) para AMS

O arquivo de configuração do keystore (`keystore.conf`) aponta Advanced Message Security para o local do keystore apropriado.

Cada um dos seguintes tipos de arquivo de configuração tem um prefixo:

CMS
Certificate Management System, as entradas de configuração são prefixadas com: `cms.`

PKCS#11
Public Key Cryptography Standard #11, entradas de configuração são prefixadas com: `pkcs11.`

IBM i **PEM**
Formato Privacy Enhanced Mail, entradas de configuração são prefixadas com: `pem.`

JKS
Java KeyStore, entradas de configuração são prefixadas com: `jks.`

JCEKS
Java Cryptographic Encryption KeyStore, entradas de configuração são prefixadas com: `jceks.`

z/OS V 9.1.0 MQ Adv. VUE **JCERACFKS**
Java Cryptographic Encryption RACF keyring KeyStore, entradas de configuração são prefixadas com: `jceracfks`.

Importante: A partir do IBM MQ 9.0, os valores `JCEKS.provider` e `JKS.provider` são ignorados. O provedor Bouncy Castle é usado, junto com qualquer provisão de JCE/JCE fornecida pelo JRE em uso. Para obter mais informações, consulte "Suporte para JREs não IBM com o AMS" na página 619.

Exemplo de estruturas para keystores:

CMS

```
cms.keystore = /dir/keystore_file
cms.certificate = certificate_label
```

PKCS#11

```
pkcs11.library = dir\cryptoki.dll
pkcs11.certificate = certificatelabel
pkcs11.token = tokenlabel
```

```
pkcs11.token_pin = tokenpin
pkcs11.secondary_keystore = dir\signers
```

IBM i PEM

```
pem.private = /dir/keystore_file_private_key
pem.public = /dir/keystore_file_public_keys
pem.password = password
```

JavaJKS

```
jks.keystore = dir/Keystore
jks.certificate = certificate_label
jks.encrypted = no
jks.keystore_pass = password
jks.key_pass = password
jks.provider = IBMJCE
```

JavaJCEKS

```
jceks.keystore = dir/Keystore
jceks.certificate = certificate_label
jceks.encrypted = no
jceks.keystore_pass = password
jceks.key_pass = password
jceks.provider = IBMJCE
```

V 9.1.0 Java JCERACFKS

```
jceracfks.keystore = safkeyring://user/keyring
jceracfks.certificate = certificate_label
```

Tabela 98. Resumo dos parâmetros necessários para cada tipo de arquivo de configuração

Parâmetros	Necessário	Tipo de arquivo de configuração			
		V 9.1.0 **Java (JKS, JCEKS e JCERACFKS)**	IBM i **PEM**	**PKCS#11**	**CMS**
keystore	✓	✓			✓
IBM i private	✓		IBM i ✓		
IBM i public	✓		IBM i ✓		
IBM i password	✓		IBM i ✓		
library	✓			✓	
certificate	✓	✓		✓	✓
token	✓			✓	
token_pin	✓			✓	

Tabela 98. Resumo dos parâmetros necessários para cada tipo de arquivo de configuração (continuação)					
		Tipo de arquivo de configuração			
Parâmetros	**Necessário**	V 9.1.0 **Java (JKS, JCEKS e JCERACFKS)**	IBM i **PEM**	**PKCS#11**	**CMS**
`secondary_keystore`	✓			✓	
`encrypted`		✓			
`keystore_pass`	✓	✓			
`key_pass`		✓			
`provider`		✓			

Observe que é possível incluir comentários usando o símbolo #

Os parâmetros de arquivo de configuração são definidos como seguir:

keystore
Somente configuração do CMS e Java. Caminho para o arquivo keystore para configuração de CMS, JKS e JCEKS.

z/OS V 9.1.0 MQ Adv. VUE URI para o conjunto de chaves RACF para configuração JCERACFKS.

Importante:

- O caminho para o arquivo keystore não deve incluir a extensão do arquivo.
- z/OS V 9.1.0 MQ Adv. VUE O URI para o conjunto de chaves RACF deve estar no formato:

  ```
  safkeyring://user/keyring
  ```

  em que:
  - *user* é o ID do usuário que possui o conjunto de chaves
  - *keyring* é o nome do conjunto de chaves.

IBM i **private**
Somente configuração do PEM. O nome do arquivo de um arquivo que contém a chave privada e o certificado no formato PEM.

IBM i **public**
Somente configuração do PEM. O nome do arquivo de um arquivo que contém certificados públicos confiáveis no formato PEM.

IBM i **password**
Somente configuração do PEM. Senha usada para decriptografar uma chave privada criptografada.

library
Somente PKCS#11. Nome do caminho da biblioteca PKCS#11.

certificate
CMS, PKCS#11 e somente configuração do Java. Etiqueta do certificado.

token
Somente PKCS#11. Rótulo do token.

token_pin
Somente PKCS#11. PIN para desbloquear o token.

secondary_keystore
Somente PKCS#11. Nome do caminho do keystore CMS, fornecido sem a extensão `.kdb`, que contém certificados âncora (certificados raiz) requeridos por certificados armazenados no token PKCS #11. O keystore secundário também pode conter os certificados intermediários na cadeia de confiança, bem como certificados do destinatário definidos na política de segurança de privacidade. Esse keystore CMS deve ser acompanhado por um arquivo stash que deve estar localizado no mesmo diretório que o keystore secundário.

encrypted
Somente configuração do Java. Status da senha.

keystore_pass
Somente configuração do Java. Senha do arquivo de armazenamento de chaves.

Nota:

- Para o keystore CMS, o AMS depende dos arquivos stash (`.sth`), enquanto que JKS e JCEKS podem requerer uma senha para o certificado e a chave privada do usuário.
- **Importante:** O armazenamento de senhas em formulário de texto simples é um risco de segurança.

Nota: Ignorado para `jceracfks`, pois o acesso não é controlado por uma senha.

key_pass
Somente configuração do Java. Senha para chave privada do usuário.

Importante: O armazenamento de senhas em formulário de texto simples é um risco de segurança.

Nota: Ignorado para `jceracfks`, pois o acesso não é controlado por uma senha.

provider
Somente configuração do Java. O provedor de segurança do Java que implementa os algoritmos criptográficos requeridos pelo certificado keystore.

Importante: As informações armazenadas no keystore são cruciais para o fluxo seguro de dados enviado usando o IBM MQ. Os administradores de segurança deverão prestar atenção especial quando estiverem designando permissões de arquivo para esses arquivos.

Exemplo do arquivo `keystore.conf`

```
# Native AMS application configuration
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

# Java AMS application configurationjceks.keystore = c:/Documents and Settings/Alice/
AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = passw0rd
jceks.key_pass = passw0rd
jceks.provider = IBMJCE
```

Tarefas relacionadas

"Protegendo as senhas no Java" na página 632
Armazenamento de keystore e senhas de chave privada como texto simples representam um risco de segurança, então o Advanced Message Security fornece uma ferramenta que pode misturar essas senhas usando a chave do usuário, que está disponível no arquivo keystore.

Suporte para JREs não IBM com o AMS

O IBM MQ classes for Java e o IBM MQ classes for JMS suportam a operação Advanced Message Security ao executar com JREs não IBM.

O Advanced Message Security (AMS) implementa o Cryptographic Message Syntax (CMS). A sintaxe CMS é usada para assinar digitalmente, compilar, autenticar ou criptografar conteúdo de mensagem arbitrário.

No IBM MQ 9.0, o suporte do Advanced Message Security no IBM MQ classes for Java e IBM MQ classes for JMS usa os pacotes Bouncy Castle de software livre para suportar o CMS. Isso significa que essas classes podem suportar a operação Advanced Message Security ao executar com JREs não IBM.

Antes da IBM MQ 9.0, o Advanced Message Security não era suportado em JREs não IBM em clientes Java. O suporte do Advanced Message Security no IBM MQ classes for Java e IBM MQ classes for JMS dependia do suporte do CMS fornecido especificamente pela implementação da IBM do Java Cryptography Extensions (JCE). Por causa dessa restrição, a funcionalidade estava disponível somente ao usar um Java runtime environment (JRE) que incluía o provedor JCE do Java.

Solaris Importantemente, o suporte em plataformas como o Solaris requer um JRE híbrido, ou seja, o JRE padrão para a plataforma com elementos adicionais fornecidos pela IBM. Em particular, o provedor JCE da IBM era necessário em vez do provedor JCE fornecido pelo JRE padrão para a plataforma.

Local e numeração de versão para arquivos JAR do Bouncy Castle

Os arquivos JAR do Bouncy Castle que são necessários para suporte para JREs não IBM são incluídos como parte do pacote de instalação do IBM MQ classes for Java e do IBM MQ classes for JMS.

Os arquivos JAR do Bouncy Castle usados são os arquivos a seguir:

O arquivo JAR do provedor, que é fundamental para as operações do Bouncy Castle.
Este arquivo JAR é chamado `bcprov-jdk15on.jar`.

O arquivo JAR "PKIX", que contém o suporte para operações CMS que são usadas pelo Advanced Message Security.
Este arquivo JAR é chamado `bcpkix-jdk15on.jar`.

V 9.1.0.9 **O arquivo JAR "util", que contém as classes usadas pelos outros arquivos jar do Bouncy Castle.**
Este arquivo JAR é chamado `bcutil-jdk15on.jar`.

Objetos Relacionados

A IBM MQ 9.1 e classes mais recentes foram testadas com JREs do IBM e com JREs do Oracle. Eles também devem ser executados com sucesso sob qualquer JRE compatível com J2SE. Entretanto, é necessário observar as dependências a seguir:

- Não há mudanças na configuração do Advanced Message Security.
- As classes Bouncy Castle são usadas somente para operações CMS. Todas as outras operações relacionadas à segurança, por exemplo, o acesso de keystore de exemplo, a criptografia real de dados e o cálculo de somas de verificação de assinatura, usam a funcionalidade fornecida pelo JRE.

  Importante: Por este motivo, o JRE usado deve incluir uma implementação de provedor JCE.
- Para usar alguns algoritmos de criptografia *avançada*, pode ser necessário instalar os arquivos de políticas *sem restrições* para a implementação JCE do JRE.

  Consulte a documentação do JRE para obter mais detalhes.
- Se você tiver ativado a segurança do Java:
  - Inclua `java.security.SecurityPermissioninsertProvider.BC` no aplicativo para que as classes do Bouncy Castle possam ser usadas como um provedor de segurança.
  - Conceda `java.security.AllPermission` aos arquivos JAR do Bouncy Castle, que são:

V 9.1.0.9 *mq_install_dir*/java/lib/bcutil-jdk15on.jar
mq_install_dir/java/lib/bcpkix-jdk15on.jar
mq_install_dir/java/lib/bcprov-jdk15on.jar

Conceitos relacionados

O que é instalado para classes do IBM MQ para JMS
O que está instalado para classes do IBM MQ para Java

Multi Intercepção de Agente do Canal de Mensagens (MCA)

A intercepção de MCA permite que um gerenciador de filas em execução sob o IBM MQ ative seletivamente as políticas a serem aplicadas para os canais de conexão do servidor.

A intercepção de MCA permite aos clientes que permanecem fora do AMS continuem conectados a um gerenciador de filas e suas mensagens sejam criptografadas e decriptografadas.

A intercepção de MCA destina-se a fornecer a capacidade do AMS quando o AMS não puder ser ativado no cliente. Observe que usar a intercepção de MCA e um cliente ativado por AMS leva à dupla proteção de mensagens que pode ser problemática para aplicativos de recebimento. Para obter informações adicionais, consulte “Desativando o Advanced Message Security no cliente” na página 622.

Nota: Os interceptores de MCA não são suportados para canais AMQP ou MQTT.

Arquivo de configuração do keystore

Por padrão, o arquivo de configuração keystore para intercepção de MCA é `keystore.conf` e está localizado no diretório `.mqs` no caminho do diretório HOME do usuário que iniciou o gerenciador de filas ou o listener. O keystore também pode ser configurado usando a variável de ambiente MQS_KEYSTORE_CONF. Para obter mais informações sobre como configurar o keystore do AMS, veja “Usando keystores e certificados” na página 614.

Para ativar a intercepção MCA, deve-se fornecer o nome de um canal que você deseja usar no arquivo de configuração keystore. Para a intercepção de MCA, somente um tipo de keystore cms pode ser usado.

Veja “Exemplo de intercepção de MCA do Advanced Message Security” na página 620 para obter um exemplo de como configurar a intercepção de MCA.

Atenção: Deve-se concluir a autenticação de cliente e a criptografia nos canais selecionados, por exemplo, usando SSL e SSLPEER ou CHLAUTH TYPE(SSLPEERMAP), para assegurar que somente os clientes autorizados possam se conectar e usar esse recurso.

IBM i

Se sua empresa usar o IBM ie você tiver selecionado uma autoridade de certificação (CA) comercial para assinar seu certificado, o Digital Certificate Manager criará uma solicitação de certificado no formato PEM (Privacy-Enhanced Mail). Deve-se encaminhar a solicitação para a CA escolhida.

Para fazer isso, deve-se usar o comando a seguir para selecionar o certificado correto para o canal especificado em `channelname`:

```
pem.certificate.channel.channelname
```

Exemplo de intercepção de MCA do Advanced Message Security

Uma tarefa de exemplo de como configurar uma intercepção de MCA do AMS.

Antes de começar

Atenção: Deve-se concluir a autenticação de cliente e a criptografia nos canais selecionados, por exemplo, usando SSL e SSLPEER ou CHLAUTH TYPE(SSLPEERMAP), para assegurar que somente os clientes autorizados possam se conectar e usar esse recurso.

Se sua empresa usar o IBM ie você tiver selecionado uma autoridade de certificação (CA) comercial para assinar seu certificado, o Digital Certificate Manager criará uma solicitação de certificado no formato PEM (Privacy-Enhanced Mail). Deve-se encaminhar a solicitação para a CA escolhida.

Sobre esta tarefa

Esta tarefa leva você através do processo de configuração do seu sistema para usar a intercepção de MCA e, em seguida, verificar a configuração.

Nota: Antes do IBM WebSphere MQ 7.5, o AMS era um produto complementar que precisava ser instalado separadamente e ter interceptores configurados para proteger aplicativos. No IBM WebSphere MQ 7.5 em diante, os interceptores são automaticamente incluídos e dinamicamente ativados no cliente do MQ e em ambientes de tempo de execução do servidor. Neste exemplo de intercepção de MCA, os interceptores são fornecidos no término do servidor do canal e um tempo de execução de cliente mais antigo é usado (na Etapa 12) para colocar uma mensagem desprotegida ao longo do canal para que ela possa ser vista para ser protegida pelos interceptores de MCA. Se esse exemplo tivesse usado um cliente IBM WebSphere MQ 7.5 ou mais recente, faria com que a mensagem fosse protegida duas vezes, porque o interceptor de tempo de execução do cliente MQ e o interceptor MCA protegem a mensagem conforme ela chega no MQ.

Atenção: Substitua `userID` no código com seu ID do usuário.

Procedimento

1. Crie o banco de dados de chave e certificados usando os seguintes a seguir para criar um shell script.

   Além disso, mude o **INSTLOC** e **KEYSTORELOC** ou executar os comandos necessários. Observe que pode não ser necessário para o certificado para o bob.

```
INSTLOC=/opt/mq90
KEYSTORELOC=/home/testusr/ssl/ams1
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. Compartilhe os certificados entre os dois bancos de dados de chaves para que cada usuário possa identificar com sucesso o outro.

   É importante que você use o método descrito na **Tarefa 5. Compartilhando certificados** no **Guia de Iniciação Rápida** (Windows ou UNIX).

3. Crie `keystore.conf` com a configuração a seguir: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. Crie e inicie o gerenciador de filas AMSQMGR1
5. Defina um listener com *port* 14567 e *control* QMGR
6. Desative a autoridade do canal ou configure as regras para a autoridade do canal.

   Consulte SET CHLAUTH para obter mais informações.

7. Parar o gerenciador de fila.
8. Configure o keystore:

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

9. Inicie o gerenciador de filas no mesmo shell.
10. Configure a política de segurança e verifique:

```
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
```

    Consulte setmqspl e dspmqspl para obter mais informações.
11. Configure a configuração do canal:

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Execute **amqsputc** por meio de um cliente do MQ que não ativa automaticamente um interceptor de MCA; por exemplo um cliente do IBM WebSphere MQ 7.1 ou anterior. Coloque as duas mensagens a seguir:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Remova a política de segurança e verifique o resultado:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

14. Procure a fila por meio de sua instalação do IBM MQ 9.0:

```
/opt/mq90/samp/bin/amqsbcg TESTQ AMSQMGR1
```

    A saída de procura mostra as mensagens no formato criptografado.
15. Configure a política de segurança e verifique o resultado:

```
setmqspl -m AMSQMGR1 -s SHA256 -e AES256 -p TESTQ -a "CN=alice,O=IBM,C=IN"
-r "CN=alice,O=IBM,C=IN"
dspmqspl -m AMSQMGR1
```

16. Execute **amqsgetc** por meio de sua instalação do IBM MQ 9.0:

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Tarefas relacionadas

“Guia de iniciação rápida para o AMS com os clientes Java” na página 602
Use este guia para configurar rapidamente o Advanced Message Security para fornecer segurança de mensagens para aplicativos do Java conectando usando ligações do cliente. No momento em que você concluir, você terá criado um armazenamento de chaves para verificar identidades do usuário e definido políticas de assinatura/criptografia para o seu gerenciador de filas.

Referências relacionadas

“Limitações conhecidas de AMS” na página 573
Há várias opções do IBM MQ que não são suportadas ou têm limitações para o Advanced Message Security.

Desativando o Advanced Message Security no cliente

Será necessário desativar o IBM MQ Advanced Message Security (AMS) se você estiver usando um cliente IBM WebSphere MQ 7.5 ou mais recente para se conectar a um gerenciador de filas de uma versão anterior do produto e um erro 2085 (MQRC_UNKNOWN_OBJECT_NAME) será. relatado.

Sobre esta tarefa

Por meio do IBM WebSphere MQ 7.5, o IBM MQ Advanced Message Security (AMS) é ativado automaticamente em um cliente IBM MQ e, portanto, por padrão, o cliente tenta verificar as políticas de segurança para objetos no gerenciador de filas. No entanto, servidores em versões anteriores do

produto, por exemplo, IBM WebSphere MQ 7.1, não têm o AMS ativado, o que faz com que o erro 2085 (MQRC_UNKNOWN_OBJECT_NAME) seja relatado.

Se esse erro for relatado, quando você estiver tentando se conectar a um gerenciador de filas por meio de uma versão anterior do produto, será possível desativar o AMS da seguinte forma:

- Para clientes Java, de qualquer uma das maneiras a seguir:
  - Configurando uma variável de ambiente AMQ_DISABLE_CLIENT_AMS.
  - Configurando a propriedade do sistema Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.
  - Usando a propriedade DisableClientAMS, na sub-rotina **Security** no arquivo `mqclient.ini`.
- Para clientes C, de uma das maneiras a seguir:
  - Configurando uma variável de ambiente MQS_DISABLE_ALL_INTERCEPT.
  - Usando a propriedade DisableClientAMS, na sub-rotina **Security** no arquivo `mqclient.ini`.

Nota: No IBM WebSphere MQ 7.5, também é possível usar a variável de ambiente AMQ_DISABLE_CLIENT_AMS... para clientes C. A partir do IBM MQ 8.0, não é mais possível usar a variável de ambiente AMQ_DISABLE_CLIENT_AMS para clientes C. Em vez disso, é necessário usar a variável de ambiente MQS_DISABLE_ALL_INTERCEPT.

Procedimento

- Para desativar o AMS no cliente, use uma das opções a seguir:

  Variável de ambiente AMQ_DISABLE_CLIENT_AMS
  É necessário configurar essa variável nos seguintes casos:
  - Se você estiver usando o Java Runtime Environment (JRE) diferente do IBM Java Runtime Environment (JRE)
  - Se estiver usando o cliente IBM WebSphere MQ 7.5 ou posterior IBM MQ classes for JMS ou IBM MQ classes for Java .

  Crie a variável de ambiente AMQ_DISABLE_CLIENT_AMS e configure-a como TRUE no ambiente em que o aplicativo está em execução. Por exemplo:

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

  Propriedade do sistema Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS
  Para os clientes IBM MQ classes for JMS e IBM MQ classes for Java, é possível configurar a propriedade do sistema Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS para o valor TRUE para o aplicativo Java.

  Por exemplo, é possível configurar a propriedade do sistema Java como uma opção `-D` quando o comando Java é chamado:

  ```
  java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/
  com.ibm.mqjms.jar  my.java.applicationClass
  ```

  Alternativamente, especifique a propriedade do sistema Java dentro de um arquivo de configuração do JMS, `jms.config`, se o aplicativo utilizar este arquivo.

  Variável de ambiente MQS_DISABLE_ALL_INTERCEPT
  Será necessário configurar essa variável se você estiver usando a IBM MQ 8.0 ou mais recente com clientes nativos e precisar desativar o AMS no cliente.

  Crie a variável de ambiente MQS_DISABLE_ALL_INTERCEPT e configure-a como TRUE no ambiente no qual o cliente está em execução. Por exemplo:

  ```
  export MQS_DISABLE_ALL_INTERCEPT =TRUE
  ```

  É possível usar a variável de ambiente MQS_DISABLE_ALL_INTERCEPT apenas para clientes C. Para clientes Java, é necessário usar a variável de ambiente AMQ_DISABLE_CLIENT_AMS.

Propriedade `DisableClientAMS` no arquivo `mqclient.ini`

É possível usar essa opção para clientes IBM MQ classes for JMS e IBM MQ classes for Java e para clientes C.

Inclua o nome da propriedade `DisableClientAMS` sob sub-rotina **`Security`** no arquivo `mqclient.ini`, conforme mostrado no exemplo a seguir:

```
Security:
DisableClientAMS=Yes
```

Também é possível ativar o AMS, conforme mostrado no exemplo a seguir:

```
Security:
DisableClientAMS=No
```

Como proceder a seguir

Para obter mais informações sobre problemas com a abertura de filas protegidas do AMS, consulte Problemas na abertura de filas protegidas ao usar o AMS com o JMS.

Conceitos relacionados

“Intercepção de Agente do Canal de Mensagens (MCA)” na página 620
A intercepção de MCA permite que um gerenciador de filas em execução sob o IBM MQ ative seletivamente as políticas a serem aplicadas para os canais de conexão do servidor.

Tarefas relacionadas

Configurando um Cliente Usando um Arquivo de Configuração

Referências relacionadas

O arquivo de configuração do IBM MQ classes for JMS

Requisitos de certificado para o AMS

Os certificados devem ter uma chave pública do RSA para que sejam usados com o Advanced Message Security.

Para obter mais informações sobre os diferentes tipos de chave pública e como criá-los, consulte “Certificados digitais e compatibilidade de CipherSpec no IBM MQ” na página 45.

Extensões do uso da chave

As extensões de uso da chave colocam restrições adicionais na forma que um certificado pode ser usado.

No Advanced Message Security, o uso da chave dos certificados X.509 v3 deve ser configurado de acordo com a especificação RFC 5280.

Para a qualidade da integridade da proteção, se as extensões de uso da chave de certificado estiverem configuradas, essa configuração deverá incluir pelo menos um dos dois:

- **`nonRepudiation`**
- **`digitalSignature`**

Para a qualidade de privacidade de proteção, se as extensões de uso da chave de certificado forem configuradas, esse conjunto deverá incluir:

- **`keyEncipherment`**

Para a qualidade de confidencialidade de proteção, se as extensões de uso de chave de certificado forem configuradas, esse conjunto deverá incluir:

- **`dataEncipherment`**

O uso estendido de chaves refina ainda mais as extensões de uso das chaves. Para todas as qualidades de proteção, se o uso estendido da chave do certificado estiver configurado, a configuração deverá incluir:

- **`emailProtection`**

Conceitos relacionados

"Qualidade de Proteção" na página 644
A proteção de políticas do Advanced Message Security implicam uma qualidade de proteção (QOP).

métodos de validação de certificado no AMS

É possível usar o Advanced Message Security para detectar e rejeitar os certificados revogados para que as mensagens em suas filas não sejam protegidas usando certificados que não cumprem as normas de segurança.

O AMS permite verificar a validade do certificado usando o Online Certificate Status Protocol (OCSP) ou a lista de revogação de certificados (CRL).

O AMS pode ser configurado para a verificação de OCSP ou CRL ou ambos. Se ambos os métodos forem ativados, então, por motivos de desempenho, o AMS usará o OCSP para o status de revogação primeiro. Se o status da revogação de um certificado for indeterminado após a verificação de OCSP, o AMS usará a verificação de CRL.

Observe que as verificações de OCSP e CRL são ativadas por padrão.

Conceitos relacionados

"Online Certificate Status Protocol (OCSP) no AMS" na página 625
O Online Certificate Status Protocol (OCSP) determina se um certificado foi revogado e, portanto, ajuda a determinar se o certificado pode ser confiável. O OCSP é ativado por padrão.

"Listas de revogação de certificado (CRLs) no AMS" na página 627
As CRLs contêm uma lista de certificados que foram marcados pela Autoridade de certificação (CA) como não mais confiável por vários motivos, por exemplo, a chave privada foi perdida ou comprometida.

Online Certificate Status Protocol (OCSP) no AMS

O Online Certificate Status Protocol (OCSP) determina se um certificado foi revogado e, portanto, ajuda a determinar se o certificado pode ser confiável. O OCSP é ativado por padrão.

O OCSP não é suportado nos sistemas IBM i.

Ativando a verificação de OCSP em interceptores nativos do Advanced Message Security

A verificação de Online Certificate Status Protocol (OCSP) no Advanced Message Security é ativada por padrão, com base nas informações dos certificados que estão sendo usados.

Procedimento

Inclua as seguintes opções no arquivo de configuração de chaves :

Nota: Todos as sub-rotinas de OCSP são opcionais e podem ser especificadas independentemente.

Opção	Descrição
`ocsp.enable=off`	Ative a verificação de OCSP se o certificado que está sendo verificada tiver uma Authority Info Access (AIA) com um método de acesso PKIX_AD_OCSP que contém uma URI na qual o OCSP está localizado. Possíveis valores: on ou `off`.
`ocsp.url=`*`responder_URL`*	O endereço da URL do respondente do OCSP. Se esta opção for omitida, então, a verificação de OCSP não AIA será desativada.
`ocsp.http.proxy.host=`*`OCSP_proxy`*	O endereço da URL do servidor proxy do OCSP. Se esta opção for omitida, um proxy não será usado para verificações de certificado não AIA on-line.

Opção	Descrição
`ocsp.http.proxy.port=`*`port_number`*	Número da porta do servidor proxy do OCSP Se essa opção for omitida, a porta padrão 8080 será usada.
`ocsp.nonce.generation=on/off`	Gere nonce ao consultar o OCSP. O valor padrão é `off`.
`ocsp.nonce.check=on/off`	Verifique o nonce após receber a resposta do OCSP. O valor padrão é `off`.
`ocsp.nonce.size=8`	Tamanho do nonce em bytes.
`ocsp.http.get=on/off`	Especifique HTTP GET como seu método de solicitação. Se essa opção estiver configurada como `off`, HTTP POST é utilizado. O valor padrão é `off`.
`ocsp.max_response_size=20480`	Tamanho máximo de resposta do respondente do OCSP fornecido em bytes.
`ocsp.cache_size=100`	Ative cache de resposta do OCSP interno e configure o limite para o número de entradas de cache.
`ocsp.timeout=30`	Tempo de espera por uma resposta do servidor, em segundos, após o qual o Advanced Message Security atinge o tempo limite.
`ocsp.unknown=ACCEPT`	Define o comportamento quando um servidor OCSP não pode ser alcançado dentro de um período de tempo limite. Valores possíveis: • `ACCEPT` Permite o certificado • `WARN` Permite o certificado e registra um aviso • `REJECT` Evita o certificado que está sendo usado e registra um erro

Ativando a verificação de OCSP no Java no AMS
Para ativar a verificação de OCSP para Java no Advanced Message Security modifique o arquivo `java.security` ou o arquivo keystore.

Sobre esta tarefa

Existem duas maneiras de ativar a verificação de OCSP no Advanced Message Security:

Usando java.security
Verifique se o certificado contém uma extensão de certificado Authority Information Access (AIA).

Procedimento

1. Se AIA não estiver configurado ou se você desejar substituir seu certificado, edite o arquivo `$JAVA_HOME/lib/security/java.security` com as seguintes propriedades:

```
ocsp.responderURL=http://url.to.responder:port
ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
```

e ative a verificação de OCSP editando o arquivo `$JAVA_HOME/lib/security/java.security` com a linha a seguir:

```
ocsp.enable=true
```

2. Se AIA estiver configurado, ative a verificação de OCSP editando o arquivo `$JAVA_HOME/lib/security/java.security` com a linha a seguir:

```
ocsp.enable=true
```

Como proceder a seguir

Se você estiver usando o Java Security Manager, para concluir a configuração, inclua a permissão a seguir do Java para `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

Usando keystore.conf

Procedimento

Inclua o atributo a seguir no arquivo de configuração:

```
ocsp.enable=true
```

Importante: A configuração desse atributo no arquivo de configuração substitui as configurações java.security.

Como proceder a seguir

Para concluir a configuração, inclua as seguintes permissões Java em `lib/security/java.policy`:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Listas de revogação de certificado (CRLs) no AMS

As CRLs contêm uma lista de certificados que foram marcados pela Autoridade de certificação (CA) como não mais confiável por vários motivos, por exemplo, a chave privada foi perdida ou comprometida.

Para validar certificados, o Advanced Message Security constrói uma cadeia de certificados que consiste no certificado do signatário e a cadeia de certificados da autoridade de certificação (CA) até uma âncora de confiança. Uma âncora de confiança é um arquivo keystore confiável que contém um certificado confiável ou um certificado de raiz confiável que é usado para assegurar a confiança de um certificado. O AMS verifica o caminho do certificado usando um algoritmo de validação de PKIX. Quando a cadeia é criada e verificada, o AMS conclui a validação de certificado que inclui a validação do problema e a data de expiração de cada certificado na cadeia em relação à data atual, verificando se a extensão do uso da chave está presente no certificado de Entidade Final. Se a extensão for anexada ao certificado, o AMS verificará se o **digitalSignature** ou **nonRepudiation** também serão definidos. Se não forem, o `MQRC_SECURITY_ERROR` será relatado e registrado. Em seguida, o AMS faz download das CRLs dos arquivos ou do LDAP, dependendo dos valores que foram especificados no arquivo de configuração. Somente as CRLs que são codificadas no formato DER são suportadas pelo AMS. Se nenhuma configuração relacionada a CRL for localizada no arquivo de configuração do keystore, o AMS não executará nenhuma verificação de validade da CRL. Para cada certificado de autoridade de

certificação o AMS consulta o LDAP para CRLs usando Nomes distintos de uma CA para localizar sua CRL. Os atributos a seguir são incluídos na consulta LDAP:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Nota: `deltaRevocationList` é suportado somente quando ele for especificado como pontos de distribuição.

Ativando o suporte à validação do certificado e lista de revogação de certificado em interceptores nativos
Deve-se modificar o arquivo de configuração de keystore para que o Advanced Message Security possa fazer download de CLRs do servidor Lightweight Directory Access Protocol (LDAP).

Sobre esta tarefa

IBM i Ativar o suporte de validação de certificado e lista de revogação de certificado em interceptores nativos não é suportado para o Advanced Message Security no IBM i.

Procedimento

Inclua as opções a seguir no arquivo de configuração:

Nota: Todos as sub-rotinas de CRL são opcionais e podem ser especificadas independentemente.

Opção	Descrição
`crl.ldap.host=`*`host_name`*	Nome do host do servidor LDAP.
`crl.ldap.port=`*`port_number`*	Número da porta do servidor LDAP. É possível especificar até 11 servidores. Vários hosts LDAP são usados para assegurar o failover transparente no caso de falha de conexão LDAP. É esperado que todos os servidores LDAP sejam réplicas e contenham os mesmos dados. Quando o interceptor do AMS Java se conectar com sucesso a um servidor LDAP ele não tentará fazer o download de CRLs a partir dos servidores restantes fornecidos.
`crl.cdp=off`	Use essa opção para verificar ou usar extensões CRLDistributionPoints em certificados.
`crl.ldap.version=3`	Número da versão do protocolo LDAP. Valores possíveis: 2 ou 3.
`crl.ldap.user=cn=`*`username`*	Efetue login no servidor LDAP. Se esse valor não for especificado, os atributos CRL no LDAP deverão ser legíveis no mundo
`crl.ldap.pass=`*`password`*	Senha para o servidor LDAP.
`crl.ldap.cache_lifetime=0`	Tempo de vida do cache de LDAP em segundos. Valores possíveis: 0-86400.
`crl.ldap.cache_size=50`	Tamanho do cache do LDAP. Esta opção pode ser especificada apenas se o valor `crl.ldap.cache_lifetime` for maior do que `0`.

Opção	Descrição
`crl.http.proxy.host=some.host.com`	Porta do servidor proxy HTTP para recuperação do CDP CRL.
`crl.http.proxy.port=8080`	Número da porta do servidor proxy Http.
`crl.http.max_response_size=204800`	O tamanho máximo de CRL, em bytes, que pode ser recuperado de um servidor HTTP que é aceito pelo GSKit.
`crl.http.timeout=30`	Tempo de espera por uma resposta do servidor, em segundos, após o qual o AMS atinge tempo limite.
`crl.http.cache_size=0`	Tamanho do cache HTTP, em bytes.
`crl.unknown=ACCEPT`	Define o comportamento quando um servidor de CRL não pode ser alcançado dentro de um período de tempo limite. Valores possíveis: • `ACCEPT` Permite o certificado • `WARN` Permite o certificado e registra um aviso • `REJECT` Evita o certificado que está sendo usado e registra um erro

Ativando o suporte à lista de revogação de certificado no Java no AMS
Para ativar o suporte de CRL no Advanced Message Security, deve-se modificar o arquivo de configuração do keystore para permitir que AMS faça download de CRLs do servidor Lightweight Directory Access Protocol (LDAP) e configure o arquivo java.security.

Procedimento

1. Inclua as opções a seguir no arquivo de configuração:

Cabeçalho	Descrição
`crl.ldap.host=`*`host_name`*	Nome do host LDAP.
`crl.ldap.port=`*`port_number`*	Número da porta do servidor LDAP. É possível especificar até 11 servidores. Vários hosts LDAP são usados para assegurar o failover transparente no caso de falha de conexão LDAP. É esperado que todos os servidores LDAP sejam réplicas e contenham os mesmos dados. Quando o interceptor do AMS Java se conectar com sucesso a um servidor LDAP ele não tentará fazer o download de CRLs a partir dos servidores restantes fornecidos. O Java não usa os valores `crl.ldap.user` e crl.ldaworldp.pass. Ele não usa um usuário e senha ao se conectar a um servidor LDAP. Como consequência, os atributos de CRL LDAP devem ser legíveis mundialmente.
`crl.cdp=on/off`	Use essa opção para verificar ou usar extensões CRLDistributionPoints em certificados.

2. Modifique o arquivo `JRE/lib/security/java.security` com as propriedades a seguir:

Nome da Propriedade	Descrição
`com.ibm.security.enableCRLDP`	Esta propriedade usa os valores a seguir: `true`, `false`. Se for configurada como `true`, ao fazer a verificação de revogação de certificado, as CRLs serão localizadas usando a URL da extensão de pontos de distribuição de CRL do certificado. Se for configurada como `false` ou não configurada, a verificação de CRL usando a extensão de pontos de distribuição de CRL será desativada.
`ibm.security.certpath.ldap.cache.lifetime`	Essa propriedade pode ser usada para configurar o tempo de vida de entradas no cache de memória de LDAP CertStore para um valor em segundos. Um valor de 0 desativa o cache; -1 significa tempo de vida ilimitado. Se não for configurado, o tempo de vida padrão será 30 segundos.
`com.ibm.security.enableAIAEXT`	Esta propriedade usa os valores a seguir: `true`, `false`. Se for configurada como `true`, quaisquer extensões de Authority Information Access que forem encontradas dentro dos certificados do caminho do certificado que está sendo construído serão examinadas para determinar se elas contêm URIs LDAP. Para cada URI LDAP localizado, um objeto LDAPCertStore será criado e incluído na coleção de CertStores que é usada para localizar outros certificados que são requeridos para construir o caminho do certificado. Se for configurada como `false` ou não configurada, objetos LDAPCertStore adicionais não serão criados.

z/OS *Ativando listas de revogação de certificado (CRLs) no z/OS*

O Advanced Message Security suporta a verificação da lista de revogação de certificado (CRL) dos certificados digitais usados para proteger os dados de mensagens

Sobre esta tarefa

Quando ativado, o Advanced Message Security irá validar certificados do destinatário quando as mensagens forem colocadas em uma fila de privacidade protegida e validar certificados do emissor quando as mensagens forem recuperadas de uma fila protegida (integridade ou privacidade). A validação nesse caso inclui a verificação de que os certificados relevantes não estão registrados em uma CRL relevante.

O Advanced Message Security usa serviços do IBM SSL do Sistema para validar os certificados de emissor e destinatário. A documentação detalhada sobre a validação de certificado do SSL do Sistema do pode ser localizada no z/OSManual de programação do Cryptographic Services System Secure Sockets Layer (SC24-5901).

Para ativar a verificação de CRL, você especifica o local de um arquivo de configuração de CRL através do DD CRLFILE na tarefa iniciada JCL para o espaço de endereço do AMS. Um arquivo de configuração CRL

de amostra que pode ser customizado é fornecido em *thlqual*.SCSQPROC(CSQ40CRL). As configurações permitidas neste arquivo são as a seguir:

Tabela 99. Variáveis de configuração de CRL do Advanced Message Security

Variável	Valores Válidos	Descrição
crl.ldap.host[.n]	*hostname -or- hostname:port*	O ipaddr/hostname do seu servidor LDAP que hospeda os CRLs dos seus certificados de emissor. Se você não especificar um número de porta para seu servidor LDAP, o número da porta especificado pelo crl.ldap.port será usado.
crl.ldap.port	*port*	O número da porta TCP/IP do seu servidor LDAP.
crl.ldap.user	*ldap_user*	O nome de usuário LDAP a ser usado ao se conectar ao servidor LDAP.
crl.ldap.pass	*ldap_password*	A senha do LDAP associada ao crl.ldap.user.

É possível especificar vários nomes de host do servidor e portas do LDAP, conforme a seguir:

```
crl.ldap.host.1 = hostname -or hostname:port
crl.ldap.host.2 = hostname -or hostname:port
crl.ldap.host.3 = hostname -or hostname:port
```

É possível especificar até 10 nomes de hosts. Se você não especificar um número de porta para os servidores LDAP, o número da porta especificado pela crl.ldap.port será usado. Cada servidor LDAP deve usar a mesma combinação crl.ldap.user/password para acesso.

Quando o CRLFILE DD for especificado, a configuração será carregada durante a inicialização do espaço de endereço do Advanced Message Security e a verificação de CRL será ativada. Se o CRLFILE DD não for especificado ou o arquivo de configuração do CRL estiver indisponível ou inválido, a verificação de CRL será desativada.

O AMS executa uma verificação de CRL usando os serviços certificado de validação do SSL do Sistema do IBM conforme a seguir:

Tabela 100. Verificações de CRL do Advanced Message Security

Operação	Qualidade de Proteção	Certificado(s) verificado(s)
PUT	Privacidade	Destinatário(s)
GET	Integridade/Privacidade	Emissor

Se uma operação de mensagem falhar uma verificação de CRL Advanced Message Security executa as ações a seguir:

Tabela 101. Comportamento de falha da verificação de CRL do Advanced Message Security

Operação	Falha na verificação de CRL
PUT	A mensagem não é colocada na fila de destino. Um código de conclusão MQCC_FAILED e um código de razão de MQRC_SECURITY_ERROR serão retornados para o aplicativo.

Tabela 101. Comportamento de falha da verificação de CRL do Advanced Message Security (continuação)	
Operação	**Falha na verificação de CRL**
GET	A mensagem é removida da fila de destino e movida para a fila de erros de proteção do sistema. Um código de conclusão MQCC_FAILED e um código de razão de MQRC_SECURITY_ERROR serão retornados para o aplicativo.

O AMS para o z/OS usa serviços do IBM SSL do Sistema para validar certificados, o que inclui verificações de CRL e de confiança. O IBM SSL do Sistema fornece variável de ambiente GSK_CRL_SECURITY_LEVEL para moderar a operação de verificação de CRL. Por exemplo:

```
GSK_CRL_SECURITY_LEVEL=MEDIUM
```

Esta variável é documentada no z/OS Manual de programação do Cryptographic Services System Secure Sockets Layer. Designações válidas incluem:

- LOW - A validação do certificado não falhará se o servidor LDAP não puder ser contatado.
- MEDIUM - A validação do certificado requer que o servidor LDAP seja contatável, mas não requer que uma CRL seja definida.
- HIGH - A validação do certificado requer que o servidor LDAP seja contatável e que uma CRL seja definida.

O padrão do IBM SSL do Sistema é MEDIUM. É possível configurar essa variável no arquivo de configuração especificado por meio do ENVARS DD na tarefa iniciada JLC para o espaço de endereço do AMS. Um arquivo de configuração da variável de ambiente de amostra é fornecido em *thlqual*.SCSQPROC(CSQ40ENV).

Nota: É responsabilidade dos administradores assegurar que serviços LDAP estejam disponíveis e manter as entradas de CRL para Autoridades de certificação relevantes.

Protegendo as senhas no Java

Armazenamento de keystore e senhas de chave privada como texto simples representam um risco de segurança, então o Advanced Message Security fornece uma ferramenta que pode misturar essas senhas usando a chave do usuário, que está disponível no arquivo keystore.

Antes de começar

O proprietário do arquivo `keystore.conf` deve assegurar que somente o proprietário do arquivo esteja intitulado para ler o arquivo. A proteção de senhas descrita neste capítulo é somente uma medida de proteção adicional.

Procedimento

1. Edite o arquivo `keystore.conf` para incluir o caminho para o rótulo de keystore e usuários.

   ```
   jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
   jceks.certificate = AliceCert
   jceks.provider = IBMJCE
   ```

2. Para executar a ferramenta, emita:

   ```
   java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
   private_key_password
   ```

   Uma saída com senhas criptografadas será gerada e poderá ser copiada para o arquivo `keystore.conf`.

Para copiar a saída para o arquivo `keystore.conf` automaticamente, execute:

```
java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
private_key_password >> ~/path_to_keystore/keystore.conf
```

Nota:

Para uma lista de locais padrão do `keystore.conf` em várias plataformas, consulte "Usando keystores e certificados" na página 614.

Exemplo

Aqui está um exemplo de tal saída:

```
#Fri Jul 30 15:20:29 CEST 2010
jceks.key_pass=MMXh997n5ZOr8uRlJmc5qity9MN2CggGBMKCDxdbn1AyPklvdgTsOLG6X3C1YT7oDzwaqZFlOR4t\r\nm
Zsc7JGAx8nqqxLnAucdGn0NWo6xnjZB1n501YGol2k/
PhaQHhFXKMAU9dKg0f8djOtCAOlX4ETe\r\nfYl9LBUt2wk87uM7dSs\=
jceks.keystore_pass=OIdeayBnSCfLG4cFuxEVrk6SYyAsdSPpDqgPf16s9s1M04cqZjNbhgjoA2EXonudHZHH+4s2drvQ
\r\nCUvQgu9GuaBMJK2F2OjtHJJ1Y4BVeLW2c2okgawo/
W2J1AdUYKkJ0raYTkDouLaTYTQeulyG0xIl\r\niD2si1xUCxhYvvyhbbY\=
jceks.encrypted=yes
```

z/OS Usando certificados no z/OS

Sobre esta tarefa

O Advanced Message Security implementa três níveis de proteção: integridade, confidencialidade e privacidade.

Com uma política de integridade, as mensagens são assinadas utilizando a chave privada do originador (o aplicativo que executa o MQPUT). A integridade fornece detecção de modificação de mensagens, mas o próprio texto da mensagem não é criptografado.

Com uma política de confidencialidade, a mensagem é criptografada quando ela é colocada na fila. A mensagem é criptografada usando uma chave simétrica e um algoritmo especificado na política relevante do Advanced Message Security. A própria chave simétrica é criptografada com a chave pública de cada destinatário (o aplicativo que está executando o MQGET). As chaves públicas estão associadas a certificados armazenados em conjuntos de chaves.

Com uma política de privacidade, as mensagens são assinadas e criptografadas.

Quando uma mensagem protegida com privacidade é retirada da fila por um aplicativo de destinatário que está executando um MQGET, a mensagem deve ser decriptografada. Como ela foi criptografada usando a chave pública do destinatário, ela deve ser decriptografada usando a chave privada do destinatário localizada em um conjunto de chaves.

z/OS *Uso de conjuntos de chaves do SAF*

O Advanced Message Security (AMS) faz uso dos serviços do conjunto de chaves SAF do z/OS para definir e gerenciar os certificados necessários para assinatura e criptografia. Produtos de segurança que são funcionalmente equivalentes ao RACF poderão ser usados em vez de RACF, se eles fornecerem o mesmo nível de suporte.

O uso eficaz dos conjuntos de chaves pode reduzir a administração necessária para gerenciar os certificados.

Depois de um certificado ser gerado (ou importado), ele deve ser conectado a um conjunto de chaves para se tornar acessível. O mesmo certificado pode ser conectado a mais de um conjunto de chaves.

O Advanced Message Security usa dois conjuntos de conjuntos de chave. Um conjunto consiste em conjuntos de chaves pertencentes aos IDs do usuário individuais que originam ou recebem mensagens. Cada conjunto de chaves contém a chave privada associada ao certificado do ID do usuário proprietário.

A chave privada de cada certificado é usada para assinar mensagens para filas protegidas por integridade ou protegidas por privacidade. Ela também é usada para decriptografar mensagens de filas protegidas por privacidade ou protegidas por confidencialidade ao receber mensagens.

O outro conjunto é um conjunto de chaves único pertencente ao usuário do espaço de endereço do AMS. Ele contém a cadeia de certificados de autoridade de certificação (CA) de assinatura necessários para validar os certificados do originador e dos destinatários da mensagem.

Quando a proteção de privacidade ou de confidencialidade é usada, o conjunto de chaves pertencente ao usuário do espaço de endereço do AMS também contém os certificados dos destinatários da mensagem. As chaves públicas nesses certificados são usadas para criptografar a chave simétrica que foi usada para criptografar os dados da mensagem quando a mensagem foi colocada na fila protegida. Quando essas mensagens são recuperadas, a chave privada de destinatários relevante é usada para decriptografar a chave simétrica que é então usada para decriptografar os dados da mensagem.

O Advanced Message Security usa um nome de conjunto de chaves de **drq.ams.keyring** ao procurar por certificados e chaves privadas. Esse é o caso para o usuário e também para os conjuntos de chaves do espaço de endereço do AMS.

Para obter uma ilustração e uma explicação adicional sobre certificados e conjuntos de chaves e o seu papel na proteção de dados, consulte Resumo das operações relacionadas a certificado.

A chave privada usada para assinar decriptografa pode ter qualquer rótulo, mas deve estar conectada como o certificado padrão.

Os certificados digitais e conjuntos de chaves são gerenciados no RACF principalmente usando o comando RACDCERT.

Para obter mais informações sobre certificados, rótulos e o comando RACDCERT, consulte *z/OS: Security Server RACF Command Language Reference* e *z/OS: Security Server RACF Security Administrator's Guide*.

z/OS *Autorizando o acesso ao comando RACDCERT*

A autorização para usar o comando RACDCERT é uma tarefa de pós-instalação que deve ter sido concluída pelo seu programador do sistema z/OS. Esta tarefa envolve a concessão de permissões relevantes para o administrador de segurança do Advanced Message Security.

Como um resumo, esses comandos são necessários para permitir o acesso ao comando RACDCERT do RACF:

```
RDEFINE FACILITY IRR.DIGTCERT.* UACC(NONE)
PERMIT IRR.DIGTCERT.* CLASS(FACILITY) ID( admin ) ACCESS(CONTROL)
SETROPTS RACLIST(FACILITY) REFRESH
```

Nesse exemplo, *admin* especifica o ID do usuário do seu administrador de segurança ou qualquer usuário que você deseja que use o comando RACDCERT.

z/OS *Criando os certificados e conjuntos de chaves*

Esta seção documenta as etapas necessárias para criar os certificados e os conjuntos de chaves necessários para usuários do z/OS do Advanced Message Security (AMS), usando uma Autoridade de Certificação (CA) do RACF.

Resolvendo problemas com certificados ao usar o Advanced Message Security no z/OS

Se você tiver tendo problemas com certificados e entradas ausentes nos keystores, será possível ativar um rastreio GSKIT.

No arquivo referenciado pelo ENVARS DD no procedimento de tarefa iniciado AMS, inclua:

```
GSK_TRACE_FILE=/u/... /gsktrace
GSK_TRACE=0xff
```

Consulte Variáveis de ambiente para obter mais informações.

Para cada acesso ao keystore, os dados são gravados no arquivo de rastreio especificado em GSK_TRACE_FILE.

Para formatar o arquivo de rastreio, use o comando:

```
gsktrace inputtrace file > output_file
```

Situação

Um cenário de um aplicativo de envio e um aplicativo de recebimento é usado para explicar as etapas necessárias.

Nos exemplos a seguir, user1 é o originador de uma mensagem e user2 é o destinatário. O ID do usuário do espaço de endereço do Advanced Message Security é WMQAMSD.

Todos os comandos nos exemplos mostrados aqui são emitidos a partir do ISPF opção 6 pelo ID do usuário administrativo admin.

z/OS *Definindo um certificado de Autoridade de certificação local*

Se você estiver usando o RACF como sua CA, deve-se criar um certificado de autoridade de certificação, se já não tiver feito isso. O comando mostrado aqui cria uma autoridade de certificação (ou assinante) do certificado. Este exemplo cria um certificado chamado AMSCA para ser usado ao criar certificados subsequentes que refletem a identidade de usuários e aplicativos do Advanced Message Security.

Este comando pode ser modificado, especificamente SUBJECTSDN, para refletir a estrutura de nomenclatura e convenções usada em sua instalação:

```
RACDCERT CERTAUTH GENCERT SUBJECTSDN(CN('AMSCA') O('ibm') C('us'))
KEYUSAGE(CERTSIGN) WITHLABEL('AMSCA')
```

Nota: Os certificados assinados com este certificado de autoridade de certificação local mostram um emissor de CN=AMSCA,O=ibm,C=us quando listados com o comando RACDCERT LIST.

z/OS *Criando um certificado digital com uma chave privada*

Um certificado digital com uma chave privada deve ser gerado para cada usuário do Advanced Message Security. No exemplo mostrado aqui, os comandos RACDCERT são usados para gerar os certificados para user1 e user2, que são assinados com o certificado de autoridade de certificação local identificado pelo rótulo de 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
```

O comando RACDCERT ALTER é necessário para incluir o atributo TRUST ao certificado. Quando um certificado é criado pela primeira vez usando este procedimento, ele possui um intervalo de data válido diferente do certificado de assinatura. Como resultado, RACF o marca como NOTRUST, o que significa que o certificado não deve ser usado. Use o comando RACDCERT ALTER para configurar o atributo TRUST.

O atributos HANDSHAKE, DATAENCRYPT e DOCSIGN de KEYUSAGE devem ser especificados para certificados usados pelo Advanced Message Security.

Tabela 102. Valores e indicadores de RACDCERT KEYUSAGE

Valor de KEYUSAGE	**Configurar Indicadores**
HANDSHAKE	digitalSignature e keyEncipherment
DATAENCRYPT	dataEncipherment
DOCSIGN	nonRepudiation
CERTSIGN	keyCertSign e cRLSign

z/OS *Criando os conjuntos de chaves do RACF*

Os comandos mostrados aqui criam um conjunto de chaves para os IDs do usuário user1, user2 definidos pelo RACF e o espaço de endereço do usuário da tarefa WMQAMSD do Advanced Message Security. O nome do conjunto de chaves é corrigido pelo Advanced Message Security e deve ser codificado conforme mostrado, sem aspas. O nome faz distinção entre maiúsculas e minúsculas.

```
RACDCERT ID(user1) ADDRING(drq.ams.keyring)
RACDCERT ID(user2) ADDRING(drq.ams.keyring)
RACDCERT ID(WMQAMSD) ADDRING(drq.ams.keyring)
```

z/OS *Conectando os certificados aos conjuntos de chaves*

Conecte os certificados de usuário e CA aos conjuntos de chaves:

```
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))
```

O certificado que contém a chave privada usada para decriptografia deve ser conectado ao conjunto de chaves do usuário como o certificado padrão.

O atributo RACDCERT USAGE(SITE) impedirá a chave privada de ser acessível no conjunto de chaves, enquanto o atributo USAGE RACDCERT(PERSONAL) permite a chave privada seja usada, se ela existir. O certificado do User2 deve estar conectado ao conjunto de chaves do espaço de endereço do Advanced Message Security, já que sua chave pública é necessária para criptografar as mensagens conforme elas são colocadas na fila. USAGE(SITE) limita a exposição da chave privada do user2.

O certificado CERTAUTH com o rótulo AMSCA deve ser conectado ao conjunto de chaves do espaço de endereço do Advanced Message Security porque ele foi usado para assinar o certificado de user1, que é o originador da mensagem. Ele é usado para validar o certificado de assinatura do user1.

z/OS *Verificação do conjunto de chaves*

O conjunto de chaves deve aparecer conforme mostrado aqui, depois que todos os comandos forem inseridos:

```
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
```

Listar os certificados individuais também mostra a associação do conjunto.

```
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<:
```

Para melhorar o desempenho, os conteúdos do drq.ams.keyring associado ao espaço de endereço do AMS são armazenados em cache durante o tempo de vida do espaço de endereço. As mudanças nesse anel de chaves não se tornam efetivas automaticamente. O administrador pode atualizar o cache:

- Parando e reiniciando o gerenciador de filas.
- Usando o comando MODIFY do z/OS:

```
F qmgrAMSM,REFRESH KEYRING
```

Tarefas relacionadas

Operando Advanced Message Security

z/OS *Resumo das operações relacionadas a certificado*

Figura 35 na página 638 ilustra os relacionamentos entre aplicativos de envio e de recebimento e os certificados relevantes. O cenário ilustrado envolve enfileiramento remoto entre dois gerenciadores de filas do z/OS usando uma política de privacidade de proteção de dados. No Figura 35 na página 638, "AMS" indica "Advanced Message Security".

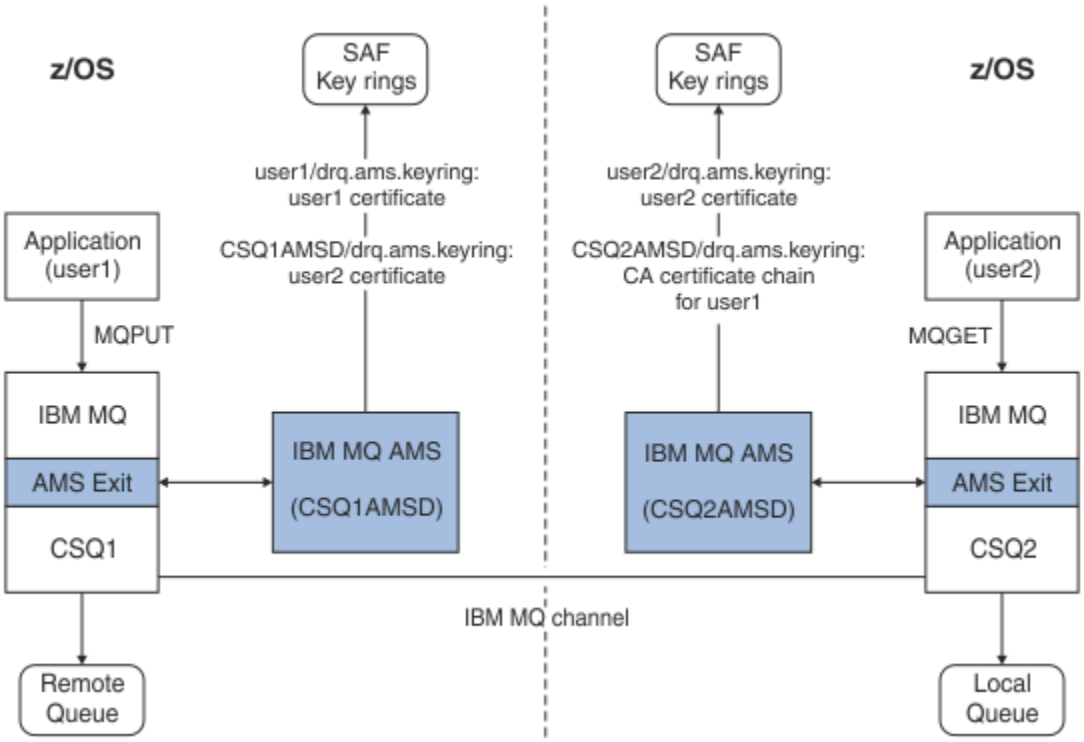


Figura 35. Relacionamentos de aplicativo e certificado

Neste diagrama, um aplicativo em execução como 'user1' coloca uma mensagem em uma fila remota gerenciada pelo gerenciador de filas CSQ1, destinada a ser recuperada por um aplicativo em execução como 'user2' de uma fila local gerenciada pelo gerenciador de filas CSQ2. O diagrama assume uma política de privacidade do Advanced Message Security, a qual significa que a mensagem é assinada e criptografada.

O Advanced Message Security intercepta a mensagem quando uma colocação ocorre e usa o certificado de user2 (armazenado no conjunto de chaves do espaço de endereço do usuário do AMS) para criptografar uma chave simétrica usada para criptografar os dados da mensagem.

Observe que o certificado do user2 é conectado ao conjunto de chaves do usuário do espaço de endereço do AMS com a opção USAGE(SITE). Isso significa que o usuário do espaço de endereço do AMS pode acessar o certificado e a chave pública, mas não a chave privada.

Na extremidade de recebimento, o Advanced Message Security intercepta a obtenção emitida por user2 e usa o certificado do user2 para decriptografar a chave simétrica, para que possa decriptografar os dados da mensagem. Em seguida, ele valida a assinatura do user1 usando a cadeia de certificados de CA do user1 do certificado armazenado no conjunto de chaves do usuário do espaço de endereço do AMS.

Perante este cenário, mas com uma política de integridade de proteção de dados, os certificados para user2 não seriam necessários.

Para usar o enfileiramento de mensagens do Advanced Message Security nas filas protegidas pelo IBM MQ que possuem uma política de proteção de mensagens de privacidade ou integridade, o Advanced Message Security deverá ter acesso a esses itens de dados:

- O certificado X.509 V2 ou V3 e a chave privada para o usuário enfileirar a mensagem.
- A cadeia de certificados usada para assinar os certificados digitais de todos os assinantes da mensagem.
- Se a política de proteção de dados for privacidade, o certificado X.509 V2 ou V3 dos destinatários-alvo. Os destinatários planejados são listados na política do Advanced Message Security associada à fila.

Para os processos e aplicativos que são executados no z/OS, o Advanced Message Security deve ter certificados em dois locais:

- Em um conjunto de chaves gerenciado por SAF associado a identidade do RACF do aplicativo de envio (o aplicativo que enfileira a mensagem protegida) ou o aplicativo de recebimento (se estiver usando privacidade).

  O certificado que o Advanced Message Security localiza é o certificado padrão e deve incluir a chave privada. O Advanced Message Security assume a identidade do usuário do z/OS do aplicativo de envio. Ou seja, ele age como um substituto para que ele possa acessar a chave privada do usuário.
- Em um conjunto de chaves gerenciado pelo SAF associado ao usuário do espaço de endereço do AMS.

  Ao enviar mensagens protegidas com privacidade esse conjunto de chaves contém os certificados de chave pública dos destinatários da mensagem. Ao receber mensagens, ele contém a cadeia de certificados da Autoridade de certificação necessários para validar a assinatura do emissor da mensagem.

Os exemplos anteriores mostrados usaram o RACF como a CA local. No entanto, é possível usar outro fornecedor de PKI (Autoridade de certificação) em sua instalação. Se você pretende usar outro produto PKI, lembre-se de que a chave privada e o certificado deverão ser importados em um conjunto de chaves associado aos IDs de usuário do z/OS RACF que se originam as mensagens do IBM MQ protegidas pelo Advanced Message Security.

É possível usar o comando RACDCERT do RACF como o mecanismo para gerar solicitações de certificado, que podem ser exportadas e enviadas para o provedor de PKI de sua escolha para serem emitidas.

A seguir está um resumo das etapas relacionadas aos certificados:

1. Solicite a criação de um certificado de autoridade de certificação, um no qual o RACF é o CA local. Omita essa etapa se estiver usando outro provedor PKI.
2. Gere certificados de usuário assinados pelo CA.
3. Crie os conjuntos de chaves para os usuários e o ID do espaço de endereço do Advanced Message Security AMS.
4. Conecte o certificado de usuário ao conjunto de chaves do usuário com o atributo padrão.
5. Conecte os certificados de destinatários para conjunto de chaves do usuário do espaço de endereço do Advanced Message Security AMS usando o atributo usage(site) (Essa etapa é necessária somente para certificados de usuário que acabarão por ser os destinatários das mensagens protegidas por privacidade).
6. Conecte as cadeias de certificado de autoridade de certificação para os emissores da mensagem para o conjunto de chaves do usuário do espaço de endereço do Advanced Message Security AMS. (Essa etapa é necessária somente para as tarefas AMS que irão verificar as assinaturas do emissor.)

z/OS *Configurando uma PKI não residente no z/OS*

O Advanced Message Security para z/OS, usa certificados digitais X.509 V3 na proteção de processamento de mensagens colocadas ou recebidos a partir do IBM MQ. O Advanced Message Security em si não cria ou gerencia o ciclo de vida desses certificados; essa função é fornecida por uma infraestrutura de chave pública (PKI). Os exemplos desta publicação que ilustram o uso de certificados usam o z/OS Security Server RACF para preencher solicitações de certificado.

Se uma PKI residente no z/OS ou não residente z/OS é usada ou não, o AMS for z/OS usa apenas os conjuntos de chaves que são gerenciados pelo RACF ou seu equivalente. Esses conjuntos de chaves são baseados em Security Authorization Facility (SAF) e são o repositório usado pelo AMS para z/OS para recuperar certificados para originadores e destinatários das mensagens colocadas ou recebidas nas filas do IBM MQ.

Para as mensagens que são originadas a partir do z/OS, que são protegidas pela política de integridade ou criptografia, o certificado e a chave privada do ID do usuário de origem devem ser armazenados em um conjunto de chaves gerenciados por SAF que está associado ao ID do usuário do z/OS do originador da mensagem.

O RACF inclui a capacidade de importar certificados e chaves privadas para os conjuntos de chaves gerenciados pelo RACF. Consulte as publicações do z/OS Security Server RACF para obter detalhes e exemplos de como carregar certificados nos conjuntos de chaves gerenciados pelo RACF.

Se a sua instalação estiver usando um dos produtos PKI suportados, consulte as publicações que acompanham o produto para obter informações sobre como implementá-lo.

Administrando as políticas de segurança do Advanced Message Security

O Advanced Message Security usa políticas de segurança para especificar a criptografia criptográfica e os algoritmos de assinatura para criptografar e autenticar mensagens que fluem através das filas.

Visão geral das políticas de segurança para AMS

As políticas de segurança do Advanced Message Security são objetos conceituais que descrevem a maneira como uma mensagem é criptograficamente criptografada e assinada.

Para obter detalhes sobre atributos da política de segurança, consulte os subtópicos a seguir:

Conceitos relacionados

"Qualidade de Proteção" na página 644
A proteção de políticas do Advanced Message Security implicam uma qualidade de proteção (QOP).

"Atributos de política de segurança no AMS" na página 643
É possível usar o Advanced Message Security para selecionar um determinado algoritmo ou método para proteger os dados.

Nomes de política no AMS

O nome da política é um nome exclusivo que identifica uma política específica do Advanced Message Security e a fila para a qual ela se aplica.

O nome da política deve ser o mesmo que o nome da fila para a qual ela deve ser aplicada. Há um mapeamento um-para-um entre uma política Advanced Message Security (AMS) e uma fila.

Ao criar uma política com o mesmo nome de uma fila, você ativa a política para essa fila. As filas sem correspondência de nomes de política não são protegidas pelo AMS.

O escopo da política é relevante ao gerenciador de filas local e suas filas. Os gerenciadores de filas remotas devem ter suas próprias políticas definidas localmente para as filas que eles gerenciam.

Algoritmo de assinatura no AMS

O algoritmo de assinatura indica o algoritmo que deve ser usado ao assinar mensagens de dados.

Valores válidos são:

- MD5
- SHA-1
- família: SHA-2
  - SHA256
  - SHA384 (comprimento da chave mínimo aceitável - 768 bits)
  - SHA512 (comprimento da chave mínimo aceitável - 768 bits)

Uma política que não especifica um algoritmo de assinatura ou especifica um algoritmo de NONE, implica que as mensagens colocadas na fila associada à política não são assinadas.

Nota: A qualidade de proteção usada para as funções put e get de mensagem deve corresponder. Se houver uma qualidade de política de incompatibilidade de proteção entre a fila e a mensagem na fila, a mensagem não será aceita e será enviada à fila de manipulação de erros. Essa regra se aplica para ambas as filas locais e remotas.

Algoritmo de criptografia no AMS

O algoritmo de criptografia indica o algoritmo que deve ser usado ao criptografar mensagens de dados colocadas na fila associada à política.

Valores válidos são:

- RC2
- DES
- 3DES
- AES128
- AES256

Uma política que não especifica um algoritmo de criptografia ou especifica um algoritmo de NONE implica que mensagens colocadas na fila associada à política não serão criptografadas.

Observe que uma política que especifica um algoritmo de criptografia diferente de NONE também deve especificar pelo menos um DN de destinatário e um algoritmo de assinatura porque as mensagens criptografadas do Advanced Message Security também são assinadas.

Importante: A qualidade de proteção usada para as funções put e get de mensagem deve corresponder. Se houver uma qualidade de política de incompatibilidade de proteção entre a fila e a mensagem na fila, a mensagem não será aceita e será enviada à fila de manipulação de erros. Essa regra se aplica para ambas as filas locais e remotas.

Tolerância no AMS

O atributo tolerância indica se o Advanced Message Security pode aceitar mensagens com nenhuma política de segurança especificada.

Ao recuperar uma mensagem de uma fila com uma política para criptografar mensagens, se a mensagem não for criptografada, ela será retornada ao aplicativo de chamada. Valores válidos são:

0
Não (**padrão**).

1
Sim.

Uma política que não especifica um valor de tolerância ou especifica 0, significa que as mensagens colocadas na fila associada à política devem corresponder às regras de política.

A tolerância é opcional e existe para facilitar o roll-out de configuração, no qual as políticas foram aplicadas a filas, mas essas filas já contêm mensagens que não possuem uma política de segurança especificada.

Nomes distintos do remetente no AMS

Os nomes distintos (DNs) do emissor identificam usuários que estão autorizados a colocar mensagens em uma fila. Um emissor usa seu certificado para assinar uma mensagem antes de colocar a mensagem em uma fila.

O Advanced Message Security (AMS) não verifica se uma mensagem foi colocada em uma fila protegida por dados por um usuário válido até que a mensagem seja recuperada. Neste momento, se a política estipular um ou mais emissores válidos e o usuário que colocou a mensagem na fila não estiver na lista de emissores válidos, o AMS retornará um erro para o aplicativo de recebimento e colocará a mensagem na fila de erros AMS.

Uma política pode ter zero ou mais DNs do emissor especificado. Se nenhum DNs do emissor for especificado para a política, qualquer emissor poderá colocar mensagens protegidas por dados na fila, desde que o certificado do emissor seja confiável. Um certificado do remetente é confiável incluindo o certificado público em um keystore disponível para o aplicativo de recebimento

Nomes distintos do emissor têm o formato a seguir:

```
CN=Common Name,O=Organization,C=Country
```

Importante:

- Todos os DNs devem estar em maiúsculas. Todos os identificadores de nome do componente no DN devem ser especificados na ordem mostrada na tabela a seguir:

Nome do Componente	Value
CN	O nome comum para o objeto deste DN, como um nome completo ou a finalidade de um dispositivo.
OU	A unidade dentro da organização com o qual o objeto do DN é afiliado, como uma divisão corporativa ou um nome do produto.
O	A organização com a qual o objeto do DN está afiliado, como uma corporação.
L	A localidade (cidade ou municipalidade) onde o objeto do DN está localizado.
Estado	O nome do estado ou da província onde o objeto do DN está localizado.
C	O país onde o objeto do nome distinto (DN) está localizado.

- Se um ou mais DNs de remetentes forem especificados para a política, somente aqueles usuários poderão colocar mensagens na fila associada com a política.
- Os DNs de remetentes, quando especificados, devem corresponder exatamente ao DN contido no certificado digital associado com o usuário que coloca a mensagem.
- O AMS suporta DNs somente com valores do conjunto de caracteres Latin-1. Para criar DNs com caracteres do conjunto, deve-se primeiro criar um certificado com um DN que foi criado na codificação UTF-8 usando o UNIX com a codificação UTF-8 ativada ou com a GUI **strmqikm**. Em seguida, deve-se criar uma política a partir de uma plataforma UNIX com codificação UTF-8 ativada ou usar o plug-in do AMS para IBM MQ.
- O método usado pelo AMS, para converter o nome do emissor de formato x.509 para DN, sempre usa ST= para o valor State ou Province.
- Os seguintes caracteres especiais precisam de caracteres de escape:

```
, (comma)
+ (plus)
" (double quote)
\ (backslash)
< (less than)
> (greater than)
; (semicolon)
```

- Se o Nome distinto contiver espaços em branco integrados, será necessário incluir o DN entre aspas duplas.

Conceitos relacionados

“Nomes distintos do destinatário no AMS” na página 642
Os nomes distintos (DN) do destinatário identificam usuários que estão autorizados a recuperar mensagens em uma fila.

Nomes distintos do destinatário no AMS

Os nomes distintos (DN) do destinatário identificam usuários que estão autorizados a recuperar mensagens em uma fila.

Uma política pode ter zero ou mais DNs do destinatário especificado. Os nomes distintos do destinatário têm o formato a seguir:

```
CN=Common Name,O=Organization,C=Country
```

Importante:

- Todos os DNs devem estar em maiúsculas. Todos os identificadores de nome do componente no DN devem ser especificados na ordem mostrada na tabela a seguir:

Nome do Componente	Value
CN	O nome comum para o objeto deste DN, como um nome completo ou a finalidade de um dispositivo.
OU	A unidade dentro da organização com o qual o objeto do DN é afiliado, como uma divisão corporativa ou um nome do produto.
O	A organização com a qual o objeto do DN está afiliado, como uma corporação.
L	A localidade (cidade ou municipalidade) onde o objeto do DN está localizado.
Estado	O nome do estado ou da província onde o objeto do DN está localizado.
C	O país onde o objeto do nome distinto (DN) está localizado.

- Se nenhum DN de destinatário for especificado para a política, qualquer usuário poderá receber mensagens da fila associada com a política.
- Se um ou mais DNs do destinatário forem especificados para a política, apenas esses usuários poderão obter mensagens da fila associada à política.
- Os DNs de destinatários, quando especificados, devem corresponder exatamente ao DN contido no certificado digital associado com o usuário que recebe a mensagem.
- O Advanced Message Security suporta DNs somente com valores do conjunto de caracteres Latin-1. Para criar DNs com caracteres do conjunto, deve-se primeiro criar um certificado com um DN que foi criado na codificação UTF-8 usando o UNIX com a codificação UTF-8 ativada ou com a GUI **strmqikm**. Em seguida, deve-se criar uma política a partir de uma plataforma UNIX com codificação UTF-8 ativada ou usar o plug-in do Advanced Message Security para IBM MQ.

Conceitos relacionados

"Nomes distintos do remetente no AMS" na página 641
Os nomes distintos (DNs) do emissor identificam usuários que estão autorizados a colocar mensagens em uma fila. Um emissor usa seu certificado para assinar uma mensagem antes de colocar a mensagem em uma fila.

Atributos de política de segurança no AMS

É possível usar o Advanced Message Security para selecionar um determinado algoritmo ou método para proteger os dados.

Uma política de segurança é um objeto conceitual que descreve a maneira como uma mensagem é criptograficamente criptografada e assinada.

Tabela 103. Atributos de política de segurança no AMS	
Atributos	**Descrição**
Nome da política	Nome exclusivo da política para um gerenciador de filas.
Algoritmo de Assinatura	O algoritmo criptográfico que é usado para assinar mensagens antes do envio.
Algoritmo de criptografia	O algoritmo criptográfico que é usado para criptografar mensagens antes do envio.
Lista de destinatários	Lista de nomes distintos (DNs) de certificado dos destinatários em potencial de uma mensagem.
Lista de verificação do DN de assinatura	Lista de DNs de assinatura para serem validados durante a recuperação da mensagem.

No Advanced Message Security, as mensagens são criptografadas com uma chave simétrica e a chave simétrica é criptografada com as chaves públicas dos destinatários. Chaves públicas são criptografadas com o algoritmo RSA, com chaves de um tamanho efetivo de até 2048 bits. A criptografia de chave assimétrica real depende do comprimento da chave do certificado.

Os algoritmos de chave simétrica suportados são os seguintes:

- RC2
- DES
- 3DES
- AES128
- AES256

O Advanced Message Security também suporta as funções hash de criptografia a seguir:

- MD5
- SHA-1
- família: SHA-2
  - SHA256
  - SHA384 (comprimento da chave mínimo aceitável - 768 bits)
  - SHA512 (comprimento da chave mínimo aceitável - 768 bits)

Nota: A qualidade de proteção usada para as funções put e get de mensagem deve corresponder. Se houver uma qualidade de política de incompatibilidade de proteção entre a fila e a mensagem na fila, a mensagem não será aceita e será enviada à fila de manipulação de erros. Essa regra se aplica para ambas as filas locais e remotas.

Qualidade de Proteção

A proteção de políticas do Advanced Message Security implicam uma qualidade de proteção (QOP).

Os três níveis de qualidade de proteção no Advanced Message Security são suplementados por um quarto nível no IBM MQ 9.0 e mais recente e todos eles dependem de algoritmos criptográficos que são usados para assinar e criptografar a mensagem:

- Privacidade - as mensagens colocadas na fila devem ser assinadas e criptografadas.
- Integridade - as mensagens colocadas na fila devem ser assinadas pelo emissor.
- Confidencialidade - as mensagens colocadas na fila devem ser criptografadas. Para obter informações adicionais, consulte “Qualidades de proteção disponíveis com AMS” na página 570
- Nenhum - Nenhuma proteção de dados é aplicável.

Uma política que determina que as mensagens devem ser assinadas quando colocadas em uma fila tem um QOP de INTEGRITY. Um QOP de INTEGRITY significa que uma política estipula um algoritmo de assinatura, mas não estipula um algoritmo de criptografia. As mensagens protegidas por integridade são também referidas como "ASSINADAS".

Uma política que determina que as mensagens devem ser assinadas e criptografadas quando colocadas em uma fila tem um QOP de PRIVACY. Um QOP de PRIVACIDADE significa que uma política estipula um algoritmo de assinatura e um algoritmo de criptografia. As mensagens protegidas por privacidade são também referidas como "SELADAS".

Uma política que estipula que as mensagens deverão ser criptografadas quando colocadas em uma fila tem uma QOP de CONFIDENCIALIDADE. Uma QOP de CONFIDENCIALIDADE significa que uma política estipula um algoritmo de criptografia.

Uma política que não estipula um algoritmo de assinatura ou um algoritmo de criptografia tem um QOP de NONE. O Advanced Message Security não fornece proteção de dados para as filas que possuem uma política com um QOP de NONE.

Gerenciando Políticas de Segurança

Uma política de segurança é um objeto conceitual que descreve a maneira como uma mensagem é criptograficamente criptografada e assinada.

O local do qual todas as tarefas administrativas relacionadas às políticas de segurança são executadas depende de qual plataforma você está usando.

- ULW No UNIX e no Windows, você usa os comandos DELETE POLICY, DISPLAY POLICYe SET POLICY (ou PCF equivalente) para gerenciar suas políticas de segurança.
  - UNIX No UNIX, as tarefas administrativas podem ser executadas em *MQ_INSTALLATION_PATH*/bin.
  - Windows Nas plataformas Windows, as tarefas administrativas podem ser executadas em qualquer local porque a variável de ambiente PATH é atualizada na instalação.
- IBM i No IBM i, os comandos DSPMQMSPL, SETMQMSPL e WRKMQMSPL serão instalados na biblioteca do sistema QSYS para o idioma principal do sistema quando o IBM MQ for instalado.

  As versões de idioma nacional adicionais serão instaladas nas bibliotecas QSYS29xx de acordo com o carregamento do recurso de idioma. Por exemplo, uma máquina com o inglês americano como o idioma principal e o coreano como o idioma secundário possui os comandos em inglês americano instalado em QSYS e o carregamento de idioma secundário em coreano no QSYS2962, já que 2962 é o carregamento de idioma para coreano.
- z/OS No z/OS, os comandos administrativos são executados usando o utilitário de política de segurança da mensagem (CSQ0UTIL). Quando as políticas forem criadas, modificadas ou excluídas no z/OS, as mudanças não serão reconhecidas pelo Advanced Message Security até que o gerenciador de filas seja parado e reiniciado ou o comando MODIFY do z/OS seja usado para atualizar a configuração de política do Advanced Message Security. Por exemplo:

```
F <qmgr ssid>AMSM,REFRESH POLICY
```

Tarefas relacionadas

“Criando políticas de segurança no AMS” na página 646
As políticas de segurança definem a maneira na qual uma mensagem será protegida quando a mensagem for colocada ou como uma mensagem deve ter sido protegida quando uma mensagem é recebida.

“Alterando Políticas de Segurança no AMS” na página 647
É possível usar o Advanced Message Security para alterar detalhes de políticas de segurança que você já definiu.

“Exibindo e fazendo dump de políticas de segurança no AMS” na página 647

Use o comando **dspmqspl** para exibir uma lista de todas as políticas de segurança ou detalhes de uma política denominada dependendo dos parâmetros da linha de comandos que você fornecer.

"Removendo políticas de segurança no AMS" na página 649
Para remover políticas de segurança no Advanced Message Security, deve-se usar o comando `setmqspl`.

Operando Advanced Message Security

Referências relacionadas

O utilitário de política de segurança da mensagem (CSQ0UTIL)

Criando políticas de segurança no AMS

As políticas de segurança definem a maneira na qual uma mensagem será protegida quando a mensagem for colocada ou como uma mensagem deve ter sido protegida quando uma mensagem é recebida.

Antes de começar

Há algumas condições de entrada que devem ser atendidas ao criar políticas de segurança:

- O gerenciador de filas deve estar em execução.
- O nome de uma política de segurança deve seguir Regras para nomenclatura de objetos IBM MQ.
- Deve-se ter a autoridade necessária para se conectar ao gerenciador de filas e criar uma política de segurança:
  - z/OS No z/OS, conceda as autoridades documentadas em O utilitário de política de segurança da mensagem (CSQ0UTIL).
  - Multi Em outras plataformas diferentes de z/OS, deve-se conceder as autoridades +connect, +inq e +chg necessárias usando o comando setmqaut.

  Para obter mais informações sobre como configurar a segurança, consulte "Configurar a segurança" na página 128.
- z/OS No z/OS, assegure-se de que os objetos do sistema necessários foram definidos de acordo com as definições em CSQ4INSM.

Exemplo

A seguir há um exemplo da criação de uma política no gerenciador de filas QMGR. A política especifica que as mensagens sejam assinadas usando o algoritmo SHA256 e criptografadas usando o algoritmo AES256 para certificados com DN: CN=joe,O=IBM,C=US and DN: CN=jane,O=IBM,C=US. Essa política está conectada ao `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
```

Aqui está um exemplo de criação de política no gerenciador de filas QMGR. A política especifica que as mensagens sejam criptografadas usando o algoritmo 3DES para certificados com DNs: CN=john,O=IBM,C=US and CN=jeff,O=IBM,C=US e assinadas com o algoritmo SHA256 para o certificado com DN: 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
```

Nota:

- A qualidade da proteção sendo usada para a mensagem de colocação e obtenção deve corresponder. Se a qualidade da política de proteção que é definida para a mensagem for mais fraca do que a definida para uma fila, a mensagem será enviada para a fila de manipulação de erros. Esta política é válida para as filas local e remota.

Referências relacionadas

Lista completa dos atributos do comando setmqspl

Alterando Políticas de Segurança no AMS

É possível usar o Advanced Message Security para alterar detalhes de políticas de segurança que você já definiu.

Antes de começar

- O gerenciador de filas no qual deseja operar deve estar em execução.
- Deve-se ter a autoridade necessária para se conectar ao gerenciador de filas e criar uma política de segurança.
  - z/OS No z/OS, conceda as autoridades documentadas em O utilitário de política de segurança da mensagem (CSQ0UTIL).
  - Multi Em outras plataformas diferentes de z/OS, deve-se conceder as autoridades +connect, +inq e +chg necessárias usando o comando setmqaut.

  Para obter mais informações sobre como configurar a segurança, consulte “Configurar a segurança” na página 128.

Sobre esta tarefa

Para mudar as políticas de segurança, aplique o comando `setmqspl` a uma política já existente fornecendo novos atributos.

Exemplo

Aqui está um exemplo da criação de uma política denominada MYQUEUE em um gerenciador de filas denominado QMGR, especificando que as mensagens devem ser criptografadas usando o algoritmo 3DES para autores (**-a**) que possuem certificados com Nome Distinto (DN) de CN=alice, O=IBM, C=US e assinado com o algoritmo SHA256 para destinatários (**-r**) que possuem certificados com DN de 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
```

Para alterar essa política, emita o comando `setmqspl` com todos os atributos do exemplo, mudando somente os valores que você deseja modificar. Neste exemplo, a política criada anteriormente é conectada a uma nova fila e seu algoritmo de criptografia é mudado para AES256:

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA256 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Referências relacionadas

setmqspl (configurar política de segurança)

Exibindo e fazendo dump de políticas de segurança no AMS

Use o comando **dspmqspl** para exibir uma lista de todas as políticas de segurança ou detalhes de uma política denominada dependendo dos parâmetros da linha de comandos que você fornecer.

Antes de começar

- Para exibir detalhes de políticas de segurança, o gerenciador de filas deve existir e estar em execução.
- Deve-se ter a autoridade necessária para se conectar ao gerenciador de filas e criar uma política de segurança.
  - z/OS No z/OS, conceda as autoridades documentadas em O utilitário de política de segurança da mensagem (CSQ0UTIL).

– Multi Em outras plataformas diferentes de z/OS, deve-se conceder as autoridades +connect, +inq e +chg necessárias usando o comando setmqaut.

Para obter mais informações sobre como configurar a segurança, consulte “Configurar a segurança” na página 128.

Sobre esta tarefa

Aqui está a lista de sinalizadores de comando **dspmqspl**:

*Tabela 104. Sinalizadores de comando **dspmqspl**.*

Sinalizador de comando	Explanation
-m	Nome do gerenciador de filas (obrigatório).
-p	Nome da política.
-export	Incluir este sinalizador gera uma saída que pode ser facilmente aplicada a um gerenciador de filas diferente.

Exemplo

O exemplo a seguir mostra como criar duas políticas de segurança para `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
```

Este exemplo mostra um comando que exibe detalhes de todas as políticas definidas para `venus.queue.manager` e a saída que ele produz:

```
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
```

Este exemplo mostra um comando que exibe detalhes de uma política de segurança selecionada definida para `venus.queue.manager` e a saída que ela produz:

```
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
```

No próximo exemplo, em primeiro lugar, criamos uma política de segurança e, em seguida, exportamos a política usando o sinalizador **-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 No z/OS, as informações de política exportadas são gravadas pelo CSQ0UTIL para o EXPORT DD.

Multi Em plataformas diferentes de z/OS, redirecione a saída para um arquivo, por exemplo:

```
dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Para importar uma política de segurança:

- Windows No Windows, execute `policies.bat`.
- UNIX No UNIX:
  1. Efetue logon como um usuário que pertence ao grupo de administração `mqm` IBM MQ.
  2. Emita `. policies.sh`..
- z/OS No z/OS use o usuário CSQ0UTIL, especificando SYSIN para o conjunto de dados que contém as informações da política exportada.

Referências relacionadas

Lista completa dos atributos do comando dspmqspl

Removendo políticas de segurança no AMS

Para remover políticas de segurança no Advanced Message Security, deve-se usar o comando `setmqspl`.

Antes de começar

Há algumas condições de entrada que devem ser atendidas ao gerenciar políticas de segurança:

- O gerenciador de filas deve estar em execução.
- Deve-se ter a autoridade necessária para se conectar ao gerenciador de filas e criar uma política de segurança.
  - z/OS No z/OS, conceda as autoridades documentadas em O utilitário de política de segurança da mensagem (CSQ0UTIL).
  - Multi Em outras plataformas diferentes de z/OS, deve-se conceder as autoridades +connect, +inq e +chg necessárias usando o comando setmqaut.

  Para obter mais informações sobre como configurar a segurança, consulte “Configurar a segurança” na página 128.

Sobre esta tarefa

Use o comando **setmqspl** com a opção **-remove**.

Exemplo

Aqui está um exemplo de remoção de uma política:

```
setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

Referências relacionadas

Lista completa dos atributos do comando setmqspl

Proteção da fila do sistema no AMS

As filas do sistema ativam a comunicação entre IBM MQ e seus aplicativos auxiliares. Sempre que um gerenciador de filas é criado, uma fila do sistema também é criada para armazenar mensagens internas e dados das mensagens do IBM MQ. É possível proteger filas do sistema com o Advanced Message Security para que somente usuários autorizados possam acessá-las ou decriptografá-las.

A proteção de fila do sistema segue o mesmo padrão que a proteção das filas regulares. Consulte o “Criando políticas de segurança no AMS” na página 646.

Windows Para usar a proteção de fila do sistema no Windows, copie o arquivo `keystore.conf` para o diretório a seguir:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

z/OS No z/OS, para fornecer proteção para o `SYSTEM.ADMIN.COMMAND.QUEUE`, o servidor de comandos deve ter acesso ao `keystore` e ao `keystore.conf`, que contêm chaves e uma configuração para que o servidor de comandos possa acessar chaves e certificados Todas as mudanças feitas na política de segurança de `SYSTEM.ADMIN.COMMAND.QUEUE` requerem o reinício do servidor de comandos.

Todas as mensagens que são enviadas e recebidas da fila de comandos são assinadas ou assinadas e criptografadas dependendo das configurações de política. Se um administrador define os signatários autorizados, as mensagens de comando que não passam pela verificação do Nome distinto (DN) do assinante não são executadas pelo servidor de comandos e não são roteadas para a fila de manipulação de erros do Advanced Message Security. Mensagens que são enviadas como respostas para as filas dinâmicas temporárias do IBM MQ Explorer não são protegidas pelo AMS.

As políticas de segurança não têm efeito sobre as filas SYSTEM a seguir:

- 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

Concedendo permissões OAM

As permissões de arquivo autorizam todos os usuários a executar os comandos `setmqspl` e `dspmqspl`. No entanto, o Advanced Message Security depende do gerenciador de autoridade de objeto (OAM) e cada tentativa de executar estes comandos por um usuário que não pertence ao grupo mqm, que é o grupo de administração do IBM MQ ou não tem permissões para ler as configurações de política de segurança que são concedidas, resulta em um erro.

Procedimento

Para conceder as permissões necessárias para um usuário, execute:

```
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
```

Nota: É necessário somente configurar estas autoridades OAM se você pretende conectar clientes para o gerenciador de filas usando o Advanced Message Security 7.0.1.

Atenção: A autoridade de navegação para SYSTEM.PROTECTION.POLICY.QUEUE não é obrigatório em todas as situações. O IBM MQ otimiza o desempenho armazenando em cache políticas para que você não tenha que procurar registros para obter detalhes da política no SYSTEM.PROTECTION.POLICY.QUEUE em todos os casos..

O IBM MQ não armazena em cache todas as políticas disponíveis. Se houver um grande número de políticas, o IBM MQ armazenará em cache um número limitado de políticas. Portanto, se o gerenciador de filas tiver um número baixo de políticas definidas, não haverá a necessidade de fornecer a opção de navegação para o SYSTEM.PROTECTION.POLICY.QUEUE.

No entanto, é necessário dar autoridade de navegação a essa fila nos casos em que há um grande número de políticas definidas ou quando você está usando clientes antigos. O SYSTEM.PROTECTION.ERROR.QUEUE é usado para colocar mensagens de erro geradas pelo código AMS. A autoridade put para essa fila é verificada apenas quando você tenta colocar uma mensagem de erro na fila. Sua autoridade put em relação à fila não é verificada quando você tenta colocar ou obter mensagens de uma fila protegida por AMS.

Concedendo permissões de segurança

Ao usar a segurança de recurso do comando, deve-se configurar as permissões para permitir que o Advanced Message Security funcione. Este tópico usa comandos do RACF nos exemplos. Se a sua empresa usa um gerenciador de segurança externo (ESM) diferente, deve-se usar os comandos equivalentes para esse ESM.

Há três aspectos para a concessão de permissões de segurança:

- "O espaço de endereço AMSM" na página 652
- "CSQ0UTIL" na página 653
- "Usando filas que possuem uma política do Advanced Message Security definida" na página 653

Notes: Os exemplos de comando usam as variáveis a seguir.

1. *QMgrName* - o nome do gerenciador de filas.

   z/OS No z/OS, esse valor também pode ser o nome de um grupo de filas compartilhadas.
2. *username* - este pode ser um nome de grupo.
3. Os exemplos mostram a classe MQQUEUE. isso também pode ser MXQUEUE, GMQQUEUE ou GMXQUEUE. Consulte "Perfis para Segurança de Fila" na página 200 para obter informações adicionais.

Além disso, se o perfil já existir, o comando RDEFINE não será necessário.

O espaço de endereço AMSM

É necessário emitir alguma segurança do IBM MQ para o nome do usuário no qual o espaço de endereço do Advanced Message Security é executado.

- Para conexão em lotes para o gerenciador de filas, emita

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
          PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Para obter acesso à SYSTEM.PROTECTION.POLICY.QUEUE, emita:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
           PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

CSQ0UTIL

O utilitário que permite que os usuários executem os comandos **setmqspl** e **dspmqspl** requer as permissões a seguir, no qual o nome do usuário é o ID do usuário do cargo:

- Para conexão em lotes para o gerenciador de filas, emita:

```
  RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
            PERMIT QMgrName.BATCH CLASS(MQCONN) ID(username) ACCESS(READ)
```

- Para acesso ao SYSTEM.PROTECTION.POLICY.QUEUE, necessário para o comando **setmqpol**, emita:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
             PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(ALTER)
```

- Para acesso ao SYSTEM.PROTECTION.POLICY.QUEUE, necessário para o comando **dspmqpol**, emita:

```
  RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
               PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

Usando filas que possuem uma política do Advanced Message Security definida

Quando um aplicativo realiza qualquer trabalho com filas que têm uma política definida nelas, o aplicativo requer permissões adicionais para permitir que o Advanced Message Security proteja as mensagens.

O aplicativo requer:

- Acesso de leitura ao SYSTEM.PROTECTION.POLICY.QUEUE. Faça isso emitindo:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE UACC(NONE)
          PERMIT QMgrName.SYSTEM.PROTECTION.POLICY.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

- Acesso de colocação ao SYSTEM.PROTECTION.ERROR.QUEUE. Faça isso emitindo:

```
RDEFINE MQQUEUE QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE UACC(NONE)
            PERMIT QMgrName.SYSTEM.PROTECTION.ERROR.QUEUE CLASS(MQQUEUE)
ID(username) ACCESS(READ)
```

IBM i Configurando certificados e o arquivo de configuração keystore no IBM i

Sua primeira tarefa ao configurar a proteção do Advanced Message Security é criar um certificado e associá-lo ao seu ambiente. A associação é configurada através de um arquivo mantido no sistema de arquivos integrado (IFS).

Procedimento

1. Para criar um certificado autoassinado usando o conjunto de ferramentas OpenSSL enviado com o IBM i, emita o seguinte comando a partir de QShell:

   ```
   /QOpenSys/usr/bin/openssl req -x509 -newkey rsa:2048 -keyout
   $HOME/private.pem -out $HOME/mycert.pem -nodes -days 365
   ```

   O comando solicita vários atributos de nome distinto para um novo certificado autoassinado, incluindo:

- Nome comum (CN=)
- Organização (O=)
- País (C=)

Isso cria uma chave privada não criptografada e um certificado correspondente, ambos em PEM (Privacy Enhanced Mail) formato.

Para simplificar, simplesmente insira os valores para nome comum, organização e país. Esses atributos e valores são importantes ao criar uma política.

Prompts e atributos adicionais podem ser customizados especificando um arquivo de configuração openssl customizado na linha de comandos com o parâmetro **-config**. Consulte a documentação do OpenSSL para obter mais detalhes sobre a sintaxe do arquivo de configuração.

Por exemplo, o comando a seguir inclui extensões adicionais do certificado 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
```

em que myconfig.cnf é um arquivo de fluxo ASCII que contém o seguinte:

```
[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. O AMS requer que o certificado e a chave privada sejam mantidos no mesmo arquivo. Emita o comando a seguir para fazer isso:

```
cat $HOME/mycert.pem >> $HOME/private.pem
```

O arquivo `private.pem` em $HOME agora contém uma chave privada e certificado correspondentes, enquanto o arquivo `mycert.pem` contém todos os certificados públicos para o qual é possível criptografar mensagens e validar assinaturas.

Os dois arquivos precisam ser associados ao seu ambiente criando um arquivo de configuração de keystore, `keystore.conf`, em sua localização padrão.

Por padrão, o AMS procura a configuração de keystore em um subdiretório `.mqs` do seu diretório inicial.

3. No QShell, crie o arquivo `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 *Criando uma política no IBM i*

Antes de criar uma política, você precisa criar uma fila para manter as mensagens protegidas.

Procedimento

1. Em um prompt de linha de comandos insira;

   ```
   CRTMQMQ QNAME(PROTECTED) QTYPE(*LCL) MQMNAME (mqmname)
   ```

   em que mqmname é o nome do gerenciador de filas.

   Use o comando DSPMQM para verificar se o gerenciador de filas é capaz de usar políticas de segurança. Assegure que **Security Policy Capability** mostre **YES*.

   A política mais simples que é possível definir é uma política de integridade, que é obtida criando uma política com um algoritmo de assinatura digital, mas nenhum algoritmo de criptografia.

   As mensagens são assinadas, mas não criptografadas. Se as mensagens devem ser criptografadas, deve-se especificar um algoritmo de criptografia e um ou mais destinatários de mensagem desejados.

   Um certificado no keystore público para um destinatário da mensagem desejada é identificada por meio de um nome distinto.
2. Exiba os nomes distintos dos certificados no keystore público, `mycert.pem` em $HOME, usando o comando a seguir no QShell:

   ```
   /QOpenSys/usr/bin/openssl x509 -in $HOME/mycert.pem -noout -subject -nameopt RFC2253
   ```

   É necessário inserir o nome distinto como um destinatário-alvo e o nome da política deve corresponder ao nome da fila a ser protegido.
3. Em um prompt de comandos da CL insira, por exemplo:

   ```
   SETMQMSPL POLICY(PROTECTED) MQMNAME (mqmname)SIGNALG(*SHA256) ENCALG(*AES256) RECIP('CN=..,
   O=.., C=..')
   ```

   em que mqmname é o nome do gerenciador de filas.

   Depois de criar a política, quaisquer mensagens que sejam colocadas, procuradas ou removidas destrutivamente através desse nome da fila estão sujeitas à política do AMS.

Referências relacionadas

Exibir Gerenciador da Fila de Mensagens (DSPMQM)

Configurar a Política de segurança do MQM (SETMQMSPL)

IBM i *Testando a política no IBM i*

Use os aplicativos de amostra fornecidos com o produto para testar suas políticas de segurança.

Sobre esta tarefa

É possível usar os aplicativos de amostra fornecidos com o IBM MQ, tais como AMQSPUT4, AMQSGET4, AMQSGBR4 e ferramentas como WRKMQMMSG para colocar, procurar e obter mensagens usando o nome da fila PROTECTED.

Desde que tudo seja configurado corretamente, não deve haver diferença no comportamento do aplicativo para o de uma fila não protegida para este usuário.

Um usuário não configurado para Advanced Message Security ou um usuário que não tem a chave privada necessária para decriptografar a mensagem, contudo, não poderá visualizar a mensagem. O usuário recebe um código de conclusão de RCFAIL, equivalente a MQCC_FAILED (2) e o código de razão de RC2063 (MQRC_SECURITY_ERROR).

Para ver se a proteção AMS está em vigor coloque algumas mensagens de teste para a fila PROTECTED, por exemplo usando AMQSPUT0. É possível então criar uma fila de alias para procurar os dados brutos protegidos enquanto em repouso.

Procedimento

Para conceder as permissões necessárias para um usuário, execute:

```
CRTMQMQ QNAME(ALIAS) QTYPE(*ALS) TGTQNAME(PROTECTED) MQMNAME(yourqm)
```

Procurar usando o nome da fila ALIAS, por exemplo usando AMQSBCG4 ou WRKMQMMSG, deve revelar mensagens `scrambled` maiores em que uma procura da fila PROTECTED mostra mensagens de texto não criptografado.

As mensagens misturadas são visíveis, mas o texto não criptografado original não é decifrável usando a fila ALIAS, pois não há política para o AMS reforçar a correspondência a esse nome. Portanto, os dados brutos protegidos são retornados.

Referências relacionadas

Configurar a Política de segurança do MQM (SETMQMSPL)

Trabalhar com Mensagens MQ (WRKMQMMSG)

Eventos de comando e configuração

Com o Advanced Message Security, é possível gerar mensagens de eventos de comando e configuração, que podem ser registradas e servir como um registro das mudanças da política para auditoria.

Os eventos de comando e configuração gerados pelo IBM MQ são mensagens do formato PCF enviadas para filas dedicadas no gerenciador de filas no qual o evento ocorre.

As mensagens de eventos de configuração são enviadas para a fila SYSTEM.ADMIN.CONFIG.EVENT.

As mensagens de eventos de comando são enviadas para a fila SYSTEM.ADMIN.COMMAND.EVENT.

Os eventos são gerados independentemente de ferramentas que você está usando para gerenciar as políticas de segurança do Advanced Message Security .

No Advanced Message Security, há quatro tipos de eventos gerados por diferentes ações em políticas de segurança:

- “Criando políticas de segurança no AMS” na página 646, que geram duas mensagens do evento do IBM MQ:
  - Um evento de configuração
  - Um evento de comando
- “Alterando Políticas de Segurança no AMS” na página 647, que gera três mensagens do evento do IBM MQ:
  - Um evento de configuração que contém os antigos valores de política de segurança
  - Um evento de configuração que contém os novos valores de política de segurança
  - Um evento de comando
- “Exibindo e fazendo dump de políticas de segurança no AMS” na página 647, que gera uma mensagem do evento do IBM MQ:
  - Um evento de comando
- “Removendo políticas de segurança no AMS” na página 649, que gera duas mensagens do evento do IBM MQ:
  - Um evento de configuração
  - Um evento de comando

Ativando e desativando a criação de log de eventos

Você controla eventos de comando e configuração usando os atributos do gerenciador de filas **CONFIGEV** e **CMDEV**. Para ativar esses eventos, configure o atributo do gerenciador de filas apropriado para ENABLED. Para desativar esses eventos, configure o atributo apropriado do gerenciador de filas para DISABLED.

Procedimento

Eventos de Configuração

Para ativar eventos de configuração, configure **CONFIGEV** para ENABLED. Para desativar eventos de configuração, configure **CONFIGEV** para DISABLED. Por exemplo, é possível ativar eventos de configuração usando o comando MQSC a seguir:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Eventos de Comando

Para ativar eventos de comando, configure **CMDEV** para ENABLED. Para ativar eventos de comandos, exceto comandos **DISPLAY MQSC** e Inquire PCF, configure **CMDEV** para NODISPLAY. Para desativar eventos de comando, configure **CMDEV** para DISABLED. Por exemplo, é possível ativar eventos de comandos usando o comando MQSC a seguir:

```
ALTER QMGR CMDEV (ENABLED)
```

Tarefas relacionadas

Controlando os eventos de configuração, de comando e de criador de logs no IBM MQ

Formato da mensagem do evento de comando

A mensagem do evento de comando consiste em estrutura MQCFH e os parâmetros PCF a seguir.

Aqui estão os valores MQCFH selecionados:

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

Nota: O valor ParameterCount é dois porque sempre existem dois parâmetros do tipo MQCFGR (grupo). Cada grupo é constituído de parâmetros apropriados. Os dados do evento consistem em dois grupos, CommandContext e CommandData.

CommandContext contém:

EventUserID

Descrição :	O ID do usuário que emitiu o comando ou a chamada que gerou o evento. (Este é o mesmo ID do usuário que será usado para verificar a autoridade para emitir o comando ou chamada; para comandos recebidos de uma fila, este também será o identificador do usuário (UserIdentifier) do MD da mensagem de comando).
Identificador	MQCACF_EVENT_USER_ID.
Tipo de dado:	MQCFST.
Comprimento Máximo:	MQ_USER_ID_LENGTH.
Retornado:	Sempre.

EventOrigin

Descrição : A origem da ação que causou o evento.

Identificador MQIACF_EVENT_ORIGIN.

Tipo de dado: MQCFIN.

Valores:

MQEVO_CONSOLE
Comando de console - linha de comandos.

MQEVO_MSG
Mensagem de comando do plug-in do IBM MQ Explorer.

Retornado: Sempre.

EventQMgr

Descrição : O gerenciador de filas no qual o comando ou chamada foi inserido. (O gerenciador de filas no qual o comando é executado e que gera o evento está no MD da mensagem do evento).

Identificador MQCACF_EVENT_Q_MGR.

Tipo de dado: MQCFST.

Comprimento Máximo: MQ_Q_MGR_NAME_LENGTH.

Retornado: Sempre.

EventAccountingToken

Descrição : Para comandos recebidos como uma mensagem (MQEVO_MSG), o token de conta (AccountingToken) do MD da mensagem de comando.

Identificador MQBACF_EVENT_ACCOUNTING_TOKEN.

Tipo de dado: MQCFBS.

Comprimento Máximo: MQ_ACCOUNTING_TOKEN_LENGTH.

Retornado: Somente se EventOrigin for MQEVO_MSG.

EventIdentityData

Descrição : Para comandos recebidos como uma mensagem (MQEVO_MSG), os dados de identificação do aplicativo (ApplIdentityData) do MD da mensagem de comando.

Identificador MQCACF_EVENT_APPL_IDENTITY.

Tipo de dado: MQCFST.

Comprimento Máximo: MQ_APPL_IDENTITY_DATA_LENGTH.

Retornado: Somente se EventOrigin for MQEVO_MSG.

EventApplType

Descrição : Para comandos recebidos como uma mensagem (MQEVO_MSG), o tipo do aplicativo (PutApplType) do MD da mensagem de comando.

Identificador MQIACF_EVENT_APPL_TYPE.

Tipo de dado: MQCFIN.

Retornado: Somente se EventOrigin for MQEVO_MSG.

EventApplName

Descrição : Para comandos recebidos como uma mensagem (MQEVO_MSG), o nome do aplicativo (PutApplName) do MD da mensagem de comando.

Identificador MQCACF_EVENT_APPL_NAME.

Tipo de dado: MQCFST.

Comprimento Máximo: MQ_APPL_NAME_LENGTH.

Retornado: Somente se EventOrigin for MQEVO_MSG.

EventApplOrigin

Descrição : Para comandos recebidos como uma mensagem (MQEVO_MSG), os dados de origem do aplicativo (ApplOriginData) do MD da mensagem de comando.

Identificador MQCACF_EVENT_APPL_ORIGIN.

Tipo de dado: MQCFST.

Comprimento Máximo: MQ_APPL_ORIGIN_DATA_LENGTH.

Retornado: Somente se EventOrigin for MQEVO_MSG.

Comando:

Descrição : O código de comando.

Identificador MQIACF_COMMAND.

Tipo de dado: MQCFIN.

Valores: **MQCMD_INQUIRE_PROT_POLICY valor numérico 205**
MQCMD_CREATE_PROT_POLICY valor numérico 206
MQCMD_DELETE_PROT_POLICY valor numérico 207
MQCMD_CHANGE_PROT_POLICY valor numérico 208
Estes são definidos no IBM MQ 8.0 `cmqcfc.h`

Retornado: Sempre.

CommandData contém elementos PCF que incluem o comando PCF.

Formato da mensagem do evento de configuração

Os eventos de configuração são mensagens PCF de formato padrão do Advanced Message Security.

Valores possíveis para o descritor de mensagens MQMD podem ser localizados em Mensagem do evento MQMD (descritor de mensagens)

Aqui estão os valores MQMD selecionados:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR           //for both CLI and command server
```

O buffer de mensagem consiste na estrutura MQCFH e a estrutura de parâmetros que a segue. Valores possíveis do MQCFH podem ser localizados em Mensagem do evento MQCFH (cabeçalho PCF).

Aqui estão os valores MQCFH selecionados:

```
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}
```

Os parâmetros seguindo MQCFH são:

EventUserID

Descrição : O ID do usuário que emitiu o comando ou a chamada que gerou o evento. (Este é o mesmo ID do usuário que será usado para verificar a autoridade para emitir o comando ou chamada; para comandos recebidos de uma fila, este também será o identificador do usuário (UserIdentifier) do MD da mensagem de comando).

Identificador **MQCACF_EVENT_USER_ID**

Tipo de dado: MQCFST.

Comprimento Máximo: MQ_USER_ID_LENGTH.

Retornado: Sempre.

SecurityId

Descrição : Valor de MQMD.AccountingToken no caso de mensagem do servidor de comandos ou SID do Windows para comando local.

Identificador **MQBACF_EVENT_SECURITY_ID**

Tipo de dado: MQCBS.

Comprimento Máximo: MQ_SECURITY_ID_LENGTH.

Retornado: Sempre.

EventOrigin

Descrição : A origem da ação que causou o evento.

Identificador **MQIACF_EVENT_ORIGIN**

Tipo de dado: MQCFIN.

Valores:

MQEVO_CONSOLE
Comando de console - linha de comandos.

MQEVO_MSG
Mensagem de comando a partir do plug-in do IBM MQ Explorer.

Retornado: Sempre.

EventQMgr

Descrição : O gerenciador de filas no qual o comando ou chamada foi inserido. (O gerenciador de filas no qual o comando é executado e que gera o evento está no MD da mensagem do evento).

Identificador **MQCACF_EVENT_Q_MGR**

Tipo de dado: MQCFST

Comprimento Máximo: MQ_Q_MGR_NAME_LENGTH

Retornado: Sempre.

ObjectType

Descrição : Tipo de objeto.

Identificador **MQIACF_OBJECT_TYPE**

Tipo de dado: MQCFIN

Valor: **MQOT_PROT_POLICY**
Política de proteção do Advanced Message Security. **1019 -** um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Retornado: Sempre.

PolicyName

Descrição : O nome da política do Advanced Message Security.

Identificador **MQCA_POLICY_NAME**.

Tipo de dado: MQCFST.

Valor: **2112 -** um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Comprimento Máximo: MQ_OBJECT_NAME_LENGTH.

Retornado: Sempre.

PolicyVersion

Descrição : A versão da política do Advanced Message Security.

Identificador **MQIA_POLICY_VERSION**

Tipo de dado: MQCFIN

Value **238 -** um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h` .

Retornado: Sempre

TolerateFlag

Descrição : O sinalizador de tolerância de política do Advanced Message Security.

Identificador **MQIA_TOLERATE_UNPROTECTED**

Tipo de dado: MQCFIN

Value **235 -** um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Retornado: Sempre.

SignatureAlgorithm

Descrição : O algoritmo de assinatura da política do Advanced Message Security.

Identificador **MQIA_SIGNATURE_ALGORITHM**

Tipo de dado: MQCFIN

Valor: **236 -** um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Retornado: Sempre que houver um algoritmo de assinatura definido na política do Advanced Message Security

EncryptionAlgorithm

Descrição : O algoritmo de criptografia da política do Advanced Message Security.

Identificador **MQIA_ENCRYPTION_ALGORITHM**

Tipo de dado: MQCFIN

Valor: **237** - um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Retornado: Sempre que houver um algoritmo de criptografia definido na política do IBM MQ

SignerDNs

Descrição : Assunto DistinguishedName dos assinantes permitidos.

Identificador **MQCA_SIGNER_DN**

Tipo de dado: MQCFSL

Valor: **2113** - um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Comprimento Máximo: Maior DN de assinante na política, mas não maior que MQ_DISTINGUISHED_NAME_LENGTH

Retornado: Sempre definido na política IBM MQ.

RecipientDNs

Descrição : Assunto DistinguishedName dos assinantes permitidos.

Identificador **MQCA_RECIPIENT_DN**

Tipo de dado: MQCFSL

Valor: **2114** - um valor numérico definido no IBM MQ 8.0 ou no arquivo `cmqc.h`.

Comprimento Máximo: Maior DN do destinatário na política, mas não maior que MQ_DISTINGUISHED_NAME_LENGTH.

Retornado: Sempre definido na política IBM MQ.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte seu representante local do IBM para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um IBM produto, programa ou serviço não se destina a estado ou significa que apenas esse produto IBM, programas ou serviços possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou aplicativos de patentes pendentes relativas aos assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum sobre tais patentes. é possível enviar pedidos de licença, por escrito, para:

Relações Comerciais e Industriais da IBM
Av. Pasteur, 138-146
Botafogo
Rio, RJ 10504-1785
U.S.A.

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

licença de propriedade intelectual
IBM World Trade Asia Corporation Licensing
IBM Japan, Ltd.
Minato-ku
Tóquio 103-8510, Japão

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas nas informações aqui contidas; essas alterações serão incorporadas em futuras edições desta publicação. IBM pode aperfeiçoar e/ou alterar no produto(s) e/ou programa(s) descritos nesta publicação a qualquer momento sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Av. Pasteur, 138-146
Av. Pasteur, 138-146

Botafogo
Rio de Janeiro, RJ
U.S.A.

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do IBM Customer Agreement, IBM Contrato de Licença do Programa Internacional ou qualquer contrato equivalente entre as partes.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disto, algumas medidas podem ter sido estimadas através de extrapolação. Os resultados reais podem variar. usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente a seus fornecedores.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio e representam somente metas e objetivos.

Essas informações contêm exemplos de dados e relatórios utilizados em operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT :

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, uso, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas.

Se estiver visualizando estas informações em formato eletrônico, as fotografias e ilustrações coloridas poderão não aparecer.

Informações sobre a Interface de Programação

As informações da interface de programação, se fornecidas, destinam-se a ajudá-lo a criar software aplicativo para uso com este programa.

Este manual contém informações sobre interfaces de programação desejadas que permitem que o cliente grave programas para obter os serviços do WebSphere MQ.

No entanto, estas informações também podem conter informações sobre diagnósticos, modificações e ajustes. As informações sobre diagnósticos, modificações e ajustes são fornecidas para ajudá-lo a depurar seu software aplicativo.

Importante: Não use essas informações de diagnóstico, modificação e ajuste como uma interface de programação, pois elas estão sujeitas a mudanças

Marcas comerciais

IBM, o logotipo IBM , ibm.com, são marcas registradas da IBM Corporation, registradas em várias jurisdições no mundo todo Uma lista atual de marcas registradas da IBM está disponível na Web em "Informações de copyright e marca registrada"www.ibm.com/legal/copytrade.shtml. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas.

Microsoft e Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Este produto inclui software desenvolvido pelo Projeto Eclipse (http://www.eclipse.org/).

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

Part Number:

(1P) P/N: