7.5

Sécurisation d' IBM WebSphere MQ

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 339.

Cette édition s'applique à la version 7 édition 5 d' IBM® WebSphere MQ et à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

Table des matières

Sécurité

La sécurité est une considération importante pour les développeurs d'applications IBM WebSphere MQ et pour les administrateurs système qui configurent les droits IBM WebSphere MQ .

Présentation de la sécurité

Cette collection de rubriques présente les concepts de sécurité d' IBM WebSphere MQ .

Les concepts et les mécanismes de sécurité, tels qu'ils s'appliquent à n'importe quel système informatique, sont présentés en premier, suivis d'une discussion de ces mécanismes de sécurité à mesure qu'ils sont implémentés dans IBM WebSphere MQ.

Concepts et mécanismes de sécurité

Cette collection de rubriques décrit les aspects de la sécurité à prendre en compte dans votre installation IBM WebSphere MQ .

Les aspects communément acceptés de la sécurité sont les suivants:

- «Identification et authentification», à la page 5
- «Authorization», à la page 6
- «Audit», à la page 6
- «Confidentialité», à la page 7
- «Intégrité des données», à la page 7

Les *mécanismes de sécurité* sont des outils et des techniques techniques utilisés pour implémenter les services de sécurité. Un mécanisme peut fonctionner seul ou avec d'autres pour fournir un service particulier. Voici des exemples de mécanismes de sécurité communs:

- «Cryptographie», à la page 7
- «Historiques des messages et signatures numériques», à la page 9
- «Certificats numériques», à la page 9
- «Public key infrastructure (PKI)», à la page 14

Lorsque vous planifiez une implémentation IBM WebSphere MQ , prenez en compte les mécanismes de sécurité dont vous avez besoin pour implémenter les aspects de sécurité qui sont importants pour vous. Pour plus d'informations sur les éléments à prendre en compte après avoir lu ces rubriques, voir «Planification de la sécurité», à la page 48.

Concepts associés

«Connexion de deux gestionnaires de files d'attente via le protocole SSL ou TLS», à la page 216
Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

«Utilisation de SSL ou TLS», à la page 115
Ces rubriques fournissent des instructions pour l'exécution de tâches uniques liées à l'utilisation de SSL ou TLS avec IBM WebSphere MQ.

Identification et authentification

L' *identification* est la possibilité d'identifier de manière unique un utilisateur d'un système ou d'une application qui s'exécute dans le système. L' *authentification* est la possibilité de prouver qu'un utilisateur ou une application est réellement qui est cette personne ou ce que cette application prétend être.

Par exemple, imaginez un utilisateur qui se connecte à un système en entrant un ID utilisateur et un mot de passe. Le système utilise l'ID utilisateur pour identifier l'utilisateur. Le système authentifie l'utilisateur au moment de la connexion en vérifiant que le mot de passe fourni est correct.

Non-répudiation

Le service de *non-répudiation* peut être considéré comme une extension du service d'identification et d'authentification. En général, la non-répudiation s'applique lorsque les données sont transmises par voie électronique ; par exemple, une commande à un courtier en actions pour acheter ou vendre des actions, ou une commande à une banque pour transférer des fonds d'un compte à un autre.

L'objectif global du service de non-répudiation est de pouvoir prouver qu'un message particulier est associé à un individu particulier.

Le service de non-répudiation peut contenir plusieurs composants, chaque composant fournissant une fonction différente. Si l'expéditeur d'un message refuse de l'envoyer, le service de non-répudiation avec une *preuve de l'origine* peut fournir au destinataire des preuves indéniables que le message a été envoyé par cette personne. Si le destinataire d'un message refuse de le recevoir, le service de non-répudiation avec *preuve de livraison* peut fournir à l'expéditeur des preuves indéniables que le message a été reçu par cette personne.

Dans la pratique, la preuve avec une quasi-certitude de 100%, ou des preuves indéniables, est un objectif difficile. Dans le monde réel, rien n'est totalement sécurisé. La gestion de la sécurité est plus axée sur la gestion des risques à un niveau acceptable pour l'entreprise. Dans un tel environnement, une attente plus réaliste du service de non-répudiation est de pouvoir fournir des preuves qui sont admissibles, et qui soutiennent votre cause, devant un tribunal.

La non-répudiation est un service de sécurité pertinent dans un environnement IBM WebSphere MQ car IBM WebSphere MQ est un moyen de transmettre des données par voie électronique. Par exemple, vous pouvez exiger des preuves simultanées qu'un message particulier a été envoyé ou reçu par une demande associée à un individu particulier.

IBM WebSphere MQ avec IBM WebSphere MQ Advanced Message Security ne fournit pas de service de non-répudiation dans le cadre de sa fonction de base. Toutefois, cette documentation du produit contient des suggestions sur la manière dont vous pouvez fournir votre propre service de non-répudiation dans un environnement WebSphere MQ en écrivant vos propres programmes d'exit.

Concepts associés

«Identification et authentification dans IBM WebSphere MQ», à la page 22
Dans IBM WebSphere MQ, vous pouvez implémenter l'identification et l'authentification à l'aide des informations de contexte de message et de l'authentification mutuelle.

Authorization

L' *autorisation* protège les ressources critiques d'un système en limitant l'accès uniquement aux utilisateurs autorisés et à leurs applications. Il empêche l'utilisation non autorisée d'une ressource ou l'utilisation d'une ressource de manière non autorisée.

Concepts associés

«Autorisation dans IBM WebSphere MQ», à la page 22
Vous pouvez utiliser l'autorisation pour limiter les actions que des personnes ou des applications particulières peuvent effectuer dans votre environnement IBM WebSphere MQ .

Audit

L' *audit* est le processus d'enregistrement et de vérification des événements pour détecter si une activité inattendue ou non autorisée a eu lieu ou si une tentative a été effectuée pour effectuer cette activité.

Pour plus d'informations sur la configuration de l'autorisation, voir «Autorisation de planification», à la page 51 et les sous-rubriques associées.

Concepts associés

«Audit dans IBM WebSphere MQ», à la page 23

IBM WebSphere MQ peut émettre des messages d'événement pour enregistrer que l'activité inhabituelle a eu lieu.

Confidentialité

Le service de *confidentialité* protège les informations sensibles contre toute divulgation non autorisée.

Lorsque des données sensibles sont stockées localement, les mécanismes de contrôle d'accès peuvent être suffisants pour les protéger en supposant que les données ne peuvent pas être lues si elles ne sont pas accessibles. Si un niveau de sécurité plus élevé est requis, les données peuvent être chiffrées.

Chiffrer des données sensibles lorsqu'elles sont transmises sur un réseau de communication, en particulier sur un réseau non sécurisé tel que l'Internet. Dans un environnement réseau, les mécanismes de contrôle d'accès ne sont pas efficaces contre les tentatives d'interception des données, telles que les écoutes téléphoniques.

Intégrité des données

Le service d' *intégrité des données* détecte s'il y a eu une modification non autorisée des données.

Les données peuvent être altérées de deux manières: accidentellement, par des erreurs de matériel et de transmission, ou en raison d'une attaque délibérée. De nombreux produits matériels et protocoles de transmission ont des mécanismes pour détecter et corriger les erreurs matérielles et de transmission. Le but du service d'intégrité des données est de détecter une attaque délibérée.

Le service d'intégrité des données vise uniquement à détecter si des données ont été modifiées. Il ne vise pas à restaurer les données dans leur état d'origine si elles ont été modifiées.

Les mécanismes de contrôle d'accès peuvent contribuer à l'intégrité des données dans la mesure où les données ne peuvent pas être modifiées si l'accès est refusé. Mais, comme pour la confidentialité, les mécanismes de contrôle de l'accès ne sont pas efficaces dans un environnement de réseautage.

Concepts cryptographiques

Cette collection de rubriques décrit les concepts de cryptographie applicables à WebSphere MQ.

Le terme *entité* est utilisé pour désigner un gestionnaire de files d'attente, un client WebSphere MQ MQI, un utilisateur individuel ou tout autre système capable d'échanger des messages.

Concepts associés

«Cryptographie dans IBM WebSphere MQ», à la page 24
IBM WebSphere MQ fournit la cryptographie à l'aide des protocoles SSL (Secure Sockets Layer) et TLS (Transport Security Layer).

Cryptographie

La cryptographie est le processus de conversion entre du texte lisible, appelé *texte en clair*, et un format illisible, appelé *texte chiffré*.

Cela se produit comme suit:

1. L'expéditeur convertit le message en texte en clair en texte chiffré. Cette partie du processus est appelée *chiffrement* (parfois *chiffrement*).
2. Le texte chiffré est transmis au récepteur.
3. Le récepteur reconvertit le message chiffré en texte en clair. Cette partie du processus est appelée *déchiffrement* (parfois *déchiffrement*).

Voir le Glossaire pour une définition de la cryptographie.

La conversion implique une séquence d'opérations mathématiques qui modifient l'apparence du message lors de la transmission mais n'affectent pas le contenu. Les techniques cryptographiques permettent de garantir la confidentialité et de protéger les messages contre l'affichage non autorisé (écoute clandestine), car un message chiffré n'est pas compréhensible. Les signatures numériques, qui

garantissent l'intégrité des messages, utilisent des techniques de chiffrement. Pour plus d'informations, voir «Signatures numériques dans SSL et TLS», à la page 20.

Les techniques cryptographiques impliquent un algorithme général, rendu spécifique par l'utilisation de clés. Il existe deux classes d'algorithme:

- Ceux qui exigent que les deux parties utilisent la même clé secrète. Les algorithmes qui utilisent une clé partagée sont appelés algorithmes *symétriques* . Figure 1, à la page 8 illustre la cryptographie à clé symétrique.
- Ceux qui utilisent une clé pour le chiffrement et une autre clé pour le déchiffrement. L'un d'eux doit être gardé secret, mais l'autre peut être public. Les algorithmes qui utilisent des paires de clés publiques et privées sont appelés algorithmes *asymétriques* . Figure 2, à la page 8 illustre la cryptographie à clé asymétrique, également appelée *cryptographie à clé publique*.

Les algorithmes de chiffrement et de déchiffrement utilisés peuvent être publics, mais la clé secrète partagée et la clé privée doivent être gardées secrètes.

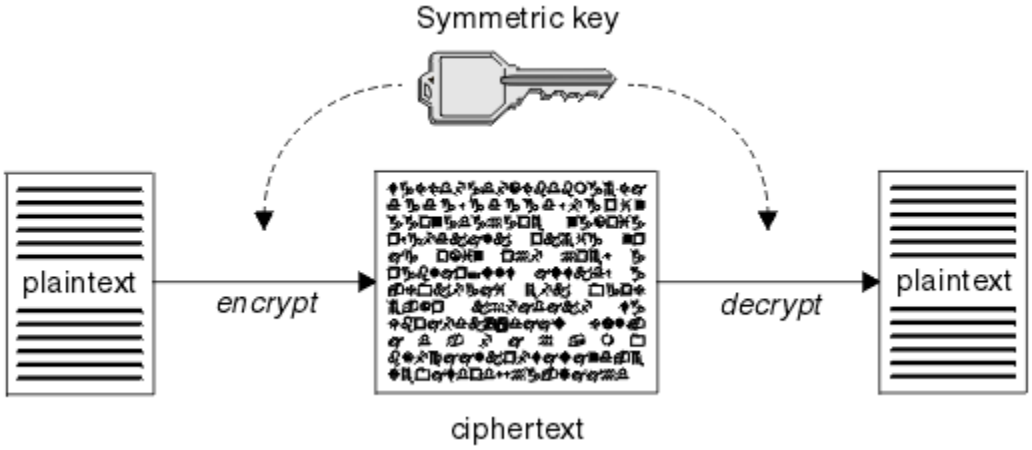


Figure 1. cryptographie à clé symétrique

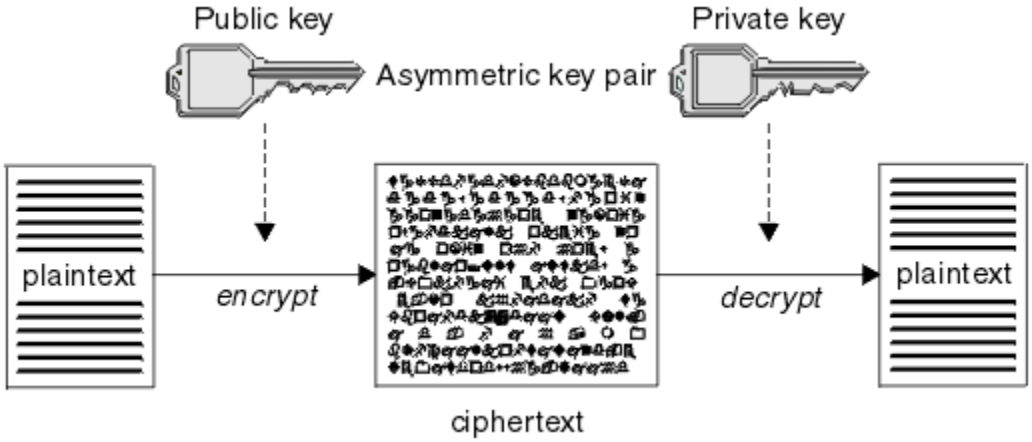


Figure 2. cryptographie à clé asymétrique

Figure 2, à la page 8 affiche le texte en clair chiffré avec la clé publique du récepteur et déchiffré avec la clé privée du récepteur. Seul le récepteur prévu détient la clé privée pour déchiffrer le texte chiffré. Notez que l'expéditeur peut également chiffrer les messages avec une clé privée, ce qui permet à quiconque détient la clé publique de l'expéditeur de déchiffrer le message, avec l'assurance que le message doit provenir de l'expéditeur.

Avec les algorithmes asymétriques, les messages sont chiffrés avec la clé publique ou la clé privée, mais ils ne peuvent être déchiffrés qu'avec l'autre clé. Seule la clé privée est secrète, la clé publique peut être connue de n'importe qui. Avec les algorithmes symétriques, la clé partagée ne doit être connue que des

deux parties. Il s'agit du *problème de distribution de clé* . Les algorithmes asymétriques sont plus lents mais présentent l'avantage qu'il n'y a pas de problème de distribution de clé.

Une autre terminologie associée à la cryptographie est:

Force
La force du chiffrement est déterminée par la taille de la clé. Les algorithmes asymétriques requièrent des clés de grande taille, par exemple:

1 024 bits	Clé asymétrique de faible puissance
2048 bits	Clé asymétrique de niveau moyen
4096 bits	Clé asymétrique de haute résistance

Les clés symétriques sont plus petites: les clés 256 bits vous donnent un chiffrement renforcé.

Algorithme de chiffrement de bloc
Ces algorithmes chiffrent les données par blocs. Par exemple, l'algorithme RC2 de RSA Data Security Inc. utilise des blocs d'une longueur de 8 octets. Les algorithmes de bloc sont généralement plus lents que les algorithmes de flux.

Algorithme de chiffrement de flux
Ces algorithmes fonctionnent sur chaque octet de données. Les algorithmes de flux sont généralement plus rapides que les algorithmes de bloc.

Historiques des messages et signatures numériques

Un résumé de message est une représentation numérique à taille fixe du contenu d'un message, calculée par une fonction de hachage. Un résumé de message peut être chiffré, formant une signature numérique.

Les messages sont intrinsèquement de taille variable. Un résumé de message est une représentation numérique de taille fixe du contenu d'un message. Un résumé de message est calculé par une fonction de hachage, qui est une transformation répondant à deux critères:

- La fonction de hachage doit être unidirectionnelle. Il ne doit pas être possible d'inverser la fonction pour trouver le message correspondant à un résumé de message particulier, sauf en testant tous les messages possibles.
- Il doit être infaisable du point de vue du calcul de trouver deux messages qui se hachent dans le même condensé.

Le résumé du message est envoyé avec le message lui-même. Le destinataire peut générer un prétraitement pour le message et le comparer avec le prétraitement de l'expéditeur. L'intégrité du message est vérifiée lorsque les deux historiques de message sont identiques. Toute altération du message au cours de la transmission se traduit presque certainement par un résumé de message différent.

Un résumé de message créé à l'aide d'une clé symétrique secrète est appelé code d'authentification de message (MAC), car il peut fournir l'assurance que le message n'a pas été modifié.

L'expéditeur peut également générer un résumé de message, puis chiffrer le résumé à l'aide de la clé privée d'une paire de clés asymétriques, formant une signature numérique. La signature doit ensuite être déchiffrée par le récepteur, avant de la comparer à un prétraitement généré localement.

Concepts associés

«Signatures numériques dans SSL et TLS», à la page 20
Une signature numérique est formée par le chiffrement d'une représentation d'un message. Le chiffrement utilise la clé privée du signataire et, pour des raisons d'efficacité, opère généralement sur un résumé de message plutôt que sur le message lui-même.

Certificats numériques

Les certificats numériques constituent une protection contre l'usurpation d'identité en certifiant qu'une clé publique appartient à une entité spécifiée. Ils sont émis par une autorité de certification.

Les certificats numériques offrent une protection contre l'emprunt d'identité, car un certificat numérique lie une clé publique à son propriétaire, qu'il s'agisse d'un individu, d'un gestionnaire de files d'attente ou d'une autre entité. Les certificats numériques sont aussi appelés certificats de clé publique car ils donnent des garanties sur l'appartenance d'une clé publique lorsque vous utilisez un schéma de clé asymétrique. Un certificat numérique contient la clé publique d'une entité et établit que la clé publique appartient à cette entité :

- Lorsque le certificat est établi pour une entité individuelle, il est appelé *certificat personnel* ou *certificat d'utilisateur*.
- Lorsque le certificat est établi pour une autorité de certification, il est appelé *certificat d'autorité de certification* ou *certificat de signataire*.

Si les clés publiques sont envoyées directement par leur propriétaire à une autre entité, il existe un risque que le message soit intercepté et que la clé publique soit remplacée par une autre. C'est ce qu'on appelle une attaque de type *homme au milieu*. La solution à ce problème consiste à échanger les clés publiques par le biais d'un tiers sécurisé qui garantit fortement que la clé publique appartient réellement à l'entité avec laquelle vous communiquez. Au lieu d'envoyer votre clé publique directement, vous demandez au tiers sécurisé de l'incorporer dans un certificat numérique. Le tiers sécurisé qui émet les certificats numériques est appelé autorité de certification, comme décrit dans «Autorités de certification», à la page 11.

Qu'est-ce qu'un certificat numérique ?
Les certificats numériques contiennent des éléments spécifiques d'informations, conformément à la norme X.509.

Les certificats numériques utilisés par WebSphere MQ sont conformes à la norme X.509 , qui spécifie les informations requises et le format d'envoi. X.509 constitue la partie de l'infrastructure d'authentification de la série X.500 de normes.

Les certificats numériques contiennent au moins les informations suivantes sur l'entité qui est certifiée :

- La clé publique du propriétaire
- Le nom distinctif du propriétaire
- Le nom distinctif de l'autorité de certification qui a émis le certificat
- La date à partir de laquelle le certificat est valide
- La date d'expiration du certificat
- Le numéro de version du format de données du certificat, comme défini dans la norme X.509. La version en cours de la norme X.509 est la version 3, et la plupart des certificats sont conformes à cette version.
- Un numéro de série. Il s'agit d'un identificateur unique affecté par l'autorité de certification qui a émis le certificat. Le numéro de série est unique au sein de l'autorité de certification qui a émis le certificat : deux certificats signés par la même autorité de certification ne peuvent pas avoir le même numéro de série.

Un certificat X.509 de version 2 contient aussi un identificateur d'émetteur et un identificateur d'objet, et un certificat X.509 de version 3 peut contenir un certain nombre d'extensions. Certaines extensions de certificat, comme l'extension Contrainte de base, sont *standard*, alors que d'autres sont propres à l'implémentation. Une extension peut être *critique*, auquel cas un système doit pouvoir reconnaître la zone ; s'il ne reconnaît pas la zone, il doit rejeter le certificat. Si une extension n'est pas critique, le système peut l'ignorer s'il ne la reconnaît pas.

La signature numérique dans un certificat personnel est générée avec la clé privée de l'autorité de certification qui a signé ce certificat. Toute personne devant vérifier le certificat personnel peut utiliser la clé publique de l'autorité de certification pour ce faire. Le certificat de l'autorité de certification contient sa clé publique.

Les certificats numériques ne contiennent pas votre clé privée. Vous devez garder votre clé privée secrète.

Exigences relatives aux certificats personnels
WebSphere MQ prend en charge les certificats numériques conformes à la norme X.509 . Elle requiert l'option d'authentification du client.

IBM WebSphere MQ étant un système d'égal à égal, il est considéré comme une authentification client dans la terminologie SSL. Par conséquent, tout certificat personnel utilisé pour l'authentification SSL doit autoriser une utilisation de clé de l'authentification client. Cette option n'étant pas activée pour tous les certificats serveur, le fournisseur de certificat peut avoir besoin d'activer l'authentification client sur l'autorité de certification racine pour le certificat sécurisé.

En plus des normes qui spécifient le format de données d'un certificat numérique, il existe également des normes pour déterminer si un certificat est valide. Ces normes ont été mises à jour au fil du temps afin de prévenir certains types de violations de la sécurité. Par exemple, les anciens certificats X.509 versions 1 et 2 n'indiquent pas si le certificat peut être légitimement utilisé pour signer d'autres certificats. Il a donc été possible pour un utilisateur malveillant d'obtenir un certificat personnel d'une source légitime et de créer de nouveaux certificats destinés à usurper l'identité d'autres utilisateurs.

Lors de l'utilisation de certificats X.509 version 3, les extensions de certificat BasicConstraints et KeyUsage sont utilisées pour spécifier les certificats qui peuvent légitimement signer d'autres certificats. La norme IETF RFC 5280 spécifie une série de règles de validation de certificat que les logiciels d'application conformes doivent implémenter afin d'éviter les attaques d'usurpation d'identité. Un ensemble de règles de certificat est appelé règle de validation de certificat.

Pour plus d'informations sur les règles de validation de certificat dans IBM WebSphere MQ, voir «Règles de validation de certificat dans IBM WebSphere MQ», à la page 35.

Autorités de certification
Une autorité de certification est un tiers sécurisé qui émet des certificats numériques pour garantir que la clé publique d'une entité appartient réellement à cette entité.

Les rôles d'une autorité de certification sont les suivants :

- A la réception d'une demande de certificat numérique, vérifier l'identité du demandeur avant de générer, signer et renvoyer le certificat personnel
- Fournir sa propre clé publique dans son certificat d'autorité de certification
- Publier des listes de certificats qui ne sont plus sécurisés dans une liste de révocation de certificat Pour plus d'informations, voir «Utilisation des certificats révoqués», à la page 157
- Fournir l'accès au statut de révocation de certificat via un serveur répondeur OSCP

Noms distinctifs
Le nom distinctif identifie de façon unique une entité dans un certificat X.509.

Les types d'attribut suivants composent généralement le nom distinctif :

SERIALNUMBER	Numéro de série du certificat
MAIL	Adresse électronique
E	Adresse électronique (dépréciée dans la préférence pour MAIL)
UID ou USERID	Identificateur utilisateur
CN	Nom CN
T	Titre
OU	Nom d'unité organisationnelle
DC	Composant de domaine
O	Nom de l'organisation
STREET	Rue/Première ligne d'adresse
L	Nom du lieu
ST (ou SP ou S)	Nom du département
PC	Code postal

C	Pays
UNSTRUCTUREDNAME	Nom d'hôte
UNSTRUCTUREDADDRESS	Adresse IP
DNQ	Qualificateur de nom distinctif

La norme X.509 définit d'autres attributs qui ne font généralement pas partie du nom distinctif mais qui peuvent fournir des extensions en option au certificat numérique.

La norme X.509 permet de spécifier un nom distinctif au format chaîne. Exemple :

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

Le nom usuel (CN) peut décrire un utilisateur individuel ou toute autre entité, par exemple un serveur Web.

Le nom distinctif peut comporter plusieurs attributs OU et DC. Une instance seulement de chacun des autres attributs est admise. L'ordre des entrées OU est important : il spécifie une hiérarchie de noms d'unité organisationnelle, dans laquelle l'unité de niveau supérieur apparaît en premier. L'ordre des entrées DC est également important.

IBM WebSphere MQ tolère certains noms distinctifs syntaxiquement inappropriés. Pour plus d'informations, voir RèglesWebSphere MQ pour les valeurs SSLPEER.

Concepts associés

«Qu'est-ce qu'un certificat numérique ?», à la page 10
Les certificats numériques contiennent des éléments spécifiques d'informations, conformément à la norme X.509.

Obtention de certificats personnels d'une autorité de certification

Vous pouvez obtenir un certificat d'une autorité de certification externe sécurisée.

Vous obtenez un certificat numérique en envoyant des informations à une autorité de certification, sous la forme d'une demande de certificat. La norme X.509 définit un format pour ces informations, mais certaines autorités de certification proposent leur propre format. Les demandes de certificat sont généralement générées par l'outil de gestion des certificats utilisé par votre système, par exemple l'outil iKeyman sur les systèmes UNIX, Linux®et Windows et RACF sur z/OS. Les informations contiennent votre nom distinctif et votre clé publique. Lorsque votre outil de gestion des certificats génère votre demande de certificat, il génère aussi votre clé privée, qui doit rester sécurisée. Ne la communiquez jamais.

Lorsque l'autorité de certification reçoit votre demande, elle vérifie votre identité avant de générer le certificat et de vous l'envoyer sous forme de certificat personnel.

La Figure 3, à la page 13 illustre le processus d'obtention d'un certificat numérique d'une autorité de certification.

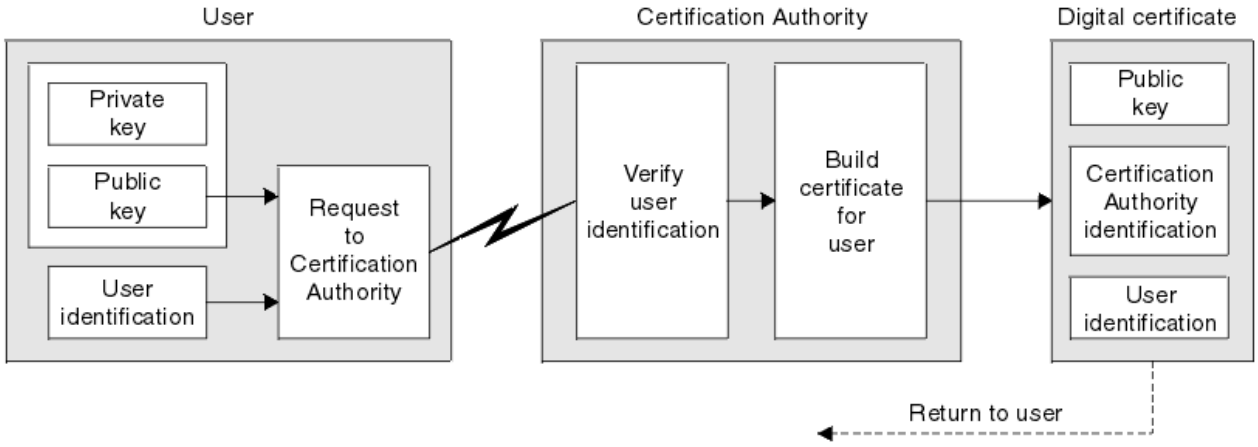


Figure 3. Obtention d'un certificat numérique

Dans le diagramme :

- L'"identification de l'utilisateur" inclut votre nom distinctif de sujet.
- L'"identification de l'autorité de certification" comprend le nom distinctif de l'autorité de certification qui émet le certificat.
-

Les certificats numériques contiennent des zones supplémentaires autres que celles affichées dans le diagramme. Pour plus d'informations sur les autres zones d'un certificat numérique, voir «Qu'est-ce qu'un certificat numérique ?», à la page 10.

Fonctionnement des chaînes de certificats
Lorsque vous recevez le certificat d'une autre entité, vous devrez peut-être utiliser une *chaîne de certificats* pour obtenir le certificat de l' *autorité de certification racine* .

La chaîne de certificats, également appelée *chemin de certification* , est une liste de certificats utilisés pour authentifier une entité. La chaîne, ou chemin, commence par le certificat de cette entité, et chaque certificat de la chaîne est signé par l'entité identifiée par le certificat suivant de la chaîne. La chaîne s'arrête avec un certificat d'autorité de certification racine. Le certificat de l'autorité de certification racine est toujours signé par l'autorité de certification elle-même. Les signatures de tous les certificats de la chaîne doivent être vérifiées jusqu'à ce que le certificat de l'autorité de certification racine soit atteint.

La Figure 4, à la page 14 illustre un chemin de certification entre le propriétaire du certificat et l'autorité de certification racine, où commence la chaîne de confiance.

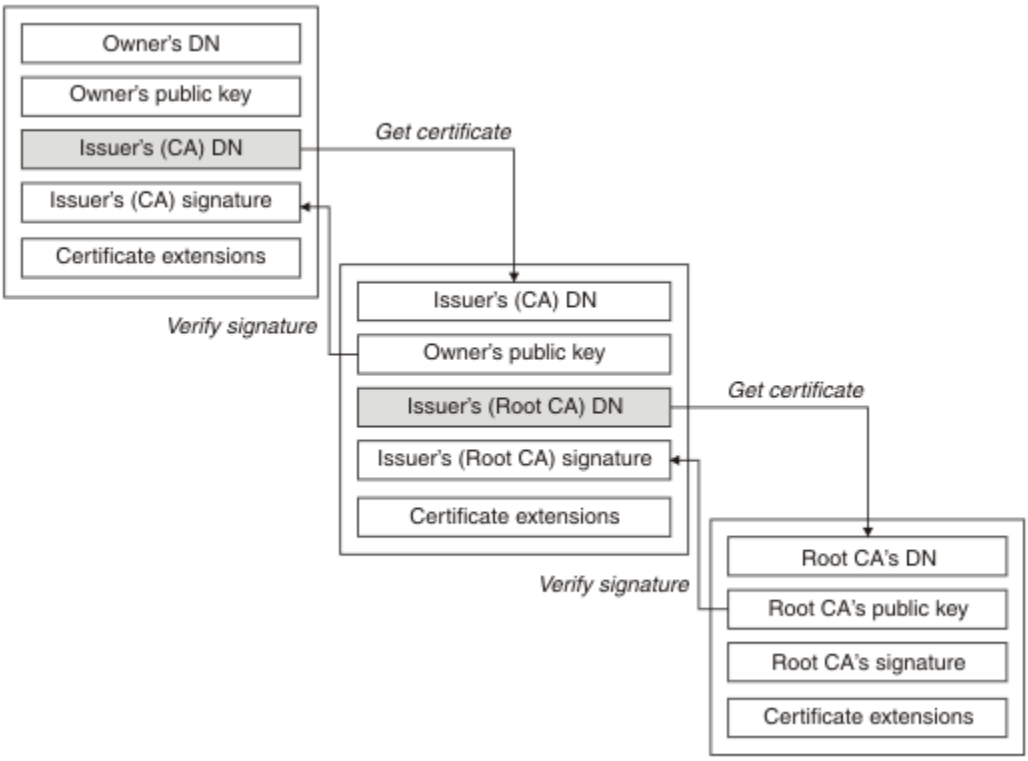


Figure 4. Chaîne de confiance

Chaque certificat peut contenir une ou plusieurs extensions. Un certificat appartenant à une autorité de certification contient généralement une extension BasicConstraints avec l'indicateur isCA défini pour indiquer qu'il est autorisé à signer d'autres certificats.

Lorsque les certificats ne sont plus valides
Les certificats numériques peuvent expirer ou être révoqués.

Les certificats numériques sont délivrés pour une période déterminée et ne sont pas valides après leur date d'expiration.

Voir le Glossaire pour une définition de l'expiration de certificat.

Les certificats peuvent être révoqués pour diverses raisons, notamment:

- Le propriétaire est parti dans une autre entreprise.
- La clé privée n'est plus secrète.

WebSphere MQ peut vérifier si un certificat est révoqué en envoyant une demande à un répondeur OCSP (Online Certificate Status Protocol) (sur les systèmes UNIX, Linux et Windows uniquement). Ils peuvent également accéder à une liste de révocation de certificat sur un serveur LDAP. Les informations de révocation OCSP et de LRC sont publiées par une autorité de certification. Pour plus d'informations, voir «Utilisation des certificats révoqués», à la page 157.

Public key infrastructure (PKI)

Une infrastructure à clé publique (ICP) est un système d'installations, de politiques et de services qui prend en charge l'utilisation de la cryptographie à clé publique pour authentifier les parties impliquées dans une transaction.

Il n'existe pas de norme unique qui définit les composants d'une infrastructure à clé publique, mais une ICP comprend généralement des autorités de certification (AC) et des autorités d'enregistrement (AR). Les autorités de certification fournissent les services suivants:

- Emission de certificats numériques

- Validation des certificats numériques
- Révocation de certificats numériques
- Distribution de clés publiques

Les normes X.509 constituent la base de l'infrastructure à clé publique conforme aux normes de l'industrie.

Pour plus d'informations sur les certificats numériques et les autorités de certification, voir «Certificats numériques», à la page 9 . Les autorités de certification vérifient que les informations fournies lors de la demande de certificats numériques. Si l'autorité de certification vérifie ces informations, l'autorité de certification peut émettre un certificat numérique au demandeur.

Une infrastructure PKI peut également fournir des outils pour la gestion des certificats numériques et des clés publiques. Une infrastructure PKI est parfois décrite comme une *hiérarchie de confiance* pour la gestion des certificats numériques, mais la plupart des définitions incluent des services supplémentaires. Certaines définitions comprennent des services de chiffrement et de signature numérique, mais ces services ne sont pas essentiels au fonctionnement d'une ICP.

Protocoles de sécurité cryptographiques SSL et TLS

Les protocoles cryptographiques fournissent des connexions sécurisées, permettant à deux parties de communiquer avec la confidentialité et l'intégrité des données. Le protocole TLS (Transport Layer Security) a évolué à partir de celui de la couche SSL (Secure Sockets Layer). IBM WebSphere MQ prend en charge SSL et TLS.

Les objectifs principaux des deux protocoles sont de garantir la confidentialité (parfois appelée *confidentialité*), l'intégrité des données, l'identification et l'authentification à l'aide de certificats numériques.

Bien que les deux protocoles soient similaires, les différences sont suffisamment importantes pour que SSL 3.0 et les différentes versions de TLS n'interopèrent pas.

Concepts associés

«Protocoles de sécurité dans IBM WebSphere MQ», à la page 24
IBM WebSphere MQ prend en charge les protocoles TLS (Transport Layer Security) et SSL (Secure Sockets Layer) afin de fournir une sécurité au niveau des liens pour les canaux de message et les canaux MQI.

Concepts SSL (Secure Sockets Layer) et TLS (Transport Layer Security)

Les protocoles SSL et TLS permettent à deux parties de s'identifier et de s'authentifier et de communiquer avec la confidentialité et l'intégrité des données. Le protocole TLS a évolué à partir du protocole Netscape SSL 3.0 , mais TLS et SSL n'interopèrent pas.

Les protocoles SSL et TLS assurent la sécurité des communications sur Internet et permettent aux applications client/serveur de communiquer de manière confidentielle et fiable. Les protocoles ont deux couches: un protocole d'enregistrement et un protocole d'établissement de liaison, et celles-ci sont superposées au-dessus d'un protocole de transport tel que TCP/IP. Ils utilisent tous deux des techniques de cryptographie asymétrique et symétrique.

Une connexion SSL ou TLS est initiée par une application qui devient le client SSL ou TLS. L'application qui reçoit la connexion devient le serveur SSL ou TLS. Chaque nouvelle session commence par un établissement de liaison, tel que défini par les protocoles SSL ou TLS.

La liste complète des CipherSpecs pris en charge par IBM WebSphere MQ est disponible à l'adresse «Définition des spécifications CipherSpec», à la page 227.

Pour plus d'informations sur le protocole SSL, voir les informations fournies à l'adresse https://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt. Pour plus d'informations sur le protocole TLS, voir les informations fournies par le groupe de travail TLS sur le site Web de l'Internet Engineering Task Force à l'adresse https://www.ietf.org

Présentation de l'établissement de liaison SSL ou TLS

L'établissement de liaison SSL ou TLS permet au client et au serveur SSL ou TLS d'établir les clés secrètes avec lesquelles ils communiquent.

Cette section fournit un récapitulatif des étapes permettant au client et au serveur SSL ou TLS de communiquer entre eux.

- Convenir de la version du protocole à utiliser.
- Sélectionnez des algorithmes de cryptographie.
- Authentifiez-vous les uns les autres en échangeant et en validant des certificats numériques.
- Utilisez des techniques de chiffrement asymétrique pour générer une clé secrète partagée, ce qui évite le problème de distribution des clés. SSL ou TLS utilise ensuite la clé partagée pour le chiffrement symétrique des messages, qui est plus rapide que le chiffrement asymétrique.

Pour plus d'informations sur les algorithmes de cryptographie et les certificats numériques, reportez-vous aux informations connexes.

Dans la présentation, les étapes impliquées dans l'établissement de liaison SSL sont les suivantes:

1. Le client SSL ou TLS envoie un message "client hello" qui répertorie les informations cryptographiques telles que la version SSL ou TLS et, dans l'ordre de préférence du client, les CipherSuites prises en charge par le client. Le message contient également une chaîne d'octets aléatoire qui est utilisée dans les calculs ultérieurs. Le protocole permet au "client hello" d'inclure les méthodes de compression de données prises en charge par le client.
2. Le serveur SSL ou TLS répond avec un message "server hello" qui contient la CipherSuite choisie par le serveur dans la liste fournie par le client, l'ID de session et une autre chaîne d'octets aléatoires. Le serveur envoie également son certificat numérique. Si le serveur requiert un certificat numérique pour l'authentification du client, il envoie une "demande de certificat client" qui inclut une liste des types de certificat pris en charge et des noms distinctifs des autorités de certification (CA) acceptables.
3. Le client SSL ou TLS vérifie le certificat numérique du serveur. Pour plus d'informations, voir «Comment SSL et TLS assurent l'identification, l'authentification, la confidentialité et l'intégrité», à la page 17.
4. Le client SSL ou TLS envoie la chaîne d'octets aléatoires qui permet au client et au serveur de calculer la clé secrète à utiliser pour le chiffrement des données de message suivantes. La chaîne d'octets aléatoires elle-même est chiffrée avec la clé publique du serveur.
5. Si le serveur SSL ou TLS a envoyé une "demande de certificat client", le client envoie une chaîne d'octets aléatoires chiffrée avec la clé privée du client, avec le certificat numérique du client, ou une "alerte de non-certificat numérique". Cette alerte n'est qu'un avertissement, mais avec certaines implémentations, l'établissement de liaison échoue si l'authentification du client est obligatoire.
6. Le serveur SSL ou TLS vérifie le certificat du client. Pour plus d'informations, voir «Comment SSL et TLS assurent l'identification, l'authentification, la confidentialité et l'intégrité», à la page 17.
7. Le client SSL ou TLS envoie au serveur un message "terminé" , qui est chiffré avec la clé secrète, indiquant que la partie client de l'établissement de liaison est terminée.
8. Le serveur SSL ou TLS envoie au client un message "finished" , qui est chiffré avec la clé secrète, indiquant que la partie serveur de l'établissement de liaison est terminée.
9. Pendant la durée de la session SSL ou TLS, le serveur et le client peuvent désormais échanger des messages qui sont chiffrés de manière symétrique avec la clé secrète partagée.

La Figure 5, à la page 17 illustre l'établissement de liaison SSL ou TLS.

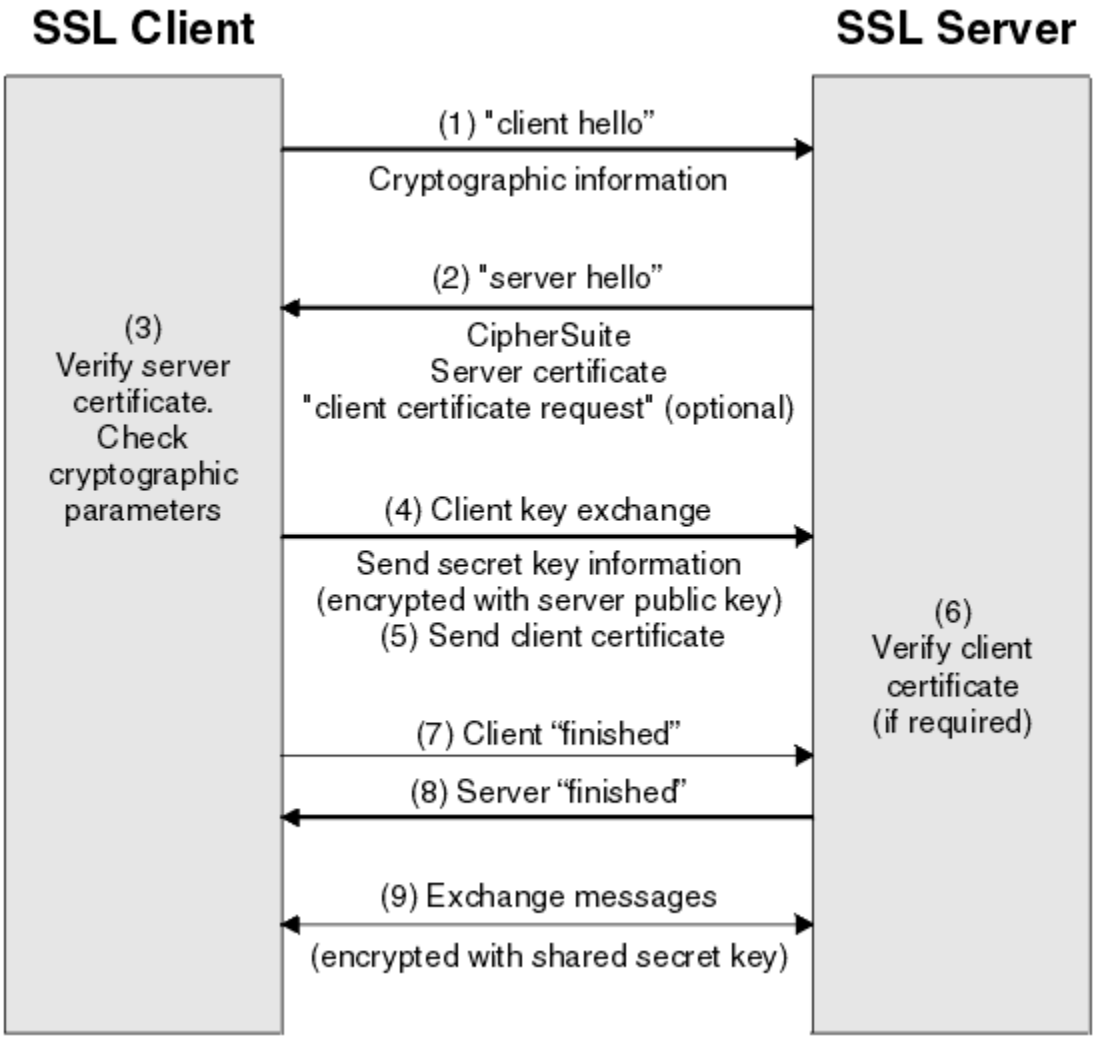


Figure 5. Présentation de l'établissement de liaison SSL ou TLS

Comment SSL et TLS assurent l'identification, l'authentification, la confidentialité et l'intégrité

Lors de l'authentification du client et du serveur, une étape exige que les données soient chiffrées avec l'une des clés d'une paire de clés asymétriques et déchiffrées avec l'autre clé de la paire. Un résumé de message est utilisé pour assurer l'intégrité.

Pour une présentation des étapes impliquées dans l'établissement de liaison TLS, voir «Présentation de l'établissement de liaison SSL ou TLS», à la page 16.

Comment SSL et TLS fournissent l'authentification

Pour l'authentification du serveur, le client utilise la clé publique du serveur pour chiffrer les données utilisées pour calculer la clé secrète. Le serveur ne peut générer la clé secrète que s'il peut déchiffrer ces données avec la clé privée appropriée.

Pour l'authentification du client, le serveur utilise la clé publique dans le certificat client pour déchiffrer les données que le client envoie lors de l'étape «5», à la page 16 de l'établissement de liaison. L'échange des messages terminés qui sont chiffrés avec la clé secrète (étapes «7», à la page 16 et «8», à la page 16 dans la présentation) confirme que l'authentification est terminée.

Si l'une des étapes d'authentification échoue, l'établissement de liaison échoue et la session se termine.

L'échange de certificats numériques lors de l'établissement de liaison SSLor TLS fait partie du processus d'authentification. Pour plus d'informations sur la façon dont les certificats fournissent une protection

contre l'usurpation d'identité, reportez-vous aux informations connexes. Les certificats requis sont les suivants, où l'autorité de certification X émet le certificat sur le client SSL ou TLS et l'autorité de certification Y émet le certificat sur le serveur SSL ou TLS:

Pour l'authentification de serveur uniquement, le serveur SSL ou TLS a besoin de:

- Certificat personnel émis sur le serveur par l'autorité de certification Y
- Clé privée du serveur

et le client SSL ou TLS a besoin:

- Le certificat de l'autorité de certification pour l'autorité de certification Y

Si le serveur SSL ou TLS requiert une authentification client, le serveur vérifie l'identité du client en vérifiant le certificat numérique du client avec la clé publique de l'autorité de certification qui a émis le certificat personnel au client, en l'occurrence l'autorité de certification X . Pour l'authentification du serveur et du client, le serveur a besoin:

- Certificat personnel émis sur le serveur par l'autorité de certification Y
- Clé privée du serveur
- Le certificat de l'autorité de certification pour l'autorité de certification X

et le client a besoin:

- Certificat personnel émis pour le client par l'autorité de certification X
- Clé privée du client
- Le certificat de l'autorité de certification pour l'autorité de certification Y

Le serveur et le client SSL ou TLS peuvent avoir besoin d'autres certificats de l'autorité de certification pour former une chaîne de certificats pour le certificat de l'autorité de certification racine. Pour plus d'informations sur les chaînes de certificats, reportez-vous aux informations associées.

Ce qui se passe lors de la vérification de certificat

Comme indiqué dans les étapes «3», à la page 16 et «6», à la page 16 de la présentation, le client SSL ou TLS vérifie le certificat du serveur et le serveur SSL ou TLS vérifie le certificat du client. Cette vérification comporte quatre aspects:

1. La signature numérique est vérifiée (voir «Signatures numériques dans SSL et TLS», à la page 20).
2. La chaîne de certificats est vérifiée ; vous devez disposer de certificats d'autorité de certification intermédiaires (voir «Fonctionnement des chaînes de certificats», à la page 13).
3. Les dates d'expiration et d'activation ainsi que la période de validité sont vérifiées.
4. Le statut de révocation du certificat est vérifié (voir «Utilisation des certificats révoqués», à la page 157).

Réinitialisation de la clé secrète

Lors d'un établissement de liaison SSL ou TLS, une *clé secrète* est générée pour chiffrer les données entre le client SSL ou TLS et le serveur. La clé secrète est utilisée dans une formule mathématique qui est appliquée aux données pour transformer du texte en clair en texte chiffré illisible et du texte chiffré en texte en clair.

La clé secrète est générée à partir du texte aléatoire envoyé dans le cadre de l'établissement de liaison et est utilisée pour chiffrer du texte en clair en texte chiffré. La clé secrète est également utilisée dans l'algorithme MAC (Message Authentication Code), qui est utilisé pour déterminer si un message a été modifié. Pour plus d'informations, voir «Historiques des messages et signatures numériques», à la page 9.

Si la clé secrète est découverte, le texte en clair d'un message peut être déchiffré à partir du texte chiffré, ou le résumé du message peut être calculé, ce qui permet de modifier les messages sans détection. Même pour un algorithme complexe, le texte en clair peut éventuellement être découvert en appliquant chaque transformation mathématique possible au texte chiffré. Pour minimiser la quantité de données

pouvant être déchiffrées ou modifiées si la clé secrète est rompue, la clé secrète peut être renégociée périodiquement. Lorsque la clé secrète a été renégociée, la clé secrète précédente ne peut plus être utilisée pour déchiffrer les données chiffrées avec la nouvelle clé secrète.

Comment SSL et TLS assurent la confidentialité

SSL et TLS utilisent une combinaison de chiffrement symétrique et asymétrique pour garantir la confidentialité des messages. Lors de l'établissement de liaison SSL ou TLS, le client et le serveur SSL ou TLS conviennent d'un algorithme de chiffrement et d'une clé secrète partagée à utiliser pour une seule session. Tous les messages transmis entre le client SSL ou TLS et le serveur sont chiffrés à l'aide de cet algorithme et de cette clé, ce qui garantit que le message reste privé même s'il est intercepté. SSL prend en charge une large gamme d'algorithmes de cryptographie. Etant donné que SSL et TLS utilisent le chiffrement asymétrique lors du transport de la clé secrète partagée, il n'y a pas de problème de distribution de clé. Pour plus d'informations sur les techniques de chiffrement, voir «Cryptographie», à la page 7.

Comment SSL et TLS assurent l'intégrité

SSL et TLS assurent l'intégrité des données en calculant un résumé de message. Pour plus d'informations, voir «Intégrité des données de messages», à la page 236.

L'utilisation de SSL ou TLS garantit l'intégrité des données, à condition que le CipherSpec de votre définition de canal utilise un algorithme de hachage, comme décrit dans le tableau dans «Définition des spécifications CipherSpec», à la page 227.

En particulier, si l'intégrité des données pose problème, vous devez éviter de choisir un CipherSpec dont l'algorithme de hachage est répertorié comme "Aucun". L'utilisation de MD5 est également fortement déconseillée car elle est désormais très ancienne et n'est plus sécurisée pour des raisons pratiques.

CipherSpecs et CipherSuites

Les protocoles de sécurité cryptographique doivent convenir des algorithmes utilisés par une connexion sécurisée. CipherSpecs et CipherSuites définissent des combinaisons spécifiques d'algorithmes.

Un CipherSpec identifie une combinaison d'algorithme de chiffrement et d'algorithme MAC (Message Authentication Code). Les deux extrémités d'une connexion TLS ou SSL doivent convenir du même CipherSpec pour pouvoir communiquer.

Important : Lorsque vous utilisez des canaux IBM WebSphere MQ , vous utilisez un CipherSpec. Lorsque vous utilisez des canaux Java, JMS ou MQTT, vous spécifiez une CipherSuite.

Pour plus d'informations sur les CipherSpecs, voir «Définition des spécifications CipherSpec», à la page 227.

Une CipherSuite est une suite d'algorithmes de cryptographie utilisés par une connexion SSL ou TLS. Une suite comprend trois algorithmes distincts:

- Algorithme d'échange de clés et d'authentification utilisé lors de l'établissement de liaison
- Algorithme de chiffrement utilisé pour chiffrer les données
- Algorithme MAC (Message Authentication Code) utilisé pour générer le résumé de message

Il existe plusieurs options pour chaque composant de la suite, mais seules certaines combinaisons sont valides lorsqu'elles sont spécifiées pour une connexion TLS ou SSL. Le nom d'une CipherSuite valide définit la combinaison des algorithmes utilisés. Par exemple, CipherSuite SSL_RSA_WITH_RC4_128_MD5 spécifie:

- Algorithme d'authentification et d'échange de clés RSA
- Algorithme de chiffrement RC4 utilisant une clé 128 bits
- Algorithme MAC MD5

Plusieurs algorithmes sont disponibles pour l'échange de clés et l'authentification, mais l'algorithme RSA est actuellement le plus utilisé. Les algorithmes de chiffrement et les algorithmes MAC utilisés sont plus variés.

Signatures numériques dans SSL et TLS

Une signature numérique est formée par le chiffrement d'une représentation d'un message. Le chiffrement utilise la clé privée du signataire et, pour des raisons d'efficacité, opère généralement sur un résumé de message plutôt que sur le message lui-même.

Les signatures numériques varient avec les données en cours de signature, contrairement aux signatures manuscrites, qui ne dépendent pas du contenu du document en cours de signature. Si deux messages différents sont signés numériquement par la même entité, les deux signatures diffèrent, mais les deux signatures peuvent être vérifiées avec la même clé publique, c'est-à-dire la clé publique de l'entité qui a signé les messages.

Les étapes du processus de signature numérique sont les suivantes:

1. L'expéditeur calcule un résumé de message, puis il chiffre le résumé à l'aide de la clé privée de l'expéditeur, en formant la signature numérique.
2. L'émetteur transmet la signature numérique avec le message.
3. Le récepteur déchiffre la signature numérique à l'aide de la clé publique de l'expéditeur, en régénérant le résumé du message de l'expéditeur.
4. Le récepteur calcule un résumé de message à partir des données de message reçues et vérifie que les deux résumés sont identiques.

La Figure 6, à la page 20 illustre ce processus.

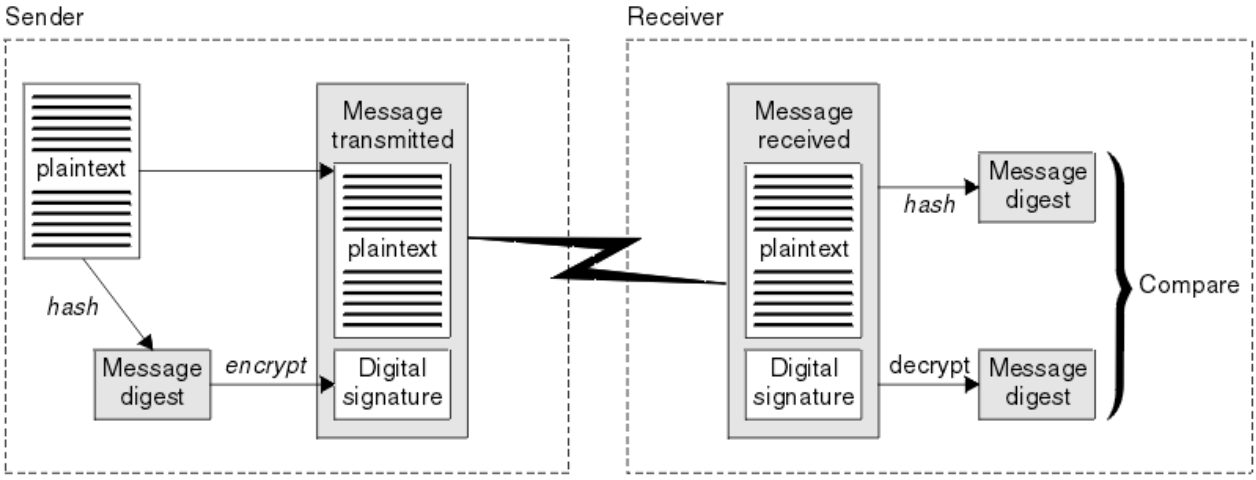


Figure 6. Processus de signature numérique

Si la signature numérique est vérifiée, le récepteur sait que:

- Le message n'a pas été modifié lors de la transmission.
- Le message a été envoyé par l'entité qui prétend l'avoir envoyé.

Les signatures numériques font partie des services d'intégrité et d'authentification. Les signatures numériques fournissent également une preuve de l'origine. Seul l'expéditeur connaît la clé privée, ce qui fournit des preuves solides que l'expéditeur est l'émetteur du message.

Remarque : Vous pouvez également chiffrer le message lui-même, ce qui protège la confidentialité des informations du message.

La norme FIPS (Federal Information Processing Standards)

Le gouvernement américain fournit des conseils techniques sur des systèmes informatiques et sur des systèmes de sécurité, y compris le chiffrement de données. Le National Institute for Standards and Technology (NIST) est un organisme important qui s'occupe des systèmes informatiques et de la sécurité.

Il émet des recommandations et établit des normes, notamment la norme FIPS (Federal Information Processing Standards).

L'une de ces normes est la norme FIPS 140-2, qui nécessite l'utilisation d'algorithmes de cryptographie puissants. Elle spécifie également des exigences pour les algorithmes de hachage à utiliser afin de protéger les paquets contre toute modification en transit.

IBM WebSphere MQ fournit une prise en charge FIPS 140-2 lorsqu'il a été configuré pour le faire.

Avec le temps, les analystes développent des attaques contre les algorithmes de chiffrement et de hachage existants. De nouveaux algorithmes sont adoptés pour résister à ces attaques. La norme FIPS 140-2 est mise à jour régulièrement afin de tenir compte de ces changements.

Agence de sécurité nationale (NSA) Suite B Cryptographie

Le gouvernement des États-Unis d'Amérique fournit des conseils techniques sur les systèmes informatiques et la sécurité, y compris le chiffrement des données. La National Security Agency (NSA) des États-Unis recommande un ensemble d'algorithmes cryptographiques interopérables dans sa norme Suite B.

La norme Suite B spécifie un mode de fonctionnement dans lequel seul un ensemble spécifique d'algorithmes cryptographiques sécurisés est utilisé. La norme Suite B spécifie:

- L'algorithme de chiffrement (AES)
- L'algorithme d'échange de clés (Elliptic Curve Diffie-Hellman, également connu sous le nom d'ECDH)
- L'algorithme de signature numérique (Elliptic Curve Digital Signature Algorithm, également appelé ECDSA)
- Les algorithmes de hachage (SHA-256 ou SHA-384)

De plus, la norme IETF RFC 6460 spécifie des profils compatibles Suite B qui définissent la configuration détaillée de l'application et le comportement nécessaires pour se conformer à la norme Suite B. Il définit deux profils:

1. Profil compatible Suite B à utiliser avec TLS version 1.2. Lorsqu'il est configuré pour une opération conforme à la suite B, seul l'ensemble restreint d'algorithmes de cryptographie listé ci-dessus sera utilisé.
2. Profil de transition à utiliser avec TLS version 1.0 ou TLS version 1.1. Ce profil permet l'interopérabilité avec les serveurs non conformes à la norme Suite B. Lorsqu'il est configuré pour l'opération de transition Suite B, des algorithmes de chiffrement et de hachage supplémentaires peuvent être utilisés.

La norme Suite B est conceptuellement similaire à la norme FIPS 140-2, car elle restreint l'ensemble des algorithmes de cryptographie activés afin de fournir un niveau de sécurité assuré.

Sur les systèmes Windows, UNIX et Linux , WebSphere MQ, peut être configuré pour être conforme au profil TLS 1.2 compatible Suite B, mais ne prend pas en charge le profil de transition Suite B. Pour plus d'informations, reportez-vous à la section «NSA Suite B Cryptography dans IBM WebSphere MQ», à la page 32.

Information associée

«La norme FIPS (Federal Information Processing Standards)», à la page 20
Le gouvernement américain fournit des conseils techniques sur des systèmes informatiques et sur des systèmes de sécurité, y compris le chiffrement de données. Le National Institute for Standards and Technology (NIST) est un organisme important qui s'occupe des systèmes informatiques et de la sécurité. Il émet des recommandations et établit des normes, notamment la norme FIPS (Federal Information Processing Standards).

IBM WebSphere MQ mécanismes de sécurité

Cette collection de rubriques explique comment implémenter les différents concepts de sécurité dans IBM WebSphere MQ.

IBM WebSphere MQ fournit des mécanismes permettant d'implémenter tous les concepts de sécurité introduits dans «Concepts et mécanismes de sécurité», à la page 5. Ces questions sont abordées plus en détail dans les sections suivantes.

Identification et authentification dans IBM WebSphere MQ

Dans IBM WebSphere MQ, vous pouvez implémenter l'identification et l'authentification à l'aide des informations de contexte de message et de l'authentification mutuelle.

Voici quelques exemples d'identification et d'authentification dans un environnement IBM WebSphere MQ :

- Chaque message peut contenir des informations de *contexte de message* . Ces informations sont conservées dans le descripteur de message. Il peut être généré par le gestionnaire de files d'attente lorsqu'un message est inséré dans une file d'attente par une application. L'application peut également fournir les informations si l'ID utilisateur associé à l'application est autorisé à le faire.

  Les informations de contexte d'un message permettent à l'application de réception de connaître l'émetteur du message. Il contient, par exemple, le nom de l'application qui a inséré le message et l'ID utilisateur associé à l'application.
- Lorsqu'un canal de transmission de messages démarre, il est possible que l'agent MCA (Message Channel Agent) à chaque extrémité du canal authentifie son partenaire. Cette technique est appelée *authentification mutuelle*. Pour l'agent MCA émetteur, il fournit l'assurance que le partenaire auquel il est sur le point d'envoyer des messages est authentique. Pour l'agent MCA récepteur, il existe une assurance similaire qu'il est sur le point de recevoir des messages d'un véritable partenaire.

Concepts associés

«Identification et authentification», à la page 5
L' *identification* est la possibilité d'identifier de manière unique un utilisateur d'un système ou d'une application qui s'exécute dans le système. L' *authentification* est la possibilité de prouver qu'un utilisateur ou une application est réellement qui est cette personne ou ce que cette application prétend être.

Autorisation dans IBM WebSphere MQ

Vous pouvez utiliser l'autorisation pour limiter les actions que des personnes ou des applications particulières peuvent effectuer dans votre environnement IBM WebSphere MQ .

Voici quelques exemples d'autorisation dans un environnement IBM WebSphere MQ :

- Autoriser uniquement un administrateur autorisé à émettre des commandes pour gérer les ressources IBM WebSphere MQ .
- Autoriser une application à se connecter à un gestionnaire de files d'attente uniquement si l'ID utilisateur associé à l'application est autorisé à le faire.
- Autoriser une application à ouvrir uniquement les files d'attente nécessaires à sa fonction.
- Autoriser une application à s'abonner uniquement aux rubriques nécessaires à sa fonction.
- Autoriser une application à effectuer uniquement les opérations sur une file d'attente qui sont nécessaires à sa fonction. Par exemple, une application peut n'avoir besoin que de parcourir les messages d'une file d'attente particulière et non d'insérer ou d'extraire des messages.

Pour plus d'informations sur la configuration de l'autorisation, voir «Autorisation de planification», à la page 51 et les sous-rubriques associées.

Concepts associés

«Authorization», à la page 6
L' *autorisation* protège les ressources critiques d'un système en limitant l'accès uniquement aux utilisateurs autorisés et à leurs applications. Il empêche l'utilisation non autorisée d'une ressource ou l'utilisation d'une ressource de manière non autorisée.

Audit dans IBM WebSphere MQ

IBM WebSphere MQ peut émettre des messages d'événement pour enregistrer que l'activité inhabituelle a eu lieu.

Voici quelques exemples d'audit dans un environnement IBM WebSphere MQ :

- Une application tente d'ouvrir une file d'attente qu'elle n'est pas autorisée à ouvrir. Un message d'événement d'instrumentation est émis. En inspectant le message d'événement, vous découvrez que cette tentative a eu lieu et pouvez décider de l'action nécessaire.
- Une application tente d'ouvrir un canal, mais la tentative échoue car SSL n'autorise pas la connexion. Un message d'événement d'instrumentation est émis. En inspectant le message d'événement, vous découvrez que cette tentative a eu lieu et pouvez décider de l'action nécessaire.

Concepts associés

«Audit», à la page 6
L' *audit* est le processus d'enregistrement et de vérification des événements pour détecter si une activité inattendue ou non autorisée a eu lieu ou si une tentative a été effectuée pour effectuer cette activité.

Confidentialité dans IBM WebSphere MQ

Vous pouvez implémenter la confidentialité dans IBM WebSphere MQ en chiffrant les messages.

Voici quelques exemples de la manière dont la confidentialité peut être assurée dans un environnement IBM WebSphere MQ :

- Une fois qu'un agent MCA émetteur obtient un message d'une file d'attente de transmission, IBM WebSphere MQ utilise SSL ou TLS pour chiffrer le message avant qu'il ne soit envoyé sur le réseau à l'agent MCA récepteur. A l'autre extrémité du canal, le message est déchiffré avant que l'agent MCA récepteur ne le place dans sa file d'attente de destination.
- Alors que les messages sont stockés dans une file d'attente locale, les mécanismes de contrôle d'accès fournis par IBM WebSphere MQ peuvent être considérés comme suffisants pour protéger leur contenu contre toute divulgation non autorisée. Toutefois, pour un niveau de sécurité plus élevé, vous pouvez utiliser IBM WebSphere MQ Advanced Message Security pour chiffrer les messages stockés dans les files d'attente.

Concepts associés

«Confidentialité», à la page 7
Le service de *confidentialité* protège les informations sensibles contre toute divulgation non autorisée.

Intégrité des données dans IBM WebSphere MQ

Vous pouvez utiliser un service d'intégrité des données pour détecter si un message a été modifié.

Voici quelques exemples de la manière dont l'intégrité des données peut être assurée dans un environnement IBM WebSphere MQ :

- Vous pouvez utiliser SSL ou TLS pour détecter si le contenu d'un message a été délibérément modifié alors qu'il était transmis sur un réseau. Dans SSL et TLS, l'algorithme de synthèse de message permet de détecter les messages modifiés en transit. Tous les CipherSpecs IBM WebSphere MQ fournissent un algorithme de prétraitement de message, à l'exception de TLS_RSA_WITH_NULL_NULL qui ne fournit pas l'intégrité des données de message.
- Lorsque les messages sont stockés dans une file d'attente locale, les mécanismes de contrôle d'accès fournis par IBM WebSphere MQ peuvent être considérés comme suffisants pour empêcher une modification délibérée du contenu des messages. Toutefois, pour un niveau de sécurité plus élevé, vous pouvez utiliser IBM WebSphere MQ Advanced Message Security pour détecter si le contenu d'un message a été délibérément modifié entre le moment où le message a été inséré dans la file d'attente et le moment où il a été extrait de la file d'attente.

Concepts associés

«Intégrité des données», à la page 7

Le service d' *intégrité des données* détecte s'il y a eu une modification non autorisée des données.

Cryptographie dans IBM WebSphere MQ

IBM WebSphere MQ fournit la cryptographie à l'aide des protocoles SSL (Secure Sockets Layer) et TLS (Transport Security Layer).

Pour plus d'informations, voir «Protocoles de sécurité dans IBM WebSphere MQ», à la page 24.

Concepts associés

«Concepts cryptographiques», à la page 7
Cette collection de rubriques décrit les concepts de cryptographie applicables à WebSphere MQ.

Protocoles de sécurité dans IBM WebSphere MQ

IBM WebSphere MQ prend en charge les protocoles TLS (Transport Layer Security) et SSL (Secure Sockets Layer) afin de fournir une sécurité au niveau des liens pour les canaux de message et les canaux MQI.

Les canaux de transmission de messages et les canaux MQI peuvent utiliser le protocole SSL ou TLS pour assurer la sécurité au niveau des liens.Un agent MCA appelant est un client SSL ou TLS et un agent MCA répondeur est un serveur SSL ou TLS. WebSphere MQ prend en charge la version 3.0 du protocole SSL et la version 1.0 et la version 1.2 du protocole TLS (Transport Layer Security). Vous spécifiez les algorithmes de cryptographie utilisés par SSL ou le protocole en fournissant un CipherSpec dans la définition de canal.

A chaque extrémité d'un canal de transmission de messages et à l'extrémité serveur d'un canal MQI, l'agent MCA agit pour le compte du gestionnaire de files d'attente auquel il est connecté. Lors de l'établissement de liaison SSL ou TLS, l'agent MCA envoie le certificat numérique du gestionnaire de files d'attente à son agent MCA partenaire à l'autre extrémité du canal. Le code WebSphere MQ à l'extrémité client d'un canal MQI agit pour le compte de l'utilisateur de l'application client WebSphere MQ . Lors de l'établissement de liaison SSL ou TLS, le code WebSphere MQ envoie le certificat numérique de l'utilisateur à l'agent MCA à l'extrémité serveur du canal MQI.

Les gestionnaires de files d'attente et les utilisateurs de client WebSphere MQ ne sont pas tenus d'avoir des certificats numériques personnels qui leur sont associés lorsqu'ils agissent en tant que clients SSL ou TLS, sauf si SSLCAUTH (REQUIRED) est spécifié côté serveur du canal.

Les certificats numériques sont stockés dans un *référentiel de clés* . The queue manager attribute *SSLKeyRepository* specifies the location of the key repository that holds the queue manager's digital certificate. Sur un système client WebSphere MQ , la variable d'environnement MQSSLKEYR indique l'emplacement du référentiel de clés qui contient le certificat numérique de l' utilisateur. Une application client WebSphere MQ peut également spécifier son emplacement dans la zone *KeyRepository* de la structure d'options de configuration SSL et TLS, MQSCO, sur un appel MQCONNX. Consultez les rubriques connexes pour plus d'informations sur les référentiels de clés et pour savoir comment spécifier leur emplacement.

Concepts associés

«Protocoles de sécurité cryptographiques SSL et TLS», à la page 15
Les protocoles cryptographiques fournissent des connexions sécurisées, permettant à deux parties de communiquer avec la confidentialité et l'intégrité des données. Le protocole TLS (Transport Layer Security) a évolué à partir de celui de la couche SSL (Secure Sockets Layer). IBM WebSphere MQ prend en charge SSL et TLS.

Prise en charge de IBM WebSphere MQ pour SSL et TLS

IBM WebSphere MQ prend en charge le protocole SSL (Secure Sockets Layer) et le protocole TLS (Transport Layer Security).

Pour plus d'informations sur les protocoles SSL et TLS, reportez-vous aux informations connexes.

IBM WebSphere MQ fournit la prise en charge suivante pour SSL version 3.0 et TLS 1.0 et TLS 1.2:

Clients Java et JMS
Ces clients utilisent la machine virtuelle Java pour fournir la prise en charge SSL et TLS.

Systèmes UNIX, Linux, and Windowset HP Integrity NonStop Server
Pour les systèmes UNIX, Linux, and Windowset HP Integrity NonStop Server , le support SSL et TLS est installé avec IBM WebSphere MQ.

Pour plus d'informations sur les prérequis pour la prise en charge de IBM WebSphere MQ SSL et TLS, voir Configuration système requise pour IBM WebSphere MQ.

Référentiel de clés SSL ou TLS
Une connexion SSL ou TLS mutuellement authentifiée requiert un référentiel de clés (qui peut être connu sous des noms différents sur des plateformes différentes) à chaque extrémité de la connexion. Le référentiel de clés inclut des certificats numériques et des clés privées.

Ces informations utilisent le terme général *référentiel de clés* pour décrire le magasin des certificats numériques et leurs clés privées associées. Les noms de magasin spécifiques utilisés sur les plateformes et les environnements qui prennent en charge SSL et TLS sont les suivants:

Java et JMS	fichier de clés et fichier de clés certifiées
Windows UNIX Linux Windows UNIX Linux Windows , systèmes UNIX and Linux	fichier de la base de données de clés

Pour plus d'informations, voir «Certificats numériques», à la page 9 et «Concepts SSL (Secure Sockets Layer) et TLS (Transport Layer Security)», à la page 15.

Une connexion SSL ou TLS mutuellement authentifiée requiert un référentiel de clés à chaque extrémité de la connexion. Le référentiel de clés peut contenir:

- Un certain nombre de certificats de l'autorité de certification provenant de différentes autorités de certification qui permettent au gestionnaire de files d'attente ou au client de vérifier les certificats qu'il reçoit de son partenaire à l'extrémité éloignée de la connexion. Les certificats individuels peuvent se trouver dans une chaîne de certificats.
- Un ou plusieurs certificats personnels reçus d'une autorité de certification. Vous associez un certificat personnel distinct à chaque gestionnaire de files d'attente ou client WebSphere MQ MQI. Les certificats personnels sont essentiels sur un client SSL ou TLS si une authentification mutuelle est requise. Si l'authentification mutuelle n'est pas requise, les certificats personnels ne sont pas nécessaires sur le client. Le référentiel de clés peut également contenir la clé privée correspondant à chaque certificat personnel.
- Demandes de certificat qui attendent d'être signées par un certificat de l'autorité de certification digne de confiance.

Pour plus d'informations sur la protection de votre référentiel de clés, voir «Protection des référentiels de clés IBM WebSphere MQ», à la page 26.

L'emplacement du référentiel de clés dépend de la plateforme que vous utilisez:

Windows UNIX Linux **Windows, systèmes UNIX and Linux**
Sous Windows, sur les systèmes UNIX and Linux , le référentiel de clés est un fichier de base de données de clés. Le nom du fichier de la base de données de clés doit avoir l'extension `.kdb`.
Par exemple, sous UNIX and Linux, le fichier de base de données de clés par défaut pour le gestionnaire de files d'attente `QM1` est `/var/mqm/qmgrs/QM1/ssl/key.kdb` . Si IBM WebSphere MQ est installé dans l'emplacement par défaut, le chemin équivalent sous Windows est `C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\key.kdb`.

Sur les systèmes Windows , UNIX and Linux , chaque fichier de base de données de clés est associé à un fichier de mot de passe secret. Ce fichier contient les mots de passe codés qui permettent aux programmes d'accéder à la base de données de clés. Le fichier de mot de passe secret doit se trouver

dans le même répertoire et avoir le même radical de fichier que la base de données de clés, et doit se terminer par le suffixe `.sth` , par exemple `/var/mqm/qmgrs/QM1/ssl/key.sth`

Remarque : Sous Windows, systèmes UNIX and Linux , les cartes matérielles de cryptographie PKCS #11 peuvent contenir les certificats et les clés qui sont conservés dans un fichier de base de données de clés. Lorsque des certificats et des clés sont stockés sur des cartes PKCS #11 , WebSphere MQ a toujours besoin d'accéder à la fois à un fichier de base de données de clés et à un fichier de mot de passe secret.

Sur les systèmes Windows et UNIX , la base de données de clés contient également la clé privée du certificat personnel associé au gestionnaire de files d'attente ou au client WebSphere MQ MQI.

Protection des référentiels de clés IBM WebSphere MQ
Le référentiel de clés pour IBM WebSphere MQ est un fichier. Assurez-vous que seul l'utilisateur prévu peut accéder au fichier de référentiel de clés. Cela empêche un intrus ou un autre utilisateur non autorisé de copier le fichier de référentiel de clés sur un autre système, puis de configurer un ID utilisateur identique sur ce système pour simuler les droits d'accès de l'utilisateur prévu.

Les droits sur les fichiers dépendent de l'umask de l'utilisateur et de l'outil utilisé. Sous Windows, les comptes IBM WebSphere MQ requièrent des droits `BypassTraverseChecking` , ce qui signifie que les droits des dossiers dans le chemin d'accès au fichier n'ont aucun effet.

Vérifiez les droits d'accès aux fichiers du référentiel de clés et assurez-vous que les fichiers et le dossier qui les contient ne sont pas lisibles par tout le monde, de préférence pas même par groupe.

La mise en lecture seule du magasin de clés est recommandée, quel que soit le système que vous utilisez, seul l'administrateur étant autorisé à activer les opérations d'écriture afin d'effectuer la maintenance.

Dans la pratique, vous devez protéger tous les magasins de clés, quel que soit l'emplacement et s'ils sont protégés par mot de passe ou non ; protégez les référentiels de clés.

Régénération du référentiel de clés du gestionnaire de files d'attente
Lorsque vous modifiez le contenu d'un référentiel de clés, le gestionnaire de files d'attente ne récupère pas immédiatement le nouveau contenu. Pour qu'un gestionnaire de files d'attente puisse utiliser le nouveau contenu du référentiel de clés, vous devez exécuter la commande REFRESH SECURITY TYPE (SSL).

Ce processus est intentionnel et évite que plusieurs canaux en cours d'exécution puissent utiliser des versions différentes d'un référentiel de clés. En tant que contrôle de sécurité, une seule version d'un référentiel de clés peut être chargée par le gestionnaire de files d'attente à la fois.

Pour plus d'informations sur la commande REFRESH SECURITY TYPE (SSL), voir REFRESH SECURITY.

Vous pouvez également actualiser un référentiel de clés à l'aide des commandes PCF ou de l'explorateur WebSphere MQ . Pour plus d'informations, voir la commande MQCMD_REFRESH_SECURITY et la rubrique *Actualisation de la sécurité SSL ou TLS* dans la section WebSphere MQ Explorer de la documentation du produit.

Concepts associés
«Actualisation de la vue d'un client du contenu du référentiel de clés SSL et des paramètres SSL», à la page 26
Pour mettre à jour l'application client avec le contenu actualisé du référentiel de clés, vous devez arrêter et redémarrer l'application client.

Actualisation de la vue d'un client du contenu du référentiel de clés SSL et des paramètres SSL
Pour mettre à jour l'application client avec le contenu actualisé du référentiel de clés, vous devez arrêter et redémarrer l'application client.

Vous ne pouvez pas actualiser la sécurité sur un client WebSphere MQ ; il n'existe pas d'équivalent de la commande REFRESH SECURITY TYPE (SSL) pour les clients (voir REFRESH SECURITY) pour plus d'informations.

Vous devez arrêter et redémarrer l'application, chaque fois que vous modifiez le certificat de sécurité, pour mettre à jour l'application client avec le contenu actualisé du référentiel de clés.

Si le redémarrage du canal actualise les configurations et que votre application possède une logique de reconnexion, vous pouvez actualiser la sécurité sur le client en exécutant la commande STOP CHL STATUS (INACTIVE).

Concepts associés

«Régénération du référentiel de clés du gestionnaire de files d'attente», à la page 26
Lorsque vous modifiez le contenu d'un référentiel de clés, le gestionnaire de files d'attente ne récupère pas immédiatement le nouveau contenu. Pour qu'un gestionnaire de files d'attente puisse utiliser le nouveau contenu du référentiel de clés, vous devez exécuter la commande REFRESH SECURITY TYPE (SSL).

FIPS (Federal Information Processing Standards)
Cette rubrique présente le programme FIPS (Federal Information Processing Standards) Cryptomodule Validation Program du US National Institute of Standards and Technology et les fonctions cryptographiques qui peuvent être utilisées sur les canaux SSL ou TLS, pour les systèmes Windows, UNIX and Linuxet z/OS .

La conformité FIPS 140-2 d'une connexion IBM WebSphere MQ SSL ou TLS sur les systèmes UNIX, Linuxet Windows est disponible ici «Federal Information Processing Standards (FIPS) pour UNIX, Linuxet Windows», à la page 27.

Si du matériel de cryptographie est présent, les modules de cryptographie utilisés par IBM WebSphere MQ peuvent être configurés pour être ceux fournis par le fabricant du matériel. Dans ce cas, la configuration est uniquement conforme à la norme FIPS si ces modules cryptographiques sont certifiés FIPS.

Au fil du temps, les normes fédérales de traitement de l'information sont mises à jour pour refléter les nouvelles attaques contre les algorithmes et les protocoles de chiffrement. Par exemple, certains CipherSpecs peuvent ne plus être certifiés FIPS. Lorsque de telles modifications se produisent, IBM WebSphere MQ est également mis à jour pour implémenter la dernière norme. Vous pouvez alors constater des changements de comportement une fois la maintenance appliquée.

Concepts associés

«Comment indiquer que seuls les CipherSpecs certifiés FIPS sont utilisés lors de l'exécution sur MQI Client», à la page 113
Créez vos référentiels de clés à l'aide d'un logiciel compatible FIPS, puis indiquez que le canal doit utiliser des CipherSpecscertifiés FIPS.

«Utilisation des commandes iKeyman, iKeycmd, runmqakm et runmqckm», à la page 119
Sur les systèmes UNIX, Linux et Windows , gérez les clés et les certificats numériques à l'aide de l'interface graphique iKeyman ou à partir de la ligne de commande à l'aide de iKeycmd ou de runmqakm.

Tâches associées

Activation de SSL dans les classes WebSphere MQ pour Java
Utilisation de Secure Sockets Layer (SSL) avec WebSphere MQ classes for JMS

Référence associée

Propriétés SSL des objets JMS

Information associée

«La norme FIPS (Federal Information Processing Standards)», à la page 20
Le gouvernement américain fournit des conseils techniques sur des systèmes informatiques et sur des systèmes de sécurité, y compris le chiffrement de données. Le National Institute for Standards and Technology (NIST) est un organisme important qui s'occupe des systèmes informatiques et de la sécurité. Il émet des recommandations et établit des normes, notamment la norme FIPS (Federal Information Processing Standards).

Federal Information Processing Standards (FIPS) pour UNIX, Linuxet Windows
Lorsque la cryptographie est requise sur un canal SSL ou TLS sous Windows, systèmes UNIX and Linux , WebSphere MQ utilise un package de cryptographie appelé IBM Crypto for C (ICC). Sur les plateformes Windows, UNIX and Linux , le logiciel ICC a transmis le programme FIPS (Federal Information Processing

Standards) Cryptomodule Validation Program du US National Institute of Standards and Technology, au niveau 140-2.

La conformité FIPS 140-2 d'une connexion WebSphere MQ SSL ou TLS sous Windows, UNIX and Linux est la suivante:

- Pour tous les canaux de transmission de messages IBM WebSphere MQ (à l'exception des types de canal CLNTCONN), la connexion est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - La version GSKit ICC installée a été certifiée conforme à la norme FIPS 140-2 sur la version du système d'exploitation et l'architecture matérielle installées.
  - L'attribut SSLFIPS du gestionnaire de files d'attente a été défini sur YES.
  - Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .
- Pour toutes les applications client IBM WebSphere MQ MQI, la connexion utilise GSKit et est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - La version GSKit ICC installée a été certifiée conforme à la norme FIPS 140-2 sur la version du système d'exploitation et l'architecture matérielle installées.
  - Vous avez indiqué que seule la cryptographie certifiée FIPS doit être utilisée, comme décrit dans la rubrique connexe pour le client MQI.
  - Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .
- Pour les classes IBM WebSphere MQ pour les applications Java utilisant le mode client, la connexion utilise les implémentations SSL et TLS de l'environnement d'exécution Java et est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - L'environnement d'exécution Java utilisé pour exécuter l'application est conforme à la norme FIPS sur la version du système d'exploitation installée et l'architecture matérielle.
  - Vous avez spécifié que seule la cryptographie certifiée FIPS doit être utilisée, comme décrit dans la rubrique connexe pour le client Java.
  - Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .
- Pour les applications IBM WebSphere MQ classes for JMS utilisant le mode client, la connexion utilise les implémentations SSL et TLS de l'environnement d'exécution Java (JRE) et est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - L'environnement d'exécution Java utilisé pour exécuter l'application est conforme à la norme FIPS sur la version du système d'exploitation installée et l'architecture matérielle.
  - Vous avez indiqué que seule la cryptographie certifiée FIPS doit être utilisée, comme décrit dans la rubrique associée pour le client JMS.
  - Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .
- Pour les applications client .NET non gérées, la connexion utilise GSKit et est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - La version GSKit ICC installée a été certifiée conforme à la norme FIPS 140-2 sur la version du système d'exploitation et l'architecture matérielle installées.
  - Vous avez spécifié que seule la cryptographie certifiée FIPS doit être utilisée, comme décrit dans la rubrique associée pour le client .NET.
  - Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .
- Pour les applications client XMS .NET non gérées, la connexion utilise GSKit et est conforme à la norme FIPS si les conditions suivantes sont remplies:
  - La version GSKit ICC installée a été certifiée conforme à la norme FIPS 140-2 sur la version du système d'exploitation et l'architecture matérielle installées.

- Vous avez spécifié que seule la cryptographie certifiée FIPS doit être utilisée, comme décrit dans la documentation XMS .NET.
- Tous les référentiels de clés ont été créés et manipulés uniquement à l'aide de logiciels conformes à la norme FIPS, tels que **runmqakm** avec l'option `-fips` .

Toutes les plateformes AIX, Linux, HP-UX, Solaris, Windowset z/OS prises en charge sont certifiées FIPS 140-2 sauf comme indiqué dans le fichier Readme inclus avec chaque groupe de correctifs ou groupe de mises à jour.

Pour les connexions SSL et TLS utilisant GSKit, le composant certifié FIPS 140-2 est nommé *ICC*. Il s'agit de la version de ce composant qui détermine la conformité à la norme GSKit FIPS sur une plateforme donnée. Pour déterminer la version d'ICC actuellement installée, exécutez la commande **dspmqver -p 64 -v** .

Voici un exemple d'extrait de la sortie **dspmqver -p 64 -v** relative à ICC:

```
  icc
 ============
@ (#)CompanyName: IBM Corporation
@(#)LegalTrademarks:  IBM
@ (#)FileDescription: IBM Crypto for C-language
@(#)FileVersion:      8.0.0.0
@ (#)LegalCopyright: Eléments sous licence-Propriété d' IBM
@ (#) ICC
@ (#) (C) Copyright IBM Corp. 2002, 2024.
@ (#) Tous droits réservés. Utilisateurs du gouvernement américain
@ (#) Droits restreints-Utilisation, duplication ou divulgation
@ (#) restreint par GSA ADP Schedule Contract avec IBM Corp.
@ (#)ProductName: icc_8.0 (générationGoldCoast ) 100415
@(#)ProductVersion:   8.0.0.0
@(#)ProductInfo:      10/04/15.03:32:19.10/04/15.18:41:51
@ (#) CMVCInfo:
```

L'instruction de certification NIST pour GSKit ICC 8 (incluse dans GSKit 8) est disponible à l'adresse suivante: Cryptographic Module Validation Program.

Si du matériel de cryptographie est présent, les modules de cryptographie utilisés par IBM WebSphere MQ peuvent être configurés pour être ceux fournis par le fabricant du matériel. Dans ce cas, la configuration est uniquement conforme à la norme FIPS si ces modules cryptographiques sont certifiés FIPS.

Remarque : Les clients SSL et TLS Solaris x86 32 bits configurés pour une opération compatible avec FIPS 140-2 échouent lors de l'exécution sur des systèmes Intel. Cet échec survient car le chargement du fichier de bibliothèque GSKit-Crypto Solaris x86 32 bits compatible avec la norme FIPS 140-2 échoue sur le jeu de circuits Intel. Sur les systèmes affectés, l'erreur AMQ9655 est signalée dans le journal des erreurs du client. Pour résoudre ce problème, désactivez la conformité à la norme FIPS 140-2 ou recompilez l'application client 64 bits, car le code 64 bits n'est pas affecté.

Restrictions DES triple imposées lors d'une opération conforme à la norme FIPS 140-2

Lorsque WebSphere MQ est configuré pour fonctionner conformément à la norme FIPS 140-2, des restrictions supplémentaires sont appliquées en relation avec Triple DES (3DES) CipherSpecs. Ces restrictions permettent la conformité à la recommandation US NIST SP800-67 .

1. Toutes les parties de la clé Triple DES doivent être uniques.
2. Aucune partie de la clé Triple DES ne peut être une clé Weak, Semi-Weak ou Possiblement-Weak selon les définitions de la norme NIST SP800-67.
3. Vous ne pouvez pas transmettre plus de 32 Go de données via la connexion avant qu'une réinitialisation de clé secrète ne soit nécessaire. Par défaut, WebSphere MQ ne réinitialise pas la clé de session secrète. Cette réinitialisation doit donc être configurée. L'échec de l'activation de la réinitialisation de la clé secrète lors de l'utilisation d'un CipherSpec Triple DES et de la conformité à la norme FIPS 140-2 entraîne la fermeture de la connexion avec l'erreur AMQ9288 après le dépassement du nombre maximal d'octets. Pour plus d'informations sur la configuration de la réinitialisation des clés secrètes, voir «Réinitialisation des clés secrètes SSL et TLS», à la page 234.

WebSphere MQ génère des clés de session Triple DES qui sont déjà conformes aux règles 1 et 2. Toutefois, pour satisfaire à la troisième restriction, vous devez activer la réinitialisation de la clé secrète lors de l'utilisation de CipherSpecs Triple DES dans une configuration FIPS 140-2. Vous pouvez également éviter d'utiliser Triple DES.

Concepts associés

«Comment indiquer que seuls les CipherSpecs certifiés FIPS sont utilisés lors de l'exécution sur MQI Client», à la page 113
Créez vos référentiels de clés à l'aide d'un logiciel compatible FIPS, puis indiquez que le canal doit utiliser des CipherSpecscertifiés FIPS.

«Utilisation des commandes iKeyman, iKeycmd, runmqakm et runmqckm», à la page 119
Sur les systèmes UNIX, Linux et Windows , gérez les clés et les certificats numériques à l'aide de l'interface graphique iKeyman ou à partir de la ligne de commande à l'aide de iKeycmd ou de runmqakm.

Tâches associées

Activation de SSL dans les classes WebSphere MQ pour Java

Utilisation de Secure Sockets Layer (SSL) avec WebSphere MQ classes for JMS

Référence associée

Propriétés SSL des objets JMS

Information associée

«La norme FIPS (Federal Information Processing Standards)», à la page 20
Le gouvernement américain fournit des conseils techniques sur des systèmes informatiques et sur des systèmes de sécurité, y compris le chiffrement de données. Le National Institute for Standards and Technology (NIST) est un organisme important qui s'occupe des systèmes informatiques et de la sécurité. Il émet des recommandations et établit des normes, notamment la norme FIPS (Federal Information Processing Standards).

SSL et TLS sur le client IBM WebSphere MQ MQI
IBM WebSphere MQ prend en charge SSL et TLS sur les clients. Vous pouvez personnaliser l'utilisation de SSL ou TLS de différentes manières.

IBM WebSphere MQ fournit une prise en charge SSL et TLS pour les clients IBM WebSphere MQ MQI sur les systèmes Windowset UNIX and Linux . Si vous utilisez des classes IBM WebSphere MQ pour Java, voir Utilisation de classes WebSphere MQ pour Java et si vous utilisez des classes IBM WebSphere MQ pour JMS, voir Utilisation de classes WebSphere MQ pour JMS. Le reste de cette section ne s'applique pas aux environnements Java ou JMS.

Vous pouvez spécifier le référentiel de clés pour un client IBM WebSphere MQ MQI avec la valeur MQSSLKEYR dans le fichier de configuration du client IBM WebSphere MQ ou lorsque votre application effectue un appel MQCONNX. Vous disposez de trois options pour spécifier qu'un canal utilise SSL:

- Utilisation d'une table de définition de canal
- Utilisation de la structure des options de configuration SSL, MQSCO, sur un appel MQCONNX
- Utilisation d' Active Directory (sur les systèmes Windows)

Vous ne pouvez pas utiliser la variable d'environnement MQSERVER pour indiquer qu'un canal utilise SSL.

Vous pouvez continuer à exécuter vos applications client IBM WebSphere MQ MQI existantes sans SSL, tant que SSL n'est pas spécifié à l'autre extrémité du canal.

Si des modifications sont apportées sur une machine client au contenu du référentiel de clés SSL, à l'emplacement du référentiel de clés SSL, aux informations d'authentification ou aux paramètres matériels de cryptographie, vous devez arrêter toutes les connexions SSL afin de refléter ces modifications dans les canaux de connexion client utilisés par l'application pour se connecter au gestionnaire de files d'attente. Une fois toutes les connexions terminées, redémarrez les canaux SSL. Tous les nouveaux paramètres SSL sont utilisés. Ces paramètres sont analogues à ceux actualisés par la commande REFRESH SECURITY TYPE (SSL) sur les systèmes de gestionnaire de files d'attente.

Lorsque votre client IBM WebSphere MQ MQI s'exécute sur un système Windows, UNIX and Linux avec du matériel de cryptographie, vous configurez ce matériel avec la variable d'environnement MQSSLCRYP.

Cette variable est équivalente au paramètre SSLCRYP de la commande ALTER QMGR MQSC. Pour obtenir une description du paramètre SSLCRYP dans la commande ALTER QMGR MQSC, voir ALTER QMGR . Si vous utilisez la version GSK_PCS11 du paramètre SSLCRYP, le libellé de jeton PKCS #11 doit être indiqué en minuscules.

La réinitialisation de la clé secrète SSL et la norme FIPS sont prises en charge sur les clients IBM WebSphere MQ MQI. Pour plus d'informations, reportez-vous aux sections «Réinitialisation des clés secrètes SSL et TLS», à la page 234 et «Federal Information Processing Standards (FIPS) pour UNIX, Linuxet Windows», à la page 27.

Pour plus d'informations sur la prise en charge de SSL pour les clients IBM WebSphere MQ MQI, voir «Configuration de la sécurité du client IBM WebSphere MQ MQI», à la page 112 .

Tâches associées

Configuration d'un client à l'aide d'un fichier de configuration

Spécification du fait qu'un canal MQI utilise SSL

Pour qu'un canal MQI utilise SSL, la valeur de l'attribut *SSLCipherSpec* du canal de connexion client doit être le nom d'un CipherSpec pris en charge par IBM WebSphere MQ sur la plateforme client.

Vous pouvez définir un canal de connexion client avec une valeur pour cet attribut de l'une des manières suivantes. Ils sont répertoriés par ordre de priorité décroissante.

1. Lorsqu'un exit PreConnect fournit une structure de définition de canal à utiliser.

   Un exit PreConnect peut fournir le nom d'un CipherSpec dans la zone *SSLCipherSpec* d'une structure de définition de canal, MQCD. Cette structure est renvoyée dans la zone **ppMQCDArrayPtr** de la structure de paramètres d'exit MQNXP utilisée par l'exit PreConnect .
2. Lorsqu'une application client WebSphere MQ MQI émet un appel MQCONNX.

   L'application peut spécifier le nom d'un CipherSpec dans la zone *SSLCipherSpec* d'une structure de définition de canal, MQCD.Cette structure est référencée par la structure d'options de connexion, MQCNO, qui est un paramètre de l'appel MQCONNX.
3. Utilisation d'une table de définition de canal du client (CCDT).

   Une ou plusieurs entrées d'une table de définition de canal du client peuvent spécifier le nom d'un CipherSpec.Par exemple, si vous créez une entrée à l'aide de la commande MQSC DEFINE CHANNEL, vous pouvez utiliser le paramètre SSLCIPH dans la commande pour spécifier le nom d'un CipherSpec.
4. Utilisation d' Active Directory sous Windows.

   Sur les systèmes Windows , vous pouvez utiliser la commande de contrôle **setmqscp** pour publier les définitions de canal de connexion client dans Active Directory. Une ou plusieurs de ces définitions peuvent spécifier le nom d'un CipherSpec.

Par exemple, si une application client fournit une définition de canal de connexion client dans une structure MQCD sur un appel MQCONNX, cette définition est utilisée de préférence aux entrées d'une table de définition de canal client accessibles par le client WebSphere MQ .

Vous ne pouvez pas utiliser la variable d'environnement MQSERVER pour fournir la définition de canal à l'extrémité client d'un canal MQI qui utilise SSL.

Pour vérifier si un certificat client a transité, affichez le statut du canal à l'extrémité serveur d'un canal pour la présence d'une valeur de paramètre de nom d'homologue.

Concepts associés

«Spécification d'un CipherSpec pour un client IBM WebSphere MQ MQI», à la page 233
Vous disposez de trois options pour spécifier un CipherSpec pour un client IBM WebSphere MQ MQI.

CipherSpecs et CipherSuites dans IBM WebSphere MQ

IBM WebSphere MQ prend en charge les CipherSpecsSSL et TLS, ainsi que les algorithmes RSA et Diffie-Hellman.

WebSphere MQ prend en charge SSL V3 et TLS V1.0 et V1.2 CipherSpecs.

WebSphere MQ prend en charge les algorithmes d'authentification et d'échange de clés RSA et Diffie-Hellman. La taille de la clé utilisée lors de l'établissement de liaison SSL peut dépendre du certificat numérique que vous utilisez, mais certains CipherSpecs incluent une spécification de la taille de la clé d'établissement de liaison. Plus la taille de clé est élevée, plus l'authentification est solide. Avec des tailles de clé plus petites, l'établissement de la liaison est plus rapide.

Concepts associés

«CipherSpecs et CipherSuites», à la page 19
Les protocoles de sécurité cryptographique doivent convenir des algorithmes utilisés par une connexion sécurisée. CipherSpecs et CipherSuites définissent des combinaisons spécifiques d'algorithmes.

NSA Suite B Cryptography dans IBM WebSphere MQ
Cette rubrique explique comment configurer IBM WebSphere MQ sur les systèmes Windows, Linuxet UNIX pour qu'il soit conforme au profil TLS 1.2 conforme à la norme Suite B.

Au fil du temps, la norme NSA Cryptography Suite B est mise à jour pour refléter les nouvelles attaques contre les algorithmes et les protocoles de chiffrement. Par exemple, certains CipherSpecs peuvent ne plus être certifiés Suite B. Lorsque de telles modifications se produisent, IBM WebSphere MQ est également mis à jour pour implémenter la dernière norme. Vous pouvez alors constater des changements de comportement une fois la maintenance appliquée. Le fichier Readme de IBM WebSphere MQ Version 7.5 répertorie la version de Suite B appliquée par chaque niveau de maintenance du produit. Si vous configurez IBM WebSphere MQ pour appliquer la conformité Suite B, consultez toujours le fichier Readme lors de la planification de l'application de la maintenance (voir IBM MQ, WebSphere MQet les fichiers README du produit MQSeries).

Sur les systèmes Windows, UNIXet Linux , IBM WebSphere MQ peut être configuré pour être conforme au profil TLS 1.2 compatible Suite B aux niveaux de sécurité indiqués dans le tableau 1.

Tableau 1. Niveaux de sécurité Suite B avec CipherSpecs et algorithmes de signature numérique autorisés

Niveau de sécurité	**CipherSpecs autorisés**	**Algorithmes de signature numérique autorisés**
128 bits	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA avec SHA-256 ECDSA avec SHA-384
192 bits	ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA avec SHA-384
Les deux[1]	ECDHE_ECDSA_AES_128_GCM_SHA256 ECDHE_ECDSA_AES_256_GCM_SHA384	ECDSA avec SHA-256 ECDSA avec SHA-384

1. Il est possible de configurer simultanément les niveaux de sécurité 128 bits et 192 bits. Etant donné que la configuration Suite B détermine les algorithmes de cryptographie minimaux acceptables, la configuration des deux niveaux de sécurité est équivalente à la configuration du niveau de sécurité 128 bits uniquement. Les algorithmes de cryptographie du niveau de sécurité 192 bits sont plus forts que le minimum requis pour le niveau de sécurité 128 bits, de sorte qu'ils sont autorisés pour le niveau de sécurité 128 bits même si le niveau de sécurité 192 bits n'est pas activé.

Remarque : Les conventions de dénomination utilisées pour le niveau de sécurité ne représentent pas nécessairement la taille de courbe elliptique ou la taille de clé de l'algorithme de chiffrement AES.

CipherSpec -conformation vers Suite B

Bien que le comportement par défaut de IBM WebSphere MQ ne soit pas conforme à la norme Suite B, IBM WebSphere MQ peut être configuré pour être conforme à l'un des niveaux de sécurité ou aux deux sur les systèmes Windows, UNIX et Linux . Suite à la configuration réussie de IBM WebSphere MQ pour utiliser Suite B, toute tentative de démarrage d'un canal sortant à l'aide d'un CipherSpec non conforme à Suite B entraîne l'erreur AMQ9282. Cette activité a également pour conséquence que le client MQI renvoie le code anomalie MQRC_CIPHER_SPEC_NOT_SUITE_B. De même, la tentative de démarrage d'un canal entrant à l'aide d'un CipherSpec non conforme à la configuration Suite B entraîne l'erreur AMQ9616.

Pour plus d'informations sur WebSphere MQ CipherSpecs, voir «Définition des spécifications CipherSpec», à la page 227

Suite B et certificats numériques

La suite B restreint les algorithmes de signature numérique qui peuvent être utilisés pour signer des certificats numériques. La suite B restreint également le type de clé publique que les certificats peuvent contenir. Par conséquent, WebSphere MQ doit être configuré pour utiliser des certificats dont l'algorithme de signature numérique et le type de clé publique sont autorisés par le niveau de sécurité Suite B configuré du partenaire distant. Les certificats numériques qui ne sont pas conformes aux exigences de niveau de sécurité sont rejetés et la connexion échoue avec l'erreur AMQ9633 ou AMQ9285.

Pour le niveau de sécurité Suite B 128 bits, la clé publique du sujet de certificat doit utiliser la courbe elliptique NIST P-256 ou la courbe elliptique NIST P-384 et être signée avec la courbe elliptique NIST P-256 ou la courbe elliptique NIST P-384 . Au niveau de la sécurité Suite B 192 bits, la clé publique du sujet de certificat est requise pour utiliser la courbe elliptique NIST P-384 et pour être signée avec la courbe elliptique NIST P-384 .

Pour obtenir un certificat adapté à une opération conforme à la suite B, utilisez la commande **runmqakm** et spécifiez le paramètre **-sig_alg** pour demander un algorithme de signature numérique approprié. Les valeurs des paramètres EC_ecdsa_with_SHA256 et EC_ecdsa_with_SHA384 **-sig_alg** correspondent à des clés de courbe elliptique signées par les algorithmes de signature numérique Suite B autorisés.

Pour plus d'informations sur la commande **runmqakm** , voir Options runmqckm et runmqakm.

Remarque : Les outils **iKeycmd** et **iKeyman** ne prennent pas en charge la création de certificats numériques pour une opération compatible avec Suite B.

Création et demande de certificats numériques

Pour créer un certificat numérique autosigné pour les tests Suite B, voir «Création d'un certificat personnel autosigné sur les systèmes UNIX, Linux, and Windows», à la page 127

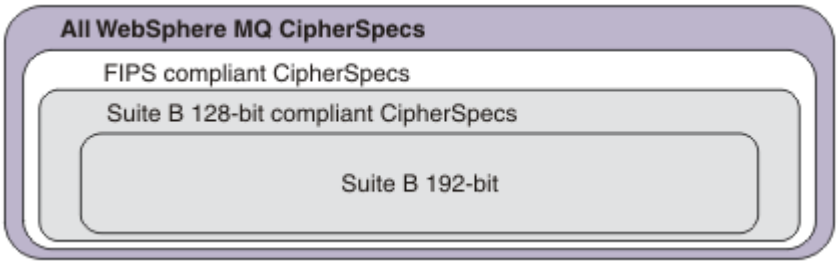
Pour demander un certificat numérique signé par une autorité de certification pour une utilisation en production Suite B, voir «Demande d'un certificat personnel sur les systèmes UNIX, Linux, and Windows», à la page 130.

Remarque : L'autorité de certification utilisée doit générer des certificats numériques qui répondent aux exigences décrites dans le document IETF RFC 6460.

FIPS 140-2 et Suite B

La norme Suite B est conceptuellement similaire à la norme FIPS 140-2, car elle restreint l'ensemble des algorithmes de cryptographie activés afin de fournir un niveau de sécurité assuré. Les CipherSpecs Suite B actuellement pris en charge peuvent être utilisés lorsque IBM WebSphere MQ est configuré pour une opération conforme à la norme FIPS 140-2. Il est donc possible de configurer WebSphere MQ pour la conformité FIPS et Suite B simultanément, auquel cas les deux ensembles de restrictions s'appliquent.

Le diagramme suivant illustre la relation entre ces sous-ensembles:



Configuration de WebSphere MQ pour une opération compatible Suite B

Pour plus d'informations sur la configuration de IBM WebSphere MQ sous Windows, UNIX et Linux pour un fonctionnement compatible avec Suite B, voir «Configuration de IBM WebSphere MQ pour Suite B», à la page 34.

IBM WebSphere MQ ne prend pas en charge les opérations compatibles Suite B sur les plateformes IBM i et z/OS . Les clients Java et JMS WebSphere MQ ne prennent pas en charge le fonctionnement compatible Suite B.

Concepts associés

«Comment indiquer que seuls les CipherSpecs certifiés FIPS sont utilisés lors de l'exécution sur MQI Client», à la page 113
Créez vos référentiels de clés à l'aide d'un logiciel compatible FIPS, puis indiquez que le canal doit utiliser des CipherSpecscertifiés FIPS.

Configuration de IBM WebSphere MQ pour Suite B
IBM WebSphere MQ peut être configuré pour fonctionner conformément à la norme NSA Suite B sur les systèmes UNIX, Linux, and Windows .

La suite B restreint l'ensemble des algorithmes de cryptographie activés afin de fournir un niveau de sécurité assuré. IBM WebSphere MQ peut être configuré pour fonctionner conformément à la Suite B afin de fournir un niveau de sécurité amélioré. Pour plus d'informations sur la suite B, voir «Agence de sécurité nationale (NSA) Suite B Cryptographie», à la page 21. Pour plus d'informations sur la configuration de la suite B et son effet sur les canaux SSL et TLS, voir «NSA Suite B Cryptography dans IBM WebSphere MQ», à la page 32.

Gestionnaire de files d'attente

Pour un gestionnaire de files d'attente, utilisez la commande **ALTER QMGR** avec le paramètre **SUITEB** pour définir les valeurs appropriées à votre niveau de sécurité requis. Pour plus d'informations, voir ALTER QMGR.

Vous pouvez également utiliser la commande PCF **MQCMD_CHANGE_Q_MGR** avec le paramètre **MQIA_SUITE_B_STRENGTH** pour configurer le gestionnaire de files d'attente pour une opération conforme à la suite B

MQI Client

Par défaut, les clients MQI n'appliquent pas la conformité Suite B. Vous pouvez activer le client MQI pour la conformité Suite B en exécutant l'une des options suivantes:

1. En définissant la zone **EncryptionPolicySuiteB** dans la structure MQSCO d'un appel MQCONNX sur une ou plusieurs des valeurs ci-dessous:
   - MQ_SUITE_B_NONE
   - MQ_SUITE_B_128_BIT
   - MQ_SUITE_B_192_BIT

   L'utilisation de MQ_SUITE_B_NONE avec une autre valeur n'est pas valide.
2. En définissant la variable d'environnement MQSUITEB sur une ou plusieurs des valeurs ci-dessous:
   - AUCUN
   - 128_BIT
   - 192_BIT

   Vous pouvez spécifier plusieurs valeurs à l'aide d'une liste séparée par des virgules. L'utilisation de la valeur NONE avec une autre valeur n'est pas valide.
3. En définissant l'attribut **EncryptionPolicySuiteB** dans la strophe SSL du fichier de configuration du client MQI sur une ou plusieurs des valeurs ci-dessous:

- AUCUN
- 128_BIT
- 192_BIT

  Vous pouvez spécifier plusieurs valeurs à l'aide d'une liste séparée par des virgules. L'utilisation de NONE avec une autre valeur n'est pas valide.

Remarque : Les paramètres du client MQI sont répertoriés par ordre de priorité. La structure MSCO de l'appel MQCONNX remplace le paramètre de la variable d'environnement MQSUITEB, qui remplace l'attribut dans la strophe SSL.

Pour plus de détails sur la structure MQSCO, voir MQSCO-Options de configuration SSL.

Pour plus d'informations sur l'utilisation de Suite B dans le fichier de configuration du client, voir Strophe SSL du fichier de configuration du client .

Pour plus d'informations sur l'utilisation de la variable d'environnement MQSUITEB, voir Variables d'environnement.

.NET

Pour les clients .NET non gérés, la propriété **MQC.ENCRYPTION_POLICY_SUITE_B** indique le type de sécurité Suite B requis.

Pour plus d'informations sur l'utilisation de Suite B dans les classes IBM WebSphere MQ for .NET, voir Classe MQEnvironment .NET.

Règles de validation de certificat dans IBM WebSphere MQ
La règle de validation de certificat détermine dans quelle mesure la validation de la chaîne de certificats est conforme aux normes de sécurité de l'industrie.

La règle de validation de certificat dépend de la plateforme et de l'environnement comme suit:

- Pour les applications Java et JMS sur toutes les plateformes, la règle de validation de certificat dépend du composant JSSE de l'environnement d'exécution Java. Pour plus d'informations sur les règles de validation de certificat, voir la documentation de votre environnement d'exécution Java.
- Pour les systèmes UNIX, Linux, and Windows , la règle de validation de certificat est fournie par GSKit et peut être configurée. Deux règles de validation de certificat différentes sont prises en charge:
  - Une règle de validation de certificat existante, utilisée pour une compatibilité et une interopérabilité maximales en amont avec les anciens certificats numériques qui ne sont pas conformes aux normes de validation de certificat IETF actuelles. Cette règle est appelée règle de base.
  - Une stratégie de validation de certificat stricte et conforme aux normes qui applique la norme RFC 5280. Cette règle est connue sous le nom de règle standard.

Pour plus d'informations sur la configuration de la règle de validation de certificat sur les systèmes UNIX, Linux, and Windows , voir «Configuration des règles de validation de certificat dans IBM WebSphere MQ», à la page 35. Pour plus d'informations sur les différences entre les règles de validation de certificat de base et standard, voir Certificate validation and trust policy design on UNIX, Linux and Windows systems .

Configuration des règles de validation de certificat dans IBM WebSphere MQ
Vous pouvez spécifier les règles de validation de certificat SSL/TLS qui sont utilisées pour valider les certificats numériques reçus des systèmes partenaires distants de quatre manières.

Sur le gestionnaire de files d'attente, la règle de validation de certificat peut être définie comme suit:

- Utilisation de l'attribut de gestionnaire de files d'attente *CERTVPOL*. Pour plus d'informations sur la définition de cet attribut, voir ALTER QMGR .

Sur le client, plusieurs méthodes peuvent être utilisées pour définir la règle de validation de certificat. Si plusieurs méthodes sont utilisées pour définir la règle, le client utilise les paramètres dans l'ordre de priorité suivant:

1. Utilisation de la zone *CertificateValPolicy* dans la structure MQSCO du client. Pour plus d'informations sur l'utilisation de cette zone, voir MQSCO-Options de configuration SSL.
2. Utilisation de la variable d'environnement client *MQCERTVPOL*. Pour plus d'informations sur l'utilisation de cette variable, voir MQCERTVPOL .
3. Utilisation de la valeur du paramètre d'optimisation de la section SSL du client, *CertificateValPolicy*. Pour plus d'informations sur l'utilisation de ce paramètre, voir Strophe SSL du fichier de configuration du client .

Pour plus d'informations sur les règles de validation de certificat, voir «Règles de validation de certificat dans IBM WebSphere MQ», à la page 35.

Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ
Cette rubrique fournit des informations sur la façon de choisir les CipherSpecs et les certificats numériques appropriés pour votre règle de sécurité, en soulignant la relation entre les CipherSpecs et les certificats numériques dans IBM WebSphere MQ.

Dans les éditions précédentes de IBM WebSphere MQ, tous les CipherSpecs SSL et TLS pris en charge utilisaient l'algorithme RSA pour les signatures numériques et l'accord de clé. Tous les types de certificat numérique pris en charge étant compatibles avec tous les CipherSpecspris en charge, il a été possible de modifier le CipherSpec pour n'importe quel canal sans avoir à modifier les certificats numériques.

Dans IBM WebSphere MQ v7.5 , seul un sous-ensemble des CipherSpecs pris en charge peut être utilisé avec tous les types de certificat numérique pris en charge. Il est donc nécessaire de choisir un CipherSpec approprié pour votre certificat numérique. De même, si la stratégie de sécurité de votre organisation requiert que vous utilisiez un CipherSpec particulier, vous devez obtenir un certificat numérique approprié pour ce CipherSpec.

L'algorithme de signature numérique MD5 et TLS 1.2

Les certificats numériques signés à l'aide de l'algorithme MD5 sont rejetés lorsque le protocole TLS 1.2 est utilisé. En effet, l'algorithme MD5 est désormais considéré comme faible par de nombreux analystes cryptographiques et son utilisation est généralement déconseillée. Si vous souhaitez utiliser des CipherSpecs plus récents basés sur le protocole TLS 1.2 , assurez-vous que les certificats numériques n'utilisent pas l'algorithme MD5 dans leurs signatures numériques. Les CipherSpecs plus anciens qui utilisent les protocoles SSL 3.0 et TLS 1.0 ne sont pas soumis à cette restriction et peuvent continuer à utiliser des certificats avec des signatures numériques MD5 .

Pour afficher l'algorithme de signature numérique d'un certificat particulier, vous pouvez utiliser la commande **runmqakm** :

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

où `cert_label` est le libellé de certificat de l'algorithme de signature numérique que vous devez afficher.

Remarque : Bien que l'outil **iKeycmd (runmqckm)** et l'interface graphique **iKeyman (strmqikm)** puissent être utilisés pour afficher une sélection d'algorithmes de signature numérique, l'outil **runmqakm** offre une plage plus large.

L'exécution de la commande **runmqakm** génère une sortie affichant l'utilisation de l'algorithme de signature spécifié:

```
Label : ibmwebspheremqexample
Key Size : 1024
Version : X509 V3
Serial : 4e4e93f1
Issuer : CN=Old Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : August 19, 2011 5:48:49 PM GMT+01:00
Not After : August 18, 2012 5:48:49 PM GMT+01:00
Public Key
    30 81 9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
    05 00 03 81 8D 00 30 81 89 02 81 81 00 98 5A 7A
    F0 18 21 EE E4 8A 6E DE C8 01 4B 3A 1E 41 90 3D
```

```
    CE 01 3F E6 32 30 6C 23 59 F0 FE 78 6D C2 80 EF
    BC 83 54 7A EB 60 80 62 6B F1 52 FE 51 9D C1 61
    80 A5 1C D4 F0 76 C7 15 6D 1F 0D 4D 31 3E DC C6
    A9 20 84 6E 14 A1 46 7D 4C F5 79 4D 37 54 0A 3B
    A9 74 ED E7 8B 0F 80 31 63 1A 0B 20 A5 99 EE 0A
    30 A6 B6 8F 03 97 F6 99 DB 6A 58 89 7F 27 34 DE
    55 08 29 D8 A9 6B 46 E6 02 17 C3 13 D3 02 03 01
    00 01
Public Key Type : RSA (1.2.840.113549.1.1.1)
Fingerprint : SHA1 :
    09 4E 4F F2 1B CB C1 F4 4F 15 C9 2A F7 32 0A 82
    DA 45 92 9F
Fingerprint : MD5 :
    44 54 81 7C 58 68 08 3A 5D 75 96 40 D5 8C 7A CB
Fingerprint : SHA256 :
    3B 47 C6 E7 7B B0 FF 85 34 E7 48 BE 11 F2 D4 35
    B7 9A 79 53 2B 07 F5 E7 65 E8 F7 84 E0 2E 82 55
Signature Algorithm : MD5WithRSASignature (1.2.840.113549.1.1.4)
Value
    3B B9 56 E6 F2 77 94 69 5B 3F 17 EA 7B 19 D0 A2
    D7 10 38 F1 88 A4 44 1B 92 35 6F 3B ED 99 9B 3A
    A5 A4 FC 72 25 5A A9 E3 B1 96 88 FC 1E 9F 9B F1
    C5 E8 8E CF C4 8F 48 7B 0E A6 BB 13 AE 2B BD D8
    63 2C 03 38 EF DC 01 E1 1F 7A 6F FB 2F 65 74 D0
    FD 99 94 BA B2 3A D5 B4 89 6C C1 2B 43 6D E2 39
    66 6A 65 CB C3 C4 E2 CC F5 49 39 A3 8B 93 5A DD
    B0 21 0B A8 B2 59 5B 24 59 50 44 89 DC 78 19 51
Trust Status : Enabled
```

La ligne `Signature Algorithm` indique que l'algorithme `MD5WithRSASignature` est utilisé. Cet algorithme étant basé sur MD5 , ce certificat numérique ne peut pas être utilisé avec les CipherSpecsTLS 1.2 .

Interopérabilité de Elliptic Curve et de RSA CipherSpecs

Les CipherSpecs ne peuvent pas tous être utilisés avec tous les certificats numériques. Il existe trois types de CipherSpec, désignés par le préfixe de nom CipherSpec . Chaque type de CipherSpec impose des restrictions différentes sur le type de certificat numérique qui peut être utilisé. Ces restrictions s'appliquent à toutes les connexions SSL et TLS de WebSphere MQ , mais sont particulièrement pertinentes pour les utilisateurs de la cryptographie Elliptic Curve.

Les relations entre les CipherSpecs et les certificats numériques sont récapitulées dans le tableau suivant:

Tableau 2. Relations entre les CipherSpecs et les certificats numériques

Tapez	CipherSpec Préfixe de nom	Description	Type de clé publique requis	Algorithme de chiffrement de signature numérique	Méthode d'établissement de clé secrète
1	ECDHE_ECDSA_	CipherSpecs qui utilisent des clés publiques Elliptic Curve, des clés secrètes Elliptic Curve et des algorithmes de signature numérique Elliptic Curve.	Elliptic Curve	ECDSA	ECDHE

Tableau 2. Relations entre les CipherSpecs et les certificats numériques (suite)

Tapez	CipherSpec Préfixe de nom	Description	Type de clé publique requis	Algorithme de chiffrement de signature numérique	Méthode d'établissement de clé secrète
2	ECDHE_RSA_	CipherSpecs qui utilisent des clés publiques RSA, des clés secrètes Elliptic Curve et des algorithmes de signature numérique Elliptic Curve.	RSA	RSA	ECDHE
3	(Tous les autres)	CipherSpecs qui utilisent des clés publiques RSA et des algorithmes de signature numérique RSA.	RSA	RSA	RSA

Remarque : Les CipherSpecs de type 1 et 2 sont uniquement pris en charge par les gestionnaires de files d'attente WebSphere MQ et les clients MQI sur les plateformes UNIX, Linux, and Windows .

La colonne de type de clé publique obligatoire indique le type de clé publique que le certificat personnel doit posséder lors de l'utilisation de chaque type de CipherSpec. Le certificat personnel est le certificat d'entité finale qui identifie le gestionnaire de files d'attente ou le client auprès de son partenaire distant.

L'algorithme de chiffrement de signature numérique fait référence à l'algorithme de chiffrement utilisé pour valider l'homologue. L'algorithme de chiffrement est utilisé avec un algorithme de hachage tel que MD5, SHA-1 ou SHA-256 pour calculer la signature numérique. Il existe différents algorithmes de signature numérique qui peuvent être utilisés, par exemple "RSA avec MD5" ou "ECDSA avec SHA-256". Dans le tableau, ECDSA fait référence à l'ensemble des algorithmes de signature numérique qui utilisent ECDSA ; RSA fait référence à l'ensemble des algorithmes de signature numérique qui utilisent RSA. Tout algorithme de signature numérique pris en charge dans l'ensemble peut être utilisé, à condition qu'il soit basé sur l'algorithme de chiffrement indiqué.

Les CipherSpecs de type 1 requièrent que le certificat personnel ait une clé publique Elliptic Curve. Lorsque ces CipherSpecs sont utilisés, l'accord de clé éphémère Elliptic Curve Diffie Hellman est utilisé pour établir la clé secrète pour la connexion.

Les CipherSpecs de type 2 requièrent que le certificat personnel ait une clé publique RSA. Lorsque ces CipherSpecs sont utilisés, l'accord de clé éphémère Elliptic Curve Diffie Hellman est utilisé pour établir la clé secrète pour la connexion.

Le type 3 CipherSpecs requiert que le certificat personnel ait une clé publique RSA. Lorsque ces CipherSpecs sont utilisés, l'échange de clés RSA est utilisé pour établir la clé secrète pour la connexion.

Cette liste de restrictions n'est pas exhaustive: selon la configuration, il peut y avoir des restrictions supplémentaires qui peuvent affecter davantage la possibilité d'interopérer. Par exemple, si WebSphere MQ est configuré pour être conforme aux normes FIPS 140-2 ou NSA Suite B, cela limite également la plage de configurations autorisées. Pour plus d'informations, reportez-vous à la section suivante.

Un gestionnaire de files d'attente WebSphere MQ ne peut utiliser qu'un seul certificat personnel pour s'identifier. Cela signifie que tous les canaux du gestionnaire de files d'attente utiliseront le même certificat numérique. Par conséquent, chaque gestionnaire de files d'attente ne peut utiliser qu'un seul

type de CipherSpec à la fois. De même, une application client WebSphere MQ ne peut utiliser qu'un seul certificat personnel pour s'identifier. Cela signifie que toutes les connexions SSL et TLS au sein d'un même processus d'application utiliseront le même certificat numérique et que, par conséquent, chaque processus d'application client ne pourra utiliser qu'un seul type de CipherSpec à la fois.

Les trois types de CipherSpec n'interagissent pas directement: il s'agit d'une limitation des normes SSL et TLS en cours. Par exemple, supposons que vous ayez choisi d'utiliser le CipherSpec ECDHE_ECDSA_AES_128_CBC_SHA256 pour un canal récepteur nommé TO.QM1 sur un gestionnaire de files d'attente nommé QM1. ECDHE_ECDSA_AES_128_CBC_SHA256 est un CipherSpecde type 1. Par conséquent, QM1 doit avoir un certificat personnel avec une clé Elliptic Curve et une signature numérique basée sur ECDSA. Tous les clients et les autres gestionnaires de files d'attente qui communiquent directement avec QM1 doivent donc disposer de certificats numériques qui répondent aux exigences CipherSpec de type 1. D'autres canaux se connectant au gestionnaire de files d'attente QM1 peuvent utiliser d'autres CipherSpecs (par exemple, ECDHE_ECDSA_3DES_EDE_CBC_SHA256), mais ils ne peuvent utiliser que des CipherSpecs de type 1 pour communiquer avec QM1.

Lors de la planification de vos réseaux WebSphere MQ , déterminez avec attention les canaux qui requièrent SSL ou TLS et assurez-vous que tous les clients et gestionnaires de files d'attente qui doivent interagir utilisent le même type de CipherSpecs et les certificats numériques appropriés. Les normes IETF RFC 4492, RFC 5246 et RFC 6460 décrivent l'utilisation détaillée de la courbe Elliptic CipherSpecs dans TLS 1.2.

Pour afficher l'algorithme de signature numérique et le type de clé publique d'un certificat numérique, vous pouvez utiliser la commande **runmqakm** :

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

où `cert_label` est le libellé du certificat dont vous devez afficher l'algorithme de signature numérique.

L'exécution de la commande **runmqakm** génère une sortie affichant le type de clé publique:

```
Label : ibmwebspheremqexample
Key Size : 384
Version : X509 V3
Serial : 9ad5eeef5d756f41
Issuer : CN=Example Certificate Authority,OU=Test,O=Example,C=US
Subject : CN=Example Queue Manager,OU=Test,O=Example,C=US
Not Before : 21 August 2011 13:10:24 GMT+01:00
Not After : 21 August 2012 13:10:24 GMT+01:00
Public Key
    30 76 30 10 06 07 2A 86 48 CE 3D 02 01 06 05 2B
    81 04 00 22 03 62 00 04 3E 6F A9 06 B6 C3 A0 11
    F8 D6 22 78 FE EF 0A FE 34 52 C0 8E AB 5E 81 73
    D0 97 3B AB D6 80 08 E7 31 E9 18 3F 6B DE 06 A7
    15 D6 9D 5B 6F 56 3B 7F 72 BB 6F 1E C9 45 1C 46
    60 BE F2 DC 1B AD AC EC 64 4C 0E 06 65 6E ED 93
    B8 F5 95 E0 F9 2A 05 D6 21 02 BD FB 06 63 A1 CC
    66 C6 8A 0A 5C 3F F7 D3
Public Key Type : EC_ecPublicKey (1.2.840.10045.2.1)
Fingerprint : SHA1 :
    3C 34 58 04 5B 63 5F 5C C9 7A E7 67 08 2B 84 43
    3D 43 7A 79
Fingerprint : MD5 :
    49 13 13 E1 B2 AC 18 9A 31 41 DC 8C B4 D6 06 68
Fingerprint : SHA256 :
    6F 76 78 68 F3 70 F1 53 CE 39 31 D9 05 C5 C5 9F
    F2 B8 EE 21 49 16 1D 90 64 6D AC EB 0C A7 74 17
Signature Algorithm : EC_ecdsa_with_SHA384 (1.2.840.10045.4.3.3)
Value
    30 65 02 30 0A B0 2F 72 39 9E 24 5A 22 FE AC 95
    0D 0C 6D 6C 2F B3 E7 81 F6 C1 36 1B 9A B0 6F 07
    59 2A A1 4C 02 13 7E DD 06 D6 FE 4B E4 03 BC B1
    AC 49 54 1E 02 31 00 90 0E 46 2B 04 37 EE 2C 5F
    1B 9C 69 E5 99 60 84 84 10 71 1A DA 63 88 33 E2
    22 CC E6 1A 4E F4 61 CC 51 F9 EE A0 8E F4 DC B5
    0B B9 72 58 C3 C7 A4
Trust Status : Enabled
```

Dans ce cas, la ligne Type de clé publique indique que le certificat possède une clé publique Elliptic Curve. Dans ce cas, la ligne Algorithme de signature indique que l'algorithme EC_ecdsa_with_SHA384 est en

cours d'utilisation: il est basé sur l'algorithme ECDSA. Par conséquent, ce certificat ne peut être utilisé qu'avec des CipherSpecsde type 1.

Vous pouvez également utiliser l'outil **iKeycmd (runmqckm)** avec les mêmes paramètres. Vous pouvez également utiliser l'interface graphique de **iKeyman (strmqikm)** pour afficher les algorithmes de signature numérique si vous ouvrez le référentiel de clés et cliquez deux fois sur le libellé du certificat. Toutefois, il est conseillé d'utiliser l'outil **runmqakm** pour afficher les certificats numériques car il prend en charge un plus large éventail d'algorithmes.

Elliptic Curve CipherSpecs et NSA Suite B

Lorsque WebSphere MQ est configuré pour se conformer au profil TLS 1.2 compatible Suite B, les CipherSpecs et les algorithmes de signature numérique autorisés sont restreints comme décrit dans «NSA Suite B Cryptography dans IBM WebSphere MQ», à la page 32. De plus, la plage de clés Elliptic Curve acceptables est réduite en fonction des niveaux de sécurité configurés.

Au niveau de la sécurité Suite B 128 bits, la clé publique du sujet de certificat est requise pour utiliser la courbe elliptique NIST P-256 ou NIST P-384 et pour être signée avec la courbe elliptique NIST P-256 ou la courbe elliptique NIST P-384 . La commande **runmqakm** peut être utilisée pour demander des certificats numériques pour ce niveau de sécurité à l'aide d'un paramètre -sig_alg de EC_ecdsa_with_SHA256ou de EC_ecdsa_with_SHA384.

Au niveau de la sécurité de la suite B 192 bits, la clé publique du sujet de certificat est requise pour utiliser la courbe elliptique NIST P-384 et pour être signée avec la courbe elliptique NIST P-384 . La commande **runmqakm** peut être utilisée pour demander des certificats numériques pour ce niveau de sécurité à l'aide d'un paramètre -sig_alg de EC_ecdsa_with_SHA384.

Les courbes elliptiques NIST prises en charge sont les suivantes:

Tableau 3. Courbes elliptiques NIST prises en charge

Nom de courbe NIST FIPS 186-3	Nom de courbe RFC 4492	Taille de clé de courbe elliptique (bits)
P-256	secp256r1	256
P-384	secp384r1	384
P-521	secp521r1	521

Remarque : La courbe elliptique P-521 du NIST ne peut pas être utilisée pour une opération conforme à la suite B.

Concepts associés

«Définition des spécifications CipherSpec», à la page 227
Spécifiez un CipherSpec à l'aide du paramètre **SSLCIPH** dans la commande **DEFINE CHANNEL** MQSC ou dans la commande **ALTER CHANNEL** MQSC.

«Comment indiquer que seuls les CipherSpecs certifiés FIPS sont utilisés lors de l'exécution sur MQI Client», à la page 113
Créez vos référentiels de clés à l'aide d'un logiciel compatible FIPS, puis indiquez que le canal doit utiliser des CipherSpecscertifiés FIPS.

«NSA Suite B Cryptography dans IBM WebSphere MQ», à la page 32
Cette rubrique explique comment configurer IBM WebSphere MQ sur les systèmes Windows, Linuxet UNIX pour qu'il soit conforme au profil TLS 1.2 conforme à la norme Suite B.

«Agence de sécurité nationale (NSA) Suite B Cryptographie», à la page 21
Le gouvernement des États-Unis d'Amérique fournit des conseils techniques sur les systèmes informatiques et la sécurité, y compris le chiffrement des données. La National Security Agency (NSA) des États-Unis recommande un ensemble d'algorithmes cryptographiques interopérables dans sa norme Suite B.

CipherSpec valeurs prises en charge dans IBM WebSphere MQ

L'ensemble de CipherSpecs par défaut autorise uniquement les valeurs suivantes:

TLS 1.0

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

TLS 1.2

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

Activation des CipherSpecs obsolètes

Par défaut, vous n'êtes pas autorisé à spécifier un CipherSpec obsolète dans une définition de canal. Si vous tentez de spécifier un CipherSpecobsolète, vous recevez le message AMQ9788 dans le journal des erreurs du gestionnaire de files d'attente.

Il est possible de réactiver les CipherSpecs obsolètes en éditant le fichier `qm.ini` . Dans la section SSL du fichier `qm.ini` , ajoutez la ligne suivante:

```
SSL:
AllowWeakCipherSpec=Yes
```

Vous pouvez également réactiver une ou plusieurs des CipherSpecs obsolètes lors de l'exécution sur le serveur en définissant la variable d'environnement *AMQ_SSL_WEAK_CIPHER_ENABLE* sur n'importe quelle valeur. Cette variable d'environnement active les CipherSpecs quelle que soit la valeur spécifiée dans le fichier `qm.ini` .

Enregistrements d'authentification de canal

Pour exercer un contrôler plus précis sur les accès accordés aux systèmes en cours de connexion au niveau d'un canal, vous pouvez utiliser les enregistrements d'authentification de canal.

Vous découvrirez peut-être que des clients essaient de se connecter à votre gestionnaire de files d'attente à l'aide d'un ID utilisateur vide ou d'un ID utilisateur de niveau supérieur, permettant à un client de procéder à des actions indésirables. Vous pouvez bloquer l'accès à ces clients à l'aide d'enregistrements d'authentification de canal. Il est également possible qu'un client accepte un ID utilisateur valide sur la plateforme client, mais inconnu ou sous un format non valide sur la plateforme serveur. Vous pouvez utiliser un enregistrement d'authentification de canal pour associer l'ID utilisateur accepté à un ID utilisateur valide.

Vous pouvez trouver une application client qui se connecte à votre gestionnaire de files d'attente et adopte un comportement indésirable. Pour protéger le serveur des problèmes que cette application pourrait provoquer, il convient de bloquer temporairement l'utilisation de l'adresse IP sur laquelle se trouve l'application client, le temps de mettre à jour les règles du pare-feu ou de corriger l'application.

Vous pouvez utiliser un enregistrement d'authentification de canal pour bloquer l'adresse IP à partir de laquelle l'application client se connecte.

Si vous avez défini un outil d'administration tel qu'IBM WebSphere MQ Explorer et un canal pour cette utilisation particulière, il est conseillé de limiter son utilisation à des ordinateurs client spécifiques. Vous pouvez utiliser un enregistrement d'authentification de canal pour permettre l'utilisation de ce canal uniquement à partir de certaines adresses IP.

Si vous venez de commencer avec des exemples d'applications s'exécutant en tant que clients, voir Préparation et exécution des exemples de programmes pour un exemple de configuration du gestionnaire de files d'attente en toute sécurité à l'aide d'enregistrements d'authentification de canal.

Pour obtenir des enregistrements d'authentification de canal afin de contrôler les canaux de communications entrantes, utilisez la commande MQSC **ALTER QMGR CHLAUTH(ENABLED)**.

Des règles **CHLAUTH** sont appliquées à un agent MCA de canal qui est créé en réponse à une nouvelle connexion entrante. Pour un agent MCA de canal créé en réponse au démarrage du canal en local, aucune règle **CHLAUTH** n'est appliquée.

Tableau 4. Emplacement de l'application des règles CHLAUTH dans différentes paires de canaux

Type de canal	**Agent MCA sur lequel les règles CHLAUTH sont appliquées**
Emetteur-récepteur	RCVR
Demandeur-serveur (démarré sur le serveur)	RQSTR
Demandeur-serveur (démarré sur le demandeur)	SVR
Demandeur-émetteur (démarré sur l'émetteur)	RQSTR
Demandeur-émetteur (démarré sur le demandeur)	Emetteur pour la connexion initiale. Demandeur pour la connexion de rappel.

Les enregistrements d'authentification de canal peuvent être créés pour l'exécution des fonctions suivantes :

- Bloquer les connexion en provenance d'adresses IP spécifiques.
- Bloquer les connexions associées à des ID utilisateur spécifiques.
- Définir une valeur MCAUSER à utiliser pour n'importe quel canal se connectant à partir d'une adresse IP spécifique.
- Définir une valeur MCAUSER à utiliser pour n'importe quel canal acceptant un ID utilisateur spécifique.
- Définir une valeur MCAUSER à utiliser pour n'importe quel canal associé à une adresse SSL ou un nom distinctif TLS spécifique.
- Définir une valeur MCAUSER à utiliser pour n'importe quel canal se connectant à partir d'un gestionnaire de files d'attente spécifique.
- Bloquer les connexions qui prétendent provenir d'un certain gestionnaire de files d'attente sauf si la connexion provient d'une adresse IP spécifique.
- Bloquer les connexions présentant un certain certificat SSL ou TLS, sauf si la connexion provient d'une adresse IP spécifique.

Ces utilisations sont expliquées plus en détails dans les sections suivantes.

Vous pouvez créer, modifier ou supprimer des enregistrements d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH** ou de la commande PCF **Set Channel Authentication Record**.

Remarque : Un grand nombre d'enregistrements d'authentification de canal peut avoir un impact négatif sur les performances d'un gestionnaire de files d'attente.

Blocage d'adresses IP

C'est normalement le rôle d'un pare-feu que de prévenir l'accès provenant de certaines adresses IP. Toutefois, il peut arriver que vous constatiez des tentatives de connexion provenant d'une adresse IP qui ne devrait pas avoir accès à votre système WebSphere MQ et que vous deviez temporairement bloquer l'adresse avant que le pare-feu ne puisse être mis à jour. Ces tentatives de connexion peuvent ne pas provenir des canaux WebSphere MQ , mais d'autres applications de socket mal configurées pour cibler votre programme d'écoute WebSphere MQ . Bloquez les adresses IP en définissant un enregistrement d'authentification de canal de type BLOCKADDR. Vous pouvez spécifier une ou plusieurs adresses, ou des modèles avec des caractères génériques.

Lorsqu'une connexion entrante est refusée en raison d'un blocage de l'adresse IP de cette manière, un message d'événement MQRC_CHANNEL_BLOCKED avec un qualificateur de code anomalie MQRQ_CHANNEL_BLOCKED_ADDRESS généré, à condition que les événements du canal soient activés et que le gestionnaire de files d'attente soit en cours d'exécution. En outre, la connexion reste ouverte pendant 30 secondes avant de renvoyer l'erreur afin de garantir que le programme d'écoute n'est pas saturé par les tentatives de connexion répétées qui sont bloquées.

Pour bloquer des adresses IP uniquement sur des canaux spécifiques ou pour éviter le délai avant le signalement de l'erreur, définissez un enregistrement d'authentification de canal de type ADDRESSMAP avec le paramètre USERSRC(NOACCESS).

Lorsqu'une connexion entrante est refusée pour cette raison, un message d'événement MQRC_CHANNEL_BLOCKED avec le qualificateur de code anomalie MQRQ_CHANNEL_BLOCKED_NOACCESS est généré, à condition que les événements du canal soient activés et que le gestionnaire de files d'attente soit en cours d'exécution.

Pour voir un exemple, consultez «Blocage d'adresses IP spécifiques», à la page 190.

Blocage d'ID utilisateur

Pour empêcher certains ID utilisateur de se connecter sur un canal client, définissez un enregistrement d'authentification du canal de type BLOCKUSER. Ce type d'enregistrement s'applique uniquement aux canaux client disponibles et non aux canaux de message. Vous avez la possibilité d'indiquer un ou plusieurs ID utilisateur individuels, mais pas d'utiliser de caractères génériques.

Chaque fois qu'une connexion entrante est refusée pour cette raison, un message d'événement MQRC_CHANNEL_BLOCKED avec un qualificateur de code anomalie MQRQ_CHANNEL_BLOCKED_USERID est généré, à condition que les événements du canal soient activés.

Pour voir un exemple, consultez «Blocage d'ID utilisateur spécifiques», à la page 192.

Vous pouvez également bloquer l'accès d'un ID utilisateur quelconque sur certains canaux en définissant un enregistrement d'authentification du canal de type USERMAP avec le paramètre USERSRC(NOACCESS).

Lorsqu'une connexion entrante est refusée pour cette raison, un message d'événement MQRC_CHANNEL_BLOCKED avec le qualificateur de code anomalie MQRQ_CHANNEL_BLOCKED_NOACCESS est généré, à condition que les événements du canal soient activés et que le gestionnaire de files d'attente soit en cours d'exécution.

Pour voir un exemple, consultez «Blocage de l'accès pour un ID utilisateur vérifié par le client», à la page 195.

Blocage de gestionnaires de files d'attente

Pour bloquer l'accès à un canal se connectant à partir d'un gestionnaire de files d'attente spécifique, définissez un enregistrement d'authentification de canal de type QMGRMAP avec le paramètre USERSRC(NOACCESS). Vous pouvez indiquer un nom de gestionnaire de files d'attente ou un modèle comportant des caractères génériques. La fonction BLOCKUSER permettant de bloquer l'accès d'un gestionnaire de files d'attente ne comporte pas d'équivalent.

Lorsqu'une connexion entrante est refusée pour cette raison, un message d'événement MQRC_CHANNEL_BLOCKED avec le qualificateur de code anomalie

MQRQ_CHANNEL_BLOCKED_NOACCESS est généré, à condition que les événements du canal soient activés et que le gestionnaire de files d'attente soit en cours d'exécution.

Pour voir un exemple, consultez «Blocage de l'accès à partir d'un gestionnaire de files d'attente éloignées», à la page 194.

Blocage des noms distinctifs SSL ou TLS

Pour bloquer l'accès à un utilisateur présentant un certificat personnel SSL ou TLS doté d'un nom distinctif spécifique, définissez un enregistrement d'authentification de canal de type SSLPEERMAP avec le paramètre USERSRC(NOACCESS). Vous pouvez indiquer un nom distinctif unique ou un modèle comportant des caractères génériques. La fonction BLOCKUSER permettant de bloquer l'accès aux noms distinctifs ne comporte pas d'équivalent.

Lorsqu'une connexion entrante est refusée pour cette raison, un message d'événement MQRC_CHANNEL_BLOCKED avec le qualificateur de code anomalie MQRQ_CHANNEL_BLOCKED_NOACCESS est généré, à condition que les événements du canal soient activés et que le gestionnaire de files d'attente soit en cours d'exécution.

Pour voir un exemple, consultez «Blocage de l'accès pour un nom distinctif SSL», à la page 195.

Mappage d'adresses IP vers les ID utilisateur requis

Pour indiquer qu'un canal se connectant à partir d'une adresse IP spécifique doit utiliser une valeur MCAUSER spécifique, définissez un enregistrement d'authentification de canal de type ADDRESSMAP. Vous pouvez indiquer une adresse unique, une plage d'adresses ou un modèle comportant des caractères génériques.

Si vous utilisez un réexpéditeur de port, une rupture de session DMZ ou toute autre configuration modifiant l'adresse IP présentée au gestionnaire de files d'attente, le mappage des adresses IP ne convient pas forcément à votre situation.

Pour voir un exemple, consultez «Mappage d'une adresse IP à un ID utilisateur MCAUSER», à la page 196.

Mappage de gestionnaires de files d'attente vers les ID utilisateur requis

Pour indiquer qu'un canal se connectant à partir d'un gestionnaire de files d'attente spécifique doit utiliser une valeur MCAUSER spécifique, définissez un enregistrement d'authentification de canal de type QMGRMAP. Vous pouvez indiquer un nom de gestionnaire de files d'attente ou un modèle comportant des caractères génériques.

Pour voir un exemple, consultez «Mappage d'un gestionnaire de files d'attente éloignées à un ID utilisateur MCAUSER», à la page 193.

Mappage des ID utilisateur vérifiés par un client vers les ID utilisateur requis

Pour indiquer qu'un ID utilisateur se connectant à partir d'un client WebSphere MQ MQI spécifique doit utiliser une valeur MCAUSER différente, définissez un enregistrement d'authentification de canal de type USERMAP. Le mappage d'ID utilisateur ne se sert pas de caractères génériques.

Pour voir un exemple, consultez «Mappage d'un ID utilisateur vérifié par le client à un ID utilisateur MCAUSER», à la page 193.

Mappage des noms distinctifs SSL ou TLS vers les ID utilisateur requis

Pour indiquer qu'un utilisateur présentant un certificat personnel SSL/TLS doté d'un nom distinctif doit utiliser une valeur MCAUSER spécifique, définissez un enregistrement d'authentification de canal de type SSLPEERMAP. Vous pouvez indiquer un nom distinctif unique ou un modèle comportant des caractères génériques.

Pour voir un exemple, consultez «Mappage d'un nom distinctif SSL ou TLS à un ID utilisateur MCAUSER», à la page 194.

Mappage de gestionnaires de files d'attente, de clients ou de noms distinctifs SSL ou TLS en fonction d'une adresse IP

Dans certains, il est possible qu'une tierce partie falsifie le nom d'un gestionnaire de files d'attente. Un certificat SSL ou TLS ou un fichier de clés peut également être volé et réutilisé. Pour vous protéger contre ces menaces, vous pouvez indiquer qu'une connexion provenant d'un certain gestionnaire de files d'attente ou client ou utilisant un certain nom distinctif doit être établie à partir d'une adresse IP spécifique. Définissez un enregistrement d'authentification de canal de type USERMAP, QMGRMAP ou SSLPEERMAP et spécifiez l'adresse IP ou le modèle d'adresse autorisé à l'aide du paramètre ADDRESS.

Pour voir un exemple, consultez «Mappage d'un gestionnaire de files d'attente éloignées à un ID utilisateur MCAUSER», à la page 193.

Interaction entre les enregistrements d'authentification de canal

Il se peut qu'un canal tentant de se connecter corresponde à plusieurs enregistrements d'authentification de canaux et que leurs effets soient contradictoires. Par exemple, un canal peut vérifier un ID utilisateur qui soit bloqué par un enregistrement BLOCKUSER, mais qui comporte un certificat SSL ou TLS correspondant à un enregistrement SSLPEERMAP qui définisse un ID utilisateur différent. De plus, si les enregistrements utilisent des caractères génériques, il se peut qu'une adresse IP unique, un gestionnaire de files d'attente ou un nom distinctif SSL ou TLS corresponde à plusieurs modèles. Par exemple, l'adresse IP 192.0.2.6 correspond aux modèles 192.0.2.0-24, 192.0.2. *, et 192.0. * 6. L'action prise varie en fonction des éléments ci-dessous.

- L'enregistrement d'authentification de canal est sélectionné de la manière suivante :
  - Un enregistrement d'authentification de canal correspondant de manière explicite au nom du canal est prioritaire sur un enregistrement dont le canal comporte des caractères génériques.
  - Un enregistrement d'authentification de canal portant un nom distinctif SSL ou TLS est prioritaire sur un enregistrement associé à un ID utilisateur, un gestionnaire de files d'attente ou une adresse IP.
  - Un enregistrement d'authentification de canal associé à un ID utilisateur ou un gestionnaire de files d'attente est prioritaire sur un enregistrement faisant appel à une adresse IP.
- Si un enregistrement d'authentification de canal équivalent est détecté et qu'il indique une valeur MCAUSER, cette dernière est affectée au canal.
- Si un enregistrement d'authentification de canal équivalent est détecté et qu'il indique que le canal ne dispose d'aucun droit d'accès, une valeur MCAUSER de type *NOACCESS est affectée au canal. Cette valeur peut ensuite être modifiée par un programme exit de sécurité.
- Si aucun enregistrement d'authentification équivalent n'est détecté, ou si un enregistrement équivalent est détecté et qu'il indique que l'ID utilisateur du canal doit être utilisé, la zone MCAUSER est examinée.
  - Si la zone MCAUSER est vide, l'ID utilisateur client est affecté au canal.
  - Si la zone MCAUSER n'est pas vide, sa valeur est affectée au canal.
- Un programme exit de sécurité est exécuté. Ce programme peut définir l'ID utilisateur du canal ou déterminer si l'accès doit être bloqué.
- Si la connexion est bloquée ou si la valeur MCAUSER est définie sur *NOACCESS, le canal s'arrête.
- Si la connexion n'est pas bloquée, l'ID utilisateur du canal défini à l'étape précédente est vérifié par rapport à la liste des utilisateurs bloqués et ce, pour tous les canaux à l'exception d'un canal client.
  - Si l'ID utilisateur figure dans la liste des utilisateurs bloqués, le canal s'arrête.
  - Si l'ID utilisateur ne figure pas dans la liste des utilisateurs bloqués, le canal s'exécute.

Lorsqu'un certain nombre d'enregistrements d'authentification des canaux correspondent à un nom de canal, une adresse IP, un nom de gestionnaire de files d'attente ou un nom distinctif SSL ou TLS, la correspondance la plus spécifique est utilisée. La correspondance la plus spécifique est définie en fonction des éléments ci-dessous.

- Pour un nom de canal :
  - La correspondance la plus spécifique est un nom sans caractère générique, par exemple, A.B.C.

- La correspondance la plus générale est un astérisque (*) unique, qui correspond à tous les noms de canaux.
- Un modèle comportant un astérisque dans la première partie est plus générique qu'un modèle comportant une valeur définie dans la première partie. Ainsi, *.B.C est plus générique que A.*.
- Un modèle comportant un astérisque dans la deuxième partie est plus générique qu'un modèle comportant une valeur définie dans la deuxième partie, et ainsi de suite pour chaque position suivante. Ainsi, A.*.C est plus générique que A.B.*
- Lorsque plusieurs modèles comportent un astérisque au même endroit, celui incluant le moins de noeuds à la suite de l'astérisque est plus générique. Par conséquent, A. * est plus générique que A.*.C

• Pour une adresse IP :
- La correspondance la plus spécifique est un nom sans caractère générique, par exemple, 192.0.2.6.
- La correspondance la plus générale est un astérisque (*) unique, qui correspond à tous les noms de canaux.
- Un modèle comportant un astérisque dans la première partie est plus générique qu'un modèle comportant une valeur définie dans la première partie. Ainsi, *.0.2.6 est plus générique que 192.*.
- Un modèle comportant un astérisque dans la deuxième partie est plus générique qu'un modèle comportant une valeur définie dans la deuxième partie, et ainsi de suite pour chaque position suivante. Ainsi, 192.*.2.6 est plus générique que 192.0.*.
- Lorsque plusieurs modèles comportent un astérisque au même endroit, celui incluant le moins de noeuds à la suite de l'astérisque est plus générique. Ainsi 192 .* est plus générique que 192.*.2.*.
- Une plage signalée par un trait d'union (-) est plus spécifique qu'un astérisque. Ainsi, 192.0.2.0-24 est plus spécifique que 192.0.2.*.
- Une plage représentant un sous-ensemble d'une autre plage est plus spécifique que la plage la plus grande. Ainsi, 192.0.2.5-15 est plus spécifique que 192.0.2.0-24.
- Les plages qui se chevauchent ne sont pas autorisées. Par exemple, vous ne pouvez pas avoir d'enregistrements d'authentification de canaux pour 192.0.2.0-15 et 192.0.2.10-20.
- Un modèle ne peut pas contenir moins d'éléments que ce qui est obligatoire, sauf si le modèle se termine par une astérisque. Par exemple 192.0.2 n'est pas valide, mais 192.0.2.* est valide.
- Un astérisque de fin doit être séparé du reste de l'adresse par le séparateur d'élément approprié (un point (.) pour IPv4, un deux-points (:) pour IPv6). Par exemple, 192.0* n'est pas valide parce que l'astérisque n'est pas un élément en soi.
- Un modèle peut contenir des astérisques supplémentaires à condition qu'aucun astérisque ne soit adjacent à l'astérisque de fin. Par exemple, 192.*.2.* est valide, mais 192.0.*.* est incorrect.
- Un modèle d'adresse IPv6 ne peut pas contenir deux fois deux points et une astérisque de fin, car l'adresse serait très ambiguë. Par exemple, 2001::* pourrait devenir 2001:0000:*, 2001:0000:0000:* etc.

• Pour un nom de gestionnaire de files d'attente :
- La correspondance la plus spécifique est un nom sans caractère générique, par exemple, 192.0.2.6.
- La correspondance la plus générale est un astérisque (*) unique, qui correspond à tous les noms de canaux.
- Un modèle comportant un astérisque dans la première partie est plus générique qu'un modèle comportant une valeur définie dans la première partie. Ainsi, *QUEUEMANAGER est plus spécifique que QUEUEMANAGER*.
- Un modèle comportant un astérisque dans la deuxième partie est plus générique qu'un modèle comportant une valeur définie dans la deuxième partie, et ainsi de suite pour chaque position suivante. Ainsi, Q*MANAGER est plus générique que QUEUE*.
- Lorsque plusieurs modèles comportent un astérisque au même endroit, celui qui contient le moins de caractères à la suite de l'astérisque est plus générique. Ainsi, Q* est plus générique que Q*MGR.

• Pour un nom distinctif SSL ou TLS, l'ordre de priorité des sous-chaînes est le suivant :

Tableau 5. Ordre de priorité des sous-chaînes

Commande	Sous-chaîne de nom distinctif	Nom
1	SERIALNUMBER=	Numéro de série du certificat
2	MAIL=	Adresse électronique
3	E=	Adresse électronique (dépréciée dans la préférence pour MAIL)
4	UID=, USERID=	Identificateur utilisateur
5	CN=	Nom usuel
6	T =	Titre
7	OU=	Unité organisationnelle
8	DC=	Composant de domaine
9	O=	Organisation
10	STREET=	Rue/Première ligne d'adresse
11	L=	Localité
12	ST=, SP=, S=	Nom de département
13	PC =	Code postal
14	C=	Pays
15	UNSTRUCTUREDNAME=	Nom d'hôte
16	UNSTRUCTUREDADDRESS=	Adresse IP
17	DNQ=	Qualificateur de nom distinctif

Par conséquent, si un certificat SSL ou TLS se présente avec un nom distinctif comportant les sous-chaînes O=IBM et C=UK, WebSphere MQ fait d'abord appel à l'enregistrement d'authentification de canal pour O=IBM avant de faire appel à l'enregistrement d'authentification de canal pour C=UK, lorsque les deux existent.

Un nom distinctif peut contenir plusieurs OU, qui doit être spécifiée dans un ordre hiérarchique, les unités organisationnelles les plus grandes spécifiées en premier. Si deux noms distinctifs sont équivalents en tous points sauf en ce qui concerne leurs valeurs d'unités organisationnelles, le nom distinctif le plus spécifique est déterminé comme suit :

1. S'ils ont des nombres d'attributs d'unités organisationnelles différents, le nom distinctif possédant le plus de valeurs d'unités organisationnelles est le plus spécifique. Cela vient du fait que le nom distinctif possédant le plus d'unités organisationnelles qualifie le nom distinctif plus en détails et apporte plus de critères de correspondance. Même si l'unité organisationnelle de niveau supérieure est un caractère générique (OU=*), le nom distinctif possédant le plus d'unités organisationnelles est toujours considéré comme le plus spécifique globalement.
2. S'ils ont le même nombre d'attributs d'unités organisationnelles, les paires de valeurs d'unités organisationnelles correspondantes sont comparées dans l'ordre de gauche à droite, celles de gauche étant celles de plus haut niveau (les moins spécifiques), selon les règles suivantes.
   a. Une unité organisationnelle sans valeur indiquée par des caractères génériques est la plus spécifique car elle ne peut correspondre qu'à une seule chaîne exacte.
   b. Une unité organisationnelle avec un seul caractère générique, que ce soit au début ou à la fin (par exemple OU=ABC* ou OU=*ABC) est la plus spécifique suivante.
   c. Une unité organisationnelle avec deux caractères génériques par exemple OU=*ABC*) est la plus spécifique qui suit.

d. Une unité organisationnelle constituée d'un seul astérisque (OU=*) est la moins spécifique.

3. Si la comparaison de chaîne est liée entre deux valeurs d'attributs de la même spécificité, alors la chaîne d'attribut la plus longue sera la plus spécifique.
4. Si la comparaison de chaîne est liée entre deux valeurs d'attributs de la même spécificité et de même longueur, le résultat est déterminé par une comparaison de chaîne ne respectant pas la casse de la portion de nom distinctif d'où sont exclus les caractères génériques.

Si deux DN sont égaux à tous égards, à l'exception de leurs valeurs de DC, les mêmes règles de correspondance s'appliquent que pour les OU, sauf que dans les valeurs de DC, la DC de gauche est le niveau le plus bas (le plus spécifique) et l'ordre de comparaison diffère en conséquence.

Affichage des enregistrements d'authentification de canaux

Pour afficher les enregistrements d'authentification de canal, utilisez la commande MQSC **DISPLAY CHLAUTH** ou la commande PCF **Inquire Channel Authentication Records**. Vous pouvez choisir de renvoyer tous les enregistrements qui correspondent au nom de canal fourni ou seulement ceux qui correspondent à un élément particulier. La correspondance explicite vous indique quel enregistrement d'authentification de canal est utilisé lorsqu'un canal tente d'établir une connexion à partir d'une adresse IP ou d'un gestionnaire de files d'attente spécifique, qu'il utilise un ID utilisateur spécifique et qu'il présente un certificat personnel SSL/TLS doté d'un nom distinctif, le cas échéant.

Concepts associés

«Sécurité de la messagerie distante», à la page 58
Cette section traite des aspects de la sécurité liés à la messagerie distante.

Sécurité des messages dans IBM WebSphere MQ

La sécurité des messages dans l'infrastructure IBM WebSphere MQ est fournie par un composant sous licence distincte IBM WebSphere MQ Advanced Message Security.

IBM WebSphere MQ Advanced Message Security (AMS) étend les services de sécurité IBM WebSphere MQ pour fournir la signature et le chiffrement des données au niveau des messages. Les services étendus garantissent que les données de message n'ont pas été modifiées entre le moment où elles sont placées à l'origine dans une file d'attente et le moment où elles sont extraites. En outre, AMS vérifie qu'un expéditeur de données de message est autorisé à placer des messages signés dans une file d'attente cible.

Concepts associés

«IBM WebSphere MQ Advanced Message Security», à la page 281
IBM WebSphere MQ Advanced Message Security (AMS) est un composant sous licence distincte de IBM WebSphere MQ Advanced Message Security qui offre un niveau de protection élevé pour les données sensibles transitant par le réseau IBM WebSphere MQ Advanced Message Security , sans affecter les applications finales.

Planification de la sécurité

Cette collection de rubriques explique ce que vous devez prendre en compte lors de la planification de la sécurité dans un environnement IBM WebSphere MQ .

Vous pouvez utiliser IBM WebSphere MQ pour une grande variété d'applications sur une large gamme de plateformes. Les exigences de sécurité sont susceptibles d'être différentes pour chaque application. Pour certains, la sécurité sera une considération cruciale.

WebSphere MQ fournit une gamme de services de sécurité de niveau liaison, y compris la prise en charge de Secure Sockets Layer (SSL) et de Transport Layer Security (TLS).

Vous devez prendre en compte certains aspects de la sécurité lors de l'implémentation de WebSphere. Sur les systèmes UNIX, Linux et Windows , si vous ignorez ces aspects et ne faites rien, vous ne pouvez pas utiliser WebSphere MQ.

Les considérations de sécurité sont décrites ci-après.

Droits d'administration de WebSphere MQ

Les administrateurs WebSphere MQ doivent disposer des droits suivants:

- Exécuter des commandes pour administrer WebSphere MQ
- Utiliser l'explorateur IBM WebSphere MQ

Pour plus d'informations, voir :

- «Droits d'administration de IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows», à la page 206

Droits d'utilisation des objets WebSphere MQ

Les applications peuvent accéder aux objets WebSphere MQ suivants en émettant des appels MQI:

- Gestionnaires de files d'attente
- Files d'attente
- Processus
- Listes de noms
- Rubriques

Les applications peuvent également utiliser des commandes PCF (Programmable Command Format) pour accéder à ces objets WebSphere MQ , ainsi que pour accéder aux canaux et aux objets d'informations d'authentification. Ces objets peuvent être protégés par WebSphere MQ de sorte que les ID utilisateur associés aux applications aient besoin de droits d'accès.

Pour plus d'informations, voir «Autorisation pour les applications d'utiliser IBM WebSphere MQ», à la page 53.

Sécurité des canaux

Les ID utilisateur associés aux agents MCA (Message Channel Agent) doivent disposer des droits d'accès à diverses ressources WebSphere MQ . Par exemple, un agent MCA doit pouvoir se connecter à un gestionnaire de files d'attente. S'il s'agit d'un agent MCA émetteur, il doit pouvoir ouvrir la file d'attente de transmission du canal. S'il s'agit d'un agent MCA récepteur, il doit pouvoir ouvrir des files d'attente de destination. Les ID utilisateur associés aux applications qui doivent administrer les canaux, les initiateurs de canal et les programmes d'écoute doivent disposer des droits d'utilisation des commandes PCF appropriées. Cependant, la plupart des applications n'ont pas besoin d'un tel accès.

Pour plus d'informations, voir «Autorisation de canal», à la page 73.

Autres considérations

Vous devez prendre en compte les aspects suivants de la sécurité uniquement si vous utilisez certaines fonctions WebSphere MQ ou des extensions de produit de base:

- «Sécurité des clusters de gestionnaires de files d'attente», à la page 82
- «Sécurité pour la publication / abonnement IBM WebSphere MQ», à la page 83
- «Sécurité pour IBM WebSphere MQ Internet Pass-thru», à la page 85

Planification de l'identification et de l'authentification

Choisissez les ID utilisateur à utiliser, ainsi que la manière et les niveaux auxquels vous souhaitez appliquer les contrôles d'authentification.

Vous devez décider de la manière dont vous allez identifier les utilisateurs de vos applications IBM WebSphere MQ , en gardant à l'esprit que différents systèmes d'exploitation prennent en charge des ID utilisateur de longueurs différentes. Vous pouvez utiliser des enregistrements d'authentification de canal pour effectuer un mappage d'un ID utilisateur à un autre ou pour spécifier un ID utilisateur en

fonction d'un attribut de la connexion. Les canaux IBM WebSphere MQ utilisant SSL ou TLS utilisent des certificats numériques comme mécanisme d'identification et d'authentification. Chaque certificat numérique possède un nom distinctif de sujet qui peut être mappé à des identités spécifiques à l'aide d'enregistrements d'authentification de canal. De plus, les certificats de l'autorité de certification dans le référentiel de clés déterminent quels certificats numériques peuvent être utilisés pour l'authentification auprès de IBM WebSphere MQ. Pour plus d'informations, voir :

- «Mappage d'un gestionnaire de files d'attente éloignées à un ID utilisateur MCAUSER», à la page 193
- «Mappage d'un ID utilisateur vérifié par le client à un ID utilisateur MCAUSER», à la page 193
- «Mappage d'un nom distinctif SSL ou TLS à un ID utilisateur MCAUSER», à la page 194
- «Mappage d'une adresse IP à un ID utilisateur MCAUSER», à la page 196

Planification de l'authentification pour une application client

Vous pouvez appliquer des contrôles d'authentification à quatre niveaux: au niveau des communications, dans les exits de sécurité, avec des enregistrements d'authentification de canal et en termes d'identification transmise à un exit de sécurité.

Il y a quatre niveaux de sécurité à prendre en compte. Le diagramme illustre un client IBM WebSphere MQ MQI connecté à un serveur. La sécurité est appliquée à quatre niveaux, comme décrit dans le texte suivant. MCA est un agent MCA.

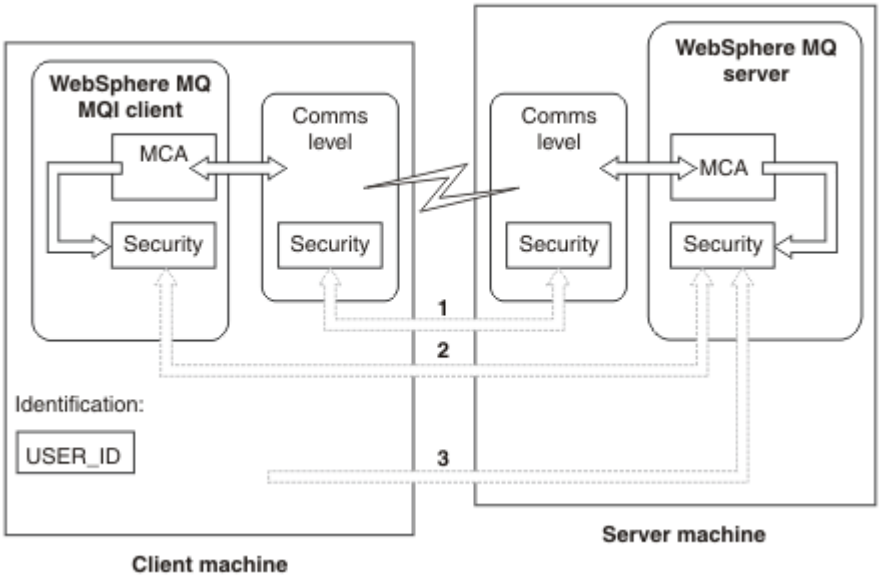


Figure 7. Sécurité dans une connexion client/serveur

1. Niveau de communication

   Voir la flèche 1. Pour implémenter la sécurité au niveau des communications, utilisez SSL ou TLS. Pour plus d'informations, voir «Protocoles de sécurité cryptographiques SSL et TLS», à la page 15

2. Enregistrements d'authentification de canal

   Voir les flèches 2 et 3. L'authentification peut être contrôlée à l'aide de l'adresse IP ou des noms distinctifs SSL/TLS au niveau de la sécurité. Un ID utilisateur peut également être bloqué ou un ID utilisateur vérifié peut être mappé à un ID utilisateur valide. Une description complète est fournie dans «Enregistrements d'authentification de canal», à la page 41.

3. Exits de sécurité de canal

   Voir la flèche 2. Les exits de sécurité de canal pour la communication de client à serveur peuvent fonctionner de la même manière que pour la communication de serveur à serveur. Une paire d'exits indépendants du protocole peut être écrite pour permettre l'authentification mutuelle du client et du serveur. Une description complète est fournie dans Programmes d'exit de sécurité de canal.

4. Identification transmise à un exit de sécurité de canal

   Voir la flèche 3. Dans les communications client-serveur, les exits de sécurité de canal n'ont pas besoin de fonctionner en tant que paire. L'exit côté client IBM WebSphere MQ peut être omis. Dans ce cas, l'ID utilisateur est placé dans le descripteur de canal (MQCD) et l'exit de sécurité côté serveur peut le modifier, si nécessaire.

   Les clients Windows envoient également des informations supplémentaires pour faciliter l'identification.

   - L'ID utilisateur transmis au serveur est l'ID utilisateur actuellement connecté sur le client.
   - ID de sécurité de l'utilisateur actuellement connecté.

   Pour faciliter l'identification sur le client IBM WebSphere MQ pour HP Integrity NonStop Server, le client transmet l'alias OSS Safeguard sous lequel l'application client s'exécute. Cet ID est généralement au format <PRIMARYGROUP>.<ALIAS>. Si nécessaire, vous pouvez mapper cet ID utilisateur à un autre ID utilisateur sur le gestionnaire de files d'attente à l'aide d'enregistrements d'authentification de canal ou d'un exit de sécurité. Pour plus d'informations sur les exits de message, voir «Mappage d'identité dans les exits de message», à la page 155. Pour plus d'informations sur la définition des enregistrements d'authentification de canal, voir «Mappage d'un ID utilisateur vérifié par le client à un ID utilisateur MCAUSER», à la page 193.

   Les valeurs de l'ID utilisateur et, le cas échéant, de l'ID de sécurité, peuvent être utilisées par l'exit de sécurité du serveur pour établir l'identité du client IBM WebSphere MQ MQI.

ID utilisateur

Si le client IBM WebSphere MQ MQI se trouve sous Windows et que le serveur IBM WebSphere MQ se trouve également sous Windows et a accès au domaine dans lequel l'ID utilisateur du client est défini, IBM WebSphere MQ prend en charge les ID utilisateur comportant jusqu'à 20 caractères. Sur les plateformes et les configurations UNIX and Linux , la longueur maximale est de 12 caractères.

Un serveur WebSphere MQ for Windows ne prend pas en charge la connexion d'un client Windows si le client s'exécute sous un ID utilisateur contenant le caractère @, par exemple, abc@d. Le code retour de l'appel MQCONN au niveau du client est MQRC_NOT_AUTHORIZED.

Toutefois, vous pouvez spécifier l'ID utilisateur à l'aide de deux caractères @, par exemple, abc@@d. Il est recommandé d'utiliser le format id@domain pour s'assurer que l'ID utilisateur est résolu de manière cohérente dans le domaine approprié ; par conséquent, abc@@d@domain.

Notez que UNKNOWN est un ID utilisateur réservé et que l'ID utilisateur NOBODY a également une signification particulière pour WebSphere MQ. La création d'ID utilisateur dans le système d'exploitation appelé UNKNOWN ou NOBODY peut avoir des résultats inattendus.

Bien que les ID utilisateur soient utilisés pour l'authentification, les groupes sont utilisés pour l'autorisation, à l'exception de Windows.

Si vous créez des comptes de service, sans tenir compte des groupes, et que vous autorisez tous les ID utilisateur différemment, chaque utilisateur peut accéder aux informations de chaque autre utilisateur.

Autorisation de planification

Planifiez les utilisateurs qui auront des droits d'administration et planifiez comment autoriser les utilisateurs des applications à utiliser les objets IBM WebSphere MQ de manière appropriée, y compris ceux qui se connectent à partir d'un client IBM WebSphere MQ MQI.

Les personnes ou les applications doivent disposer d'un accès leur permettant d'utiliser IBM WebSphere MQ. L'accès dont ils ont besoin dépend des rôles qu'ils assument et des tâches qu'ils doivent effectuer. L'autorisation dans IBM WebSphere MQ peut être divisée en deux catégories principales:

- Autorisation d'effectuer des opérations d'administration
- Autorisation pour les applications d'utiliser IBM WebSphere MQ

Les deux classes d'opération sont contrôlées par le même composant et un individu peut être autorisé à effectuer les deux catégories d'opération.

Les rubriques suivantes fournissent des informations supplémentaires sur des domaines d'autorisation spécifiques que vous devez prendre en compte:

Droit d'administration de IBM WebSphere MQ

Les administrateurs IBM WebSphere MQ doivent disposer des droits nécessaires pour exécuter diverses fonctions. Ces droits sont obtenus de différentes manières sur différentes plateformes.

Les administrateurs IBM WebSphere MQ doivent disposer des droits suivants:

- Exécuter des commandes pour administrer IBM WebSphere MQ
- Utilisez laIBM WebSphere MQ Explorer

Pour plus d'informations, voir la rubrique correspondant à votre système d'exploitation.

Droits d'administration de IBM WebSphere MQ sur les systèmes UNIX et Windows

Un administrateur IBM WebSphere MQ est membre du groupe mqm. Ce groupe a accès à toutes les ressources IBM WebSphere MQ et peut émettre des commandes de contrôle IBM WebSphere MQ . Un administrateur peut accorder des droits spécifiques à un groupe d'utilisateurs.

Pour être administrateur IBM WebSphere MQ sur les systèmes UNIX et Windows , un utilisateur doit être membre du *groupe mqm*. Ce groupe est créé automatiquement lorsque vous installez WebSphere MQ. Pour permettre aux utilisateurs d'émettre des commandes de contrôle, vous devez les ajouter au groupe mqm. Cela inclut l'utilisateur root sur les systèmes UNIX .

Les utilisateurs qui ne sont pas membres du groupe mqm peuvent se voir octroyer des privilèges d'administration, mais ils ne peuvent pas émettre de commandes de contrôle IBM WebSphere MQ et ils sont autorisés à exécuter uniquement les commandes pour lesquelles l'accès leur a été accordé.

En outre, sur les systèmes Windows , les comptes SYSTEM et Administrator disposent d'un accès complet aux ressources IBM WebSphere MQ .

Tous les membres du groupe mqm ont accès à toutes les ressources WebSphere MQ sur le système, y compris la possibilité d'administrer tout gestionnaire de files d'attente exécuté sur le système. Cet accès peut être révoqué uniquement en supprimant un utilisateur du groupe mqm. Sur les systèmes Windows , les membres du groupe Administrateurs ont également accès à toutes les ressources WebSphere MQ .

Les administrateurs peuvent utiliser la commande de contrôle **runmqsc** pour émettre des commandes WebSphere MQ Script (MQSC). Lorsque **runmqsc** est utilisé en mode indirect pour envoyer des commandes MQSC à un gestionnaire de files d'attente éloignées, chaque commande MQSC est encapsulée dans une commande Escape PCF. Les administrateurs doivent disposer des droits requis pour que les commandes MQSC soient traitées par le gestionnaire de files d'attente éloignées.

WebSphere MQ Explorer émet des commandes PCF pour effectuer des tâches d'administration. Les administrateurs n'ont pas besoin de droits supplémentaires pour utiliser WebSphere MQ Explorer afin d'administrer un gestionnaire de files d'attente sur le système local. Lorsque WebSphere MQ Explorer est utilisé pour administrer un gestionnaire de files d'attente sur un autre système, les administrateurs doivent disposer des droits requis pour que les commandes PCF soient traitées par le gestionnaire de files d'attente éloignées.

Pour plus d'informations sur les vérifications des droits d'accès effectuées lors du traitement des commandes PCF et MQSC, voir les rubriques suivantes:

- Pour les commandes qui fonctionnent sur les gestionnaires de files d'attente, les files d'attente, les canaux, les processus, les listes de noms et les objets d'informations d'authentification, voir «Autorisation pour les applications d'utiliser IBM WebSphere MQ», à la page 53.
- Pour les commandes qui fonctionnent sur les canaux, les initiateurs de canal, les programmes d'écoute et les clusters, voir Sécurité des canaux.

Pour plus d'informations sur les droits dont vous avez besoin pour administrer WebSphere MQ sur les systèmes UNIX et Windows , voir les informations connexes.

Autorisation pour les applications d'utiliser IBM WebSphere MQ

Lorsque les applications accèdent à des objets, les ID utilisateur associés aux applications doivent disposer des droits appropriés.

Les applications peuvent accéder aux objets IBM WebSphere MQ suivants en émettant des appels MQI:

- Gestionnaires de files d'attente
- Files d'attente
- Processus
- Listes de noms
- Rubriques

Les applications peuvent également utiliser des commandes PCF pour administrer des objets IBM WebSphere MQ . Lorsque la commande PCF est traitée, elle utilise le contexte de droits de l'ID utilisateur qui a inséré le message PCF.

Les applications, dans ce contexte, incluent celles écrites par les utilisateurs et les fournisseurs.

Les applications qui utilisent IBM WebSphere MQ classes for Java, IBM WebSphere MQ classes for JMS, IBM WebSphere MQ classes for .NET ou Message Service Clients for C/C++ and .NET utilisent l'interface MQI indirectement.

Les agents MCA émettent également des appels MQI et les ID utilisateur associés aux agents MCA doivent disposer des droits d'accès à ces objets WebSphere MQ . Pour plus d'informations sur ces ID utilisateur et sur les droits dont ils ont besoin, voir «Autorisation de canal», à la page 73.

Lorsque des vérifications des droits d'accès sont effectuées

Les vérifications des droits d'accès sont effectuées lorsqu'une application tente d'accéder à un gestionnaire de files d'attente, à une file d'attente, à un processus ou à une liste de noms.

Les vérifications sont effectuées dans les cas suivants:

Lorsqu'une application se connecte à un gestionnaire de files d'attente à l'aide d'un appel MQCONN ou MQCONNX

Le gestionnaire de files d'attente demande au système d'exploitation l'ID utilisateur associé à l'application. Le gestionnaire de files d'attente vérifie ensuite que l'ID utilisateur est autorisé à s'y connecter et conserve l'ID utilisateur pour les vérifications ultérieures.

Les utilisateurs n'ont pas besoin de se connecter à IBM WebSphere MQ. IBM WebSphere MQ suppose que les utilisateurs sont connectés au système d'exploitation sous-jacent et qu'ils ont été authentifiés par celui-ci.

Lorsqu'une application ouvre un objet IBM WebSphere MQ à l'aide d'un appel MQOPEN ou MQPUT1

Toutes les vérifications de droits sont effectuées lorsqu'un objet est ouvert, et non lors d'un accès ultérieur. Par exemple, des vérifications des droits d'accès sont effectuées lorsqu'une application ouvre une file d'attente. Elles ne sont pas effectuées lorsque l'application insère des messages dans la file d'attente ou extrait des messages de la file d'attente.

Lorsqu'une application ouvre un objet, elle indique les types d'opération qu'elle doit effectuer sur l'objet. Par exemple, une application peut ouvrir une file d'attente pour parcourir les messages qu'elle contient, en extraire des messages, mais pas pour y placer des messages. Pour chaque type d'opération, le gestionnaire de files d'attente vérifie que l'ID utilisateur associé à l'application dispose des droits permettant d'effectuer cette opération.

Lorsqu'une application ouvre une file d'attente, les vérifications des droits d'accès sont effectuées sur l'objet nommé dans la zone `ObjectName` du descripteur d'objet. La zone `ObjectName` est utilisée sur les appels `MQOPEN` ou `MQPUT1` . Si l'objet est une file d'attente alias ou une définition de file d'attente éloignée, les vérifications des droits sont effectuées sur l'objet lui-même. Elles ne sont pas effectuées sur la file d'attente dans laquelle la file d'attente alias ou la définition de file d'attente éloignée est résolue. Cela signifie que l'utilisateur n'a pas besoin de droits pour y accéder. Limitez les droits de création de files d'attente aux utilisateurs privilégiés. Si vous ne le faites pas, les utilisateurs peuvent ignorer le contrôle d'accès normal simplement en créant un alias.

Une application peut faire explicitement référence à une file d'attente éloignée. Il définit les zones `ObjectName` et `ObjectQMgrName` du descripteur d'objet sur les noms de la file d'attente éloignée et du gestionnaire de files d'attente éloignées. Les vérifications des droits d'accès sont effectuées sur la file d'attente de transmission portant le même nom que le gestionnaire de files d'attente éloignées. Sous UNIX, Linux, and Windows, une vérification est effectuée par rapport au profil RQMNAME qui correspond au nom du gestionnaire de files d'attente éloignées, si la mise en cluster est utilisée. Une application peut référencer une file d'attente de cluster de manière explicite en définissant la zone `ObjectName` dans le descripteur d'objet sur le nom de la file d'attente de cluster. Les vérifications des droits d'accès sont effectuées sur la file d'attente de transmission du cluster, `SYSTEM.CLUSTER.TRANSMIT.QUEUE`.

Les droits d'accès à une file d'attente dynamique sont basés sur la file d'attente modèle dont elle est dérivée, mais ne sont pas nécessairement les mêmes ; voir la remarque 1.

L'ID utilisateur utilisé par le gestionnaire de files d'attente pour les vérifications des droits d'accès est obtenu à partir du système d'exploitation. L'ID utilisateur est obtenu lorsque l'application se connecte au gestionnaire de files d'attente. Une application dûment autorisée peut émettre un appel `MQOPEN` en spécifiant un autre ID utilisateur ; des vérifications de contrôle d'accès sont ensuite effectuées sur l'autre ID utilisateur. L'utilisation d'un autre ID utilisateur ne modifie pas l'ID utilisateur associé à l'application, mais uniquement celui utilisé pour les vérifications de contrôle d'accès.

Lorsqu'une application s'abonne à une rubrique à l'aide d'un appel `MQSUB`

Lorsqu'une application s'abonne à une rubrique, elle spécifie le type d'opération qu'elle doit effectuer. Il s'agit de créer un abonnement, de modifier un abonnement existant ou de reprendre un abonnement existant sans le modifier. Pour chaque type d'opération, le gestionnaire de files d'attente vérifie que l'ID utilisateur associé à l'application est autorisé à effectuer l'opération.

Lorsqu'une application s'abonne à une rubrique, les vérifications des droits d'accès sont effectuées sur les objets de rubrique qui se trouvent dans l'arborescence de rubriques. Les objets de rubrique se trouvent au niveau ou au-dessus du point de l'arborescence de rubriques auquel l'application s'est abonnée. Les vérifications des droits d'accès peuvent impliquer des vérifications sur plusieurs objets de rubrique. L'ID utilisateur utilisé par le gestionnaire de files d'attente pour les vérifications des droits d'accès est obtenu à partir du système d'exploitation. L'ID utilisateur est obtenu lorsque l'application se connecte au gestionnaire de files d'attente.

Le gestionnaire de files d'attente effectue des vérifications des droits d'accès sur les files d'attente d'abonné, mais pas sur les files d'attente gérées.

Lorsqu'une application supprime une file d'attente dynamique permanente à l'aide d'un appel `MQCLOSE`

Le descripteur d'objet spécifié dans l'appel `MQCLOSE` n'est pas nécessairement le même que celui renvoyé par l'appel `MQOPEN` qui a créé la file d'attente dynamique permanente. S'il est différent, le gestionnaire de files d'attente vérifie l'ID utilisateur associé à l'application qui a émis l'appel `MQCLOSE` . Il vérifie que l'ID utilisateur est autorisé à supprimer la file d'attente.

Lorsqu'une application qui ferme un abonnement pour le supprimer ne l'a pas créé, les droits appropriés sont requis pour le supprimer.

Lorsqu'une commande PCF qui fonctionne sur un objet WebSphere MQ est traitée par le serveur de commandes

Cette règle inclut le cas où une commande PCF agit sur un objet d'informations d'authentification.

L'ID utilisateur utilisé pour les vérifications des droits d'accès est celui qui se trouve dans la zone `UserIdentifier` du descripteur de message de la commande PCF. Cet ID utilisateur doit disposer des droits requis sur le gestionnaire de files d'attente dans lequel la commande est traitée. La commande MQSC équivalente encapsulée dans une commande Escape PCF est traitée de la même manière. Pour plus d'informations sur la zone `UserIdentifier` et sur la manière dont elle est définie, voir «Contexte de message», à la page 55.

Droits de l'utilisateur de remplacement

Lorsqu'une application ouvre un objet ou s'abonne à une rubrique, elle peut fournir un ID utilisateur sur l'appel MQOPEN, MQPUT1ou MQSUB. Il peut demander au gestionnaire de files d'attente d'utiliser cet ID utilisateur pour les vérifications des droits d'accès au lieu de celui associé à l'application.

L'application réussit à ouvrir l'objet uniquement si les deux conditions suivantes sont remplies:

- L'ID utilisateur associé à l'application a le droit de fournir un ID utilisateur différent pour les vérifications des droits. L'application est dite disposer de *droits d'utilisateur de remplacement*.
- L'ID utilisateur fourni par l'application a le droit d'ouvrir l'objet pour les types d'opération demandés ou de s'abonner à la rubrique.

Contexte de message

Les informations de *contexte de message* permettent à l'application qui extrait un message de découvrir l'origine du message. Les informations sont conservées dans les zones du descripteur de message et les zones sont divisées en trois parties logiques

Ces parties sont les suivantes:

contexte d'identité
: Ces zones contiennent des informations sur l'utilisateur de l'application qui a inséré le message dans la file d'attente.

contexte d'origine
: Ces zones contiennent des informations sur l'application elle-même et sur le moment où le message a été inséré dans la file d'attente.

contexte utilisateur
: Ces zones contiennent les propriétés de message que les applications peuvent utiliser pour sélectionner les messages que le gestionnaire de files d'attente doit distribuer.

Lorsqu'une application insère un message dans une file d'attente, elle peut demander au gestionnaire de files d'attente de générer les informations de contexte dans le message. Il s'agit de l'action par défaut. Il peut également indiquer que les zones de contexte ne doivent pas contenir d'informations. L'ID utilisateur associé à une application ne nécessite aucun droit spécial pour effectuer l'une ou l'autre de ces opérations.

Une application peut définir les zones de contexte d'identité dans un message, ce qui permet au gestionnaire de files d'attente de générer le contexte d'origine ou de définir toutes les zones de contexte. Une application peut également transmettre les zones de contexte d'identité d'un message qu'elle a extrait à un message qu'elle place dans une file d'attente, ou transmettre toutes les zones de contexte. Toutefois, l'ID utilisateur associé à une application requiert des droits d'accès pour définir ou transmettre des informations de contexte. Une application indique qu'elle a l'intention de définir ou de transmettre des informations de contexte lorsqu'elle ouvre la file d'attente dans laquelle elle est sur le point d'insérer des messages et que ses droits sont vérifiés à ce stade.

Voici une brève description de chacune des zones de contexte:

contexte d'identité

UserIdentifier
: ID utilisateur associé à l'application qui a inséré le message. Si le gestionnaire de files d'attente définit cette zone, elle est définie sur l'ID utilisateur obtenu à partir du système d'exploitation lorsque l'application se connecte au gestionnaire de files d'attente.

AccountingToken
: Informations pouvant être utilisées pour facturer le travail effectué à la suite du message.

ApplIdentityData
: Si l'ID utilisateur associé à une application est autorisé à définir les zones de contexte d'identité ou à définir toutes les zones de contexte, l'application peut définir cette zone sur n'importe quelle valeur liée à l'identité. Si le gestionnaire de files d'attente définit cette zone, elle est mise à blanc.

Contexte d'origine

PutApplType
Type de l'application qui a inséré le message ; une transaction CICS , par exemple.

PutApplName
Nom de l'application qui a inséré le message.

PutDate
Date à laquelle le message a été inséré.

PutTime
Heure à laquelle le message a été inséré.

ApplOriginData
Si l'ID utilisateur associé à une application a le droit de définir toutes les zones de contexte, l'application peut définir cette zone sur n'importe quelle valeur liée à l'origine. Si le gestionnaire de files d'attente définit cette zone, elle est mise à blanc.

Contexte utilisateur

Les valeurs suivantes sont prises en charge pour **MQINQMP** ou **MQSETMP**:

MQPD_USER _CONTEXT

La propriété est associée au contexte utilisateur.

Aucune autorisation spéciale n'est requise pour pouvoir définir une propriété associée au contexte utilisateur à l'aide de l'appel MQSETMP.

Sur un gestionnaire de files d'attente V7.0 ou ultérieure, une propriété associée au contexte utilisateur est sauvegardée comme décrit pour MQOO_SAVE_ALL_CONTEXT. Une instruction MQPUT avec MQOO_PASS_ALL_CONTEXT spécifiée entraîne la copie de la propriété du contexte sauvegardé dans le nouveau message.

MQPD_NO_CONTEXT

La propriété n'est pas associée à un contexte de message.

Une valeur non reconnue est rejetée avec MQRC_PD_ERROR. La valeur initiale de cette zone est **MQPD_NO_CONTEXT**.

Pour une description détaillée de chacune des zones de contexte, voir MQMD-Descripteur de message. Pour plus d'informations sur l'utilisation du contexte de message, voir Contexte de message.

Droits d'utilisation des objets IBM WebSphere MQ sur les systèmes UNIX, Linux et Windows

Le composant de service d'autorisation fourni avec IBM WebSphere MQ est appelé *gestionnaire des droits d'accès aux objets (OAM)*. Il fournit un contrôle d'accès via des vérifications d'authentification et d'autorisation.

1. Authentification.

   La vérification de l'authentification effectuée par la méthode d'accès aux objets (OAM) fournie avec IBM WebSphere MQ est de base et n'est effectuée que dans des circonstances spécifiques. Il n'est pas destiné à répondre aux exigences strictes attendues dans un environnement hautement sécurisé.

   La méthode d'accès aux objets (OAM) effectue son contrôle d'authentification lorsqu'une application se connecte à un gestionnaire de files d'attente et que les conditions suivantes sont remplies.

   Si une structure MQCSP a été fournie par l'application de connexion et que l'attribut *AuthenticationType* de la structure MQCSP reçoit la valeur MQCSP_AUTH_USER_ID_AND_PWD, la vérification est effectuée par l'OAM dans sa fonction MQZID_AUTHENTICATE_USER. Il s'agit de la vérification: l'ID utilisateur dans la structure MQCSP est comparé à l'ID utilisateur dans *IdentityContext* (MQZIC) pour déterminer s'il correspond. S'ils ne correspondent pas, la vérification échoue.

Cette vérification de base n'est pas destinée à être une authentification complète de l'utilisateur. Par exemple, il n'y a pas de vérification de l'authenticité de l'utilisateur en vérifiant le mot de passe fourni dans la structure MQCSP. De plus, si l'application omet une structure MQCSP, aucune vérification n'est effectuée.

Si des services d'authentification plus complets sont requis dans le gestionnaire de files d'attente via le composant de service d'autorisation, la méthode d'accès aux objets (OAM) fournie avec IBM WebSphere MQ ne l'offre pas. Vous devez écrire un nouveau composant de service d'autorisation ou en obtenir un auprès d'un fournisseur.

2. Autorisation.

   Les vérifications d'autorisation sont exhaustives et visent à répondre à la plupart des exigences normales.

   Les vérifications d'autorisation sont effectuées lorsqu'une application émet un appel MQI pour accéder à un gestionnaire de files d'attente, une file d'attente, un processus, une rubrique ou une liste de noms. Ils sont également exécutés à d'autres moments, par exemple lorsqu'une commande est exécutée par le serveur de commandes.

Sur les systèmes UNIX, Linux et Windows , le *service d'autorisation* fournit le contrôle d'accès lorsqu'une application émet un appel MQI pour accéder à un objet IBM WebSphere MQ qui est un gestionnaire de files d'attente, une file d'attente, un processus, une rubrique ou une liste de noms. Cela inclut la vérification des droits d'utilisateur de remplacement et des droits de définition ou de transmission des informations de contexte.

Sous Windows, la méthode d'accès aux objets (OAM) accorde aux membres du groupe Administrateurs le droit d'accéder à tous les objets IBM WebSphere MQ , même lorsque le contrôle UAC est activé.

En outre, sur les systèmes Windows , le compte SYSTEM dispose d'un accès complet aux ressources IBM WebSphere MQ .

Le service d'autorisation permet également de vérifier les droits d'accès lorsqu'une commande PCF s'exécute sur l'un de ces objets IBM WebSphere MQ ou sur un objet d'informations d'authentification. La commande MQSC équivalente encapsulée dans une commande Escape PCF est traitée de la même manière.

Le service d'autorisation est un *service installable*, ce qui signifie qu'il est implémenté par un ou plusieurs *composants de service installables*. Chaque composant est appelé à l'aide d'une interface documentée. Cela permet aux utilisateurs et aux fournisseurs de fournir des composants pour augmenter ou remplacer ceux fournis par les produits IBM WebSphere MQ .

Le composant de service d'autorisation fourni avec IBM WebSphere MQ est appelé *gestionnaire des droits d'accès aux objets (OAM)*. La méthode d'accès aux objets (OAM) est automatiquement activée pour chaque gestionnaire de files d'attente que vous créez.

La méthode d'accès aux objets (OAM) gère une liste de contrôle d'accès (ACL) pour chaque objet IBM WebSphere MQ auquel elle contrôle l'accès. Sur les systèmes UNIX and Linux , seuls les ID groupe peuvent apparaître dans une liste de contrôle d'accès. Cela signifie que tous les membres d'un groupe ont les mêmes droits. Sur les systèmes Windows , les ID utilisateur et les ID groupe peuvent apparaître dans une liste de contrôle d'accès. Cela signifie que des droits peuvent être accordés à des utilisateurs et à des groupes individuels.

Une limitation de 12 caractères s'applique au groupe et à l'ID utilisateur. Les plateformes UNIX limitent généralement la longueur d'un ID utilisateur à 12 caractères. AIX et Linux ont augmenté cette limite, mais IBM WebSphere MQ continue d'observer une restriction de 12 caractères sur toutes les plateformes UNIX . Si vous utilisez un ID utilisateur de plus de 12 caractères, IBM WebSphere MQ le remplace par la valeur "UNKNOWN". Ne définissez pas d'ID utilisateur avec la valeur "UNKNOWN".

La méthode d'accès aux objets (OAM) peut authentifier un utilisateur et modifier les zones de contexte d'identité appropriées. Vous pouvez l'activer en spécifiant une structure de paramètres de sécurité de connexion (MQCSP) sur un appel MQCONNX. La structure est transmise à la fonction OAM Authenticate User (MQZ_AUTHENTICATE_USER), qui définit les zones de contexte d'identité appropriées. Si une connexion MQCONNX est établie à partir d'un client IBM WebSphere MQ , les informations du MQCSP

sont transmises au gestionnaire de files d'attente auquel le client se connecte via la connexion client et le canal de connexion serveur. Si des exits de sécurité sont définis sur ce canal, le MQCSP est transmis à chaque exit de sécurité et peut être modifié par l'exit. Les exits de sécurité peuvent également créer le MQCSP. Pour plus de détails sur l'utilisation des exits de sécurité dans ce contexte, voir Programmes d'exit de sécurité de canal.

Sur les systèmes UNIX, Linux et Windows , la commande de contrôle **setmqaut** accorde et révoque les droits et est utilisée pour gérer les listes de contrôle d'accès. Par exemple, la commande

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

permet aux membres du groupe VOYAGER de parcourir les messages dans la file d'attente MOON.EUROPA appartenant au gestionnaire de files d'attente JUPITER. Il permet également aux membres d'extraire des messages de la file d'attente. Pour révoquer ces droits ultérieurement, entrez la commande suivante:

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

La commande :

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

permet aux membres du groupe VOYAGER d'insérer des messages dans n'importe quelle file d'attente dont le nom commence par les caractères `MOON.` . MOON.* est le nom d'un profil générique.Un *profil générique* vous permet d'accorder des droits pour un ensemble d'objets à l'aide d'une seule commande **setmqaut** .

La commande de contrôle **dspmqaut** permet d'afficher les droits en cours d'un utilisateur ou d'un groupe sur un objet spécifié.La commande de contrôle **dmpmqaut** est également disponible pour afficher les droits en cours associés aux profils génériques.

Si vous ne souhaitez pas de vérification des droits d'accès, par exemple, dans un environnement de test, vous pouvez désactiver la méthode d'accès aux objets (OAM).

Utilisation de PCF pour accéder aux commandes OAM
Sur les systèmes UNIX, Linux et Windows , vous pouvez utiliser des commandes PCF pour accéder aux commandes d'administration OAM.

Les commandes PCF et les commandes OAM équivalentes sont les suivantes:

Tableau 6. Commandes PCF et commandes OAM équivalentes

Commande PCF	**Commande OAM**
Consulter des enregistrements de droits	dmpmqaut
Consulter les droits de l'entité	dspmqaut
Définir l'enregistrement de droits d'accès	setmqaut
Supprimer l'enregistrement de droits d'accès	setmqaut avec l'option -remove

Les commandes **setmqaut** et **dmpmqaut** sont limitées aux membres du groupe mqm. Les commandes PCF équivalentes peuvent être exécutées par des utilisateurs de n'importe quel groupe disposant des droits dsp et chg sur le gestionnaire de files d'attente.

Pour plus d'informations sur l'utilisation de ces commandes, voir Introduction to Programmable Command Formats .

Sécurité de la messagerie distante

Cette section traite des aspects de la sécurité liés à la messagerie distante.

Vous devez autoriser les utilisateurs à utiliser les fonctions IBM WebSphere MQ . Il est organisé en fonction des actions à entreprendre en ce qui concerne les objets et les définitions. Exemple :

- Les gestionnaires de files d'attente peuvent être démarrés et arrêtés par des utilisateurs autorisés
- Les applications doivent se connecter au gestionnaire de files d'attente et disposer des droits d'utilisation des files d'attente
- Les canaux de transmission de messages doivent être créés et contrôlés par des utilisateurs autorisés
- Les objets sont conservés dans des bibliothèques et l'accès à ces bibliothèques peut être restreint

L'agent MCA sur un site distant doit vérifier que le message en cours de distribution provient d'un utilisateur autorisé à le faire sur ce site distant. En outre, comme les agents MCA peuvent être démarrés à distance, il peut être nécessaire de vérifier que les processus distants qui tentent de démarrer vos agents MCA sont autorisés à le faire. Il y a quatre façons possibles pour vous de faire face à cette situation:

1. Utilisez de manière appropriée l'attribut PutAuthority de votre définition de canal RCVR, RQSTR ou CLUSRCVR pour contrôler l'utilisateur utilisé pour les vérifications d'autorisation au moment où les messages entrants sont placés dans vos files d'attente. Voir la description de la commande DEFINE CHANNEL dans le guide des commandes MQSC.
2. Implémentez des enregistrements d'authentification de canal pour rejeter les tentatives de connexion non souhaitées ou pour définir une valeur MCAUSER basée sur les éléments suivants: l'adresse IP distante, l'ID utilisateur distant, le nom distinctif de sujet (DN) SSL ou TLS fourni ou le nom du gestionnaire de files d'attente distant.
3. Implémentez la vérification de la sécurité de l' *exit utilisateur* pour vous assurer que le canal de transmission de messages correspondant est autorisé. La sécurité de l'installation hébergeant le canal correspondant garantit que tous les utilisateurs sont correctement autorisés, de sorte que vous n'avez pas besoin de vérifier les messages individuels.
4. Implémentez le traitement des messages de l' *exit utilisateur* pour vous assurer que les messages individuels sont vérifiés pour l'autorisation.

Sécurité des objets sur les systèmes UNIX and Linux

Les utilisateurs d'administration doivent faire partie du groupe mqm sur votre système (y compris root) si cet ID doit utiliser les commandes d'administration IBM WebSphere MQ .

Vous devez toujours exécuter amqcrsta en tant qu'ID utilisateur "mqm".

ID utilisateur sur les systèmes UNIX and Linux

Le gestionnaire de files d'attente convertit tous les identificateurs utilisateur en majuscules ou en casse mixte en minuscules. Le gestionnaire de files d'attente insère ensuite les identificateurs d'utilisateur dans la partie contextuelle d'un message ou vérifie leur autorisation. Les autorisations sont donc basées uniquement sur des identificateurs en minuscules.

Sécurité des objets sur les systèmes Windows

Les utilisateurs d'administration doivent faire partie du groupe mqm et du groupe d'administrateurs sur les systèmes Windows si cet ID doit utiliser les commandes d'administration IBM WebSphere MQ .

ID utilisateur sur les systèmes Windows

Sur les systèmes Windows , *si aucun exit de message n'est installé*, le gestionnaire de files d'attente convertit en minuscules les identificateurs d'utilisateur en majuscules ou en casse mixte. Le gestionnaire de files d'attente insère ensuite les identificateurs d'utilisateur dans la partie contextuelle d'un message ou vérifie leur autorisation. Les autorisations sont donc basées uniquement sur des identificateurs en minuscules.

ID utilisateur sur tous les systèmes

Sur les plateformes autres que Windows , les systèmes UNIX and Linux utilisent des majuscules pour les ID utilisateur dans les messages.

Pour permettre à Windows, aux systèmes UNIX and Linux d'utiliser des ID utilisateur en minuscules dans les messages, les conversions suivantes sont effectuées par l'agent MCA sur ces plateformes:

A la fin de l'envoi
Les caractères alphabétiques de tous les ID utilisateur sont convertis en caractères majuscules si aucun exit de message n'est installé.

A l'extrémité réceptrice
Les caractères alphabétiques de tous les ID utilisateur sont convertis en minuscules si aucun exit de message n'est installé.

Les conversions automatiques ne sont pas effectuées si vous fournissez un exit de message sur les systèmes UNIX, Linux et Windows pour une autre raison.

Utilisation d'un service d'autorisation personnalisé

IBM WebSphere MQ fournit un service d'autorisation installable. Vous pouvez choisir d'installer un autre service.

Le composant de service d'autorisation fourni avec IBM WebSphere MQ est appelé Object Authority Manager (OAM). Si la méthode d'accès aux objets (OAM) ne fournit pas les fonctions d'autorisation dont vous avez besoin, vous pouvez écrire votre propre composant de service d'autorisation. Les fonctions de service installables qui doivent être implémentées par un composant de service d'autorisation sont décrites dans Informations de référence de l'interface des services installables.

Contrôle d'accès pour les clients

Le contrôle d'accès est basé sur les ID utilisateur. Il peut y avoir de nombreux ID utilisateur à administrer, et les ID utilisateur peuvent être dans des formats différents. Vous pouvez définir la propriété de canal de connexion serveur MCAUSER sur une valeur d'ID utilisateur spéciale à utiliser par les clients.

Le contrôle d'accès dans IBM WebSphere MQ est basé sur les ID utilisateur. L'ID utilisateur du processus qui effectue des appels MQI est normalement utilisé. Pour les clients MQ MQI, l'agent MCA de connexion serveur effectue des appels MQI pour le compte des clients MQ MQI. Vous pouvez sélectionner un autre ID utilisateur pour l'agent MCA de connexion serveur à utiliser pour effectuer des appels MQI. L'ID utilisateur alternatif peut être associé au poste de travail client ou à tout élément que vous choisissez pour organiser et contrôler l'accès des clients. L'ID utilisateur doit disposer des droits nécessaires sur le serveur pour émettre des appels MQI. Il est préférable de choisir un autre ID utilisateur que d'autoriser les clients à effectuer des appels MQI avec les droits de l'agent MCA de connexion serveur.

Tableau 7. ID utilisateur utilisé par un canal de connexion serveur

ID utilisateur	En cas d'utilisation
ID utilisateur défini par un exit de sécurité	Utilisé sauf s'il est bloqué par une règle **CHLAUTH TYPE(BLOCKUSER)** . Pour plus d'informations, voir la section suivante, «Définition de l'ID utilisateur dans un exit de sécurité», à la page 61 .
ID utilisateur défini par une règle CHLAUTH	Utilisé sauf si remplacé par un exit de sécurité. Pour plus d'informations, voir Enregistrements d'authentification de canal .
ID utilisateur défini dans l'attribut **MCAUSER** de la définition de canal SVRCONN	Utilisé sauf s'il est remplacé par un exit de sécurité ou une règle CHLAUTH.
ID utilisateur transmis à partir de la machine client	Utilisé lorsqu'aucun ID utilisé n'est défini par d'autres moyens.

Tableau 7. ID utilisateur utilisé par un canal de connexion serveur (suite)	
ID utilisateur	**En cas d'utilisation**
ID utilisateur ayant démarré le canal de connexion serveur	Utilisé lorsqu'aucun ID utilisateur n'est défini par d'autres moyens et qu'aucun ID utilisateur client n'est transmis. Pour plus d'informations, voir la section suivante, «ID utilisateur qui exécute le programme de canal», à la page 62 .

Etant donné que l'agent MCA de connexion serveur effectue des appels MQI pour le compte d'utilisateurs distants, il est important de prendre en compte les implications de sécurité de l'agent MCA de connexion serveur qui émet des appels MQI pour le compte de clients distants et de savoir comment administrer l'accès d'un nombre potentiellement élevé d'utilisateurs.

- L'une des approches consiste pour l'agent MCA de connexion serveur à émettre des appels MQI avec ses propres droits d'accès. Mais attention, il est normalement indésirable pour l'agent MCA de connexion serveur, avec ses puissantes fonctions d'accès, d'émettre des appels MQI pour le compte des utilisateurs client.
- Une autre approche consiste à utiliser l'ID utilisateur qui provient du client. L'agent MCA de connexion serveur peut émettre des appels MQI à l'aide des fonctions d'accès de l'ID utilisateur client. Cette approche pose un certain nombre de questions à prendre en considération:
  1. Il existe différents formats pour l'ID utilisateur sur différentes plateformes. Cela provoque parfois des problèmes si le format de l'ID utilisateur sur le client diffère des formats acceptables sur le serveur.
  2. Il existe potentiellement de nombreux clients, avec des ID utilisateur différents et qui changent. Les ID doivent être définis et gérés sur le serveur.
  3. L'ID utilisateur est-il digne de confiance? Tout ID utilisateur peut être transmis à partir d'un client, pas nécessairement l'ID de l'utilisateur connecté. Par exemple, le client peut transmettre un ID avec des droits `mqm` complets qui ont été définis intentionnellement uniquement sur le serveur pour des raisons de sécurité.
- L'approche préférée consiste à définir des jetons d'identification client sur le serveur, et donc à limiter les capacités des applications connectées au client. Cette opération est généralement effectuée en définissant la propriété de canal de connexion serveur MCAUSER sur une valeur d'ID utilisateur spéciale à utiliser par les clients et en définissant quelques ID à utiliser par les clients ayant un niveau d'autorisation différent sur le serveur.

Définition de l'ID utilisateur dans un exit de sécurité

Pour les clients IBM WebSphere MQ MQI, le processus qui émet les appels MQI est l'agent MCA de connexion serveur. L'ID utilisateur utilisé par l'agent MCA de connexion serveur est contenu dans les zones `MCAUserIdentifier` ou `LongMCAUserIdentifier` du MQCD. Le contenu de ces zones est défini par:

- Toutes les valeurs définies par les exits de sécurité
- ID utilisateur du client
- MCAUSER (dans la définition de canal de connexion serveur)

L'exit de sécurité peut remplacer les valeurs qui lui sont visibles lorsqu'il est appelé.

- Si l'attribut MCAUSER du canal de connexion serveur est défini sur une valeur non vide, la valeur MCAUSER est utilisée.
- Si l'attribut MCAUSER du canal de connexion serveur est vide, l'ID utilisateur reçu du client est utilisé.
- Si l'attribut MCAUSER du canal de connexion serveur est vide et qu'aucun ID utilisateur n'est reçu du client, l'ID utilisateur qui a démarré le canal de connexion serveur est utilisé.

Assurez-vous que la zone MCAUSER est limitée à 12 caractères sur les plateformes Windows car tous les caractères supplémentaires seront tronqués, ce qui peut entraîner des échecs d'autorisation.

Le client IBM WebSphere MQ ne transite pas l'ID utilisateur vérifié vers le serveur lorsqu'un exit de sécurité côté client est en cours d'utilisation.

ID utilisateur qui exécute le programme de canal

Lorsque les zones d'ID utilisateur sont dérivées de l'ID utilisateur qui a démarré le canal de connexion serveur, la valeur suivante est utilisée:

- Pour z/OS, ID utilisateur affecté à la tâche démarrée de l'initiateur de canal par la table des procédures démarrées z/OS .
- Pour TCP/IP (nonz/OS), l'ID utilisateur de l'entrée `inetd.conf` ou l'ID utilisateur qui a démarré le programme d'écoute.
- Pour SNA (nonz/OS), l'ID utilisateur de l'entrée SNA Server ou (s'il n'y en a pas) la demande de connexion entrante, ou l'ID utilisateur qui a démarré le programme d'écoute.
- Pour NetBIOS ou SPX, l'ID utilisateur qui a démarré le programme d'écoute.

S'il existe des définitions de canal de connexion serveur dont l'attribut MCAUSER est à blanc, les clients peuvent utiliser cette définition de canal pour se connecter au gestionnaire de files d'attente avec des droits d'accès déterminés par l'ID utilisateur fourni par le client. Il peut s'agir d'un risque de sécurité si le système sur lequel s'exécute le gestionnaire de files d'attente autorise des connexions réseau non autorisées. Le canal de connexion serveur par défaut IBM WebSphere MQ (SYSTEM.DEF.SVRCONN) a l'attribut MCAUSER à blanc. Pour éviter les accès non autorisés, mettez à jour l'attribut MCAUSER de la définition par défaut avec un ID utilisateur qui n'a pas accès aux objets IBM WebSphere MQ MQ .

Casse des ID utilisateur

Lorsque vous définissez un canal avec `runmqsc`, l'attribut MCAUSER est mis en majuscules sauf si l'ID utilisateur est placé entre apostrophes.

Pour les serveurs sur les systèmes UNIX, Linux et Windows , le contenu de la zone `MCAUserIdentifier` reçue du client est modifié en minuscules.

Pour les serveurs sous IBM i, le contenu de la zone `LongMCAUserIdentifier` reçue du client est mis en majuscules.

Pour les serveurs sur les systèmes UNIX and Linux , le contenu de la zone `LongMCAUserIdentifier` reçue du client est remplacé par des minuscules.

Par défaut, l'ID utilisateur transmis lorsqu'une application de liaison MQ JMS est utilisée est l'ID utilisateur de la machine virtuelle Java sur laquelle l'application est exécutée.

Il est également possible de transmettre un ID utilisateur via la méthode `createQueueConnection` .

Planification de la confidentialité

Planifiez le maintien de la confidentialité de vos données.

Vous pouvez implémenter la confidentialité au niveau de l'application ou au niveau du lien. Vous pouvez choisir d'utiliser SSL ou TLS, auquel cas vous devez planifier votre utilisation des certificats numériques. Vous pouvez également utiliser des programmes d'exit de canal si les fonctions standard ne répondent pas à vos besoins.

Concepts associés

«Comparatif de la sécurité au niveau des liaisons et de la sécurité au niveau de l'application», à la page 63

Cette rubrique contient des informations sur divers aspects de la sécurité au niveau des liens et de la sécurité au niveau des applications, et compare les deux niveaux de sécurité.

«Programmes d'exit de canal», à la page 68

Les *programmes d'exit de canal* sont des programmes appelés à des endroits définis dans la séquence de traitement d'un agent MCA. Les utilisateurs et les fournisseurs peuvent écrire leurs propres programmes d'exit de canal. Certains sont fournis par IBM.

«Protection des canaux avec SSL», à la page 75
La prise en charge de SSL dans IBM WebSphere MQ utilise l'objet d'informations d'authentification du gestionnaire de files d'attente et diverses commandes MQSC. Vous devez également tenir compte de votre utilisation des certificats numériques.

Comparatif de la sécurité au niveau des liaisons et de la sécurité au niveau de l'application

Cette rubrique contient des informations sur divers aspects de la sécurité au niveau des liens et de la sécurité au niveau des applications, et compare les deux niveaux de sécurité.

La sécurité au niveau des liens et des applications est illustrée dans Figure 8, à la page 63.

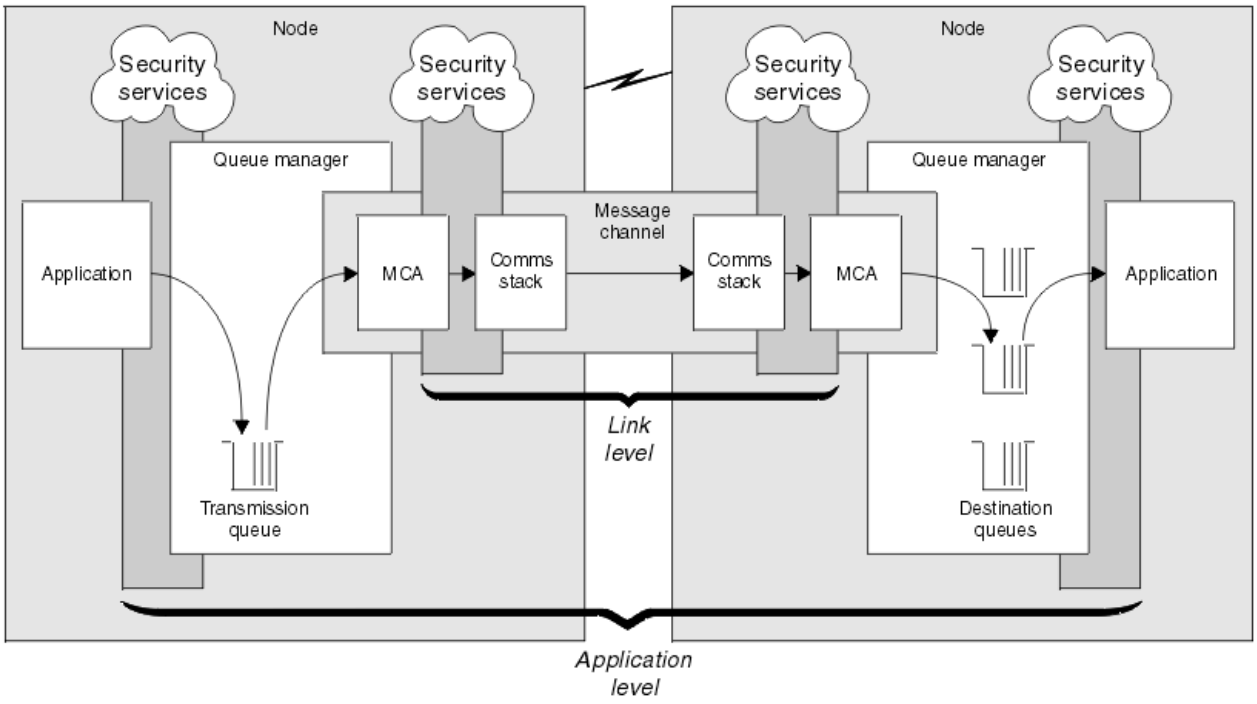


Figure 8. Sécurité au niveau des liens et sécurité au niveau des applications

Protection des messages dans les files d'attente

La sécurité au niveau des liaisons peut protéger les messages lorsqu'ils sont transférés d'un gestionnaire de files d'attente à un autre. Il est particulièrement important lorsque les messages sont transmis sur un réseau non sécurisé. Toutefois, il ne peut pas protéger les messages lorsqu'ils sont stockés dans des files d'attente d'un gestionnaire de files d'attente source, d'un gestionnaire de files d'attente de destination ou d'un gestionnaire de files d'attente intermédiaire.

La sécurité au niveau de l'application, par comparaison, peut protéger les messages lorsqu'ils sont stockés dans des files d'attente et s'applique même lorsque la mise en file d'attente répartie n'est pas utilisée. Il s'agit de la différence majeure entre la sécurité au niveau de la liaison et la sécurité au niveau de l'application, illustrée dans la Figure 8, à la page 63.

Les gestionnaires de files d'attente ne s'exécutent pas dans des environnements contrôlés et sécurisés

Si un gestionnaire de files d'attente s'exécute dans un environnement contrôlé et sécurisé, les mécanismes de contrôle d'accès fournis par WebSphere MQ peuvent être considérés comme suffisants

pour protéger les messages stockés dans ses files d'attente. Cela est particulièrement vrai si seule la mise en file d'attente locale est impliquée et que les messages ne quittent jamais le gestionnaire de files d'attente. Dans ce cas, la sécurité au niveau de l'application peut être considérée comme inutile.

La sécurité au niveau de l'application peut également être considérée comme inutile si des messages sont transférés vers un autre gestionnaire de files d'attente qui s'exécute également dans un environnement contrôlé et sécurisé ou s'ils sont reçus d'un tel gestionnaire de files d'attente. La sécurité au niveau de l'application est d'autant plus nécessaire lorsque des messages sont transférés vers ou reçus d'un gestionnaire de files d'attente qui ne s'exécute pas dans un environnement contrôlé et sécurisé.

Différences de coût

La sécurité au niveau de l'application peut coûter plus cher que la sécurité au niveau de la liaison en termes d'administration et de performances.

Le coût de l'administration est probablement plus élevé car il y a potentiellement plus de contraintes à configurer et à gérer. Par exemple, vous pouvez être amené à vous assurer qu'un utilisateur particulier n'envoie que certains types de message et qu'il n'envoie des messages qu'à certaines destinations. A l'inverse, il peut être nécessaire de s'assurer qu'un utilisateur particulier ne reçoit que certains types de message et qu'il ne reçoit que des messages provenant de certaines sources. Au lieu de gérer les services de sécurité au niveau des liens sur un canal de messages unique, vous devrez peut-être configurer et gérer des règles pour chaque paire d'utilisateurs qui échangent des messages sur ce canal.

Il peut y avoir un impact sur les performances si les services de sécurité sont appelés à chaque fois qu'une application insère ou reçoit un message.

Les organisations ont tendance à prendre en compte d'abord la sécurité au niveau des liens car elle peut être plus facile à mettre en oeuvre. Ils prennent en compte la sécurité au niveau de l'application s'ils découvrent que la sécurité au niveau des liens ne répond pas à toutes leurs exigences.

Disponibilité des composants

Généralement, dans un environnement distribué, un service de sécurité requiert un composant sur au moins deux systèmes. Par exemple, un message peut être chiffré sur un système et déchiffré sur un autre. Cela s'applique à la sécurité au niveau de la liaison et à la sécurité au niveau de l'application.

Dans un environnement hétérogène, avec des plateformes différentes en cours d'utilisation, chacune avec des niveaux de fonction de sécurité différents, les composants requis d'un service de sécurité peuvent ne pas être disponibles pour chaque plateforme sur laquelle ils sont nécessaires et sous une forme facile à utiliser. Il s'agit probablement d'un problème plus important pour la sécurité au niveau de l'application que pour la sécurité au niveau de la liaison, en particulier si vous prévoyez de fournir votre propre sécurité au niveau de l'application en achetant des composants à partir de diverses sources.

Messages dans une file d'attente de rebut

Si un message est protégé par la sécurité au niveau de l'application, il peut y avoir un problème si, pour une raison quelconque, le message n'atteint pas sa destination et est placé dans une file d'attente de messages non livrés. Si vous ne savez pas comment traiter le message à partir des informations du descripteur de message et de l'en-tête de la lettre morte, vous devrez peut-être inspecter le contenu des données d'application. Vous ne pouvez pas effectuer cette opération si les données de l'application sont chiffrées et que seul le destinataire prévu peut les déchiffrer.

Ce que la sécurité au niveau de l'application ne peut pas faire

La sécurité au niveau de l'application n'est pas une solution complète. Même si vous implémentez la sécurité au niveau de l'application, vous pouvez tout de même avoir besoin de certains services de sécurité au niveau de la liaison. Exemple :

- Lorsqu'un canal démarre, l'authentification mutuelle des deux agents MCA peut toujours être requise. Cette opération ne peut être effectuée que par un service de sécurité au niveau de la liaison.

- La sécurité au niveau de l'application ne peut pas protéger l'en-tête de la file d'attente de transmission, MQXQH, qui inclut le descripteur de message imbriqué. Il ne peut pas non plus protéger les données dans les flux de protocole de canal WebSphere MQ autres que les données de message. Seule la sécurité au niveau de la liaison peut fournir cette protection.
- Si les services de sécurité au niveau de l'application sont appelés à l'extrémité serveur d'un canal MQI, les services ne peuvent pas protéger les paramètres des appels MQI envoyés via le canal. En particulier, les données d'application d'un appel MQPUT, MQPUT1ou MQGET ne sont pas protégées. Seule la sécurité au niveau des liens peut fournir la protection dans ce cas.

sécurité au niveau des liaisons

La *sécurité de niveau liaison* fait référence aux services de sécurité qui sont appelés, directement ou indirectement, par un agent MCA, le sous-système de communication ou une combinaison des deux.

La sécurité au niveau des liens est illustrée dans la Figure 8, à la page 63.

Voici quelques exemples de services de sécurité au niveau des liens:

- L'agent MCA à chaque extrémité d'un canal de transmission de messages peut authentifier son partenaire. Cette opération est effectuée lorsque le canal démarre et qu'une connexion de communication a été établie, mais avant que les messages ne commencent à circuler. Si l'authentification échoue à l'une des extrémités, le canal est fermé et aucun message n'est transféré. Il s'agit d'un exemple de service d'identification et d'authentification.
- Un message peut être chiffré à l'extrémité émettrice d'un canal et déchiffré à l'extrémité réceptrice. Il s'agit d'un exemple de service de confidentialité.
- Un message peut être vérifié à l'extrémité réceptrice d'un canal pour déterminer si son contenu a été volontairement modifié lors de sa transmission sur le réseau. Voici un exemple de service d'intégrité des données.

Sécurité au niveau de la liaison fournie par IBM WebSphere MQ

Le principal moyen de mise à disposition de la confidentialité et de l'intégrité des données dans IBM WebSphere MQ consiste à utiliser SSL ou TLS. Pour plus d'informations sur l'utilisation de SSL et TLS dans IBM WebSphere MQ, voir «Prise en charge de IBM WebSphere MQ pour SSL et TLS», à la page 24. Pour l'authentification, IBM WebSphere MQ fournit la fonction permettant d'utiliser les enregistrements d'authentification de canal. Les enregistrements d'authentification de canal offrent un contrôle précis de l'accès accordé aux systèmes de connexion, au niveau des canaux individuels ou des groupes de canaux. Pour plus d'informations, voir «Enregistrements d'authentification de canal», à la page 41.

Mise à disposition de votre propre sécurité de niveau de liaison

Cette collection de rubriques décrit comment vous pouvez fournir vos propres services de sécurité au niveau des liens. L'écriture de vos propres programmes d'exit de canal est le principal moyen de fournir vos propres services de sécurité de niveau de liaison.

Les programmes d'exit de canal sont introduits dans «Programmes d'exit de canal», à la page 68.
La même rubrique décrit également le programme d'exit de canal fourni avec IBM WebSphere MQ for Windows (programme d'exit de canal SSPI). Ce programme d'exit de canal est fourni au format source afin que vous puissiez modifier le code source en fonction de vos besoins. Si ce programme d'exit de canal ou les programmes d'exit de canal disponibles auprès d'autres fournisseurs ne répondent pas à vos besoins, vous pouvez concevoir et écrire vos propres programmes. Cette rubrique explique comment les programmes d'exit de canal peuvent fournir des services de sécurité. Pour plus d'informations sur l'écriture d'un programme d'exit de canal, voir Ecriture de programmes d'exit de canal.

Sécurité au niveau de la liaison à l'aide d'un exit de sécurité

Les exits de sécurité fonctionnent normalement par paires, une à chaque extrémité d'un canal. Ils sont appelés immédiatement après la fin de la négociation de données initiale au démarrage du canal.

Les exits de sécurité peuvent être utilisés pour fournir l'identification et l'authentification, le contrôle d'accès et la confidentialité.

Sécurité au niveau de la liaison à l'aide d'un exit de message
Un exit de message ne peut être utilisé que sur un canal de transmission de messages et non sur un canal MQI. Il a accès à l'en-tête de la file d'attente de transmission, MQXQH, qui inclut le descripteur de message imbriqué, et aux données d'application d'un message. Il peut modifier le contenu du message et modifier sa longueur.

Un exit de message peut être utilisé à n'importe quelle fin qui nécessite l'accès à l'ensemble du message plutôt qu'à une partie de celui-ci.

Les exits de message peuvent être utilisés pour fournir l'identification et l'authentification, le contrôle d'accès, la confidentialité, l'intégrité des données et la non-répudiation, et pour des raisons autres que la sécurité.

Sécurité au niveau de la liaison à l'aide des exits d'envoi et de réception
Les exits d'envoi et de réception peuvent être utilisés sur les canaux de message et MQI. Ils sont appelés pour tous les types de données qui circulent sur un canal et pour les flux dans les deux sens.

Les exits d'émission et de réception ont accès à chaque segment de transmission. Ils peuvent modifier son contenu et sa longueur.

Sur un canal de transmission, si un MCA a besoin de fractionner un message et de l'envoyer dans plus d'un segment de transmission, une sortie d'émission est appelée pour chaque segment de transmission contenant une partie du message et, à la réception, une sortie de réception est appelée pour chaque segment de transmission. Il en est de même sur un canal MQI si les paramètres d'entrée ou de sortie d'un appel MQI sont trop grands pour être envoyés dans un segment de transmission unique.

Sur un canal MQI, l'octet 10 d'un segment de transmission identifie l'appel MQI et indique si le segment de transmission contient les paramètres d'entrée ou de sortie de l'appel. Les exits d'envoi et de réception peuvent examiner cet octet pour déterminer si l'appel MQI contient des données d'application qui peuvent avoir besoin d'être protégées.

Lorsqu'un exit d'émission est appelé pour la première fois, pour acquérir et initialiser les ressources dont il a besoin, il peut demander à l'agent MCA de réserver une quantité d'espace spécifiée dans la mémoire tampon qui contient un segment de transmission. Lorsqu'il est appelé ultérieurement pour traiter un segment de transmission, il peut utiliser cet espace pour ajouter une clé chiffrée ou une signature numérique, par example. L'exit de réception correspondent à l'autre extrémité du canal peut supprimer les données ajoutées par l'exit d'émission et les utiliser pour traiter le segment de transmission.

Les sorties d'émission et de réception sont mieux adaptées à des fins dans lesquelles elles n'ont pas besoin de comprendre la structure des données qu'elles traitent et peuvent donc traiter chaque segment de transmission comme un objet binaire.

Les exits d'envoi et de réception peuvent être utilisés pour assurer la confidentialité et l'intégrité des données, ainsi que pour des utilisations autres que la sécurité.

Tâches associées
Identification de l'appel API dans un programme d'exit d'envoi ou de réception

sécurité au niveau de l'application
La *sécurité au niveau de l'application* fait référence aux services de sécurité appelés à l'interface entre une application et un gestionnaire de files d'attente auquel elle est connectée.

Ces services sont appelés lorsque l'application émet des appels MQI au gestionnaire de files d'attente. Les services peuvent être appelés, directement ou indirectement, par l'application, le gestionnaire de files d'attente, un autre produit prenant en charge WebSphere MQ, ou une combinaison de ces deux éléments. La sécurité au niveau de l'application est illustrée dans la Figure 8, à la page 63.

La sécurité au niveau de l'application est également appelée *sécurité de bout en bout* ou *sécurité au niveau des messages*.

Voici quelques exemples de services de sécurité au niveau de l'application:

- Lorsqu'une application place un message dans une file d'attente, le descripteur de message contient un ID utilisateur associé à l'application. Toutefois, il n'existe aucune donnée, telle qu'un mot de passe

chiffré, qui peut être utilisée pour authentifier l'ID utilisateur. Un service de sécurité peut ajouter ces données. Lorsque le message est finalement extrait par l'application de réception, un autre composant du service peut authentifier l'ID utilisateur à l'aide des données qui ont été transmises avec le message.Il s'agit d'un exemple de service d'identification et d'authentification.

- Un message peut être chiffré lorsqu'il est placé dans une file d'attente par une application et déchiffré lorsqu'il est extrait par l'application réceptrice.Il s'agit d'un exemple de service de confidentialité.
- Un message peut être vérifié lorsqu'il est extrait par l'application de réception. Cette vérification détermine si son contenu a été délibérément modifié depuis sa première mise en file d'attente par l'application émettrice.Voici un exemple de service d'intégrité des données.

Planification pour Advanced Message Security
IBM WebSphere MQ Advanced Message Security (AMS) est un composant sous licence distincte de IBM WebSphere MQ qui offre un niveau de protection élevé pour les données sensibles transitant par le réseau IBM WebSphere MQ , sans affecter les applications finales.

Si vous déplacez des informations très sensibles ou précieuses, en particulier des informations confidentielles ou liées au paiement, telles que les dossiers des patients ou les détails de la carte de crédit, vous devez accorder une attention particulière à la sécurité de l'information. S'assurer que les informations qui circulent dans l'entreprise conservent leur intégrité et sont protégées contre tout accès non autorisé constitue un défi et une responsabilité permanents. Vous êtes également susceptible d'être tenu de respecter les règles de sécurité, au risque de sanctions en cas de non-conformité.

Vous pouvez développer vos propres extensions de sécurité dans IBM WebSphere MQ. Cependant, de telles solutions nécessitent des compétences spécialisées et peuvent être compliquées et coûteuses à maintenir. IBM WebSphere MQ Advanced Message Security vous aide à relever ces défis lorsque vous déplacez des informations dans l'entreprise entre pratiquement tous les types de système informatique commercial.

IBM WebSphere MQ Advanced Message Security étend les fonctions de sécurité de IBM WebSphere MQ comme suit:

- Il fournit une protection des données de bout en bout au niveau de l'application pour votre infrastructure de messagerie point à point, à l'aide du chiffrement ou de la signature numérique des messages.
- Il fournit une sécurité complète sans écrire de code de sécurité complexe ni modifier ou recompiler les applications existantes.
- Il utilise la technologie PKI (Public Key Infrastructure) pour fournir des services d'authentification, d'autorisation, de confidentialité et d'intégrité des données pour les messages.
- Il fournit l'administration des règles de sécurité pour les grands systèmes et les serveurs distribués.
- Il prend en charge les serveurs et les clients IBM WebSphere MQ .
- Il s'intègre à IBM WebSphere MQ Managed File Transfer pour fournir une solution de messagerie sécurisée de bout en bout.

Pour plus d'informations, voir «IBM WebSphere MQ Advanced Message Security», à la page 281.

Mise à disposition de votre propre sécurité au niveau de l'application
Cette collection de rubriques décrit comment vous pouvez fournir vos propres services de sécurité au niveau de l'application.

Pour vous aider à implémenter la sécurité au niveau de l'application, IBM WebSphere MQ fournit deux exits, l'exit d'API et l'exit de croisement d'API.

Ces exits peuvent fournir des services d'identification et d'authentification, de contrôle d'accès, de confidentialité, d'intégrité des données et de non-répudiation, ainsi que d'autres fonctions non liées à la sécurité.

Si l'exit d'API ou l'exit de croisement d'API n'est pas pris en charge dans votre environnement système, vous pouvez envisager d'autres moyens de fournir votre propre sécurité au niveau de l'application. L'une des méthodes consiste à développer une API de niveau supérieur qui encapsule l'interface MQI. Les

programmeurs utilisent ensuite cette API, à la place de l'interface MQI, pour écrire des applications IBM WebSphere MQ .

Les raisons les plus courantes de l'utilisation d'une API de niveau supérieur sont les suivantes:

- Pour masquer les fonctions plus avancées de l'interface MQI aux programmeurs.
- Pour appliquer des normes dans l'utilisation de l'interface MQI.
- Pour ajouter une fonction à l'interface MQI. Cette fonction supplémentaire peut être des services de sécurité.

Certains produits fournisseurs utilisent cette technique pour fournir une sécurité au niveau de l'application pour IBM WebSphere MQ.

Si vous prévoyez de fournir des services de sécurité de cette manière, notez ce qui suit concernant la conversion des données:

- Si un jeton de sécurité, tel qu'une signature numérique, a été ajouté aux données d'application dans un message, tout code effectuant une conversion de données doit être conscient de la présence de ce jeton.
- Un jeton de sécurité peut avoir été dérivé d'une image binaire des données d'application. Par conséquent, toute vérification du jeton doit être effectuée avant la conversion des données.
- Si les données d'application d'un message ont été chiffrées, elles doivent être déchiffrées avant la conversion des données.

Programmes d'exit de canal

Les *programmes d'exit de canal* sont des programmes appelés à des endroits définis dans la séquence de traitement d'un agent MCA. Les utilisateurs et les fournisseurs peuvent écrire leurs propres programmes d'exit de canal. Certains sont fournis par IBM.

Il existe plusieurs types de programme d'exit de canal, mais seuls quatre ont un rôle à jouer pour assurer la sécurité au niveau des liens:

- Exit de sécurité
- Exit de message
- Exit d'émission
- Exit de réception

Ces quatre types de programme d'exit de canal sont illustrés dans Figure 9, à la page 69 et sont décrits dans les rubriques suivantes.

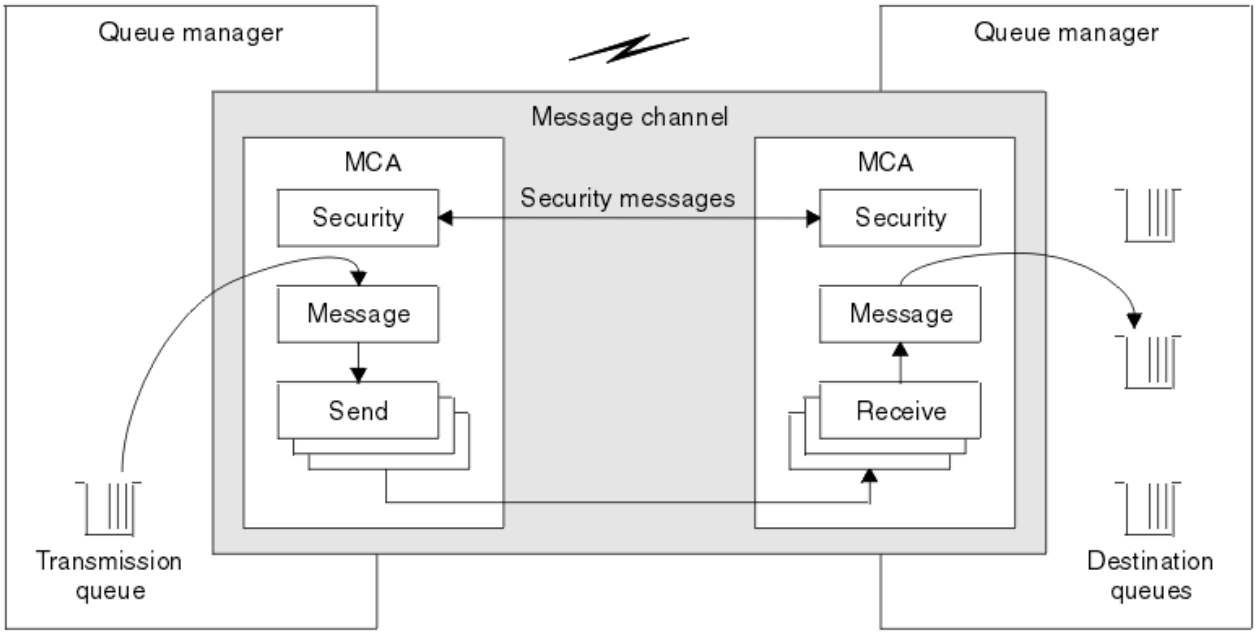


Figure 9. Exits de sécurité, de message, d'envoi et de réception sur un canal de message

Concepts associés

Programmes d'exit de canal pour les canaux de messagerie

Présentation de l'exit de sécurité

Les exits de sécurité fonctionnent normalement par paires. Ils sont appelés avant le flux de messages et leur but est de permettre à un agent MCA d'authentifier son partenaire.

Les *exits de sécurité* fonctionnent normalement par paires, une à chaque extrémité d'un canal. Ils sont appelés immédiatement après la fin de la négociation de données initiale au démarrage du canal, mais avant que les messages ne commencent à circuler. L'objectif principal de l'exit de sécurité est d'activer l'agent MCA à chaque extrémité d'un canal pour authentifier son partenaire. Cependant, rien n'empêche un exit de sécurité d'exécuter une autre fonction, même une fonction qui n'a rien à voir avec la sécurité.

Les exits de sécurité peuvent communiquer entre eux en envoyant des *messages de sécurité*. Le format du message de sécurité est défini par l'utilisateur. Un résultat possible de l'échange de messages de sécurité est que l'un des exits de sécurité peut décider de ne pas poursuivre. Dans ce cas, le canal est fermé et les messages ne circulent pas. S'il n'y a un exit de sécurité qu'à une seule extrémité d'un canal, l'exit est toujours appelé et peut choisir de continuer ou de fermer le canal.

Les exits de sécurité peuvent être appelés sur les canaux de message et MQI. Le nom d'un exit de sécurité est spécifié en tant que paramètre dans la définition de canal à chaque extrémité d'un canal.

Pour plus d'informations sur les exits de sécurité, voir «Sécurité au niveau de la liaison à l'aide d'un exit de sécurité», à la page 65.

Exit de message

Les exits de message fonctionnent uniquement sur les canaux de message et fonctionnent normalement par paires. Un exit de message peut fonctionner sur l'ensemble du message et y apporter diverses modifications.

Les exits de message aux extrémités émettrice et réceptrice d'un canal fonctionnent normalement par paires. Un exit de message à l'extrémité émettrice d'un canal est appelé une fois que l'agent MCA a reçu un message de la file d'attente de transmission. A l'extrémité réceptrice d'un canal, un exit de message est appelé avant que l'agent MCA n'insère un message dans sa file d'attente de destination.

Un exit de message a accès à l'en-tête de file d'attente de transmission, MQXQH, qui inclut le descripteur de message imbriqué, et aux données d'application d'un message. Un exit de message peut modifier le contenu du message et modifier sa longueur. Un changement de longueur peut être le résultat de la

compression, de la décompression, du chiffrement ou du déchiffrement du message. Il peut également être le résultat de l'ajout de données au message ou de la suppression de données de celui-ci.

Les exits de message peuvent être utilisés à n'importe quelle fin qui nécessite l'accès à l'ensemble du message, plutôt qu'à une partie de celui-ci, et pas nécessairement pour des raisons de sécurité.

Un exit de message peut déterminer que le message qu'il est en train de traiter ne doit pas continuer vers sa destination. L'agent MCA place ensuite le message dans la file d'attente des messages non livrés. Un exit de message peut également fermer le canal.

Les exits de message peuvent être appelés uniquement sur les canaux de message et non sur les canaux MQI. En effet, l'objectif d'un canal MQI est d'activer les paramètres d'entrée et de sortie des appels MQI entre l'application client IBM WebSphere MQ MQI et le gestionnaire de files d'attente.

Le nom d'un exit de message est indiqué en tant que paramètre dans la définition de canal à chaque extrémité d'un canal. Vous pouvez également spécifier une liste d'exits de message à exécuter successivement.

Pour plus d'informations sur les exits de message, voir «Sécurité au niveau de la liaison à l'aide d'un exit de message», à la page 66.

Exits d'envoi et de réception

Les exits d'envoi et de réception fonctionnent généralement par paires. Ils fonctionnent sur des segments de transmission et sont utilisés au mieux lorsque la structure des données qu'ils traitent n'est pas pertinente.

Un *exit d'émission* à une extrémité d'un canal et un *exit de réception* à l'autre extrémité fonctionnent normalement par paires. Un exit d'émission est appelé juste avant qu'un agent MCA ne lance un envoi de communications pour envoyer des données via une connexion de communication. Un exit de réception est appelé juste après qu'un agent MCA a repris le contrôle à la suite d'une réception de communications et a reçu des données d'une connexion de communication. Si le partage de conversations est en cours d'utilisation, sur un canal MQI, une instance différente d'exit d'émission et de réception est appelée pour chaque conversation.

Les flux du protocole de canal IBM WebSphere MQ entre deux agents MCA sur un canal de transmission de messages contiennent des informations de contrôle ainsi que des données de message. De même, sur un canal MQI, les flux contiennent des informations de contrôle ainsi que les paramètres des appels MQI. Les exits d'envoi et de réception sont appelés pour tous les types de données.

Les données de message ne circulent que dans une seule direction sur un canal de message mais, sur un canal MQI, les paramètres d'entrée d'un flux d'appel MQI dans une direction et les paramètres de sortie dans l'autre. Sur les canaux de message et MQI, contrôlez les flux d'informations dans les deux sens. Par conséquent, les exits d'émission et de réception peuvent être appelés aux deux extrémités d'un canal.

L'unité de données qui est transmise dans un flux unique entre deux MCM est appelée *segment de transmission*. Les exits d'émission et de réception ont accès à chaque segment de transmission. Ils peuvent modifier son contenu et sa longueur. Toutefois, un exit d'émission ne doit pas modifier les 8 premiers octets d'un segment de transmission. Ces 8 octets font partie de l'en-tête de protocole de canal IBM WebSphere MQ . Il existe également des restrictions sur la mesure dans laquelle un exit d'émission peut augmenter la longueur d'un segment de transmission. En particulier, un exit d'émission ne peut pas augmenter sa longueur au-delà de la longueur maximale négociée entre les deux agents MCA au démarrage du canal.

Sur un canal de transmission, si un message est trop volumineux pour être envoyé dans un seul segment de transmission, l'agent MCA émetteur fractionne le message et l'envoie dans plusieurs segments de transmission. En conséquence, une sortie d'émission est appelée pour chaque segment de transmission contenant une partie du message et, à la réception, une sortie de réception est appelée pour chaque segment de transmission. L'agent MCA récepteur reconstitue le message des segments de transmission après qu'ils ont été traités par l'exit de réception.

De même, sur un canal MQI, les paramètres d'entrée ou de sortie d'un appel MQI sont envoyés dans plusieurs segments de transmission s'ils sont trop grands. Cela peut se produire, par exemple, sur un appel MQPUT, MQPUT1ou MQGET si les données d'application sont suffisamment volumineuses.

Compte tenu de ces considérations, il est plus approprié d'utiliser des exits d'émission et de réception à des fins dans lesquelles ils n'ont pas besoin de comprendre la structure des données qu'ils traitent et peuvent donc traiter chaque segment de transmission comme un objet binaire.

Un exit d'émission ou de réception peut fermer un canal.

Les noms d'un exit d'émission et d'un exit de réception sont spécifiés en tant que paramètres dans la définition de canal à chaque extrémité d'un canal. Vous pouvez également spécifier une liste d'exits d'émission à exécuter successivement. De même, vous pouvez spécifier une liste d'exits de réception.

Pour plus d'informations sur les exits d'envoi et de réception, voir «Sécurité au niveau de la liaison à l'aide des exits d'envoi et de réception», à la page 66.

Planification de l'intégrité des données

Planifiez la manière de préserver l'intégrité de vos données.

Vous pouvez implémenter l'intégrité des données au niveau de l'application ou du lien.

Au niveau de l'application, vous pouvez choisir d'utiliser IBM WebSphere MQ Advanced Message Security pour signer numériquement les messages afin de vous protéger contre les modifications non autorisées. Vous pouvez également utiliser des programmes d'exit API si les fonctions standard ne répondent pas à vos besoins.

Au niveau des liens, vous pouvez choisir d'utiliser SSL ou TLS, auquel cas vous devez planifier votre utilisation des certificats numériques. Vous pouvez également utiliser des programmes d'exit de canal si les fonctions standard ne répondent pas à vos besoins.

Concepts associés

«Protection des canaux avec SSL», à la page 75
La prise en charge de SSL dans IBM WebSphere MQ utilise l'objet d'informations d'authentification du gestionnaire de files d'attente et diverses commandes MQSC. Vous devez également tenir compte de votre utilisation des certificats numériques.

«Intégrité des données dans IBM WebSphere MQ», à la page 23
Vous pouvez utiliser un service d'intégrité des données pour détecter si un message a été modifié.

«Planification pour Advanced Message Security», à la page 67
IBM WebSphere MQ Advanced Message Security (AMS) est un composant sous licence distincte de IBM WebSphere MQ qui offre un niveau de protection élevé pour les données sensibles transitant par le réseau IBM WebSphere MQ , sans affecter les applications finales.

Référence associée

Référence d'exit API

Structures de données et appels d'exit de canal

Planification de l'audit

Décidez des données à auditer et de la manière dont vous allez capturer et traiter les informations d'audit. Vérifiez que votre système est correctement configuré.

La surveillance de l'activité comporte plusieurs aspects. Les aspects que vous devez prendre en compte sont souvent définis par des exigences d'auditeur, et ces exigences sont souvent dictées par des normes réglementaires telles que la loi HIPAA (Health Insurance Portability and Accountability Act) ou la loi SOX (Sarbanes-Oxley). IBM WebSphere MQ fournit des fonctions destinées à faciliter la conformité à ces normes.

Déterminez si vous êtes intéressé uniquement par les exceptions ou si vous êtes intéressé par tous les comportements du système.

Certains aspects de l'audit peuvent également être considérés comme une surveillance opérationnelle ; une distinction pour l'audit est que vous examinez souvent les données historiques, et pas seulement les alertes en temps réel. La surveillance est traitée dans la section Surveillance et performances .

Données à auditer

Prenez en compte les types de données ou d'activité que vous devez auditer, comme décrit dans les sections suivantes:

Modifications apportées à IBM WebSphere MQ à l'aide des interfaces IBM WebSphere MQ
Configurez IBM WebSphere MQ pour émettre des événements d'instrumentation, en particulier des événements de commande et des événements de configuration.

Modifications apportées à IBM WebSphere MQ en dehors de son contrôle
Certaines modifications peuvent affecter le comportement de IBM WebSphere MQ , mais elles ne peuvent pas être directement surveillées par IBM WebSphere MQ. Par exemple, vous pouvez modifier les fichiers de configuration `mqs.ini`, `qm.ini`et `mqclient.ini`, créer et supprimer des gestionnaires de files d'attente, installer des fichiers binaires tels que des programmes d'exit utilisateur et modifier les droits d'accès aux fichiers. Pour surveiller ces activités, vous devez utiliser des outils exécutés au niveau du système d'exploitation. Différents outils sont disponibles et adaptés aux différents systèmes d'exploitation. Vous pouvez également avoir des journaux créés par des outils associés, tels que *sudo*.

Contrôle opérationnel de IBM WebSphere MQ
Vous devrez peut-être utiliser les outils du système d'exploitation pour auditer les activités telles que le démarrage et l'arrêt des gestionnaires de files d'attente. Dans certains cas, IBM WebSphere MQ peut être configuré pour émettre des événements d'instrumentation.

Activité d'application dans IBM WebSphere MQ
Pour auditer les actions des applications, par exemple l'ouverture de files d'attente et l'insertion et l'obtention de messages, configurez IBM WebSphere MQ pour émettre les événements appropriés.

Alertes d'intrus
Pour auditer les tentatives d'atteinte à la sécurité, configurez votre système pour qu'il émet des événements d'autorisation. Les événements de canal peuvent également être utiles pour afficher l'activité, en particulier si un canal se termine de manière inattendue.

Planification de la capture, de l'affichage et de l'archivage des données d'audit

La plupart des éléments dont vous avez besoin sont signalés comme des messages d'événement IBM WebSphere MQ . Vous devez choisir des outils qui peuvent lire et mettre en forme ces messages. Si vous êtes intéressé par le stockage et l'analyse à long terme, vous devez les déplacer vers un mécanisme de mémoire secondaire tel qu'une base de données. Si vous ne traitez pas ces messages, ils restent dans la file d'attente d'événements, ce qui peut entraîner le remplissage de la file d'attente. Vous pouvez décider d'implémenter un outil qui exécute automatiquement des actions en fonction de certains événements ; par exemple, pour émettre une alerte lorsqu'un incident de sécurité se produit.

Vérification de la configuration correcte de votre système

Un ensemble de tests est fourni avec IBM WebSphere MQ Explorer. Utilisez ces éléments pour rechercher les problèmes éventuels dans les définitions d'objet.

Vérifiez également régulièrement que la configuration du système correspond à vos attentes. Bien que les événements de commande et de configuration puissent signaler une modification, il est également utile de vider la configuration et de la comparer à une copie correcte connue.

Planification de la sécurité par topologie

Cette section traite de la sécurité dans des situations spécifiques, à savoir pour les canaux, les clusters de gestionnaires de files d'attente, les applications de publication / abonnement et de multidiffusion, et lors de l'utilisation d'un pare-feu.

Pour plus d'informations, voir les sous-rubriques suivantes:

Autorisation de canal

Lorsque vous envoyez ou recevez un message via un canal, vous avez besoin d'un ID utilisateur ayant accès à diverses ressources IBM WebSphere MQ .

Pour recevoir des messages au moment de l'opération PUT pour les agents MCA, vous pouvez utiliser l'ID utilisateur associé à l'agent MCA ou l'ID utilisateur associé au message.

Au moment de la connexion, vous pouvez mapper l'ID utilisateur vérifié à un autre utilisateur, à l'aide des enregistrements d'authentification de canal **CHLAUTH** .

Dans WebSphere MQ, les canaux peuvent être protégés par le support SSL ou TLS.

Les ID utilisateur associés aux canaux d'envoi et de réception, à l'exception du canal émetteur où l'attribut MCAUSER n'est pas utilisé, requièrent l'accès aux ressources suivantes:

- L'ID utilisateur associé à un canal émetteur requiert l'accès au gestionnaire de files d'attente, à la file d'attente de transmission, à la file d'attente de rebut et à toute autre ressource requise par les exits de canal.
- L'ID utilisateur MCAUSER d'un canal récepteur requiert les droits *+ setall* .

  En effet, le canal récepteur doit créer le MQMD complet, y compris toutes les zones de contexte, à l'aide des données qu'il a reçues du canal émetteur distant.

  Le gestionnaire de files d'attente requiert donc que l'utilisateur exécutant cette activité dispose des droits *+ setall* . Ces droits *+ setall* doivent être accordés à l'utilisateur pour:

  – Toutes les files d'attente dans lesquelles le canal récepteur insère des messages de manière valide.
  – Objet gestionnaire de files d'attente. Pour plus d'informations, voir Autorisations de contexte .
- L'ID utilisateur MCAUSER d'un canal récepteur sur lequel l'émetteur a demandé un message de rapport COA requiert le droit *+ passid* sur la file d'attente de transmission qui renvoie le message de rapport. Sans ces droits, les messages d'erreur AMQ8077 sont consignés.
- Avec l'ID utilisateur associé au canal récepteur, vous pouvez ouvrir les files d'attente cible pour y placer des messages.

  Cela implique l'interface MQI (Message queuing Interface), de sorte que des vérifications de contrôle d'accès supplémentaires peuvent être nécessaires si vous n'utilisez pas WebSphere MQ Object Authority Manager (OAM). Vous pouvez indiquer si les vérifications d'autorisation sont effectuées sur l'ID utilisateur associé à l'agent MCA (comme décrit dans cette rubrique) ou sur l'ID utilisateur associé au message (à partir de la zone MQMD UserIdentifier).

  Pour les types de canal auxquels il s'applique, le paramètre **PUTAUT** d'une définition de canal indique l'ID utilisateur utilisé pour ces vérifications.

  – Le canal utilise par défaut le compte de service du gestionnaire de files d'attente, qui dispose de droits d'administration complets et ne nécessite aucune autorisation spéciale

    Dans le cas des canaux de connexion serveur, les connexions d'administration sont bloquées par défaut par les règles CHLAUTH et nécessitent une mise à disposition explicite.

    Les canaux de type récepteur, demandeur et récepteur de cluster permettent l'administration locale par tout gestionnaire de files d'attente adjacent, sauf si l'administrateur prend des mesures pour restreindre cet accès.
  – Si vous utilisez un ID utilisateur qui ne dispose pas des privilèges d'administration WebSphere , vous devez accorder les droits dsp et ctrlx pour le canal à cet ID utilisateur pour que le canal fonctionne. L'attribut MCAUSER n'est pas utilisé pour le type de canal SDR.
  – Si vous utilisez l'ID utilisateur associé au message, il est probable que l'ID utilisateur provient d'un système distant.

    Cet ID utilisateur de système distant doit être reconnu par le système cible. Par exemple, exécutez les commandes suivantes:

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

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

où *Profil* est un canal.

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

où *Profil* est une file d'attente de rebut, si elle est définie.

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

où *Profil* est une liste de files d'attente autorisées.

Avertissement : Soyez prudent lorsque vous autorisez un ID utilisateur à placer des messages dans la file d'attente de commandes ou dans d'autres files d'attente système sensibles.

L'ID utilisateur associé à l'agent MCA dépend du type d'agent MCA. Il existe deux types d'agent MCA:

Agent MCA appelant
Les agents MCA qui initient un canal. Les agents MCA appelants peuvent être démarrés en tant que processus individuels, en tant qu'unités d'exécution de l'initiateur de canal ou en tant qu'unités d'exécution d'un pool de processus. L'ID utilisateur utilisé est l'ID utilisateur associé au processus parent (initiateur de canal) ou l'ID utilisateur associé au processus qui démarre l'agent MCA.

Agent MCA répondeur
Les agents MCA répondeurs sont des agents MCA démarrés à la suite d'une demande d'un agent MCA appelant. Les agents MCA répondeurs peuvent être démarrés en tant que processus individuels, en tant qu'unités d'exécution du programme d'écoute ou en tant qu'unités d'exécution d'un pool de processus. L'ID utilisateur peut être l'un des types suivants (dans cet ordre de préférence):

1. Sur APPC, l'agent MCA appelant peut indiquer l'ID utilisateur à utiliser pour l'agent MCA répondeur. Cet ID est appelé ID utilisateur réseau et s'applique uniquement aux canaux démarrés en tant que processus individuels. Définissez l'ID utilisateur réseau à l'aide du paramètre USERID de la définition de canal.
2. Si le paramètre **USERID** n'est pas utilisé, la définition de canal de l'agent MCA répondeur peut indiquer l'ID utilisateur que l'agent MCA doit utiliser. Définissez l'ID utilisateur à l'aide du paramètre **MCAUSER** de la définition de canal.
3. Si l'ID utilisateur n'a été défini par aucune des deux méthodes précédentes, l'ID utilisateur du processus qui démarre l'agent MCA ou l'ID utilisateur du processus parent (le programme d'écoute) est utilisé.

Concepts associés

«Enregistrements d'authentification de canal», à la page 41
Pour exercer un contrôler plus précis sur les accès accordés aux systèmes en cours de connexion au niveau d'un canal, vous pouvez utiliser les enregistrements d'authentification de canal.

Propriétés de l'enregistrement d'authentification de canal

Protection des définitions d'initialisateur de canal

Seuls les membres du groupe mqm peuvent manipuler les initiateurs de canal.

Les initiateurs de canal IBM WebSphere MQ ne sont pas des objets IBM WebSphere MQ ; leur accès n'est pas contrôlé par la méthode d'accès aux objets (OAM). IBM WebSphere MQ n'autorise pas les utilisateurs ou les applications à manipuler ces objets, sauf si leur ID utilisateur est membre du groupe mqm. Si vous disposez d'une application qui émet la commande PCF `StartChannelInitiator`, l'ID utilisateur spécifié dans le descripteur de message PCF doit être membre du groupe mqm sur le gestionnaire de files d'attente cible.

Un ID utilisateur doit également être membre du groupe mqm sur la machine cible pour émettre les commandes MQSC équivalentes via la commande Escape PCF ou à l'aide de `runmqsc` en mode indirect.

Files d'attente de transmission

Les gestionnaires de files d'attente placent automatiquement les messages éloignés dans une file d'attente de transmission ; aucun droit spécial n'est requis à cet effet.

Toutefois, si vous devez placer un message directement dans une file d'attente de transmission, vous devez disposer d'une autorisation spéciale ; voir Tableau 10, à la page 95.

Exits de canal

Si les enregistrements d'authentification de canal ne conviennent pas, vous pouvez utiliser des exits de canal pour une sécurité accrue. Un exit de sécurité établit une connexion sécurisée entre deux programmes d'exit de sécurité. Un programme est destiné à l'agent MCA émetteur et un programme est destiné à l'agent MCA récepteur.

Pour plus d'informations sur les exits de canal, voir «Programmes d'exit de canal», à la page 68 .

Protection des canaux avec SSL

La prise en charge de SSL dans IBM WebSphere MQ utilise l'objet d'informations d'authentification du gestionnaire de files d'attente et diverses commandes MQSC. Vous devez également tenir compte de votre utilisation des certificats numériques.

Commandes et attributs pour la prise en charge de SSL

Le protocole SSL (Secure Sockets Layer) offre une sécurité de canal, avec une protection contre l'écoute clandestine, la contrefaçon et l'usurpation d'identité. La prise en charge de SSL par IBM WebSphere MQ vous permet de spécifier, dans la définition de canal, qu'un canal particulier utilise la sécurité SSL. Vous pouvez également spécifier les détails du type de sécurité de votre choix, par exemple l'algorithme de chiffrement que vous souhaitez utiliser.

Les commandes MQSC suivantes prennent en charge SSL:

ALTER AUTHINFO
Modifie les attributs d'un objet d'informations d'authentification.

DEFINE AUTHINFO
Crée un objet d'informations d'authentification.

DELETE AUTHINFO
Supprime un objet d'informations d'authentification.

INFORMATIONS D'AUTHENTIFICATION D'AFFICHAGE
Affiche les attributs d'un objet d'informations d'authentification spécifique.

Les paramètres de gestionnaire de files d'attente suivants prennent en charge SSL:

SSLCRLNL
L'attribut SSLCRLNL spécifie une liste de noms d'objets d'informations d'authentification qui sont utilisés pour fournir des emplacements de révocation de certificat afin de permettre une vérification améliorée des certificats TLS/SSL.

SSLCRYP
Sur les systèmes Windows, UNIX and Linux , définit l'attribut de gestionnaire de files d'attente SSLCryptoHardware . Cet attribut est le nom de la chaîne de paramètres que vous pouvez utiliser pour configurer le matériel cryptographique que vous avez sur votre système.

SSLEV
Détermine si un message d'événement SSL est signalé si un canal utilisant SSL ne parvient pas à établir une connexion SSL.

SSLFIPS
Indique si seuls les algorithmes certifiés FIPS doivent être utilisés si la cryptographie est effectuée dans IBM WebSphere MQ, plutôt que dans le matériel de cryptographie. Si le matériel de cryptographie est configuré, les modules de cryptographie fournis par le produit matériel sont utilisés et ceux-ci peuvent être certifiés FIPS à un niveau particulier. Cela dépend du produit matériel utilisé.

SSLKEYR
Sur les systèmes Windows,UNIX and Linux , associe un référentiel de clés à un gestionnaire de files d'attente. La base de données de clés est conservée dans une base de données de clés *GSKit* . (IBM Global Security Kit (GSKit) vous permet d'utiliser la sécurité SSL sur les systèmes WindowsetUNIX and Linux .)

SSLRKEYC
Nombre d'octets à envoyer et à recevoir dans une conversation SSL avant la renégociation de la clé secrète. Le nombre d'octets inclut les informations de contrôle envoyées par l'agent MCA.

Les paramètres de canal suivants prennent en charge SSL:

SSLCAUTH
Indique si IBM WebSphere MQ requiert et valide un certificat du client SSL.

SSLCIPH
Indique la force et la fonction de chiffrement (CipherSpec), par exemple NULL_MD5 ou RC4_MD5_US. Le CipherSpec doit correspondre aux deux extrémités du canal.

SSLPEER
Indique le nom distinctif (identificateur unique) des partenaires autorisés.

Cette section décrit les commandes `setmqaut`, `dspmqaut`, `dmpmqaut`, `rcrmqobj`, `rcdmqimg`et `dspmqfls` pour la prise en charge de l'objet d'informations d'authentification. Il décrit également la commande iKeycmd pour la gestion des certificats sur les systèmes UNIX and Linux et l'outil runmqakm pour la gestion des certificats sur les systèmes UNIX, Linux et Windows . Reportez-vous aux sections suivantes :

- setmqaut
- dspmqaut
- dmpmqaut
- rcrmqobj
- rcdmqimg
- dspmqfls
- Gestion des clés et des certificats

Pour une présentation de la sécurité des canaux à l'aide de SSL, voir

- «Prise en charge de IBM WebSphere MQ pour SSL et TLS», à la page 24

Pour plus de détails sur les commandes MQSC associées à SSL, voir

- ALTER AUTHINFO
- DEFINE AUTHINFO
- DELETE AUTHINFO
- DISPLAY AUTHINFO

Pour plus de détails sur les commandes PCF associées à SSL, voir

- Change, Copy, and Create Authentication Information Object
- Delete Authentication Information Object
- Inquire Authentication Information Object

Certificats autosignés et signés par une autorité de certification

Il est important de planifier votre utilisation des certificats numériques, à la fois lorsque vous développez et testez votre application, et pour son utilisation en production. Vous pouvez utiliser des certificats signés par une autorité de certification ou des certificats autosignés, en fonction de l'utilisation des gestionnaires de files d'attente et des applications client.

Certificats signés par une autorité de certification
Pour les systèmes de production, procurez-vous vos certificats auprès d'une autorité de certification digne de confiance. Lorsque vous obtenez un certificat d'une autorité de certification externe, vous payez pour le service.

certificats autosignés
Lors du développement de votre application, vous pouvez utiliser des certificats autosignés ou des certificats émis par une autorité de certification locale, en fonction de la plateforme:

Sur les systèmes Windows, UNIXet Linux , vous pouvez utiliser des certificats autosignés. Voir «Création d'un certificat personnel autosigné sur les systèmes UNIX, Linux, and Windows», à la page 127 pour des instructions.

Les certificats autosignés ne conviennent pas à une utilisation en production pour les raisons suivantes :

- Les certificats autosignés ne peuvent pas être révoqués, ce qui peut permettre à un agresseur de usurper une identité après qu'une clé privée a été compromise. Les autorités de certification peuvent révoquer un certificat compromis, pour en empêcher toute utilisation future. Les certificats signés par une autorité de certification sont donc plus sûrs à utiliser dans un environnement de production, bien que les certificats autosignés soient plus pratiques pour un système de test.
- Les certificats autosignés n'arrivent jamais à expiration. Ce comportement est pratique et sûr dans un environnement de test, mais dans un environnement de production, les certificats restent ouverts et donc sujets à des violations de sécurité. Ce risque est aggravé du fait que les certificats autosignés ne peuvent pas être révoqués.
- Un certificat autosigné est utilisé à la fois comme certificat personnel et comme certificat d'autorité de certification racine (ou ancrage sécurisé). Un utilisateur avec un certificat personnel autosigné doit pouvoir l'utiliser pour signer d'autres certificats personnels. En général, cela n'est pas vrai des certificats personnels émis par une autorité de certification et représente un risque important.

CipherSpecs et certificats numériques

Seul un sous-ensemble des CipherSpecs pris en charge peut être utilisé avec tous les types de certificat numérique pris en charge. Il est donc nécessaire de choisir un CipherSpec approprié pour votre certificat numérique. De même, si la stratégie de sécurité de votre organisation requiert l'utilisation d'un CipherSpec particulier, vous devez obtenir un certificat numérique approprié.

Pour plus d'informations sur la relation entre les CipherSpecs et les certificats numériques, voir «Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36

Règles de validation de certificat

La norme IETF RFC 5280 spécifie une série de règles de validation de certificat que les logiciels d'application conformes doivent implémenter afin d'éviter les attaques d'usurpation d'identité. Un ensemble de règles de validation de certificat est appelé règle de validation de certificat. Pour plus d'informations sur les règles de validation de certificat dans WebSphere MQ, voir «Règles de validation de certificat dans IBM WebSphere MQ», à la page 35.

Services de sécurité SNA LU 6.2

L'unité logique SNA 6.2 offre la cryptographie au niveau de la session, l'authentification au niveau de la session et l'authentification au niveau de la conversation.

Remarque : Cette collection de rubriques suppose que vous avez une connaissance de base de l'architecture SNA (Systems Network Architecture). L'autre documentation mentionnée dans cette section contient une brève introduction aux concepts et à la terminologie pertinents. Si vous avez besoin d'une introduction technique plus complète à SNA, voir *Systems Network Architecture Technical Overview*, GC30-3073.

SNA LU 6.2 fournit trois services de sécurité:

- Cryptographie de niveau session

- Authentification au niveau de la session
- Authentification au niveau de la conversation

Pour la cryptographie au niveau de la session et l'authentification au niveau de la session, SNA utilise l'algorithme *Data Encryption Standard (DES)* . L'algorithme DES est un algorithme de chiffrement par blocs qui utilise une clé symétrique pour le chiffrement et le déchiffrement des données. La longueur du bloc et de la clé est de 8 octets.

Cryptographie de niveau session
La *cryptographie au niveau de la session* chiffre et déchiffre les données de session à l'aide de l'algorithme DES. Il peut donc être utilisé pour fournir un service de confidentialité de niveau liaison sur les canaux SNA LU 6.2 .

Les unités logiques peuvent fournir une cryptographie de données obligatoire (ou obligatoire), une cryptographie de données sélective ou aucune cryptographie de données.

Dans une *session cryptographique obligatoire*, une unité logique chiffre toutes les unités de demande de données sortantes et déchiffre toutes les unités de demande de données entrantes.

Dans une *session cryptographique sélective*, une unité logique chiffre uniquement les unités de demande de données spécifiées par le programme de transaction d'envoi (TP). L'unité logique émettrice signale que les données sont chiffrées en définissant un indicateur dans l'en-tête de demande. En vérifiant cet indicateur, la LU réceptrice peut savoir quelles unités de requête déchiffrer avant de les transmettre à la TP réceptrice.

Dans un réseau SNA, les agents MCA WebSphere MQ sont des programmes de transaction. Les agents MCA ne demandent pas de chiffrement pour les données qu'ils envoient. La cryptographie sélective de données n'est donc pas une option ; seule la cryptographie de données obligatoire ou aucune cryptographie de données est possible sur une session.

Pour plus d'informations sur l'implémentation de la cryptographie de données obligatoire, voir la documentation de votre sous-système SNA. Reportez-vous à la même documentation pour plus d'informations sur les formes de chiffrement plus fortes pouvant être utilisées sur votre plateforme, comme le chiffrement Triple DES 24 octets sur z/OS.

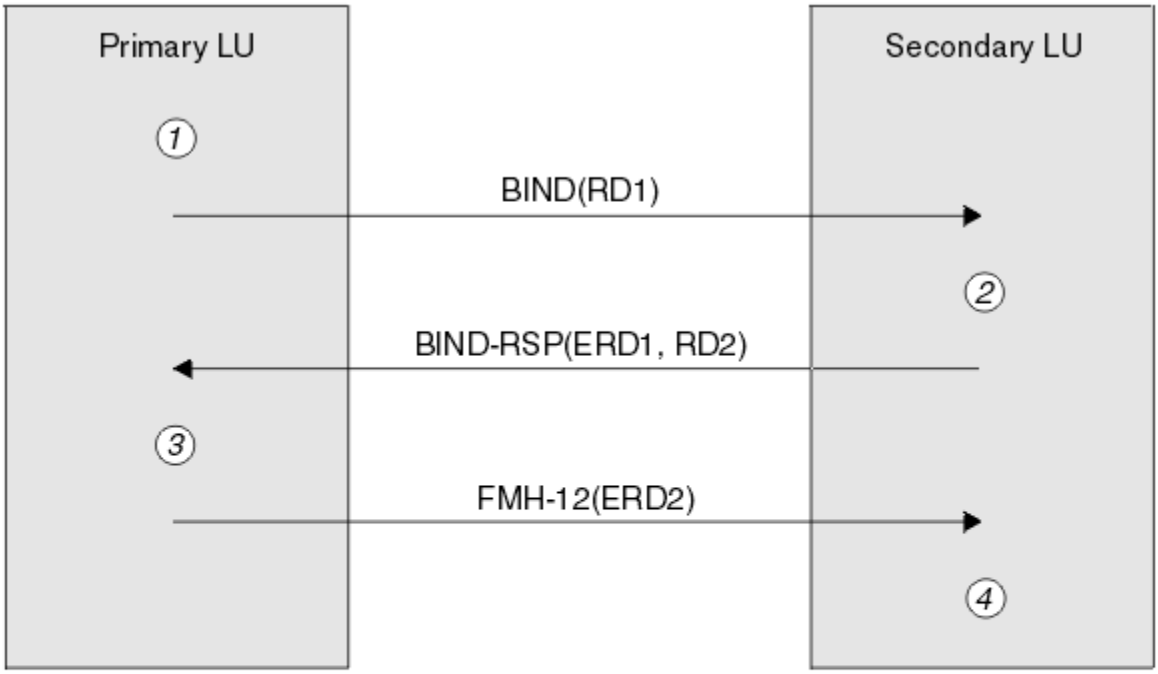
Pour plus d'informations sur la cryptographie de niveau session, voir *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Authentification au niveau de la session
L' *authentification au niveau de la session* est un protocole de sécurité au niveau de la session qui permet à deux unités logiques de s'authentifier l'une l'autre lors de l'activation d'une session. Elle est également appelée *vérification LU-LU*.

Etant donné qu'une unité logique est effectivement la "passerelle" dans un système à partir du réseau, vous pouvez considérer que ce niveau d'authentification est suffisant dans certaines circonstances. Par exemple, si votre gestionnaire de files d'attente doit échanger des messages avec un gestionnaire de files d'attente éloignées qui s'exécute dans un environnement contrôlé et sécurisé, vous pouvez être prêt à faire confiance aux identités des autres composants du système distant une fois que l'unité logique a été authentifiée.

L'authentification au niveau de la session est effectuée par chaque unité logique qui vérifie le mot de passe de son partenaire. Le mot de passe est appelé *mot de passe LU-LU* car un mot de passe est établi entre chaque paire d'unités logiques. Le mode d'établissement d'un mot de passe LU-LU dépend de l'implémentation et est hors de la portée de SNA.

La Figure 10, à la page 79 illustre les flux d'authentification au niveau de la session.



Legend:

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

Figure 10. Flux pour l'authentification au niveau de la session

Le protocole d'authentification au niveau de la session est le suivant. Les nombres de la procédure correspondent aux nombres de Figure 10, à la page 79.

1. L'unité logique principale génère une valeur de données aléatoire (RD1) et l'envoie à l'unité logique secondaire dans la demande BIND.
2. Lorsque la LU secondaire reçoit la requête BIND avec les données aléatoires, elle chiffre les données à l'aide de l'algorithme DES avec sa copie du mot de passe LU-LU comme clé. L'unité logique secondaire génère ensuite une deuxième valeur de données aléatoires (RD2) et l'envoie, avec les données chiffrées (ERD1), à l'unité logique principale dans la réponse BIND.
3. Lorsque l'unité logique principale reçoit la réponse BIND, elle calcule sa propre version des données chiffrées à partir des données aléatoires qu'elle a générées à l'origine. Pour ce faire, il utilise l'algorithme DES avec sa copie du mot de passe LU-LU comme clé. Il compare ensuite sa version aux données chiffrées qu'il a reçues dans la réponse BIND. Si les deux valeurs sont identiques, l'unité logique principale sait que l'unité logique secondaire possède le même mot de passe et que l'unité logique secondaire est authentifiée. Si les deux valeurs ne correspondent pas, l'unité logique principale met fin à la session.

   L'unité logique principale chiffre ensuite les données aléatoires qu'elle a reçues dans la réponse BIND et envoie les données chiffrées (ERD2) à l'unité logique secondaire dans un en-tête de gestion de fonction 12 (FMH-12).
4. Lorsque l'unité logique secondaire reçoit le FMH-12, elle calcule sa propre version des données chiffrées à partir des données aléatoires qu'elle a générées. Il compare ensuite sa version aux données chiffrées qu'il a reçues dans le FMH-12. Si les deux valeurs sont identiques, l'unité logique principale est authentifiée. Si les deux valeurs ne correspondent pas, l'unité logique secondaire met fin à la session.

Dans une version améliorée du protocole, qui offre une meilleure protection contre les attaques de l'homme du milieu, la LU secondaire calcule un code d'authentification de message (MAC) DES à partir de RD1, RD2et du nom qualifié complet de la LU secondaire, en utilisant sa copie du mot de passe LU-LU comme clé. L'unité logique secondaire envoie l'adresse MAC à l'unité logique principale dans la réponse BIND au lieu de ERD1.

L'unité logique principale authentifie l'unité logique secondaire en calculant sa propre version du MAC, qu'elle compare au MAC reçu dans la réponse BIND. L'unité logique principale calcule ensuite une seconde adresse MAC à partir de RD1 et RD2, et envoie l'adresse MAC à l'unité logique secondaire dans FMH-12 au lieu de ERD2.

L'unité logique secondaire authentifie l'unité logique principale en calculant sa propre version du deuxième MAC, qu'elle compare avec le MAC reçu dans le FMH-12.

Pour plus d'informations sur la configuration de l'authentification au niveau de la session, voir la documentation de votre sous-système SNA. Pour plus d'informations sur l'authentification de niveau session, voir *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808.

Authentification au niveau de la conversation
Lorsqu'un programme transactionnel local tente d'allouer une conversation avec un programme transactionnel partenaire, l'unité logique locale envoie une demande de connexion à l'unité logique partenaire, en lui demandant de connecter le programme transactionnel partenaire. Dans certaines circonstances, la demande d'association peut contenir des informations de sécurité que l'unité logique partenaire peut utiliser pour authentifier le TP local. Il s'agit de l' *authentification au niveau de la conversation*ou de la *vérification de l'utilisateur final*.

Les rubriques suivantes décrivent comment IBM WebSphere MQ fournit la prise en charge de l'authentification au niveau de la conversation.

Pour plus d'informations sur l'authentification au niveau de la conversation, voir *Systems Network Architecture LU 6.2 Reference: Peer Protocols*, SC31-6808. Pour des informations spécifiques à z/OS, voir *z/OS MVS Planning: APPC/MVS Management*, SA22-7599.

Pour plus d'informations sur CPI-C, voir *Common Programming Interface Communications CPI-C Specification*, SC31-6180. Pour plus d'informations sur APPC/MVS TP Conversation Callable Services, voir *z/OS MVS Programming: Writing Transaction Programs for APPC/MVS*, SA22-7621.

Prise en charge de l'authentification au niveau de la conversation dans IBM WebSphere MQ sur les systèmes UNIX et Windows
Utilisez cette rubrique pour obtenir une vue d'ensemble du fonctionnement de l'authentification au niveau de la conversation sur UNIX, Linux, and Windows.

La prise en charge de l'authentification au niveau de la conversation dans IBM WebSphere MQ for WebSphere MQ sur les systèmes UNIX et WebSphere MQ for Windows est illustrée dans la Figure 11, à la page 81. Les numéros du diagramme correspondent aux numéros de la description qui suit.

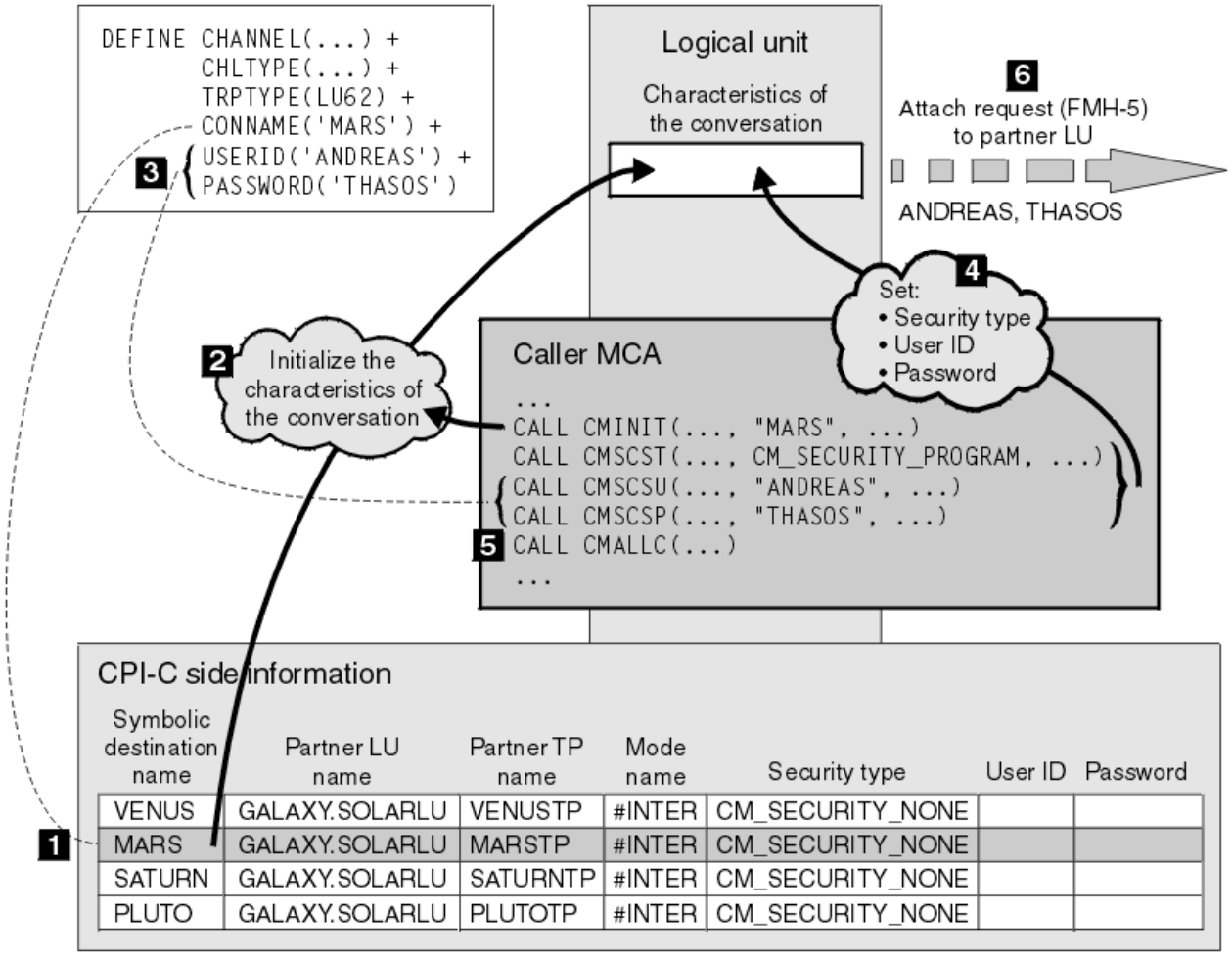


Figure 11. WebSphere MQ prise en charge de l'authentification au niveau de la conversation

Sur les systèmes IBM i, UNIX et Windows , un agent MCA utilise des appels CPI-C (Common Programming Interface Communications) pour communiquer avec un agent MCA partenaire sur un réseau SNA. Dans la définition de canal à l'extrémité appelante d'un canal, la valeur du paramètre CONNAME est un nom de destination symbolique qui identifie une entrée d'informations côté CPI-C (1). Cette entrée indique:

- Nom de l'unité logique partenaire
- Nom du programme transactionnel partenaire, qui est un agent MCA répondeur
- Nom du mode à utiliser pour la conversation

Une entrée d'informations complémentaires peut également spécifier les informations de sécurité suivantes:

- Type de sécurité.

  Les types de sécurité couramment implémentés sont CM_SECURITY_NONE, CM_SECURITY_PROGRAM et CM_SECURITY_SAME, mais d'autres sont définis dans la spécification CPI-C.
- ID utilisateur.
- Un mot de passe.

Un agent MCA appelant se prépare à allouer une conversation avec un agent MCA répondeur en émettant l'appel CPI-C CMINIT, en utilisant la valeur de CONNAME comme l'un des paramètres de l'appel. L'appel CMINIT identifie, pour le bénéfice de l'unité logique locale, l'entrée d'informations complémentaires que l'agent MCA a l'intention d'utiliser pour la conversation. L'unité logique locale utilise les valeurs de cette entrée pour initialiser les caractéristiques de la conversation (2).

L'agent MCA appelant vérifie ensuite les valeurs des paramètres USERID et PASSWORD dans la définition de canal (3). Si USERID est défini, l'agent MCA appelant émet les appels CPI-C suivants (4):

- CMSCST, pour définir le type de sécurité de la conversation sur CM_SECURITY_PROGRAM.
- CMSCSU, pour définir l'ID utilisateur de la conversation sur la valeur USERID.
- CMSCSP, pour définir le mot de passe de la conversation sur la valeur PASSWORD. CMSCSP n'est pas appelé sauf si PASSWORD est défini.

Le type de sécurité, l'ID utilisateur et le mot de passe définis par ces appels remplacent toutes les valeurs précédemment acquises à partir de l'entrée d'informations complémentaires.

L'agent MCA appelant émet ensuite l'appel CPI-C CMALLC pour allouer la conversation (5). En réponse à cet appel, l'unité logique locale envoie une demande d'association (Function Management Header 5, ou FMH-5) à l'unité logique partenaire (6).

Si l'unité logique partenaire accepte un ID utilisateur et un mot de passe, les valeurs USERID et PASSWORD sont incluses dans la demande d'association. Si l'unité logique partenaire n'accepte pas d'ID utilisateur et de mot de passe, les valeurs ne sont pas incluses dans la demande d'association. L'unité logique locale détermine si l'unité logique partenaire accepte un ID utilisateur et un mot de passe dans le cadre d'un échange d'informations lorsque les unités logiques se lient pour former une session.

Dans une version ultérieure de la demande d'association, un remplacement de mot de passe peut se produire entre les unités logiques au lieu d'un mot de passe clair.Un remplaçant de mot de passe est un code d'authentification de message DES (MAC) ou un résumé de message SHA-1 , formé à partir du mot de passe. Les remplacements de mot de passe ne peuvent être utilisés que si les deux unités logiques les prennent en charge.

Lorsque l'unité logique partenaire reçoit une demande d'association entrante contenant un ID utilisateur et un mot de passe, elle peut utiliser l'ID utilisateur et le mot de passe à des fins d'identification et d'authentification. En faisant référence aux listes de contrôle d'accès, l'unité logique partenaire peut également déterminer si l'ID utilisateur a le droit d'allouer une conversation et de connecter l'agent MCA répondeur.

En outre, l'agent MCA répondeur peut s'exécuter sous l'ID utilisateur inclus dans la demande d'association.Dans ce cas, l'ID utilisateur devient l'ID utilisateur par défaut pour l'agent MCA répondeur et est utilisé pour les vérifications des droits d'accès lorsque l'agent MCA tente de se connecter au gestionnaire de files d'attente. Il peut également être utilisé pour les vérifications des droits d'accès ultérieures lorsque l'agent MCA tente d'accéder aux ressources du gestionnaire de files d'attente.

La manière dont un ID utilisateur et un mot de passe dans une demande de connexion peuvent être utilisés pour l'identification, l'authentification et le contrôle d'accès dépend de l'implémentation. Pour des informations spécifiques à votre sous-système SNA, reportez-vous à la documentation appropriée.

Si USERID n'est pas défini, l'agent MCA appelant n'appelle pas CMSCST, CMSCSU et CMSCSP. Dans ce cas, les informations de sécurité qui circulent dans une demande d'association sont uniquement déterminées par ce qui est spécifié dans l'entrée d'informations complémentaires et par ce que l'unité logique partenaire accepte.

Sécurité des clusters de gestionnaires de files d'attente

Bien que les clusters de gestionnaires de files d'attente soient pratiques à utiliser, vous devez accorder une attention particulière à leur sécurité.

Un *cluster de gestionnaires de files d'attente* est un réseau de gestionnaires de files d'attente associés de manière logique. Un gestionnaire de files d'attente qui est membre d'un cluster est appelé *gestionnaire de files d'attente de cluster*.

Une file d'attente appartenant à un gestionnaire de files d'attente de cluster peut être rendue connue des autres gestionnaires de files d'attente du cluster. Cette file d'attente est appelée *file d'attente de cluster*. Tout gestionnaire de files d'attente d'un cluster peut envoyer des messages à des files d'attente de cluster sans avoir besoin de l'un des éléments suivants:

- Une définition de file d'attente éloignée explicite pour chaque file d'attente de cluster

- Canaux définis explicitement vers et depuis chaque gestionnaire de files d'attente éloignées
- Une file d'attente de transmission distincte pour chaque canal sortant

Vous pouvez créer un cluster dans lequel au moins deux gestionnaires de files d'attente sont des clones. Cela signifie qu'ils possèdent des instances des mêmes files d'attente locales, y compris des files d'attente locales déclarées comme files d'attente de cluster, et qu'ils peuvent prendre en charge des instances des mêmes applications serveur.

Lorsqu'une application connectée à un gestionnaire de files d'attente de cluster envoie un message à une file d'attente de cluster comportant une instance sur chacun des gestionnaires de files d'attente clonés, IBM WebSphere MQ décide à quel gestionnaire de files d'attente elle doit être envoyée. Lorsque de nombreuses applications envoient des messages à la file d'attente de cluster, WebSphere MQ équilibre la charge de travail entre chacun des gestionnaires de files d'attente ayant une instance de la file d'attente. Si l'un des systèmes hébergeant un gestionnaire de files d'attente cloné est défaillant, WebSphere MQ continue d'équilibrer la charge de travail entre les gestionnaires de files d'attente restants jusqu'à ce que le système défaillant soit redémarré.

Si vous utilisez des clusters de gestionnaires de files d'attente, vous devez prendre en compte les problèmes de sécurité suivants:

- Autoriser uniquement les gestionnaires de files d'attente sélectionnés à envoyer des messages à votre gestionnaire de files d'attente
- Autoriser uniquement les utilisateurs sélectionnés d'un gestionnaire de files d'attente éloignées à envoyer des messages à une file d'attente de votre gestionnaire de files d'attente
- Autoriser les applications connectées à votre gestionnaire de files d'attente à envoyer des messages uniquement aux files d'attente éloignées sélectionnées

Ces considérations sont pertinentes même si vous n'utilisez pas de clusters, mais elles deviennent plus importantes si vous utilisez des clusters.

Si une application peut envoyer des messages à une file d'attente de cluster, elle peut envoyer des messages à n'importe quelle autre file d'attente de cluster sans avoir besoin de définitions de file d'attente éloignée, de files d'attente de transmission ou de canaux supplémentaires. Il est donc plus important de déterminer si vous devez restreindre l'accès aux files d'attente de cluster sur votre gestionnaire de files d'attente et de limiter les files d'attente de cluster auxquelles vos applications peuvent envoyer des messages.

Des considérations de sécurité supplémentaires s'appliquent uniquement si vous utilisez des clusters de gestionnaires de files d'attente:

- Autoriser uniquement les gestionnaires de files d'attente sélectionnés à rejoindre un cluster
- Forcer les gestionnaires de files d'attente indésirables à quitter un cluster

Pour plus d'informations sur toutes ces considérations, voir Maintien de la sécurité des clusters.

Tâches associées

«Empêcher les gestionnaires de files d'attente de recevoir des messages», à la page 259
Vous pouvez empêcher un gestionnaire de files d'attente de cluster de recevoir des messages qu'il n'est pas autorisé à recevoir à l'aide de programmes d'exit.

Sécurité pour la publication / abonnement IBM WebSphere MQ

Des considérations de sécurité supplémentaires sont à prendre en compte si vous utilisez la fonction de publication / abonnement IBM WebSphere MQ .

Dans un système de publication / abonnement, il existe deux types d'application: le diffuseur de publications et l'abonné. Les *diffuseurs de publications* fournissent des informations sous la forme de messages IBM WebSphere MQ . Lorsqu'un diffuseur de publications publie un message, il spécifie une *rubrique*qui identifie l'objet des informations contenues dans le message.

Les *abonnés* sont les consommateurs des informations qui sont publiées. Un abonné spécifie les rubriques qui l'intéressent en s'y abonnant.

Le *gestionnaire de files d'attente* est une application fournie avec IBM WebSphere MQ Publish / Subscribe. Il reçoit les messages publiés des diffuseurs de publications et les demandes d'abonnement des abonnés, et achemine les messages publiés vers les abonnés. Un abonné reçoit des messages uniquement sur les sujets auxquels il s'est abonné.

Pour plus d'informations, voir Sécurité de publication / abonnement.

Sécurité de multidiffusion

Utilisez ces informations pour comprendre pourquoi des processus de sécurité peuvent être nécessaires avec IBM WebSphere MQ Multicast.

IBM WebSphere MQ Multicast ne dispose pas de sécurité intégrée. Les contrôles de sécurité sont gérés dans le gestionnaire de files d'attente au moment de l'opération MQOPEN et le paramètre de zone MQMD est géré par le client. Certaines applications du réseau peuvent ne pas être des applications IBM WebSphere MQ (par exemple, des applications LLM, voir Interopérabilité multidiffusion avec WebSphere MQ Low Latency Messaging pour plus d'informations). Par conséquent, vous pouvez être amené à implémenter vos propres procédures de sécurité car les applications de réception ne peuvent pas être certaines de la validité des zones de contexte.

Il existe trois processus de sécurité à prendre en compte:

Contrôle d'accès

Le contrôle d'accès dans IBM WebSphere MQ est basé sur les ID utilisateur. Pour plus d'informations sur ce sujet, voir «Contrôle d'accès pour les clients», à la page 60.

Sécurité réseau

Un réseau isolé peut être une option de sécurité viable pour empêcher les faux messages. Il est possible qu'une application de l'adresse de groupe de multidiffusion publie des messages malveillants à l'aide de fonctions de communication natives, qui ne peuvent pas être distinguées des messages MQ car elles proviennent d'une application de la même adresse de groupe de multidiffusion.

Il est également possible qu'un client sur l'adresse de groupe de multidiffusion reçoive des messages destinés à d'autres clients sur la même adresse de groupe de multidiffusion.

L'isolement du réseau de multidiffusion garantit que seuls les clients et les applications valides y ont accès. Cette précaution de sécurité peut empêcher l'entrée de messages malveillants et la sortie d'informations confidentielles.

Pour plus d'informations sur les adresses réseau de groupe de multidiffusion, voir: Définition du réseau approprié pour le trafic de multidiffusion

Signatures numériques

Une signature numérique est formée par le chiffrement d'une représentation d'un message. Le chiffrement utilise la clé privée du signataire et, pour des raisons d'efficacité, opère généralement sur un résumé de message plutôt que sur le message lui-même. La signature numérique d'un message avant une opération MQPUT est une bonne précaution de sécurité, mais ce processus peut avoir un impact négatif sur les performances s'il existe un volume important de messages.

Les signatures numériques varient en fonction des données en cours de signature. Si deux messages différents sont signés numériquement par la même entité, les deux signatures diffèrent, mais les deux signatures peuvent être vérifiées avec la même clé publique, c'est-à-dire la clé publique de l'entité qui a signé les messages.

Comme indiqué précédemment dans cette section, il est possible qu'une application sur l'adresse de groupe de multidiffusion publie des messages malveillants à l'aide de fonctions de communication natives, qui ne peuvent pas être distinguées des messages MQ . Les signatures numériques fournissent une preuve de l'origine, et seul l'expéditeur connaît la clé privée, ce qui fournit des preuves solides que l'expéditeur est l'émetteur du message.

Pour plus d'informations sur ce sujet, voir «Concepts cryptographiques», à la page 7.

Pare-feux et passe-système Internet

Normalement, vous utilisez un pare-feu pour empêcher l'accès à partir d'adresses IP hostiles, par exemple lors d'une attaque par refus de service. Toutefois, vous devrez peut-être temporairement bloquer les adresses IP dans IBM WebSphere MQ, peut-être en attendant qu'un administrateur de sécurité mette à jour les règles de pare-feu.

Pour bloquer une ou plusieurs adresses IP, créez un enregistrement d'authentification de canal de type BLOCKADDR ou ADDRESSMAP. Pour plus d'informations, voir «Blocage d'adresses IP spécifiques», à la page 190.

Sécurité pour IBM WebSphere MQ Internet Pass-thru

Le passe-système Internet peut simplifier la communication via un pare-feu, mais cela a des implications sur la sécurité.

IBM WebSphere MQ Internet passe-système est une extension de produit de base IBM WebSphere MQ fournie dans SupportPac MS81.

WebSphere MQ Internet Pass-thru permet à deux gestionnaires de files d'attente d'échanger des messages ou à une application client WebSphere MQ de se connecter à un gestionnaire de files d'attente sur Internet sans nécessiter de connexion TCP/IP directe. Cela est utile si un pare-feu interdit une connexion TCP/IP directe entre deux systèmes. Le passage du protocole de canal WebSphere MQ à l'entrée et à la sortie d'un pare-feu est plus simple et plus facile à gérer en tunnelisant les flux dans HTTP ou en agissant en tant que proxy. A l'aide de SSL (Secure Sockets Layer), il peut également être utilisé pour chiffrer et déchiffrer les messages envoyés sur Internet.

Lorsque votre système WebSphere MQ communique avec IPT, sauf si vous utilisez SSLProxyMode dans IPT, vérifiez que le CipherSpec utilisé par WebSphere MQ correspond au CipherSuite utilisé par IPT:

- Lorsqu'IPT agit en tant que serveur SSL ou TLS et que WebSphere MQ se connecte en tant que client SSL ou TLS, le CipherSpec utilisé par WebSphere MQ doit correspondre à un CipherSuite activé dans le fichier de clés IPT approprié.
- Lorsqu'IPT agit en tant que client SSL ou TLS et se connecte à un serveur WebSphere MQ SSL ou TLS, l'IPT CipherSuite doit correspondre au CipherSpec défini sur le canal WebSphere MQ récepteur.

Si vous effectuez une migration depuis IPT vers la prise en charge SSL et TLS WebSphere MQ intégrée, transférez les certificats numériques depuis IPT à l'aide d' iKeyman.

Pour plus d'informations, voir WebSphere MQ Internet Pass-Thru (SupportPac MS81).

Configuration de la sécurité

Cette collection de rubriques contient des informations spécifiques aux différents systèmes d'exploitation et à l'utilisation des clients.

Configuration de la sécurité sur les systèmes UNIX, Linux, and Windows

Considérations de sécurité spécifiques aux systèmes UNIX, Linux, and Windows .

Les gestionnaires de files d'attente IBM WebSphere MQ transfèrent des informations potentiellement utiles. Vous devez donc utiliser un système de droits d'accès pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder à vos gestionnaires de files d'attente. Prenez en compte les types de contrôle de sécurité suivants:

Qui peut administrer IBM WebSphere MQ
Vous pouvez définir l'ensemble des utilisateurs qui peuvent émettre des commandes pour administrer IBM WebSphere MQ.

Qui peut utiliser les objets IBM WebSphere MQ
Vous pouvez définir les utilisateurs (généralement des applications) qui peuvent utiliser des appels MQI et des commandes PCF pour effectuer les opérations suivantes:

- Qui peut se connecter à un gestionnaire de files d'attente.
- Qui peut accéder aux objets (files d'attente, définitions de processus, listes de noms, canaux, canaux de connexion client, programmes d'écoute, services et objets d'informations d'authentification) et quel type d'accès ils ont à ces objets.
- Qui peut accéder aux messages IBM WebSphere MQ .
- Qui peut accéder aux informations de contexte associées à un message.

Sécurité des canaux
Vous devez vous assurer que les canaux utilisés pour envoyer des messages aux systèmes distants peuvent accéder aux ressources requises.

Vous pouvez utiliser les fonctions d'exploitation standard pour accorder l'accès aux bibliothèques de programmes, aux bibliothèques de liens MQI et aux commandes. Toutefois, le répertoire contenant les files d'attente et les autres données du gestionnaire de files d'attente est privé pour IBM WebSphere MQ; n'utilisez pas les commandes du système d'exploitation standard pour accorder ou révoquer des autorisations sur les ressources MQI.

Connexion à IBM WebSphere MQ à l'aide de Terminal Services

Le droit d'utilisateur **Create global objects** peut entraîner des problèmes si vous utilisez Terminal Services.

Si vous vous connectez à un système Windows à l'aide de Terminal Services et que vous rencontrez des problèmes lors de la création ou du démarrage d'un gestionnaire de files d'attente, cela peut être dû au droit utilisateur, **Create global objects**, dans les versions récentes de Windows.

Le droit d'utilisateur **Create global objects** limite les utilisateurs autorisés à créer des objets dans l'espace de nom global. Pour qu'une application puisse créer un objet global, elle doit être en cours d'exécution dans l'espace de nom global ou l'utilisateur sous lequel l'application est exécutée doit disposer du droit d'utilisateur **Create global objects** .

Les administrateurs ont le droit d'utilisateur **Create global objects** appliqué par défaut, de sorte qu'un administrateur peut créer et démarrer des gestionnaires de files d'attente lorsqu'il est connecté à l'aide de Terminal Services sans modifier les droits utilisateur.

Si les différentes méthodes d'administration de WebSphere MQ ne fonctionnent pas lorsque vous utilisez les services de terminal, essayez de définir le droit utilisateur **Create global objects** :

1. Ouvrez le panneau Outils d'administration:

   Windows 2003 et Windows XP
   Accédez à ce panneau à l'aide de **Panneau de configuration** > **Outils d'administration**.

   Windows Vista et Windows Server 2008
   Accédez à ce panneau à l'aide du **Panneau de configuration** > **Système et maintenance** > **Outils d'administration**.
2. Cliquez deux fois sur **Stratégie de sécurité locale**.
3. Développez `Local Policies`.
4. Cliquez sur `User Rights Assignment`.
5. Ajoutez le nouvel utilisateur ou le nouveau groupe à la règle **Create global objects** .

Création et gestion de groupes sous Windows

Ces instructions vous guide tout au long du processus d'administration des groupes sur un poste de travail ou une machine serveur membre.

Pour les contrôleurs de domaine, les utilisateurs et les groupes sont administrés via Active Directory. Pour plus de détails sur l'utilisation d' Active Directory , reportez-vous aux instructions appropriées du système d'exploitation.

Les modifications que vous apportez à l'appartenance à un groupe d'un principal ne sont pas reconnues tant que le gestionnaire de files d'attente n'est pas redémarré ou que vous émettez la commande MQSC REFRESH SECURITY (ou l'équivalent PCF).

Utilisez le panneau Gestion de l'ordinateur pour gérer les utilisateurs et les groupes. Toute modification apportée à l'utilisateur actuellement connecté risque de ne pas être prise en compte tant que l'utilisateur ne se reconnecte pas.

Windows 2003 et Windows XP
Accédez à ce panneau à l'aide des **Panneau de configuration** > **Outils d'administration** > **Gestion de l'ordinateur**.

Windows Vista et Windows Server 2008
Accédez à ce panneau à l'aide du **Panneau de configuration** > **Système et maintenance** > **Outils d'administration** > **Gestion de l'ordinateur**.

Windows 7
Accédez à ce panneau à l'aide de **Outils d'administration** > **Gestion de l'ordinateur**

Création d'un groupe sous Windows

Créez un groupe à l'aide du panneau de commande.

Procédure

1. Ouvrir le panneau de commande
2. Cliquez deux fois sur **Outils d'administration**.
   Le panneau Outils d'administration s'ouvre.
3. Cliquez deux fois sur **Gestion de l'ordinateur**.
   Le panneau Gestion de l'ordinateur s'ouvre.
4. Développez **Utilisateurs et groupes locaux**.
5. Cliquez avec le bouton droit de la souris sur **Groupes**et sélectionnez **Nouveau groupe ...**.
   Le panneau Nouveau groupe s'affiche.
6. Entrez un nom approprié dans la zone Nom du groupe, puis cliquez sur **Créer**.
7. Cliquez sur **Fermer**.

Ajout d'un utilisateur à un groupe sous Windows

Ajoutez un utilisateur à un groupe à l'aide du panneau de commande.

Procédure

1. Ouvrir le panneau de commande
2. Cliquez deux fois sur **Outils d'administration**.
   Le panneau Outils d'administration s'ouvre.
3. Cliquez deux fois sur **Gestion de l'ordinateur**.
   Le panneau Gestion de l'ordinateur s'ouvre.
4. Dans le panneau Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**.
5. Sélectionnez **Utilisateurs**
6. Cliquez deux fois sur l'utilisateur que vous souhaitez ajouter à un groupe.
   Le panneau des propriétés utilisateur s'affiche.
7. Sélectionnez l'onglet **Membre de** .
8. Sélectionnez le groupe auquel vous souhaitez ajouter l'utilisateur. Si le groupe de votre choix n'est pas visible:
   a) Cliquez sur **Ajouter...**.
      Le panneau Sélectionner des groupes s'affiche.

b) Cliquez sur **Emplacements ...**.

Le panneau Emplacements s'affiche.

c) Sélectionnez l'emplacement du groupe auquel vous souhaitez ajouter l'utilisateur dans la liste et cliquez sur **OK**.

d) Entrez le nom du groupe dans la zone fournie.

Vous pouvez également cliquer sur **Avancé ...** puis **Rechercher maintenant** pour répertorier les groupes disponibles dans l'emplacement actuellement sélectionné. A partir d'ici, sélectionnez le groupe auquel vous souhaitez ajouter l'utilisateur et cliquez sur **OK**.

e) Cliquez sur **OK**.

Le panneau des propriétés utilisateur s'affiche avec le groupe que vous avez ajouté.

f) Sélectionnez le groupe.

9. Cliquez sur **OK**.

Le panneau Gestion de l'ordinateur s'affiche.

Affichage des personnes faisant partie d'un groupe sous Windows

Affichez les membres d'un groupe à l'aide du panneau de commande.

Procédure

1. Ouvrir le panneau de commande
2. Cliquez deux fois sur **Outils d'administration**.

   Le panneau Outils d'administration s'ouvre.
3. Cliquez deux fois sur **Gestion de l'ordinateur**.

   Le panneau Gestion de l'ordinateur s'ouvre.
4. Dans le panneau Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**.
5. Sélectionnez **Groupes**.
6. Cliquez deux fois sur un groupe. Le panneau des propriétés de groupe s'affiche.

   Le panneau des propriétés de groupe s'affiche.

Résultats

Les membres du groupe s'affichent.

Suppression d'un utilisateur d'un groupe sous Windows

Supprimez un utilisateur d'un groupe à l'aide du panneau de commande.

Procédure

1. Ouvrir le panneau de commande
2. Cliquez deux fois sur **Outils d'administration**.

   Le panneau Outils d'administration s'ouvre.
3. Cliquez deux fois sur **Gestion de l'ordinateur**.

   Le panneau Gestion de l'ordinateur s'ouvre.
4. Dans le panneau Gestion de l'ordinateur, développez **Utilisateurs et groupes locaux**.
5. Sélectionnez **Utilisateurs**.
6. Cliquez deux fois sur l'utilisateur que vous souhaitez ajouter à un groupe.

   Le panneau des propriétés utilisateur s'affiche.
7. Sélectionnez l'onglet **Membre de** .
8. Sélectionnez le groupe dont vous souhaitez supprimer l'utilisateur, puis cliquez sur **Supprimer**.
9. Cliquez sur **OK**.

Le panneau Gestion de l'ordinateur s'affiche.

Résultats
Vous venez de supprimer l'utilisateur du groupe.

Création et gestion de groupes sous HP-UX

Sous HP-UX, si vous n'utilisez pas NIS ou NIS +, utilisez le gestionnaire d'administration système (SAM) pour gérer les groupes.

Création d'un groupe sous HP-UX
Ajout d'un utilisateur à un groupe à l'aide du gestionnaire d'administration système

Procédure
1. Dans le gestionnaire d'administration système (SAM), cliquez deux fois sur Comptes pour les utilisateurs et les groupes.
2. Cliquez deux fois sur Groupes.
3. Sélectionnez Ajouter dans le menu déroulant Actions pour afficher le panneau Ajouter un nouveau groupe.
4. Entrez le nom du groupe et sélectionnez les utilisateurs que vous souhaitez ajouter au groupe.
5. Cliquez sur Appliquer pour créer le groupe.

Résultats
Vous venez de créer un groupe.

Ajout d'un utilisateur à un groupe sous HP-UX
Ajoutez un utilisateur à un groupe à l'aide du gestionnaire d'administration système.

Procédure
1. Dans le gestionnaire d'administration système (SAM), cliquez deux fois sur Comptes pour les utilisateurs et les groupes.
2. Cliquez deux fois sur Groupes.
3. Mettez en évidence le nom du groupe et sélectionnez Modifier dans le menu déroulant Actions pour afficher le panneau Modifier un groupe existant.
4. Sélectionnez un utilisateur à ajouter au groupe et cliquez sur Ajouter.
5. Si vous souhaitez ajouter d'autres utilisateurs au groupe, répétez l'étape 4 pour chaque utilisateur.
6. Une fois que vous avez fini d'ajouter des noms à la liste, cliquez sur OK.

Résultats
Vous venez d'ajouter un utilisateur à un groupe.

Affichage des personnes faisant partie d'un groupe sous HP-UX
Affichage des personnes faisant partie d'un groupe à l'aide du gestionnaire d'administration système

Procédure
1. Dans le gestionnaire d'administration système (SAM), cliquez deux fois sur Comptes pour les utilisateurs et les groupes.
2. Cliquez deux fois sur Groupes.
3. Mettez en évidence le nom du groupe et sélectionnez Modifier dans la liste déroulante Actions pour afficher le panneau Modifier un groupe existant et afficher la liste des utilisateurs du groupe.

Résultats
Les membres du groupe s'affichent.

Suppression d'un utilisateur d'un groupe sous HP-UX
Supprimez un utilisateur d'un groupe à l'aide du gestionnaire d'administration système.

Procédure

1. Dans le gestionnaire d'administration système (SAM), cliquez deux fois sur Comptes pour les utilisateurs et les groupes.
2. Cliquez deux fois sur Groupes.
3. Mettez en évidence le nom du groupe et sélectionnez Modifier dans le menu déroulant Actions pour afficher le panneau Modifier un groupe existant.
4. Sélectionnez un utilisateur à supprimer du groupe et cliquez sur Supprimer.
5. Si vous souhaitez supprimer d'autres utilisateurs du groupe, répétez l'étape 4 pour chaque utilisateur.
6. Lorsque vous avez fini de supprimer des noms de la liste, cliquez sur OK.

Résultats
Vous venez de supprimer un utilisateur d'un groupe

Création et gestion de groupes sous AIX

Sous AIX, si vous n'utilisez pas NIS ou NIS +, utilisez SMITTY pour gérer les groupes.

Création d'un groupe
Créez un groupe à l'aide de SMITTY.

Procédure

1. Dans SMITTY, sélectionnez Sécurité et utilisateurs et appuyez sur Entrée.
2. Sélectionnez Groupes et appuyez sur Entrée.
3. Sélectionnez Ajouter un groupe et appuyez sur Entrée.
4. Entrez le nom du groupe et les noms des utilisateurs que vous souhaitez ajouter au groupe, séparés par des virgules.
5. Appuyez sur Entrée pour créer le groupe.

Résultats
Vous venez de créer un groupe.

Ajout d'un utilisateur à un groupe
Ajoutez un utilisateur à un groupe à l'aide de SMITTY.

Procédure

1. Dans SMITTY, sélectionnez Sécurité et utilisateurs et appuyez sur Entrée.
2. Sélectionnez Groupes et appuyez sur Entrée.
3. Sélectionnez Modifier / Afficher les caractéristiques des groupes et appuyez sur Entrée.
4. Entrez le nom du groupe pour afficher la liste des membres du groupe.
5. Ajoutez les noms des utilisateurs que vous souhaitez ajouter au groupe, séparés par des virgules.
6. Appuyez sur Entrée pour ajouter les noms au groupe.

Affichage des personnes faisant partie d'un groupe
Permet d'afficher les personnes faisant partie d'un groupe utilisant SMITTY.

Procédure

1. Dans SMITTY, sélectionnez Sécurité et utilisateurs et appuyez sur Entrée.
2. Sélectionnez Groupes et appuyez sur Entrée.
3. Sélectionnez Modifier / Afficher les caractéristiques des groupes et appuyez sur Entrée.
4. Entrez le nom du groupe pour afficher la liste des membres du groupe.

Résultats

Les membres du groupe s'affichent.

Suppression d'un utilisateur d'un groupe

Supprimez un utilisateur d'un groupe à l'aide de SMITTY.

Procédure

1. Dans SMITTY, sélectionnez Sécurité et utilisateurs et appuyez sur Entrée.
2. Sélectionnez Groupes et appuyez sur Entrée.
3. Sélectionnez Modifier / Afficher les caractéristiques des groupes et appuyez sur Entrée.
4. Entrez le nom du groupe pour afficher la liste des membres du groupe.
5. Supprimez les noms des utilisateurs que vous souhaitez supprimer du groupe.
6. Appuyez sur Entrée pour supprimer les noms du groupe.

Résultats

Vous venez de supprimer un utilisateur d'un groupe.

Création et gestion de groupes sous Solaris

Sous Solaris, si vous n'utilisez pas NIS ou NIS +, utilisez le fichier `/etc/group` pour gérer les groupes.

Création d'un groupe sous Solaris

Création d'un groupe à l'aide de la commande **groupadd** .

Procédure

Entrez la commande suivante : `groupadd` *`group-name`*
où *group-name* est le nom du groupe.

Résultats

Le fichier `/etc/group` contient les informations de groupe.

Ajout d'un utilisateur à un groupe sous Solaris

Ajoutez un utilisateur à un groupe à l'aide de la commande **usermod** .

Procédure

Pour ajouter un membre à un groupe supplémentaire, exécutez la commande `usermod` et répertoriez les groupes supplémentaires dont l'utilisateur est actuellement membre, ainsi que les groupes supplémentaires dont l'utilisateur doit devenir membre.
Par exemple, si l'utilisateur est membre du groupe `groupa`et doit également devenir membre de `groupb` , utilisez la commande suivante: `usermod -G groupa,groupb` *`user-name`* , où *user-name* est le nom d'utilisateur.

Affichage des personnes faisant partie d'un groupe sous Solaris

Pour découvrir qui est membre d'un groupe, examinez l'entrée de ce groupe dans le fichier `/etc/group` .

Suppression d'un utilisateur d'un groupe sous Solaris
Supprimez un utilisateur d'un groupe à l'aide de la commande **usermod** .

Procédure

Pour supprimer un membre d'un groupe supplémentaire, exécutez la commande **usermod** qui répertorie les groupes supplémentaires dont l'utilisateur doit rester membre.
Par exemple, si le groupe principal de l'utilisateur est `users` et que l'utilisateur est également membre des groupes `mqm`, `groupa` et `groupb`, pour supprimer l'utilisateur du groupe `mqm` , la commande suivante est utilisée: `usermod -G groupa,groupb` *`user-name`*, où *`user-name`* est le nom d'utilisateur.

Création et gestion de groupes sur Linux

Sous Linux, si vous n'utilisez pas NIS ou NIS +, utilisez le fichier `/etc/group` pour gérer les groupes.

Création d'un groupe sous Linux
Créez un groupe à l'aide de la commande **groupadd** .

Procédure

Pour créer un groupe, entrez la commande suivante: `groupadd -g` *`group-ID group-name`*
où *group-ID* est l'identificateur numérique du groupe et *group-name* est le nom du groupe.

Résultats
Le fichier `/etc/group` contient les informations de groupe.

Ajout d'un utilisateur à un groupe sous Linux
Ajoutez un utilisateur à un groupe à l'aide de la commande **usermod** .

Procédure

Pour ajouter un membre à un groupe supplémentaire, exécutez la commande `usermod` et répertoriez les groupes supplémentaires dont l'utilisateur est actuellement membre, ainsi que les groupes supplémentaires dont l'utilisateur doit devenir membre.
Par exemple, si l'utilisateur est membre du groupe `groupa`et doit également devenir membre de `groupb` , la commande suivante est utilisée: `usermod -G groupa,groupb` *`user-name`*
où *`user-name`* est le nom d'utilisateur.

Affichage des personnes faisant partie d'un groupe sur Linux
Affichez les personnes qui se trouvent dans un groupe à l'aide de la commande **getent** .

Procédure

Pour afficher les membres d'un groupe, entrez la commande suivante: `getent group` *`group-name`*
où *group-name* est le nom du groupe.

Suppression d'un utilisateur d'un groupe
Supprimez un utilisateur d'un groupe à l'aide de la commande **usermod** .

Procédure

Pour supprimer un membre d'un groupe supplémentaire, exécutez la commande **usermod** qui répertorie les groupes supplémentaires dont l'utilisateur doit rester membre.
Par exemple, si le groupe principal de l'utilisateur est `users` et que l'utilisateur est également membre des groupes `mqm`, `groupa` et `groupb`, pour supprimer l'utilisateur du groupe `mqm` , la commande suivante est utilisée: `usermod -G groupa,groupb` *`user-name`*

où *user-name* est le nom d'utilisateur.

Fonctionnement des autorisations

Les tables de spécification d'autorisation dans les rubriques de cette section définissent précisément le fonctionnement des autorisations et les restrictions qui s'appliquent.

Les tableaux s'appliquent aux situations suivantes:

- Applications qui émettent des appels MQI
- Programmes d'administration qui émettent des commandes MQSC sous forme de fichiers PCF d'échappement
- Programmes d'administration qui émettent des commandes PCF

Dans cette section, les informations sont présentées sous la forme d'un ensemble de tables qui spécifient les éléments suivants:

Action à exécuter
Option MQI, commande MQSC ou commande PCF.

Objet de contrôle d'accès
File d'attente, processus, gestionnaire de files d'attente, liste de noms, informations d'authentification, canal, canal de connexion client, programme d'écoute ou service.

Autorisation requise
Exprimée sous la forme d'une constante MQZAO_.

Dans les tableaux, les constantes préfixées par MQZAO_ correspondent aux mots clés de la liste d'autorisation de la commande `setmqaut` pour l'entité particulière. Par exemple, MQZAO_BROWSE correspond au mot clé `+browse`, MQZAO_SET_ALL_CONTEXT correspond au mot clé `+setall`, etc. Ces constantes sont définies dans le fichier d'en-tête cmqzc.h, fourni avec le produit.

Autorisations pour les appels MQI

MQCONN, **MQOPEN**, **MQPUT1**et **MQCLOSE** peuvent nécessiter des vérifications d'autorisation. Les tableaux de cette rubrique récapitulent les autorisations requises pour chaque appel.

Une application est autorisée à émettre des appels et des options MQI spécifiques uniquement si l'identificateur utilisateur sous lequel elle s'exécute (ou dont elle peut assumer les autorisations) a reçu l'autorisation appropriée.

Quatre appels MQI peuvent nécessiter des vérifications d'autorisation: **MQCONN**, **MQOPEN**, **MQPUT1**et **MQCLOSE**.

Pour MQOPEN et MQPUT1, la vérification des droits d'accès est effectuée sur le nom de l'objet ouvert et non sur le ou les noms, ce qui se produit après la résolution d'un nom. Par exemple, une application peut être autorisée à ouvrir une file d'attente alias sans avoir le droit d'ouvrir la file d'attente de base dans laquelle l'alias est résolu. La règle est que la vérification est effectuée sur la première définition rencontrée lors du processus de résolution d'un nom qui n'est pas un alias de gestionnaire de files d'attente, sauf si la définition d'alias de gestionnaire de files d'attente est ouverte directement ; c'est-à-dire que son nom est affiché dans la zone *ObjectName* du descripteur d'objet. Des droits sont toujours nécessaires pour l'objet en cours d'ouverture. Dans certains cas, des droits d'accès supplémentaires indépendants de la file d'attente, obtenus via une autorisation pour l'objet gestionnaire de files d'attente, sont requis.

Tableau 8, à la page 94, Tableau 9, à la page 94, Tableau 10, à la page 95et Tableau 11, à la page 95 récapitulent les autorisations requises pour chaque appel. Dans les tableaux *Non applicable* , le contrôle d'autorisation n'est pas pertinent pour cette opération ; *Pas de contrôle* signifie qu'aucun contrôle d'autorisation n'est effectué.

Remarque : Vous ne trouverez aucune mention des listes de noms, des canaux, des canaux de connexion client, des programmes d'écoute, des services ou des objets d'informations d'authentification dans ces tables. En effet, aucune des autorisations ne s'applique à ces objets, à l'exception de MQOO_INQUIRE, pour lequel les mêmes autorisations s'appliquent que pour les autres objets.

L'autorisation spéciale MQZAO_ALL_MQI inclut toutes les autorisations dans les tables qui sont pertinentes pour le type d'objet, à l'exception de MQZAO_DELETE et MQZAO_DISPLAY, qui sont classées comme autorisations d'administration.

Pour modifier l'une des options de contexte de message, vous devez disposer des autorisations appropriées pour émettre l'appel. Par exemple, pour utiliser MQOO_SET_IDENTITY_CONTEXT ou MQPMO_SET_IDENTITY_CONTEXT, vous devez disposer du droit `+setid` .

Tableau 8. Autorisation de sécurité requise pour les appels MQCONN

Autorisation requise pour:	**Objet de file d'attente («1», à la page 95)**	**Objet Processus**	**Objet gestionnaire de files d'attente**
MQCONN	Non applicable	Non applicable	MQZAO_CONNECT

Tableau 9. Autorisation de sécurité requise pour les appels MQOPEN

Autorisation requise pour:	**Objet de file d'attente («1», à la page 95)**	**Objet Processus**	**Objet gestionnaire de files d'attente**
MQOO_INTERROGATION	MQZAO_INQUIRE	MQZAO_INQUIRE	MQZAO_INQUIRE
MQOO_BROWSE	MQZAO_PARCOURIR	Non applicable	Aucun contrôle
MQOO_ENTRÉE_ *	MQZAO_ENTREE	Non applicable	Aucun contrôle
MQOO_SAVE_ ALL_CONTEXT **(«2», à la page 95)**	MQZAO_ENTREE	Non applicable	Non applicable
MQOO_OUTPUT (file d'attente normale) **(«3», à la page 95)**	MQZAO_OUTPUT	Non applicable	Non applicable
MQOO_PASS_IDENTITY_C ONTEXT **(«4», à la page 95)**	MQZAO_PASS_ IDENTITY_CONTEXT	Non applicable	Aucun contrôle
MQOO_PASS_ALL_ CONTEXT **(«4», à la page 95, «5», à la page 95)**	MQZAO_PASS _ALL_CONTEXT	Non applicable	Aucun contrôle
MQOO_SET_ IDENTITY_CONTEXT **(«4», à la page 95, «5», à la page 95)**	MQZAO_SET_IDENTITY_C ONTEXT	Non applicable	MQZAO_SET_ IDENTITY_CONTEXT **(«6», à la page 95)**
MQOO_SET_ ALL_CONTEXT **(«4», à la page 95, «7», à la page 95)**	MQZAO_SET_ALL_CONTE XT	Non applicable	MQZAO_SET_ ALL_CONTEXT **(«6», à la page 95)**
MQOO_OUTPUT (file d'attente de transmission) **(«8», à la page 95)**	MQZAO_SET_ALL_CONTE XT	Non applicable	MQZAO_SET_ ALL_CONTEXT **(«6», à la page 95)**
MQOO_SET	MQZAO_SET	Non applicable	Aucun contrôle
MQOO_ALTERNATE_ AUTORITE UTILISATEUR	**(«9», à la page 96)**	**(«9», à la page 96)**	MQZAO_ALTERNATE_ USER_AUTHORITY **(«9», à la page 96, «10», à la page 96)**

Tableau 10. Autorisation de sécurité requise pour les appels MQPUT1			
Autorisation requise pour:	**Objet de file d'attente («1», à la page 95)**	**Objet Processus**	**Objet gestionnaire de files d'attente**
MQPMO_PASS_ IDENTITY_CONTEXT	MQZAO_PASS_ IDENTITY_CONTEXT **(«11», à la page 96)**	Non applicable	Aucun contrôle
MQPMO_PASS_ALL _CONTEXT	MQZAO_PASS_ ALL_CONTEXT **(«11», à la page 96)**	Non applicable	Aucun contrôle
MQPMO_SET_IDENTITY_C ONTEXT	MQZAO_SET_ IDENTITY_CONTEXT **(«11», à la page 96)**	Non applicable	MQZAO_SET_ IDENTITY_CONTEXT **(«6», à la page 95)**
MQPMO_SET_ALL_CONTE XT	MQZAO_SET_ ALL_CONTEXT **(«11», à la page 96)**	Non applicable	MQZAO_SET_ ALL_CONTEXT **(«6», à la page 95)**
(File d'attente de transmission) **(«8», à la page 95)**	MQZAO_SET_ALL_CONTE XT	Non applicable	MQZAO_SET_ ALL_CONTEXT **(«6», à la page 95)**
MQPMO_ALTERNATE_USE R_AUTHORITY	**(«12», à la page 96)**	Non applicable	MQZAO_ALTERNATE_ USER_AUTHORITY **(«10», à la page 96)**

Tableau 11. Autorisation de sécurité requise pour les appels MQCLOSE			
Autorisation requise pour:	**Objet de file d'attente («1», à la page 95)**	**Objet Processus**	**Objet gestionnaire de files d'attente**
MQCO_DELETE	MQZAO_DELETE **(«13», à la page 96)**	Non applicable	Non applicable
MQCO_DELETE _PURGE	MQZAO_DELETE **(«13», à la page 96)**	Non applicable	Non applicable

Remarques relatives aux tableaux:

1. Si vous ouvrez une file d'attente modèle:
   - Le droit MQZAO_DISPLAY est requis pour la file d'attente modèle, en plus du droit d'ouverture de la file d'attente modèle pour le type d'accès pour lequel vous l'ouvrez.
   - Les droits MQZAO_CREATE ne sont pas nécessaires pour créer la file d'attente dynamique.
   - L'ID utilisateur utilisé pour ouvrir la file d'attente modèle reçoit automatiquement tous les droits spécifiques à la file d'attente (équivalents à MQZAO_ALL) pour la file d'attente dynamique créée.
2. MQOO_INPUT_ * doit également être spécifié. Valide pour une file d'attente locale, modèle ou alias.
3. Cette vérification est effectuée pour tous les cas de sortie, à l'exception des files d'attente de transmission (voir la remarque «8», à la page 95).
4. MQOO_OUTPUT doit également être spécifié.
5. MQOO_PASS_IDENTITY_CONTEXT est également impliqué par cette option.
6. Ce droit est requis pour l'objet gestionnaire de files d'attente et la file d'attente particulière.
7. MQOO_PASS_IDENTITY_CONTEXT, MQOO_PASS_ALL_CONTEXT et MQOO_SET_IDENTITY_CONTEXT sont également impliquées par cette option.
8. Cette vérification est effectuée pour une file d'attente locale ou modèle dont l'attribut de file d'attente *Utilisation* est MQUS_TRANSMISSION et qui est ouverte directement pour la sortie. Elle ne

s'applique pas si une file d'attente éloignée est ouverte (soit en spécifiant les noms du gestionnaire de files d'attente éloignées et de la file d'attente éloignée, soit en indiquant le nom d'une définition locale de la file d'attente éloignée).

9. Au moins l'une des options MQOO_INQUIRE (pour tout type d'objet) ou MQOO_BROWSE, MQOO_INPUT_ *, MQOO_OUTPUT ou MQOO_SET (pour les files d'attente) doit également être spécifiée. La vérification effectuée est la même que pour les autres options spécifiées, à l'aide de l'identificateur d'utilisateur de remplacement fourni pour les droits sur les objets nommés spécifiques, et des droits d'application en cours pour la vérification MQZAO_ALTERNATE_USER_IDENTIFIER.
10. Cette autorisation permet de spécifier tout ID *AlternateUser* .
11. Une vérification MQZAO_OUTPUT est également effectuée si la file d'attente ne possède pas l'attribut de file d'attente *Usage* MQUS_TRANSMISSION.
12. La vérification effectuée est la même que pour les autres options spécifiées, à l'aide de l'identificateur d'utilisateur de remplacement fourni pour le droit de file d'attente nommé spécifique et du droit d'application en cours pour la vérification MQZAO_ALTERNATE_USER_IDENTIFIER.
13. La vérification n'est effectuée que si les deux conditions suivantes sont remplies:
    - Une file d'attente dynamique permanente est en cours de fermeture et de suppression.
    - La file d'attente n'a pas été créée par l'appel MQOPEN qui a renvoyé le descripteur d'objet utilisé.

    Sinon, il n'y a pas de contrôle.

Autorisations pour les commandes MQSC dans les fichiers PCF d'échappement

Ces informations récapitulent les autorisations requises pour chaque commande MQSC contenue dans Escape PCF.

Non applicable signifie que cette opération n'est pas pertinente pour ce type d'objet.

L'ID utilisateur sous lequel le programme qui soumet la commande s'exécute doit également disposer des droits suivants:

- Droits MQZAO_CONNECT sur le gestionnaire de files d'attente
- Droit MQZAO_DISPLAY sur le gestionnaire de files d'attente afin d'exécuter des commandes PCF
- Droit d'émettre la commande MQSC dans le texte de la commande Escape PCF

ALTER *objet*

Objet	**Autorisation requise**
File d'attente	MODIFICATION MQZAO_DE
Topic	MODIFICATION MQZAO_DE
Processus	MODIFICATION MQZAO_DE
Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Liste de noms	MODIFICATION MQZAO_DE
Informations d'authentification	MODIFICATION MQZAO_DE
Canal	MODIFICATION MQZAO_DE
Canal de connexion client	MODIFICATION MQZAO_DE
Programme d'écoute	MODIFICATION MQZAO_DE
Service	MODIFICATION MQZAO_DE
Information de communication	MODIFICATION MQZAO_DE

CLEAR *objet*

Objet	Autorisation requise
File d'attente	MQZAO_CLEAR
Topic	MQZAO_CLEAR
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	Non applicable
Canal de connexion client	Non applicable
Programme d'écoute	Non applicable
Service	Non applicable
Information de communication	Non applicable

DEFINE *objet* NOREPLACE («1», à la page 101)

Objet	Autorisation requise
File d'attente	MQZAO_CREATE **(«2», à la page 101)**
Topic	MQZAO_CREATE **(«2», à la page 101)**
Processus	MQZAO_CREATE **(«2», à la page 101)**
Gestionnaire de files d'attente	Non applicable
Liste de noms	MQZAO_CREATE **(«2», à la page 101)**
Informations d'authentification	MQZAO_CREATE **(«2», à la page 101)**
Canal	MQZAO_CREATE **(«2», à la page 101)**
Canal de connexion client	MQZAO_CREATE **(«2», à la page 101)**
Programme d'écoute	MQZAO_CREATE **(«2», à la page 101)**
Service	MQZAO_CREATE **(«2», à la page 101)**
Information de communication	MQZAO_CREATE **(«2», à la page 101)**

DEFINE *objet* REPLACE («1», à la page 101, «3», à la page 101)

Objet	Autorisation requise
File d'attente	MODIFICATION MQZAO_DE
Topic	MODIFICATION MQZAO_DE
Processus	MODIFICATION MQZAO_DE
Gestionnaire de files d'attente	Non applicable
Liste de noms	MODIFICATION MQZAO_DE
Informations d'authentification	MODIFICATION MQZAO_DE
Canal	MODIFICATION MQZAO_DE

Objet	Autorisation requise
Canal de connexion client	MODIFICATION MQZAO_DE
Programme d'écoute	MODIFICATION MQZAO_DE
Service	MODIFICATION MQZAO_DE
Information de communication	MODIFICATION MQZAO_DE

DELETE *objet*

Objet	Autorisation requise
File d'attente	MQZAO_DELETE
Topic	MQZAO_DELETE
Processus	MQZAO_DELETE
Gestionnaire de files d'attente	Non applicable
Liste de noms	MQZAO_DELETE
Informations d'authentification	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de connexion client	MQZAO_DELETE
Programme d'écoute	MQZAO_DELETE
Service	MQZAO_DELETE
Information de communication	MQZAO_DELETE

DISPLAY *objet*

Objet	Autorisation requise
File d'attente	MQZAO_DISPLAY
Topic	MQZAO_DISPLAY
Processus	MQZAO_DISPLAY
Gestionnaire de files d'attente	MQZAO_DISPLAY
Liste de noms	MQZAO_DISPLAY
Informations d'authentification	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY
Canal de connexion client	MQZAO_DISPLAY
Programme d'écoute	MQZAO_DISPLAY
Service	MQZAO_DISPLAY
Information de communication	MQZAO_DISPLAY

START *objet*

Objet	Autorisation requise
File d'attente	Non applicable
Topic	Non applicable

Objet	Autorisation requise
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	CONTROLE MQZ
Canal de connexion client	Non applicable
Programme d'écoute	CONTROLE MQZ
Service	CONTROLE MQZ
Information de communication	Non applicable

STOP *objet*

Objet	Autorisation requise
File d'attente	Non applicable
Topic	Non applicable
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	CONTROLE MQZ
Canal de connexion client	Non applicable
Programme d'écoute	CONTROLE MQZ
Service	CONTROLE MQZ
Information de communication	Non applicable

Commandes relatives aux canaux

Commande	Objet	Autorisation requise
Envoyer une commande PING à un canal	Canal	CONTROLE MQZ
Réinitialisation du canal	Canal	MQZAO_CONTRÔLE_ÉTENDU
Résolution du canal	Canal	MQZAO_CONTRÔLE_ÉTENDU

Commandes d'abonnement

Commande	Objet	Autorisation requise
ALTER SUB	Topic	CONTROLE MQZ
DEFINE SUB	Topic	CONTROLE MQZ
SUPPRIMER DES SOUS	Topic	CONTROLE MQZ
DISPLAY SUB	Topic	MQZAO_DISPLAY

Commandes de sécurité

Commande	Objet	Autorisation requise
SET AUTHREC	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
DELETE AUTHREC	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Paramètre DISPLAY AUTHREC	Gestionnaire de files d'attente	MQZAO_DISPLAY
DISPLAY AUTHSERV	Gestionnaire de files d'attente	MQZAO_DISPLAY
AFFICHER ENTAUTH	Gestionnaire de files d'attente	MQZAO_DISPLAY
SET CHLAUTH	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
AFFICHER CHLAUTH	Gestionnaire de files d'attente	MQZAO_DISPLAY
REFRESH SECURITY	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE

Affichages de statut

Commande	Objet	Autorisation requise
DISPLAY CHSTATUS	Gestionnaire de files d'attente	MQZAO_DISPLAY Notez que les droits `+inq` (ou de manière équivalente MQZAO_INQUIRE) sont requis sur la file d'attente de transmission si le type de canal est CLUSSDR.
DISPLAY LSSTATUS	Gestionnaire de files d'attente	MQZAO_DISPLAY
AFFICHAGE DE PUBSUB	Gestionnaire de files d'attente	MQZAO_DISPLAY
STATUT DU JEU DE CARACTÈRES D'AFFICHAGE	Gestionnaire de files d'attente	MQZAO_DISPLAY
STATUT DE L'AFFICHAGE	Gestionnaire de files d'attente	MQZAO_DISPLAY
DISPLAY TPSTATUS	Gestionnaire de files d'attente	MQZAO_DISPLAY

Commandes relatives aux clusters

Commande	Objet	Autorisation requise
DISPLAY CLUSQMGR	Gestionnaire de files d'attente	MQZAO_DISPLAY
Actualiser le cluster	Appartenance au groupe'mqm'requise	
Réinitialisation d'un cluster	Appartenance au groupe'mqm'requise	
SUSPEND QMGR	Appartenance au groupe'mqm'requise	
RESUME QMGR	Appartenance au groupe'mqm'requise	

Autres commandes d'administration

Commande	Objet	Autorisation requise
PING QMGR	Gestionnaire de files d'attente	MQZAO_DISPLAY
ACTUALISEZ LE GESTIONNAIRE DE FILES D'ATTENTE	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE

Commande	Objet	Autorisation requise
RESET QMGR	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
DISPLAY CONN	Gestionnaire de files d'attente	MQZAO_DISPLAY
ARRETER CONN	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE

Remarque :

1. Pour les commandes DEFINE, le droit MQZAO_DISPLAY est également requis pour l'objet LIKE si un tel droit est spécifié, ou sur le système SYSTEM.DEFAULT.xxx si LIKE est omis.
2. Les droits MQZAO_CREATE ne sont pas spécifiques à un objet ou à un type d'objet particulier. Le droit de création est accordé pour tous les objets d'un gestionnaire de files d'attente spécifié, en spécifiant un type d'objet QMGR dans la commande `setmqaut` .
3. Ceci s'applique si l'objet à remplacer existe déjà. Si ce n'est pas le cas, la vérification est celle de DEFINE *objet* NOREPLACE.

Information associée

Mise en cluster : meilleures pratiques d'utilisation REFRESH CLUSTER

Autorisations pour les commandes PCF

Cette section récapitule les autorisations requises pour chaque commande PCF.

Aucune vérification signifie qu'aucune vérification d'autorisation n'est effectuée ; *Non applicable* signifie que cette opération n'est pas pertinente pour ce type d'objet.

L'ID utilisateur sous lequel le programme qui soumet la commande s'exécute doit également disposer des droits suivants:

- Droits MQZAO_CONNECT sur le gestionnaire de files d'attente
- Droit MQZAO_DISPLAY sur le gestionnaire de files d'attente afin d'exécuter des commandes PCF

L'autorisation spéciale MQZAO_ALL_ADMIN inclut toutes les autorisations de la liste suivante qui sont pertinentes pour le type d'objet, à l'exception de MQZAO_CREATE, qui n'est pas spécifique à un objet ou à un type d'objet particulier.

Modifier *objet*

Objet	Autorisation requise
File d'attente	MODIFICATION MQZAO_DE
Rubrique	MODIFICATION MQZAO_DE
Processus	MODIFICATION MQZAO_DE
Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Liste de noms	MODIFICATION MQZAO_DE
Informations d'authentification	MODIFICATION MQZAO_DE
Canal	MODIFICATION MQZAO_DE
Canal de connexion client	MODIFICATION MQZAO_DE
Programme d'écoute	MODIFICATION MQZAO_DE
Service	MODIFICATION MQZAO_DE
Information de communication	MODIFICATION MQZAO_DE

Effacer *objet*

Objet	Autorisation requise
File d'attente	MQZAO_CLEAR
Rubrique	MQZAO_CLEAR
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	Non applicable
Canal de connexion client	Non applicable
Programme d'écoute	Non applicable
Service	Non applicable
Information de communication	Non applicable

Copiez *objet* (sans remplacement) (1)

Objet	Autorisation requise
File d'attente	MQZAO_CREATE **(2)**
Rubrique	MQZAO_CREATE **(2)**
Processus	MQZAO_CREATE **(2)**
Gestionnaire de files d'attente	Non applicable
Liste de noms	MQZAO_CREATE **(2)**
Informations d'authentification	MQZAO_CREATE **(2)**
Canal	MQZAO_CREATE **(2)**
Canal de connexion client	MQZAO_CREATE **(2)**
Programme d'écoute	MQZAO_CREATE **(2)**
Service	MQZAO_CREATE **(2)**
Information de communication	MQZAO_CREATE **(«2», à la page 107)**

Copiez *objet* (avec remplacement) (1, 4)

Objet	Autorisation requise
File d'attente	MODIFICATION MQZAO_DE
Rubrique	MODIFICATION MQZAO_DE
Processus	MODIFICATION MQZAO_DE
Gestionnaire de files d'attente	Non applicable
Liste de noms	MODIFICATION MQZAO_DE
Informations d'authentification	MODIFICATION MQZAO_DE
Canal	MODIFICATION MQZAO_DE

Objet	Autorisation requise
Canal de connexion client	MODIFICATION MQZAO_DE
Programme d'écoute	MODIFICATION MQZAO_DE
Service	MODIFICATION MQZAO_DE
Information de communication	MODIFICATION MQZAO_DE

Créer *objet* (sans remplacement) (3)

Objet	Autorisation requise
File d'attente	MQZAO_CREATE **(2)**
Rubrique	MQZAO_CREATE **(2)**
Processus	MQZAO_CREATE **(2)**
Gestionnaire de files d'attente	Non applicable
Liste de noms	MQZAO_CREATE **(2)**
Informations d'authentification	MQZAO_CREATE **(2)**
Canal	MQZAO_CREATE **(2)**
Canal de connexion client	MQZAO_CREATE **(2)**
Programme d'écoute	MQZAO_CREATE **(2)**
Service	MQZAO_CREATE **(2)**
Information de communication	MQZAO_CREATE **(2)**

Créez *objet* (avec remplacement) (3, 4)

Objet	Autorisation requise
File d'attente	MODIFICATION MQZAO_DE
Rubrique	MODIFICATION MQZAO_DE
Processus	MODIFICATION MQZAO_DE
Gestionnaire de files d'attente	Non applicable
Liste de noms	MODIFICATION MQZAO_DE
Informations d'authentification	MODIFICATION MQZAO_DE
Canal	MODIFICATION MQZAO_DE
Canal de connexion client	MODIFICATION MQZAO_DE
Programme d'écoute	MODIFICATION MQZAO_DE
Service	MODIFICATION MQZAO_DE
Information de communication	MODIFICATION MQZAO_DE

Supprimer *objet*

Objet	Autorisation requise
File d'attente	MQZAO_DELETE
Rubrique	MQZAO_DELETE

Objet	Autorisation requise
Processus	MQZAO_DELETE
Gestionnaire de files d'attente	Non applicable
Liste de noms	MQZAO_DELETE
Informations d'authentification	MQZAO_DELETE
Canal	MQZAO_DELETE
Canal de connexion client	MQZAO_DELETE
Programme d'écoute	MQZAO_DELETE
Service	MQZAO_DELETE
Information de communication	MQZAO_DELETE

Interroger *objet*

Objet	Autorisation requise
File d'attente	MQZAO_DISPLAY
Rubrique	MQZAO_DISPLAY
Processus	MQZAO_DISPLAY
Gestionnaire de files d'attente	MQZAO_DISPLAY
Liste de noms	MQZAO_DISPLAY
Informations d'authentification	MQZAO_DISPLAY
Canal	MQZAO_DISPLAY
Canal de connexion client	MQZAO_DISPLAY
Programme d'écoute	MQZAO_DISPLAY
Service	MQZAO_DISPLAY
Information de communication	MQZAO_DISPLAY

Interroger les noms d' *objet*

Objet	Autorisation requise
File d'attente	Aucun contrôle
Topic	Aucun contrôle
Processus	Aucun contrôle
Gestionnaire de files d'attente	Aucun contrôle
Liste de noms	Aucun contrôle
Informations d'authentification	Aucun contrôle
Canal	Aucun contrôle
Canal de connexion client	Aucun contrôle
Programme d'écoute	Aucun contrôle
Service	Aucun contrôle

Objet	Autorisation requise
Information de communication	Aucun contrôle

Démarrez *objet*

Objet	Autorisation requise
File d'attente	Non applicable
Topic	Non applicable
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	CONTROLE MQZ
Canal de connexion client	Non applicable
Programme d'écoute	CONTROLE MQZ
Service	CONTROLE MQZ
Information de communication	Non applicable

Arrêter *objet*

Objet	Autorisation requise
File d'attente	Non applicable
Topic	Non applicable
Processus	Non applicable
Gestionnaire de files d'attente	Non applicable
Liste de noms	Non applicable
Informations d'authentification	Non applicable
Canal	CONTROLE MQZ
Canal de connexion client	Non applicable
Programme d'écoute	CONTROLE MQZ
Service	CONTROLE MQZ
Information de communication	Non applicable

Commandes relatives aux canaux

Commande	Objet	Autorisation requise
Ping Channel	Canal	CONTROLE MQZ
Reset Channel	Canal	MQZAO_CONTRÔLE_ÉTENDU
Resolve Channel	Canal	MQZAO_CONTRÔLE_ÉTENDU

Commandes d'abonnement

Commande	Objet	Autorisation requise
Modifier un abonnement	Topic	CONTROLE MQZ
Créer un abonnement	Topic	CONTROLE MQZ
Supprimer l'abonnement	Topic	CONTROLE MQZ
Consulter un abonnement	Topic	MQZAO_DISPLAY

Commandes de sécurité

Commande	Objet	Autorisation requise
Définition de l'enregistrement de droits d'accès	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Supprimer l'enregistrement de droits d'accès	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Consulter des enregistrements de droits	Gestionnaire de files d'attente	MQZAO_DISPLAY
Consulter un service de droits d'accès	Gestionnaire de files d'attente	MQZAO_DISPLAY
Interroger les droits d'accès de l'entité	Gestionnaire de files d'attente	MQZAO_DISPLAY
Définir l'enregistrement d'authentification de canal	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Consulter les enregistrements d'authentification de canal	Gestionnaire de files d'attente	MQZAO_DISPLAY
Régénérer la sécurité	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE

Affichages de statut

Commande	Objet	Autorisation requise
Inquire Channel Status	Gestionnaire de files d'attente	MQZAO_DISPLAY Notez que les droits `+inq` (ou de manière équivalente MQZAO_INQUIRE) sont requis sur la file d'attente de transmission si le type de canal est CLUSSDR.
Interroger le statut du programme d'écoute de canal	Gestionnaire de files d'attente	MQZAO_DISPLAY
Interroger le statut de publication / d'abonnement	Gestionnaire de files d'attente	MQZAO_DISPLAY
Interroger le statut de l'abonnement	Gestionnaire de files d'attente	MQZAO_DISPLAY
Consulter le statut d'un service	Gestionnaire de files d'attente	MQZAO_DISPLAY
Consulter le statut d'une rubrique	Gestionnaire de files d'attente	MQZAO_DISPLAY

Commandes relatives aux clusters

Commande	Objet	Autorisation requise
Inquire Cluster Queue Manager	Gestionnaire de files d'attente	MQZAO_DISPLAY
Refresh Cluster	Appartenance au groupe'mqm'requise	
Reset Cluster	Appartenance au groupe'mqm'requise	
Suspend Queue Manager Cluster	Appartenance au groupe'mqm'requise	
Resume Queue Manager Cluster	Appartenance au groupe'mqm'requise	

Autres commandes d'administration

Commande	Objet	Autorisation requise
Ping Queue Manager	Gestionnaire de files d'attente	MQZAO_DISPLAY
Refresh Queue Manager	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Reset Queue Manager	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE
Reset Queue Statistics	File d'attente	MQZAO_DISPLAY et MQZAO_CHANGE
Consulter une connexion	Gestionnaire de files d'attente	MQZAO_DISPLAY
Arrêter une connexion	Gestionnaire de files d'attente	MODIFICATION MQZAO_DE

Remarque :

1. Pour les commandes de copie, le droit MQZAO_DISPLAY est également requis pour l'objet From.
2. Les droits MQZAO_CREATE ne sont pas spécifiques à un objet ou à un type d'objet particulier. Le droit de création est accordé pour tous les objets d'un gestionnaire de files d'attente spécifié, en spécifiant un type d'objet QMGR dans la commande `setmqaut` .
3. Pour les commandes de création, les droits MQZAO_DISPLAY sont également requis pour le système SYSTEM.DEFAULT.* .
4. Ceci s'applique si l'objet à remplacer existe déjà. Si ce n'est pas le cas, la vérification est la même que pour la copie ou la création sans remplacement.

Remarques spéciales relatives à la sécurité sous Windows

Certaines fonctions de sécurité se comportent différemment sur les différentes versions de Windows.

La sécurité IBM WebSphere MQ s'appuie sur les appels à l'API du système d'exploitation pour obtenir des informations sur les autorisations utilisateur et les appartenances à des groupes. Certaines fonctions ne se comportent pas de la même manière sur les systèmes Windows . Cette collection de rubriques inclut des descriptions de la manière dont ces différences peuvent affecter la sécurité IBM WebSphere MQ lorsque vous exécutez IBM WebSphere MQ dans un environnement Windows .

Programme d'exit de canal SSPI

WebSphere MQ for Windows fournit un programme d'exit de sécurité, qui peut être utilisé sur les canaux de message et MQI. L'exit est fourni en tant que code source et code objet et fournit une authentification unidirectionnelle et bidirectionnelle.

L'exit de sécurité utilise l'interface SSPI (Security Support Provider Interface), qui fournit les fonctions de sécurité intégrées des plateformes Windows .

L'exit de sécurité fournit les services d'identification et d'authentification suivants:

authentification unidirectionnelle
Cela utilise la prise en charge de l'authentification Windows NT LAN Manager (NTLM). NTLM permet aux serveurs d'authentifier leurs clients. Il ne permet pas à un client d'authentifier un serveur ou à un serveur d'en authentifier un autre. NTLM a été conçu pour un environnement réseau dans lequel les serveurs sont supposés être authentiques. NTLM est pris en charge sur toutes les plateformes Windows prises en charge par WebSphere MQ Version 7.0.

Ce service est généralement utilisé sur un canal MQI pour permettre à un gestionnaire de files d'attente serveur d'authentifier une application client MQI WebSphere MQ . Une application client est identifiée par l'ID utilisateur associé au processus en cours d'exécution.

Pour effectuer l'authentification, l'exit de sécurité à l'extrémité client d'un canal acquiert un jeton d'authentification auprès de NTLM et envoie le jeton dans un message de sécurité à son partenaire à l'autre extrémité du canal. L'exit de sécurité partenaire transmet le jeton à NTLM, qui vérifie que le jeton est authentique. Si l'exit de sécurité partenaire n'est pas satisfait de l'authenticité du jeton, il demande à l'agent MCA de fermer le canal.

Authentification bidirectionnelle ou mutuelle
Cela utilise les services d'authentification Kerberos . Le protocole Kerberos ne suppose pas que les serveurs d'un environnement réseau sont authentiques. Les serveurs peuvent authentifier les clients et d'autres serveurs, et les clients peuvent authentifier les serveurs. Kerberos est pris en charge sur toutes les plateformes Windows prises en charge par WebSphere MQ Version 7.0.

Ce service peut être utilisé sur les canaux de message et MQI. Sur un canal de transmission de messages, il fournit une authentification mutuelle des deux gestionnaires de files d'attente. Sur un canal MQI, il permet au gestionnaire de files d'attente du serveur et à l'application client WebSphere MQ MQI de s'authentifier les uns les autres. Un gestionnaire de files d'attente est identifié par son nom préfixé par la chaîne `ibmMQSeries/`. Une application client est identifiée par l'ID utilisateur associé au processus en cours d'exécution.

Pour effectuer l'authentification mutuelle, l'exit de sécurité initiateur acquiert un jeton d'authentification auprès du serveur de sécurité Kerberos et envoie le jeton dans un message de sécurité à son partenaire. L'exit de sécurité partenaire transmet le jeton au serveur Kerberos , qui vérifie qu'il est authentique. Le serveur de sécurité Kerberos génère un second jeton que le partenaire envoie dans un message de sécurité à l'exit de sécurité initiateur. L'exit de sécurité initiateur demande ensuite au serveur Kerberos de vérifier que le deuxième jeton est authentique. Lors de cet échange, si l'un des exits de sécurité n'est pas satisfait de l'authenticité du jeton envoyé par l'autre, il demande à l'agent MCA de fermer le canal.

L'exit de sécurité est fourni au format source et au format objet. Vous pouvez utiliser le code source comme point de départ pour l'écriture de vos propres programmes d'exit de canal ou vous pouvez utiliser le module d'objet tel qu'il est fourni. Le module d'objet possède deux points d'entrée, l'un pour l'authentification unidirectionnelle à l'aide de la prise en charge de l'authentification NTLM et l'autre pour l'authentification bidirectionnelle à l'aide des services d'authentification Kerberos .

Pour plus d'informations sur le fonctionnement du programme d'exit de canal SSPI et pour savoir comment l'implémenter, voir Utilisation de l'exit de sécurité SSPI sur les systèmes Windows.

Lorsque vous obtenez une erreur'group not found'sous Windows

Ce problème peut survenir car WebSphere MQ perd l'accès au groupe mqm local lorsque des serveurs Windows sont promus ou rétrogradés à partir de contrôleurs de domaine. Pour résoudre ce problème, recréez le groupe mqm local.

Le symptôme est une erreur indiquant l'absence d'un groupe mqm local, par exemple:

```
>crtmqm qm0
AMQ8066:Local mqm group not found.
```

La modification de l'état d'une machine entre le serveur et le contrôleur de domaine peut affecter le fonctionnement de WebSphere MQ, car WebSphere MQ utilise un groupe mqm défini en local. Lorsqu'un serveur est promu en tant que contrôleur de domaine, la portée passe de locale à locale. Lorsque la machine est rétrogradée sur le serveur, tous les groupes locaux de domaine sont supprimés. Cela signifie

que le passage d'une machine d'un serveur à un contrôleur de domaine et le retour au serveur perdent l'accès à un groupe mqm local.

Pour résoudre ce problème, recréez le groupe mqm local à l'aide des outils de gestion Windows standard. Etant donné que toutes les informations d'appartenance au groupe sont perdues, vous devez rétablir les utilisateurs WebSphere MQ privilégiés dans le groupe mqm local nouvellement créé. Si la machine est un membre de domaine, vous devez également ajouter le groupe mqm de domaine au groupe mqm local pour accorder aux ID utilisateur du domaine privilégié WebSphere MQ le niveau de droits requis.

Lorsque vous rencontrez des problèmes avec IBM WebSphere MQ et les contrôleurs de domaine sous Windows

Certains problèmes peuvent se produire avec les paramètres de sécurité lorsque les serveurs Windows sont promus en contrôleurs de domaine.

Lors de la promotion des serveurs Windows 2000, Windows 2003 ou Windows Server 2008 vers des contrôleurs de domaine, vous avez la possibilité de sélectionner un paramètre de sécurité par défaut ou non lié aux droits des utilisateurs et des groupes. Cette option contrôle si des utilisateurs arbitraires peuvent extraire des appartenances à des groupes à partir du répertoire actif. Etant donné que WebSphere MQ s'appuie sur les informations d'appartenance à un groupe pour implémenter sa stratégie de sécurité, il est important que l'ID utilisateur qui effectue des opérations WebSphere MQ puisse déterminer les appartenances à des groupes d'autres utilisateurs.

Sous Windows 2000, lorsqu'un domaine est créé à l'aide de l'option de sécurité par défaut, l'ID utilisateur par défaut créé par WebSphere MQ lors du processus d'installation peut obtenir des appartenances à des groupes pour d'autres utilisateurs, selon les besoins. Le produit s'installe ensuite normalement, en créant des objets par défaut, et le gestionnaire de files d'attente peut déterminer les droits d'accès des utilisateurs locaux et de domaine si nécessaire.

Sous Windows 2000, lorsqu'un domaine est créé à l'aide de l'option de sécurité autre que celle par défaut, ou sous Windows 2003 et Windows Server 2008 lorsqu'un domaine est créé à l'aide de l'option de sécurité par défaut, l'ID utilisateur créé par WebSphere MQ lors de l'installation ne peut pas toujours déterminer les appartenances au groupe requises. Dans ce cas, vous devez connaître:

- Comportement de Windows 2000 avec des droits de sécurité autres que ceux par défaut, ou Windows 2003 et Windows Server 2008 avec des droits de sécurité par défaut
- Comment autoriser les membres du groupe mqm de domaine à lire l'appartenance à un groupe
- Comment configurer un service IBM WebSphere MQ Windows pour qu'il s'exécute sous un utilisateur de domaine

Domaine Windows 2000 avec droits de sécurité non définis par défaut, ou domaine Windows 2003 et Windows Server 2008 avec droits de sécurité par défaut

Le comportement de l'installation de WebSphere MQ diffère sur ces systèmes d'exploitation celui que l'installation est réalisée par un utilisateur local ou par un utilisateur du domaine.

Si un utilisateur **local** installe WebSphere MQ, l'assistant de préparation de WebSphere MQ détecte que l'utilisateur local créé pour le service IBM WebSphere MQ Windows peut extraire les informations d'appartenance au groupe de l'utilisateur qui effectue l'installation. L'assistant de préparation de WebSphere MQ pose des questions à l'utilisateur sur la configuration du réseau afin de déterminer si d'autres comptes utilisateur sont définis sur les contrôleurs de domaine s'exécutant sous Windows 2000 ou version ultérieure. Si tel est le cas, le service IBM WebSphere MQ Windows doit s'exécuter sous un compte utilisateur de domaine avec des paramètres et des droits spécifiques. L'assistant de préparation de WebSphere MQ invite l'utilisateur à entrer les détails du compte de cet utilisateur. Son aide en ligne fournit des détails sur le compte utilisateur de domaine requis qui peut être envoyé à l'administrateur de domaine.

Si un utilisateur de **domaine** installe WebSphere MQ, l'assistant de préparation de WebSphere MQ détecte que l'utilisateur local créé pour le service IBM WebSphere MQ Windows ne peut pas extraire les informations d'appartenance au groupe de l'utilisateur qui effectue l'installation. Dans ce cas, l'assistant de préparation de WebSphere MQ invite toujours l'utilisateur à indiquer les détails du compte utilisateur de domaine à utiliser par le service IBM WebSphere MQ Windows .

Lorsque le service IBM WebSphere MQ Windows doit utiliser un compte utilisateur de domaine, WebSphere MQ ne peut pas fonctionner correctement tant qu'il n'a pas été configuré à l'aide de l'assistant de préparation de WebSphere MQ . L'assistant de préparation de WebSphere MQ ne permet pas à l'utilisateur de poursuivre avec d'autres tâches tant que le service Windows n'a pas été configuré avec un compte approprié.

Si un domaine Windows 2000 a été configuré avec des droits de sécurité autres que ceux par défaut, la solution habituelle pour permettre à WebSphere MQ de fonctionner correctement consiste à le configurer avec un compte utilisateur de domaine approprié, comme décrit ci-dessus.

Pour plus d'informations, voir Création et configuration de comptes de domaine pour WebSphere MQ .

Configuration des services IBM WebSphere MQ pour une exécution sous un utilisateur de domaine sous Windows
Utilisez l'assistant de préparation d' IBM WebSphere MQ pour entrer les détails du compte utilisateur de domaine. Vous pouvez également utiliser le panneau Gestion de l'ordinateur pour modifier les détails de la **connexion** pour le service IBM WebSphere MQ spécifique à l'installation.

Pour plus d'informations, voir Modification du mot de passe du compte utilisateur du service IBM WebSphere MQ Windows

Application de fichiers modèle de sécurité à Windows

L'application d'un modèle peut affecter les paramètres de sécurité appliqués aux fichiers et répertoires WebSphere MQ . Si vous utilisez le modèle hautement sécurisé, appliquez-le avant d'installer WebSphere MQ.

Windows prend en charge les fichiers de modèle de sécurité texte que vous pouvez utiliser pour appliquer des paramètres de sécurité uniformes à un ou plusieurs ordinateurs avec le composant logiciel enfichable MMC Configuration et analyse de la sécurité. En particulier, Windows fournit plusieurs modèles qui incluent une série de paramètres de sécurité dans le but de fournir des niveaux de sécurité spécifiques. Ces modèles incluent Compatible, Secure et Hautement Secure.

L'application de l'un de ces modèles peut affecter les paramètres de sécurité appliqués aux fichiers et répertoires WebSphere MQ . Si vous souhaitez utiliser le modèle hautement sécurisé, configurez votre machine avant d'installer WebSphere MQ.

Si vous appliquez le modèle hautement sécurisé à une machine sur laquelle WebSphere MQ est déjà installé, tous les droits que vous avez définis sur les fichiers et répertoires WebSphere MQ sont supprimés. Etant donné que ces droits sont supprimés, vous perdez *Administrator*, *mqm*et, le cas échéant, l'accès du groupe *Everyone* à partir des répertoires d'erreurs.

Groupes imbriqués

L'utilisation de groupes imbriqués est soumise à des restrictions. Elles résultent en partie du niveau fonctionnel du domaine et en partie des restrictions WebSphere MQ .

Active Directory peut prendre en charge différents types de groupe dans un contexte de domaine en fonction du niveau fonctionnel du domaine. Par défaut, les domaines Windows 2003 se trouvent au niveau fonctionnel *Windows 2000 mixte* . (Windows Server 2003, Windows XP, Windows Vista et Windows Server 2008 suivent tous le modèle de domaine Windows 2003.) Le niveau fonctionnel de domaine détermine les types de groupe pris en charge et le niveau d'imbrication autorisé lors de la configuration des ID utilisateur dans un environnement de domaine. Reportez-vous à la documentation Active Directory pour plus de détails sur la portée du groupe et les critères d'inclusion.

Outre les exigences relatives à Active Directory , des restrictions supplémentaires sont imposées sur les ID utilisés par WebSphere MQ. Les API réseau utilisées par WebSphere MQ ne prennent pas en charge toutes les configurations prises en charge par le niveau fonctionnel de domaine. Par conséquent, WebSphere MQ ne peut pas interroger les appartenances aux groupes des ID de domaine présents dans un groupe local de domaine qui est ensuite imbriqué dans un groupe local. En outre, l'imbrication multiple de groupes globaux et universels n'est pas prise en charge. Toutefois, les groupes globaux ou universels immédiatement imbriqués sont pris en charge.

Configuration de droits supplémentaires pour les applications Windows se connectant à IBM WebSphere MQ

Le compte sous lequel les processus IBM WebSphere MQ s'exécutent peut nécessiter une autorisation supplémentaire pour que l'accès à SYNCHRONISER aux processus d'application puisse être accordé.

Vous pouvez rencontrer des problèmes si vous avez des applications Windows , par exemple des pages ASP, qui se connectent à IBM WebSphere MQ et qui sont configurées pour s'exécuter à un niveau de sécurité supérieur à la normale.

IBM WebSphere MQ requiert l'accès SYNCHRONISER aux processus d'application afin de coordonner certaines actions. L'APAR IC35116 a été modifié IBM WebSphere MQ de sorte que les privilèges appropriés soient spécifiés. Toutefois, le compte sous lequel les processus IBM WebSphere MQ s'exécutent peut nécessiter une autorisation supplémentaire pour que l'accès demandé puisse être accordé.

Lorsqu'une application serveur tente pour la première fois de se connecter à un gestionnaire de files d'attente, IBM WebSphere MQ modifie le processus pour accorder les droits SYNCHRONISER aux administrateurs IBM WebSphere MQ . Pour configurer des droits supplémentaires sur l'ID utilisateur sous lequel les processus IBM WebSphere MQ s'exécutent, procédez comme suit:

1. Démarrez l'outil Stratégie de sécurité locale, cliquez sur Paramètres de sécurité-> Stratégies locales-> Affectations de droits d'utilisateur, cliquez sur "Déboguer les programmes".
2. Cliquez deux fois sur "Déboguer les programmes", puis ajoutez votre ID utilisateur IBM WebSphere MQ à la liste

Si le système se trouve dans un domaine Windows et que le paramètre de règle effectif n'est toujours pas défini, même si le paramètre de règle locale est défini, l'ID utilisateur doit être autorisé de la même manière au niveau du domaine, à l'aide de l'outil de règle de sécurité du domaine.

Configuration de la sécurité sous HP Integrity NonStop Server

Considérations de sécurité spécifiques aux systèmes HP Integrity NonStop Server .

Le client IBM WebSphere MQ pour HP Integrity NonStop Server prend en charge les protocoles TLS (Transport Layer Security) et SSL (Secure Sockets Layer) pour assurer la sécurité au niveau de la liaison lorsque vous vous connectez à un gestionnaire de files d'attente. Ces protocoles sont pris en charge à l'aide d'une implémentation d' OpenSSL. OpenSSL requiert une source de données aléatoires pour fournir des opérations cryptographiques puissantes.

OpenSSL

Présentation de la sécurité OpenSSL pour le client IBM WebSphere MQ for HP Integrity NonStop Server.

Le kit d'outils OpenSSL est une implémentation open source des protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) pour les communications sécurisées sur un réseau.

Le kit d'outils est développé par le projet OpenSSL . Pour plus d'informations sur le projet OpenSSL , voir https://www.openssl.org. Le client IBM WebSphere MQ pour HP Integrity NonStop Server contient des versions modifiées des bibliothèques OpenSSL et de la commande **openssl** . Les bibliothèques et la commande **openssl** sont portées à partir du kit d'outils OpenSSL 1.0.1cet sont fournies sous forme de code objet uniquement. Aucun code source n'est fourni.

Les bibliothèques OpenSSL sont chargées par les programmes d'application client IBM WebSphere MQ de manière dynamique, selon les besoins. Seules les bibliothèques OpenSSL fournies par IBM WebSphere MQ sont prises en charge pour une utilisation avec les applications client IBM WebSphere MQ .

La commande **openssl** , qui peut être utilisée à des fins de gestion des certificats, est installée dans le répertoire OSS `opt_installation_path/opt/mqm/bin`.

A l'aide de la commande **openssl** , vous pouvez créer et gérer des clés et des certificats numériques à l'aide de différents formats de données communs, et effectuer des tâches d'autorité de certification (CA) simples.

Le format par défaut des données de clé et de certificat traitées par OpenSSL est le format PEM (Privacy Enhanced Mail). Les données au format PEM sont des données ASCII codées en base64 . Les données peuvent donc être transférées à l'aide de systèmes textuels tels que le courrier électronique, et peuvent être coupées et collées à l'aide d'éditeurs de texte et de navigateurs Web. PEM est une norme Internet pour les échanges cryptographiques textuels et est spécifiée dans les RFC Internet 1421, 1422, 1423 et 1424. IBM WebSphere MQ suppose qu'un fichier portant l'extension `.pem` contient des données au format PEM. Un fichier au format PEM peut contenir plusieurs certificats et d'autres objets codés, et peut inclure des commentaires.

La prise en charge de SSL IBM WebSphere MQ sur d'autres systèmes d'exploitation peut exiger que les données de clé et de certificat des fichiers soient codées à l'aide de règles de codage distinctif (DER). DER est un ensemble de règles de codage permettant d'utiliser la notation ASN.1 dans les communications sécurisées. Les données codées à l'aide de DER sont des données binaires et le format des données de clé et de certificat codées à l'aide de DER est également appelé PKCS#12 ou PFX. Un fichier contenant ces données possède généralement l'extension `.p12` ou `.pfx`. La commande **openssl** peut être convertie entre le format PEM et le format PKCS#12 .

Démon d'entropie

OpenSSL requiert une source de données aléatoires pour fournir des opérations cryptographiques puissantes. La génération de nombres aléatoires est une fonction généralement fournie par le système d'exploitation ou par un processus démon à l'échelle du système. Le système d'exploitation HP Integrity NonStop Server ne fournit pas cette fonction dans le système d'exploitation.

Lorsque vous utilisez le support SSL et TLS fourni avec le client IBM WebSphere MQ pour HP Integrity NonStop Server, un processus appelé démon d'entropie est nécessaire pour fournir la source de données aléatoires. Lorsque vous démarrez un canal client qui requiert SSL ou TLS, OpenSSL s'attend à ce qu'un démon d'entropie s'exécute et fournisse ses services sur un socket dans le système de fichiers OSS à l'adresse `/etc/egd-pool`.

Un démon d'entropie n'est pas fourni par le client IBM WebSphere MQ pour HP Integrity NonStop Server. Le client IBM WebSphere MQ pour HP Integrity NonStop Server est testé avec les démons d'entropie suivants:

- amqjkdm0 (comme fourni par le serveur IBM WebSphere MQ 5.3)
- `/usr/local/bin/prngd` (version 0.9.27, telle que fournie par HP Integrity NonStop Server Open Source Technical Library)

Configuration de la sécurité du client IBM WebSphere MQ MQI

Vous devez prendre en compte la sécurité du client IBM WebSphere MQ MQI pour que les applications client n'aient pas un accès illimité aux ressources du serveur.

Lors de l'exécution d'une application client, n'exécutez pas l'application à l'aide d'un ID utilisateur disposant de droits d'accès plus nombreux que nécessaire ; par exemple, un utilisateur du groupe `mqm` ou même l'utilisateur `mqm` lui-même.

En exécutant une application en tant qu'utilisateur disposant de trop de droits d'accès, vous risquez que l'application accède à des parties du gestionnaire de files d'attente et les modifie, soit par accident, soit par malveillance.

Il existe deux aspects de la sécurité entre une application client et son serveur de gestionnaire de files d'attente: l'authentification et le contrôle d'accès.

- L'authentification peut être utilisée pour s'assurer que l'application client, exécutée en tant qu'utilisateur spécifique, est bien celle qu'elle dit être. En utilisant l'authentification, vous pouvez empêcher un agresseur d'accéder à votre gestionnaire de files d'attente en empruntant l'une de vos applications.

  Vous devez utiliser l'authentification mutuelle dans SSL ou TLS. Pour plus d'informations, voir «Utilisation de SSL ou TLS», à la page 115

- Le contrôle d'accès peut être utilisé pour accorder ou supprimer des droits d'accès pour un utilisateur ou un groupe d'utilisateurs spécifique. En exécutant une application client avec un utilisateur créé spécifiquement (ou un utilisateur appartenant à un groupe spécifique), vous pouvez ensuite utiliser des contrôles d'accès pour vous assurer que l'application ne peut pas accéder à des parties de votre gestionnaire de files d'attente auxquelles l'application n'est pas censée accéder.

  Lors de la configuration du contrôle d'accès, vous devez tenir compte des règles d'authentification de canal et de la zone MCAUSER sur un canal. Ces deux fonctions permettent de modifier l'ID utilisateur utilisé pour vérifier les droits de contrôle d'accès.

  Pour plus d'informations sur le contrôle d'accès, voir «Autorisation de l'accès aux objets», à la page 166.

Si vous avez configuré une application client pour qu'elle se connecte à un canal spécifique avec un ID restreint, mais que le canal possède un ID administrateur défini dans sa zone MCAUSER, à condition que l'application client se connecte correctement, l'ID administrateur est utilisé pour les vérifications de contrôle d'accès. Par conséquent, l'application client dispose de droits d'accès complets à votre gestionnaire de files d'attente.

Pour plus d'informations sur l'attribut MCAUSER, voir «Mappage d'un ID utilisateur vérifié par le client à un ID utilisateur MCAUSER», à la page 193.

Les règles d'authentification de canal peuvent également être utilisées comme méthode de contrôle de l'accès à un gestionnaire de files d'attente, en définissant des règles et des critères spécifiques pour l'acceptation d'une connexion.

Pour plus d'informations sur les règles d'authentification de canal, voir: «Enregistrements d'authentification de canal», à la page 41.

Comment indiquer que seuls les CipherSpecs certifiés FIPS sont utilisés lors de l'exécution sur MQI Client

Créez vos référentiels de clés à l'aide d'un logiciel compatible FIPS, puis indiquez que le canal doit utiliser des CipherSpecscertifiés FIPS.

Pour être conformes à la norme FIPS lors de l'exécution, les référentiels de clés doivent avoir été créés et gérés à l'aide de logiciels conformes à la norme FIPS tels que runmqakm avec l'option -fips.

Vous pouvez spécifier qu'un canal SSL ou TLS doit utiliser uniquement des CipherSpecs certifiés FIPS de trois manières, répertoriées par ordre de priorité:

1. Définissez la zone FipsRequired dans la structure MQSCO sur MQSSL_FIPS_YES.
2. Définissez la variable d'environnement MQSSLFIPS sur YES.
3. Définissez l'attribut SSLFipsRequired sur YES dans le fichier de configuration du client.

Par défaut, les CipherSpecs certifiés FIPS ne sont pas requis.

Ces valeurs ont la même signification que les valeurs de paramètre équivalentes sur ALTER QMGR SSLFIPS (voir ALTER QMGR). Si le processus client ne dispose actuellement d'aucune connexion SSL ou TLS active et qu'une valeur FipsRequired est correctement spécifiée sur un MQCONNX SSL, toutes les connexions SSL suivantes associées à ce processus doivent utiliser uniquement les CipherSpecs associées à cette valeur. Cela s'applique jusqu'à ce que cette connexion et toutes les autres connexions SSL ou TLS soient arrêtées, à l'étape où une connexion MQCONNX ultérieure peut fournir une nouvelle valeur pour FipsRequired.

Si du matériel de cryptographie est présent, les modules de cryptographie utilisés par WebSphere MQ peuvent être configurés pour être ceux fournis par le produit matériel et ils peuvent être certifiés FIPS à un niveau particulier. Les modules configurables et leur certification FIPS dépendent du produit matériel utilisé.

Dans la mesure du possible, si les CipherSpecs FIPS uniquement sont configurés, le client MQI rejette les connexions qui spécifient un CipherSpec non FIPS avec MQRC_SSL_INITIALIZATION_ERROR. WebSphere MQ ne garantit pas le rejet de toutes ces connexions et il est de votre responsabilité de déterminer si votre configuration WebSphere MQ est compatible FIPS.

Concepts associés

«Federal Information Processing Standards (FIPS) pour UNIX, Linuxet Windows», à la page 27
Lorsque la cryptographie est requise sur un canal SSL ou TLS sous Windows, systèmes UNIX and Linux , WebSphere MQ utilise un package de cryptographie appelé IBM Crypto for C (ICC). Sur les plateformes Windows, UNIX and Linux , le logiciel ICC a transmis le programme FIPS (Federal Information Processing Standards) Cryptomodule Validation Program du US National Institute of Standards and Technology, au niveau 140-2.

Strophe SSL du fichier de configuration client

Référence associée

FipsRequired (MQLONG)

MQSSLFIPS

Exécution d'applications client SSL ou TLS avec plusieurs installations de GSKit V8.0 sous AIX

Les applications client SSL ou TLS sur AIX peuvent rencontrer des MQRC_CHANNEL_CONFIG_ERROR et des erreurs AMQ6175 lors de l'exécution sur des systèmes AIX avec plusieurs installations GSKit V8.0 .

Lors de l'exécution d'applications client sur un système AIX avec plusieurs installations GSKit V8.0 , les appels de connexion client peuvent renvoyer MQRC_CHANNEL_CONFIG_ERROR lors de l'utilisation de SSL ou TLS. /var/mqm/errors consigne l'erreur d'enregistrement AMQ6175 et AMQ9220 pour l'application client défaillante, par exemple:

```
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 ----------------------------------------------------------
```

Cette erreur est généralement due au fait que le paramètre de la variable d'environnement LIBPATH ou LD_LIBRARY_PATH a amené le client IBM WebSphere MQ à charger un ensemble mixte de bibliothèques à partir de deux installations GSKit V8.0 différentes. L'exécution d'une application clientIBM WebSphere MQ dans un environnement Db2 peut provoquer cette erreur.

Pour éviter cette erreur, incluez les répertoires de bibliothèque IBM WebSphere MQ à l'avant du chemin d'accès à la bibliothèque afin que les bibliothèques IBM WebSphere MQ soient prioritaires. Pour ce faire, utilisez la commande **setmqenv** avec le paramètre **-k** , par exemple:

```
. /usr/mqm/bin/setmqenv -s -k
```

Pour plus d'informations sur l'utilisation de la commande **setmqenv** , voir setmqenv (set WebSphere MQ environment)

Configuration des communications pour SSL ou TLS sur les systèmes UNIX, Linux, and Windows

Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

Pour configurer votre installation SSL ou TLS, vous devez définir vos canaux pour utiliser les protocoles SSL ou TLS. Vous devez également créer et gérer vos certificats numériques. Sur les systèmes UNIX, Linux et Windows , vous pouvez effectuer les tests avec des certificats autosignés.

Les certificats autosignés ne peuvent pas être révoqués, ce qui pourrait permettre à un agresseur de usurper une identité après qu'une clé privée a été compromise. Les autorités de certification peuvent révoquer un certificat compromis, pour en empêcher toute utilisation future. Les certificats signés par une autorité de certification sont donc plus sûrs à utiliser dans un environnement de production, bien que les certificats autosignés soient plus pratiques pour un système de test.

Pour plus d'informations sur la création et la gestion des certificats, voir «Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows», à la page 119.

Cette collection de rubriques présente certaines des tâches liées à la configuration des communications SSL et fournit des conseils étape par étape sur l'exécution de ces tâches.

Vous pouvez également vouloir tester l'authentification des clients SSL ou TLS, qui constitue une partie facultative des protocoles. Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation de IBM WebSphere MQ, le serveur SSL ou TLS demande toujours un certificat au client.

Sur les systèmes UNIX, Linux et Windows , le client SSL ou TLS envoie un certificat uniquement s'il en a un libellé au format IBM WebSphere MQ correct:

- Pour un gestionnaire de files d'attente, le format est `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente remplacé par des minuscules. Par exemple, pour `QM1`, `ibmwebspheremqqm1`
- Pour un client IBM WebSphere MQ , `ibmwebspheremq` suivi de votre ID utilisateur de connexion est passé en minuscules, par exemple `ibmwebspheremqmyuserid`.

IBM WebSphere MQ utilise le préfixe `ibmwebspheremq` sur un libellé pour éviter toute confusion avec les certificats d'autres produits. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie pas de certificat, l'authentification échoue uniquement si l'extrémité du canal agissant en tant que serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur de paramètre SSLPEER définie. Pour plus d'informations, voir «Connexion de deux gestionnaires de files d'attente via le protocole SSL ou TLS», à la page 216.

Utilisation de SSL ou TLS

Ces rubriques fournissent des instructions pour l'exécution de tâches uniques liées à l'utilisation de SSL ou TLS avec IBM WebSphere MQ.

La plupart d'entre eux sont utilisés comme étapes dans les tâches de niveau supérieur décrites dans les sections suivantes:

- «Identification et authentification des utilisateurs», à la page 151
- «Autorisation de l'accès aux objets», à la page 166
- «Confidentialité des messages», à la page 215
- «Intégrité des données de messages», à la page 236
- «Maintien de la sécurité des clusters», à la page 255

Utilisation de SSL ou TLS sous HP Integrity NonStop Server

Décrit l'implémentation de la sécurité IBM WebSphere MQ client for HP Integrity NonStop Server OpenSSL , y compris les services de sécurité, les composants, les versions de protocole prises en charge, les CipherSpecsprises en charge et les fonctionnalités de sécurité non prises en charge.

IBM WebSphere MQ La prise en charge de SSL et TLS fournit les services de sécurité suivants pour les canaux client:

- Authentification du serveur et, éventuellement, authentification du client.
- Chiffrement et déchiffrement des données qui transitent par un canal.
- Vérifications d'intégrité sur les données qui transitent par un canal.

La prise en charge SSL et TLS fournie avec le client IBM WebSphere MQ pour HP Integrity NonStop Server comprend les composants suivants:

- Les bibliothèques OpenSSL et la commande **openssl** .
- IBM WebSphere MQ commande de dissimulation de mot de passe, **amqrsslc**.

Les composants requis suivants pour l'opération de canal client SSL ou TLS ne sont pas fournis avec le client IBM WebSphere MQ pour HP Integrity NonStop Server:

- Démon d'entropie fournissant une source de données aléatoires pour la cryptographie OpenSSL .

Versions de protocole prises en charge

Le client IBM WebSphere MQ pour HP Integrity NonStop Server prend en charge les versions de protocole suivantes:

- SSL 3.0
- TLS 1.0
- TLS 1.2

CipherSpecs pris en charge

Le client IBM WebSphere MQ pour HP Integrity NonStop Server prend en charge les versions CipherSpecs suivantes:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- RC4_SHA_US
- RC4_MD5_US
- TRIPLE_DES_SHA_US
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (déprécié)
- DES_SHA_EXPORT1024
- RC4_56_SHA_EXPORT1024
- RC4_MD5_EXPORT
- RC2_MD5_EXPORT
- DES_SHA_EXPORT

- TLS_RSA_WITH_DES_CBC_SHA
- NULL_SHA
- NULL_MD5
- FIPS_WITH_DES_CBC_SHA
- FIPS_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384

Fonctionnalité de sécurité non prise en charge

Le client IBM WebSphere MQ pour HP Integrity NonStop Server ne prend actuellement pas en charge:

- PKCS#11 Prise en charge du matériel de cryptographie
- Vérification de la liste de révocation de certificat LDAP
- Vérification du protocole OCSP Online Certificate Status Protocol
- FIPS 140-2, contrôles de la suite de chiffrement NSA SUITE B

Gestion des certificats

Utilisez un ensemble de fichiers pour stocker les informations de certificat numérique et de révocation de certificat.

La prise en charge SSL et TLS de IBM WebSphere MQ utilise un ensemble de fichiers pour stocker les informations de certificat numérique et de révocation de certificat. Ces fichiers se trouvent dans un répertoire spécifié à l'aide d'un programme via la zone KeyRepository dans la structure MQSCO transmise lors de l'appel MQCONNX, par la variable d'environnement *MQSSLKEYR* , ou dans la strophe SSL de `mqclient.ini` à l'aide de l'attribut SSLKeyRepository .

La structure MQSCO est prioritaire sur la variable d'environnement MQSSLKEYR qui est prioritaire sur la valeur de la section du fichier ini.

Important : L'emplacement du référentiel de clés indique un emplacement de répertoire et non un nom de fichier sur la plateforme HP Integrity NonStop Server .

Le client IBM WebSphere MQ for HP Integrity NonStop Server utilise les fichiers nommés suivants, sensibles à la casse, dans l'emplacement du référentiel de clés:

- «Espace de stockage de certificats personnel», à la page 118
- «Magasin de clés de confiance de certificat», à la page 118
- «Fichier de dissimulation de phrase passe», à la page 118
- «Fichier de liste de révocation de certificat», à la page 118

Espace de stockage de certificats personnel
Le fichier de magasin de certificats personnels, `cert.pem`.

Ce fichier contient le certificat personnel et la clé privée chiffrée à utiliser par le client, au format PEM. L'existence de ce fichier est facultative lorsque vous utilisez des canaux SSL ou TLS qui ne nécessitent pas d'authentification client. Lorsque l'authentification du client est requise par le canal et que SSLCAUTH (REQUIRED) est spécifié dans la définition de canal, ce fichier doit exister et contenir à la fois le certificat et la clé privée chiffrée.

Les droits d'accès aux fichiers doivent être définis sur ce fichier pour permettre l'accès en lecture au propriétaire du magasin de certificats.

Un fichier `cert.pem` correctement formaté doit contenir exactement deux sections avec les en-têtes et pieds de page suivants:

```
-----BEGIN PRIVATE KEY-----
Base 64 ASCII encoded private key data here
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

La phrase passe de la clé privée chiffrée est stockée dans le fichier de dissimulation de phrase passe, `Stash.sth`.

Magasin de clés de confiance de certificat
Le fichier de clés certifiées du certificat, `trust.pem`.

Ce fichier contient les certificats nécessaires à la validation des certificats personnels utilisés par les gestionnaires de files d'attente auxquels le client se connecte, au format PEM. Le magasin de clés de confiance de certificat est obligatoire pour tous les canaux client SSL ou TLS.

Les droits d'accès aux fichiers doivent être définis pour limiter l'accès en écriture à ce fichier.

Un fichier `trust.pem` correctement formaté doit contenir une ou plusieurs sections avec les en-têtes et pieds de page suivants:

```
-----BEGIN CERTIFICATE-----
Base 64 ASCII encoded certificate data here
-----END CERTIFICATE-----
```

Fichier de dissimulation de phrase passe
Le fichier de dissimulation de la phrase passe, `Stash.sth`.

Ce fichier est un format binaire privé pour IBM WebSphere MQ et contient la phrase de passe chiffrée à utiliser lorsque vous accédez à la clé privée contenue dans le fichier `cert.pem` . La clé privée elle-même est stockée dans le magasin de certificats `cert.pem` .

Ce fichier est créé ou modifié à l'aide de l'outil de ligne de commande IBM WebSphere MQ **amqrsslc** avec le paramètre **-s** . Par exemple, où le répertoire `/home/alice` contient un fichier `cert.pem` :

```
amqrsslc -s /home/alice/cert

  Enter password for Keystore /home/alice/cert.pem :
    password

  Stashed the password in file /home/alice/Stash.sth
```

Les droits d'accès aux fichiers doivent être définis sur ce fichier pour permettre l'accès en lecture au propriétaire du magasin de certificats personnels associé.

Fichier de liste de révocation de certificat
Le fichier de liste de révocation de certificat, `crl.pem`.

Ce fichier contient les listes de révocation de certificat (CRL) que le client utilise pour valider les certificats numériques, au format PEM. L'existence de ce fichier est facultative. Si ce fichier n'est pas présent, aucune vérification de révocation de certificat n'est effectuée lorsque vous validez des certificats.

Les droits d'accès aux fichiers doivent être définis pour limiter l'accès en écriture à ce fichier.

Un fichier `crl.pem` correctement formaté doit contenir une ou plusieurs sections avec les en-têtes et pieds de page suivants:

```
-----BEGIN X509 CRL-----
Base 64 ASCII encoded CRL data here
-----END X509 CRL-----
```

Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows

Sur les systèmes UNIX, Linux et Windows , la prise en charge de SSL (Secure Sockets Layer) est installée avec IBM WebSphere MQ.

Pour plus d'informations sur les règles de validation de certificat, voir Validation de certificat et conception de règles de confiance.

Utilisation des commandes iKeyman, iKeycmd, runmqakm et runmqckm

Sur les systèmes UNIX, Linux et Windows , gérez les clés et les certificats numériques à l'aide de l'interface graphique iKeyman ou à partir de la ligne de commande à l'aide de iKeycmd ou de runmqakm.

- Pour les systèmes **UNIX and Linux** :
  - Utilisez la commande **strmqikm** pour démarrer l'interface graphique iKeyman .
  - La commande **runmqckm** permet d'effectuer des tâches à l'aide de l'interface de ligne de commande iKeycmd .
  - Utilisez la commande **runmqakm** pour effectuer des tâches avec l'interface de ligne de commande runmqakm. La syntaxe de commande de **runmqakm** est identique à celle de **runmqckm**.

    Si vous devez gérer les certificats SSL d'une manière conforme à la norme FIPS, utilisez la commande **runmqakm** à la place des commandes **runmqckm** ou **strmqikm** .

  Voir Gestion des clés et des certificats pour une description complète des interfaces de ligne de commande pour les commandes **runmqckm** et **runmqakm** .

  Si vous utilisez des certificats ou des clés stockés sur du matériel de cryptographie PKCS #11, notez que iKeycmd et iKeyman sont des programmes 64 bits. Etant donné que les modules externes requis pour la prise en charge de PKCS #11 seront chargés dans un processus 64 bits, une bibliothèque PKCS #11 64 bits doit être installée pour l'administration du matériel de cryptographie. Les plateformes Windows et Linux x86 32 bits sont les seules exceptions, car les programmes iKeyman et iKeycmd sont 32 bits sur ces plateformes.

  Sur les plateformes suivantes, où l'environnement d'exécution Java était 32 bits dans les versions antérieures du produit, mais est 64 bits uniquement dans IBM WebSphere MQ Version 7.5, vous devrez peut-être installer des pilotes PKCS#11 supplémentaires adaptés au mode d'adressage de l'environnement d'exécution Java **iKeyman** et **iKeycmd** . En effet, le pilote PKCS#11 doit utiliser le même mode d'adressage que l'environnement d'exécution Java. Le tableau suivant illustre les modes d'adressage de l'environnement d'exécution JavaIBM WebSphere MQ Version 7.5.

Tableau 12. IBM WebSphere MQ Version 7.5 Modes d'adressage de l'environnement d'exécution Java

Plateforme	**Modes d'adressage de l'environnement d'exécution Java**
Windows (32 bits ou 64 bits)	32
Linux for System x 32 bits	32
Linux pour System x 64 bits	64

Tableau 12. IBM WebSphere MQ Version 7.5 Modes d'adressage de l'environnement d'exécution Java (suite)

Plateforme	Modes d'adressage de l'environnement d'exécution Java
Linux pour System p	64
Linux pour System z	64
HP-UX	64
Solaris SPARC	64
Solaris x86-64	64
AIX	64

Avant d'exécuter la commande **strmqikm** pour démarrer l'interface graphique d' iKeyman , vérifiez que vous travaillez sur une machine capable d'exécuter le système X-Window et que vous effectuez les opérations suivantes:

- Définissez la variable d'environnement DISPLAY, par exemple:

```
export DISPLAY=mypc:0
```

- Vérifiez que votre variable d'environnement PATH contient **/usr/bin** et **/bin**. Cette opération est également requise pour les commandes **runmqckm** et **runmqakm** . Exemple :

```
export PATH=$PATH:/usr/bin:/bin
```

- Pour les systèmes **Windows** :
  - Utilisez la commande **strmqikm** pour démarrer l'interface graphique iKeyman .
  - La commande **runmqckm** permet d'effectuer des tâches à l'aide de l'interface de ligne de commande iKeycmd .

    Si vous devez gérer les certificats SSL d'une manière conforme à la norme FIPS, utilisez la commande **runmqakm** à la place des commandes **runmqckm** ou **strmqikm** .

Pour demander le traçage SSL sur les systèmes UNIX, Linux ou Windows , voir strmqtrc.

Référence associée

Commandes runmqckm et runmqakm

Configuration d'un référentiel de clés sur les systèmes UNIX, Linux, and Windows

Vous pouvez configurer un référentiel de clés à l'aide de l'interface utilisateur iKeyman ou à l'aide des commandes **iKeycmd** ou **runmqakm** .

Pourquoi et quand exécuter cette tâche

Une connexion SSL ou TLS requiert un *référentiel de clés* à chaque extrémité de la connexion. Chaque gestionnaire de files d'attente IBM WebSphere MQ et IBM WebSphere MQ MQI client doivent avoir accès à un référentiel de clés. Pour plus d'informations, voir «Référentiel de clés SSL ou TLS», à la page 25.

Sur les systèmes UNIX, Linux, and Windows , les certificats numériques sont stockés dans un fichier de base de données de clés géré à l'aide de l'interface utilisateur **iKeyman** ou des commandes **iKeycmd** ou **runmqakm** . Ces certificats numériques comportent des libellés. Un libellé spécifique associe un certificat personnel à un gestionnaire de files d'attente ou à IBM WebSphere MQ MQI client. SSL et TLS utilisent ce certificat à des fins d'authentification. Sur les systèmes UNIX, Linux, and Windows , IBM WebSphere MQ utilise `ibmwebspheremq` comme préfixe de libellé pour éviter toute confusion avec les certificats d'autres produits. Le préfixe est suivi du nom du gestionnaire de files d'attente ou de l'ID de connexion de

l'utilisateur IBM WebSphere MQ MQI client , remplacé par des minuscules. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le nom du fichier de la base de données de clés comprend un chemin et un nom de radical:

- Sur les systèmes UNIX and Linux , le chemin par défaut d'un gestionnaire de files d'attente (défini lors de la création du gestionnaire de files d'attente) est `/var/mqm/qmgrs/<queue_manager_name>/ssl`.

  Sur les systèmes Windows , le chemin par défaut est *MQ_INSTALLATION_PATH*`\Qmgrs\`*queue_manager_name*`\ssl`, où *MQ_INSTALLATION_PATH* est le répertoire dans lequel IBM WebSphere MQ est installé. Par exemple, `C:\program files\IBM\WebSphere MQ\Qmgrs\QM1\ssl`.

  Le nom de radical par défaut est `key`. Vous pouvez éventuellement choisir votre propre chemin et nom de radical, mais l'extension doit être `.kdb`.

  Si vous choisissez votre propre chemin ou nom de fichier, définissez les droits d'accès au fichier pour contrôler étroitement l'accès à ce dernier.
- Pour un client WebSphere MQ , il n'existe pas de chemin ou de nom de radical par défaut. Contrôler étroitement l'accès à ce fichier. L'extension doit être `.kdb`.

Ne créez pas de référentiels de clés sur un système de fichiers qui ne prend pas en charge les verrous de niveau fichier, par exemple NFS version 2 sur les systèmes Linux .

Pour plus d'informations sur la vérification et la spécification du nom de fichier de la base de données de clés, voir «Modification de l'emplacement du référentiel de clés d'un gestionnaire de files d'attente sur les systèmes UNIX, Linux ou Windows», à la page 125 . Vous pouvez spécifier le nom du fichier de la base de données de clés avant ou après la création du fichier de la base de données de clés.

L'ID utilisateur à partir duquel vous exécutez les commandes **iKeyman** ou **iKeycmd** doit disposer de droits d'accès en écriture pour le répertoire dans lequel le fichier de base de données de clés est créé ou mis à jour. Pour un gestionnaire de files d'attente utilisant le répertoire `ssl` par défaut, l'ID utilisateur à partir duquel vous exécutez **iKeyman** ou **iKeycmd** doit être membre du groupe mqm. Pour un IBM WebSphere MQ MQI client, si vous exécutez **iKeyman** ou **iKeycmd** à partir d'un ID utilisateur différent de celui sous lequel le client s'exécute, vous devez modifier les droits d'accès aux fichiers pour permettre à IBM WebSphere MQ MQI client d'accéder au fichier de la base de données de clés lors de l'exécution. Pour plus d'informations, voir «Accès et sécurisation de vos fichiers de base de données de clés sous Windows», à la page 123 ou «Accès et sécurisation de vos fichiers de la base de données clé sous les systèmes UNIX and Linux», à la page 123.

Dans **iKeyman** ou **iKeycmd** version 7.0, les nouvelles bases de données de clés sont automatiquement remplies avec un ensemble de certificats d'autorité de certification prédéfinis. Dans **iKeyman** ou **iKeycmd** version 8.0, les bases de données de clés ne sont pas automatiquement remplies, ce qui rend la configuration initiale plus sécurisée car vous incluez uniquement les certificats de l'autorité de certification de votre choix dans votre fichier de base de données de clés.

Remarque : En raison de ce changement de comportement pour GSKit version 8.0 qui entraîne l'ajout automatique des certificats d'autorité de certification au référentiel, vous devez ajouter manuellement vos certificats d'autorité de certification préférés. Ce changement de comportement vous offre un contrôle plus granulaire sur les certificats de l'autorité de certification utilisés. Voir «Ajout de certificats d'autorité de certification par défaut dans un référentiel de clés vide sur les systèmes UNIX, Linux, and Windows avec GSKit version 8.0», à la page 124.

Vous créez la base de données de clés à l'aide de la ligne de commande ou de l'interface utilisateur **strmqikm** (iKeyman).

Remarque : Si vous devez gérer les certificats TLS d'une manière compatible avec FIPS, utilisez la commande **runmqakm** . L'interface utilisateur **strmqikm** ne fournit pas d'option compatible FIPS.

Procédure

Créez une base de données de clés à l'aide de la ligne de commande.

1. Exécutez l'une des commandes suivantes:
   - Sur les systèmes UNIX, Linux, and Windows :

     ```
     runmqckm -keydb -create -db filename -pw password -type cms -stash
     ```

   - Utilisation de runmqakm:

     ```
     runmqakm -keydb -create -db filename -pw password -type cms
         -stash -fips -strong
     ```

   où :

   -db *nom_fichier*
   Indique le nom de fichier qualifié complet d'une base de données de clés CMS et doit avoir l'extension de fichier `.kdb`.

   -pw *mot_de_passe*
   Indique le mot de passe de la base de données de clés CMS.

   -type *cms*
   Indique le type de base de données. (Pour IBM WebSphere MQ, il doit s'agir de `cms`.)

   -stash
   Sauvegarde le mot de passe de la base de données de clés dans un fichier.

   -fips
   Désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

   -forte
   Vérifie que le mot de passe entré répond aux exigences minimales de puissance de mot de passe. Les exigences minimales pour un mot de passe sont les suivantes:
   - Le mot de passe doit avoir une longueur minimale de 14 caractères.
   - Le mot de passe doit contenir au moins un caractère minuscule, un caractère majuscule et un chiffre ou un caractère spécial. Les caractères spéciaux incluent l'astérisque (*), le signe dollar ($), le signe nombre (#) et le signe pourcentage (%). Un espace est classé comme un caractère spécial.
   - Chaque caractère peut apparaître au maximum trois fois dans un mot de passe.
   - Un maximum de deux caractères consécutifs dans le mot de passe peut être identique.
   - Tous les caractères se trouvent dans le jeu de caractères ASCII imprimables standard compris entre 0x20 et 0x7E.

Vous pouvez également créer une base de données de clés à l'aide de l'interface utilisateur **strmqikm** (iKeyman).

2. Sur les systèmes UNIX and Linux , connectez-vous en tant que superutilisateur. Sur les systèmes Windows , connectez-vous en tant qu'administrateur ou en tant que membre du groupe MQM.
3. Démarrez l'interface utilisateur iKeyman en exécutant la commande **strmqikm** .
4. Dans le menu **Fichier de base de données de clés** , cliquez sur **Nouveau**.

   La fenêtre Nouveau s'ouvre.
5. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
6. Dans la zone **Nom de fichier** , entrez un nom de fichier.

   Cette zone contient déjà le texte `key.kdb`. Si votre nom de radical est `key`, laissez cette zone inchangée. Si vous avez spécifié un autre nom de radical, remplacez `key` par votre nom de radical. Toutefois, vous ne devez pas modifier l'extension `.kdb` .
7. Dans la zone **Emplacement** , entrez le chemin d'accès.

   Exemple :

- Pour un gestionnaire de files d'attente: `/var/mqm/qmgrs/QM1/ssl` (sur les systèmes UNIX and Linux) ou `C:\Program Files\IBM\WebSphere MQ\qmgrs\QM1\ssl` (sur les systèmes Windows).

  Le chemin doit correspondre à la valeur de l'attribut **SSLKeyRepository** du gestionnaire de files d'attente.
- Pour un client IBM WebSphere MQ : `/var/mqm/ssl` (sur les systèmes UNIX and Linux) ou `C:\mqm\ssl` (sur les systèmes Windows).

8. Cliquez sur **Ouvrir**.

   La fenêtre Password Prompt s'ouvre.
9. Entrez un mot de passe dans la zone **Mot de passe** , puis entrez-le à nouveau dans la zone **Confirmer le mot de passe** .
10. Cochez la case **Stocker le mot de passe dans un fichier** .

    Remarque : Si vous ne stockez pas le mot de passe, les tentatives de démarrage des canaux SSL ou TLS échouent car ils ne peuvent pas obtenir le mot de passe requis pour accéder au fichier de la base de données de clés.
11. Cliquez sur **OK**.

    La fenêtre Certificats personnels s'ouvre.
12. Définissez les droits d'accès comme décrit dans «Accès et sécurisation de vos fichiers de base de données de clés sous Windows», à la page 123 ou «Accès et sécurisation de vos fichiers de la base de données clé sous les systèmes UNIX and Linux», à la page 123.

Accès et sécurisation de vos fichiers de base de données de clés sous Windows
Il se peut que les fichiers de la base de données de clés ne disposent pas des droits d'accès appropriés. Vous devez définir l'accès approprié à ces fichiers.

Définissez le contrôle d'accès aux fichiers *key*`.kdb`, *key*`.sth`, *key*`.crl`et *key*`.rdb`, où *key* est le nom de radical de votre base de données de clés, pour accorder des droits à un ensemble restreint d'utilisateurs.

Envisagez d'accorder l'accès comme suit:

droits complets
BUILTIN\Administrators, NT AUTHORITY\SYSTEM et l'utilisateur qui a créé les fichiers base de données.

droit de lecture
Pour un gestionnaire de files d'attente, le groupe mqm local uniquement. Cela suppose que l'agent MCA s'exécute sous un ID utilisateur dans le groupe mqm.

Pour un client, ID utilisateur sous lequel le processus client est exécuté.

Accès et sécurisation de vos fichiers de la base de données clé sous les systèmes UNIX and Linux
Il se peut que les fichiers de la base de données de clés ne disposent pas des droits d'accès appropriés. Vous devez définir l'accès approprié à ces fichiers.

Pour un gestionnaire de files d'attente, définissez les droits d'accès aux fichiers de la base de données de clés de sorte que les processus de gestionnaire de files d'attente et de canal puissent les lire si nécessaire, mais que les autres utilisateurs ne puissent pas les lire ou les modifier. Normalement, l'utilisateur mqm a besoin de droits d'accès en lecture. Si vous avez créé le fichier de la base de données de clés en vous connectant en tant qu'utilisateur mqm, les droits sont probablement suffisants ; si vous n'étiez pas l'utilisateur mqm, mais un autre utilisateur du groupe mqm, vous devrez probablement accorder des droits de lecture à d'autres utilisateurs du groupe mqm.

De même pour un client, définissez des droits sur les fichiers de la base de données de clés afin que les processus de l'application client puissent les lire lorsque cela est nécessaire, mais les autres utilisateurs ne peuvent pas les lire ou les modifier. Normalement, l'utilisateur sous lequel le processus client s'exécute a besoin de droits de lecture. Si vous avez créé le fichier de la base de données de clés en vous connectant en tant que cet utilisateur, les droits sont probablement suffisants ; si vous n'étiez

pas l'utilisateur du processus client, mais un autre utilisateur de ce groupe, vous devrez probablement accorder des droits de lecture à d'autres utilisateurs du groupe.

Définissez les droits sur les fichiers *key*.kdb, *key*.sth, *key*.crlet *key*.rdb, où *key* est le nom de radical de votre base de données de clés, pour lire et écrire pour le propriétaire du fichier, et pour lire pour le groupe d'utilisateurs mqm ou client (-rw-r -----).

Ajout de certificats d'autorité de certification par défaut dans un référentiel de clés vide sur les systèmes UNIX, Linux, and Windows avec GSKit version 8.0
Suivez cette procédure pour ajouter un ou plusieurs des certificats de l'autorité de certification par défaut à un référentiel de clés vide avec GSKit version 8.

Dans GSKit version 7.0, le comportement lors de la création d'un nouveau référentiel de clés consistait à ajouter automatiquement un ensemble de certificats d'autorité de certification par défaut pour les autorités de certification fréquemment utilisées. Pour GSKit version 8, ce comportement a changé de sorte que les certificats de l'autorité de certification ne sont plus automatiquement ajoutés au référentiel. L'utilisateur est désormais tenu d'ajouter manuellement des certificats de l'autorité de certification dans le référentiel de clés.

Utilisation d'iKeyman

Suivez les étapes suivantes sur la machine sur laquelle vous souhaitez ajouter le certificat de l'autorité de certification :

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sur les systèmes UNIX, Linux et Windows).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de clés dans lequel vous souhaitez ajouter le certificat, par exemple key.kdb.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de clés s'affiche dans la zone **Nom du fichier**.
8. Dans la zone **Key database content**, sélectionnez **Signer Certificates**.
9. Cliquez sur **Remplir**. La fenêtre Ajouter un certificat de l'autorité de certification s'ouvre.
10. Les certificats de l'autorité de certification pouvant être ajoutés au référentiel sont affichés dans une structure d'arborescence hiérarchique. Sélectionnez l'entrée de niveau supérieur pour l'organisation dont vous souhaitez faire confiance aux certificats de l'autorité de certification pour afficher la liste complète des certificats de l'autorité de certification valides.
11. Sélectionnez dans la liste les certificats de l'autorité de certification que vous souhaitez approuver et cliquez sur **OK**. Les certificats sont ajoutés au référentiel de clés.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour répertorier, puis ajoutez des certificats d'autorité de certification à l'aide de iKeycmd:

- Exécutez la commande suivante pour répertorier les certificats de l'autorité de certification par défaut avec les organisations qui les émettent:

```
runmqckm -cert -listsigners
```

- Exécutez la commande suivante pour ajouter tous les certificats de l'autorité de certification pour l'organisation spécifiée dans la zone *label* :

```
runmqckm -cert -populate -db filename -pw password -label label
```

où :

-db *filename*	est le nom de chemin qualifié complet de la base de données de clés.
-pw *password*	est le mot de passe de la base de données de clés.
-label *label*	correspond au libellé du certificat.

Remarque : L'ajout d'un certificat d'autorité de certification à un référentiel de clés permet à WebSphere MQ de faire confiance à tous les certificats personnels signés par ce certificat d'autorité de certification. Réfléchissez soigneusement aux autorités de certification auxquelles vous souhaitez faire confiance et ajoutez uniquement l'ensemble de certificats de l'autorité de certification requis pour authentifier vos clients et vos gestionnaires. Il n'est pas recommandé d'ajouter l'ensemble complet des certificats de l'autorité de certification par défaut sauf s'il s'agit d'une exigence définitive pour votre politique de sécurité.

Localisation du référentiel de clés d'un gestionnaire de files d'attente sur les systèmes UNIX, Linux, and Windows

Utilisez cette procédure pour obtenir l'emplacement du fichier de base de données de clés de votre gestionnaire de files d'attente

Procédure

1. Affichez les attributs de votre gestionnaire de files d'attente à l'aide de l'une des commandes MQSC suivantes:

   ```
   DISPLAY QMGR ALL
   DISPLAY QMGR SSLKEYR
   ```

   Vous pouvez également afficher les attributs de votre gestionnaire de files d'attente à l'aide des commandes IBM WebSphere MQ Explorer ou PCF.
2. Recherchez dans le résultat de la commande le chemin et le nom de la racine du fichier de la base de données de clés.
   Par exemple :
   a. sur les systèmes UNIX and Linux : `/var/mqm/qmgrs/QM1/ssl/key`, où `/var/mqm/qmgrs/QM1/ssl` est le chemin et `key` est le nom du radical
   b. sous Windows: *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl\key`, où *MQ_INSTALLATION_PATH*`\qmgrs\QM1\ssl` est le chemin et `key` le nom du radical. *MQ_INSTALLATION_PATH* représente le répertoire de haut niveau dans lequel WebSphere MQ est installé.

Modification de l'emplacement du référentiel de clés d'un gestionnaire de files d'attente sur les systèmes UNIX, Linux ou Windows

Vous pouvez modifier l'emplacement du fichier de la base de données de clés de votre gestionnaire de files d'attente en utilisant divers moyens, notamment la commande MQSC ALTER QMGR.

Vous pouvez modifier l'emplacement du fichier de base de données de clés de votre gestionnaire de files d'attente à l'aide de la commande MQSC ALTER QMGR pour définir l'attribut de référentiel de clés de votre gestionnaire de files d'attente. Par exemple, sur les systèmes UNIX and Linux :

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/QM1/ssl/MyKey')
```

Le fichier de la base de données de clés possède le nom de fichier qualifié complet: `/var/mqm/qmgrs/QM1/ssl/MyKey.kdb`

Sous Windows :

```
ALTER QMGR SSLKEYR('C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\Mykey')
```

Le fichier de la base de données de clés possède le nom de fichier qualifié complet: `C:\Program Files\IBM\WebSphere MQ\Qmgrs\QM1\ssl\Mykey.kdb`

Avertissement : Veillez à ne pas inclure l'extension `.kdb` dans le nom de fichier du mot clé SSLKEYR, car le gestionnaire de files d'attente l'ajoute automatiquement.

Vous pouvez également modifier les attributs de votre gestionnaire de files d'attente à l'aide des commandes WebSphere MQ Explorer ou PCF.

Lorsque vous modifiez l'emplacement du fichier de base de données de clés d'un gestionnaire de files d'attente, les certificats ne sont pas transférés à partir de l'ancien emplacement. Si le fichier de base de données de clés auquel vous accédez est un nouveau fichier de base de données de clés, vous devez le remplir avec les certificats de l'autorité de certification et les certificats personnels dont vous avez besoin, comme décrit dans «Importation d'un certificat personnel dans un référentiel de clés sur des systèmes UNIX, Linux, and Windows», à la page 140.

Localisation du référentiel de clés pour un client IBM WebSphere MQ MQI sur des systèmes UNIX, Linux, and Windows

L'emplacement du référentiel de clés est indiqué par la variable MQSSLKEYR ou spécifié dans l'appel MQCONNX.

Examinez la variable d'environnement MQSSLKEYR pour obtenir l'emplacement du fichier de la base de données de clés du client IBM WebSphere MQ MQI. Exemple :

```
echo $MQSSLKEYR
```

Vérifiez également votre application, car le nom de fichier de la base de données de clés peut également être défini dans un appel MQCONNX, comme décrit dans «Spécification de l'emplacement du référentiel de clés pour un client IBM WebSphere MQ MQI sur des systèmes UNIX, Linux, and Windows», à la page 126. La valeur définie dans un appel MQCONNX remplace la valeur de MQSSLKEYR.

Spécification de l'emplacement du référentiel de clés pour un client IBM WebSphere MQ MQI sur des systèmes UNIX, Linux, and Windows

Il n'existe pas de référentiel de clés par défaut pour un client IBM WebSphere MQ MQI. Vous pouvez spécifier son emplacement de deux manières. Assurez-vous que le fichier de la base de données de clés est accessible uniquement par les utilisateurs ou les administrateurs prévus afin d'empêcher toute copie non autorisée vers d'autres systèmes.

Vous pouvez spécifier l'emplacement du fichier de la base de données de clés du client IBM WebSphere MQ MQI de deux manières:

- Définition de la variable d'environnement MQSSLKEYR. Par exemple, sur les systèmes UNIX and Linux :

  ```
  export MQSSLKEYR=/var/mqm/ssl/key
  ```

  Le fichier de la base de données de clés possède le nom de fichier complet:

  ```
  /var/mqm/ssl/key.kdb
  ```

  Sous Windows :

  ```
  set MQSSLKEYR=C:\Program Files\IBM\WebSphere MQ\ssl\key
  ```

Le fichier de la base de données de clés possède le nom de fichier complet:

```
C:\Program Files\IBM\WebSphere MQ\ssl\key.kdb
```

Remarque : L'extension .kdb est une partie obligatoire du nom de fichier, mais elle n'est pas incluse dans la valeur de la variable d'environnement.

- Indiquez le chemin et le nom de la racine du fichier de la base de données de clés dans la zone *KeyRepository* de la structure MQSCO lorsqu'une application effectue un appel MQCONNX. Pour plus d'informations sur l'utilisation de la structure MQSCO dans MQCONNX, voir Présentation de MQSCO .

Lorsque les modifications apportées aux certificats ou au magasin de certificats prennent effet sur les systèmes UNIX, Linux ou Windows.

Lorsque vous modifiez les certificats dans un magasin de certificats ou l'emplacement du magasin de certificats, les modifications sont prises en compte en fonction du type de canal et de la manière dont le canal est en cours d'exécution.

Les modifications apportées aux certificats dans le fichier de base de données de clés et à l'attribut de référentiel de clés prennent effet dans les situations suivantes:

- Lorsqu'un nouveau processus de canal unique sortant exécute pour la première fois un canal SSL.
- Lorsqu'un nouveau processus de canal unique TCP/IP entrant reçoit pour la première fois une demande de démarrage d'un canal SSL.
- Lorsque la commande MQSC REFRESH SECURITY TYPE (SSL) est émise pour actualiser l'environnement SSL Websphere MQ .
- Pour les processus d'application client, lorsque la dernière connexion SSL du processus est fermée. La prochaine connexion SSL prendra en compte les modifications apportées au certificat.
- Pour les canaux qui s'exécutent en tant qu'unités d'exécution d'un processus de regroupement de processus (amqrmppa), lorsque le processus de regroupement de processus est démarré ou redémarré et qu'il exécute d'abord un canal SSL. Si le processus de regroupement de processus a déjà exécuté un canal SSL et que vous souhaitez que la modification soit prise en compte immédiatement, exécutez la commande MQSC REFRESH SECURITY TYPE (SSL).
- Pour les canaux qui s'exécutent en tant qu'unités d'exécution de l'initiateur de canal, lorsque l'initiateur de canal est démarré ou redémarré et qu'il exécute d'abord un canal SSL. Si le processus initiateur de canal a déjà exécuté un canal SSL et que vous souhaitez que la modification soit prise en compte immédiatement, exécutez la commande MQSC REFRESH SECURITY TYPE (SSL).
- Pour les canaux qui s'exécutent en tant qu'unités d'exécution d'un programme d'écoute TCP/IP, lorsque le programme d'écoute est démarré ou redémarré et qu'il reçoit pour la première fois une demande de démarrage d'un canal SSL. Si le programme d'écoute a déjà exécuté un canal SSL et que vous souhaitez que la modification soit prise en compte immédiatement, exécutez la commande MQSC REFRESH SECURITY TYPE (SSL).

Vous pouvez également actualiser l'environnement SSL WebSphere MQ à l'aide des commandes IBM WebSphere MQ Explorer ou PCF.

Création d'un certificat personnel autosigné sur les systèmes UNIX, Linux, and Windows

Vous pouvez créer un certificat autosigné en utilisant iKeyman, iKeycmdou runmqakm.

Remarque : IBM WebSphere MQ ne prend pas en charge les algorithmes SHA-3 ou SHA-5 . Vous pouvez utiliser les noms d'algorithme de signature numérique SHA384WithRSA et SHA512WithRSA car ces deux algorithmes sont membres de la famille SHA-2 .

Les noms d'algorithme de signature numérique SHA3WithRSA et SHA5WithRSA sont obsolètes car ils sont de forme abrégée SHA384WithRSA et SHA512WithRSA respectivement.

Pour plus d'informations sur la raison pour laquelle vous pouvez utiliser des certificats autosignés, voir «Utilisation de certificats autosignés pour l'authentification mutuelle de deux gestionnaires de file d'attente», à la page 216.

Tous les certificats numériques ne peuvent pas être utilisés avec tous les CipherSpecs. Veillez à créer un certificat compatible avec les CipherSpecs que vous devez utiliser. WebSphere MQ prend en charge trois types différents de CipherSpec. Pour plus de détails, voir «Interopérabilité de Elliptic Curve et de RSA CipherSpecs», à la page 37 dans la rubrique «Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36 . Pour utiliser les CipherSpecs de type 1 (dont les noms commencent par ECDHE_ECDSA_), vous devez utiliser la commande **runmqakm** pour créer le certificat et spécifier un paramètre d'algorithme de signature Elliptic Curve ECDSA ; par exemple, **-sig_alg** EC_ecdsa_with_SHA384 .

Utilisation d'iKeyman

iKeyman ne fournit pas d'option compatible avec la norme FIPS. Si vous devez gérer les certificats SSL ou TLS d'une manière compatible avec FIPS, utilisez la commande **runmqakm** .

Utilisez la procédure suivante pour obtenir un certificat autosigné pour votre gestionnaire de files d'attente ou pour le client WebSphere MQ MQI:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** .
2. Dans le menu **Fichier de base de données de clés** , cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de base de données de clés dans lequel vous souhaitez sauvegarder le certificat, par exemple key . kdb.
6. Cliquez sur **Ouvrir**. La fenêtre d'invite de mot de passe s'affiche.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** .
8. Dans le menu **Créer** , cliquez sur **Nouveau certificat autosigné**. La fenêtre Créer un certificat autosigné s'affiche.
9. Dans la zone **Key Label** , entrez:
   - Pour un gestionnaire de files d'attente, ibmwebspheremq suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour QM1, ibmwebspheremqqm1ou,
   - Pour un client WebSphere MQ , ibmwebspheremq suivi de votre ID utilisateur de connexion est réduit en minuscules, par exemple ibmwebspheremqmyuserid .
10. Entrez ou sélectionnez une valeur pour n'importe quelle zone du **Distinguished name**ou pour l'une des zones **Subject alternative name** .
11. Pour les autres zones, acceptez le valeurs par défaut proposées ou bien tapez ou sélectionnez-en de nouvelles. Pour plus d'informations sur les noms distinctifs, voir «Noms distinctifs», à la page 11.
12. Cliquez sur **OK**. La liste **Certificats personnels** affiche le libellé du certificat personnel autosigné que vous avez créé.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour créer un certificat personnel autosigné à l'aide de iKeycmd ou de runmqakm:

- Utilisation de iKeycmd sur les systèmes UNIX, Linux et Windows :

```
runmqckm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
```

```
 -x509version version -expire days
 -sig_alg algorithm
```

A la place de -dn *distinguished_name* , vous pouvez utiliser -san_dsname *DNS_names* , -san_emailaddr *email_addresses* ou -san_ipaddr *IP_addresses* .

- Utilisation de runmqakm:

```
runmqakm -cert -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -x509version version -expire days

        -fips -sig_alg algorithm
```

-db *filename*	Nom de fichier complet d'une base de données de clés CMS.
-pw *password*	Mot de passe de la base de données de clés CMS.
-label *label*	Libellé de clé associé au certificat.
-dn *distinguished_name*	Le nom distinctif X.500 est placé entre guillemets. Au moins un attribut est requis. Vous pouvez fournir plusieurs attributs d'unité organisationnelle ou de centre de données.
-size *key_size*	Taille de la clé. Pour iKeycmd, la valeur peut être 512 ou 1024. Pour runmqakm, la valeur peut être 512, 1024, 2048 ou 4096.
-x509version *version*	Version du certificat X.509 à créer. La valeur peut être 1, 2 ou 3. La valeur par défaut est 3.
-expire *days*	Délai d'expiration en jours du certificat. La valeur par défaut est 365 jours pour un certificat.
-fips	indique que la commande est exécutée en mode FIPS. Ce mode désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.
-sig_alg	Pour runmqakm, algorithme de hachage utilisé lors de la création d'un certificat autosigné. Cet algorithme de hachage est utilisé pour créer la signature associée au certificat auto-signé nouvellement créé. La valeur peut être 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. La valeur par défaut est SHA1WithRSA.

`-sig_alg`	Pour iKeycmd, algorithme de signature asymétrique utilisé pour la création de la paire de clés de l'entrée. La valeur peut être `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` , `SHAWithDSAou` `SHAWithRSA`. La valeur par défaut est `SHA1WithRSA`.
`-san_dnsname` *`DNS_names`*	Liste de noms DNS séparés par des virgules ou des espaces pour l'entrée en cours de création.
`-san_emailaddr` *`email_addresses`*	Liste d'adresses électroniques séparées par des virgules ou des espaces pour l'entrée en cours de création.
`-san_ipaddr` *`IP_addresses`*	Liste d'adresses IP séparées par des virgules ou des espaces pour l'entrée en cours de création.

distributed *Demande d'un certificat personnel sur les systèmes UNIX, Linux, and Windows*

Vous pouvez demander un certificat personnel à l'aide du **strmqikm** (iKeyman) Interface graphique ou à partir de la ligne de commande à l'aide des commandes **runmqckm** ou **runmqakm** . Si vous devez gérer les certificats SSL ou TLS d'une manière compatible avec FIPS, utilisez la commande **runmqakm** .

Pourquoi et quand exécuter cette tâche

Vous pouvez demander un certificat personnel à l'aide de l'interface graphique iKeyman ou à partir de la ligne de commande, sous réserve des remarques suivantes:

- WebSphere MQ ne prend pas en charge les algorithmes SHA-3 ou SHA-5 . Vous pouvez utiliser les noms d'algorithme de signature numérique SHA384WithRSA et SHA512WithRSA car ces deux algorithmes sont membres de la famille SHA-2 .
- Les noms d'algorithme de signature numérique SHA3WithRSA et SHA5WithRSA sont obsolètes car ils sont de forme abrégée SHA384WithRSA et SHA512WithRSA respectivement.
- Tous les certificats numériques ne peuvent pas être utilisés avec tous les CipherSpecs. Veillez à demander un certificat compatible avec les CipherSpecs que vous devez utiliser. WebSphere MQ prend en charge trois types différents de CipherSpec. Pour plus de détails, voir «Interopérabilité de Elliptic Curve et de RSA CipherSpecs», à la page 37 dans la rubrique «Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36 .
- Pour utiliser les CipherSpecs de type 1 (dont les noms commencent par `ECDHE_ECDSA_`), vous devez utiliser la commande **runmqakm** pour demander le certificat et spécifier un paramètre d'algorithme de signature Elliptic Curve ECDSA ; par exemple, **-sig_alg** `EC_ecdsa_with_SHA384`.
- Seule la commande runmqakm fournit une option compatible FIPS.
- Si vous utilisez du matériel de cryptographie, voir «Demande d'un certificat personnel pour votre matériel PKCS #11», à la page 147.

Utilisation de l'interface utilisateur iKeyman

Pourquoi et quand exécuter cette tâche

iKeyman ne fournit pas d'option compatible avec la norme FIPS. Si vous devez gérer les certificats SSL ou TLS d'une manière compatible avec FIPS, utilisez la commande **runmqakm** .

Procédure

Pour appliquer un certificat personnel à l'aide de l'interface utilisateur iKeyman , procédez comme suit:

1. Démarrez l'interface utilisateur iKeyman à l'aide de la commande **strmqikm** .

2. Dans le menu **Fichier de base de données de clés** , cliquez sur **Ouvrir**.

   La fenêtre **Ouvrir** s'ouvre.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez générer la demande ; par exemple, `key.kdb`.
6. Cliquez sur **Ouvrir**.

   La fenêtre **Invite de mot de passe** s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**.

   Le nom de votre fichier de base de données de clés est affiché dans la zone **Nom de fichier** .
8. Dans le menu **Créer** , cliquez sur **Nouvelle demande de certificat**. La fenêtre **Créer une demande de clé et de certificat** s'ouvre.
9. Dans la zone **Key Label** , entrez les libellés suivants:
   - Pour un gestionnaire de files d'attente, entrez `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour un gestionnaire de files d'attente appelé `QM1`, entrez `ibmwebspheremqqm1`.
   - Pour un IBM WebSphere MQ MQI client, entrez `ibmwebspheremq` suivi de votre ID utilisateur de connexion, en minuscules ; par exemple, `ibmwebspheremqmyuserid` .
10. Entrez ou sélectionnez une valeur pour n'importe quelle zone de la zone **Nom distinctif** ou pour l'une des zones **Nom alternatif du sujet** . Pour les autres zones, acceptez le valeurs par défaut proposées ou bien tapez ou sélectionnez-en de nouvelles.

    Pour plus d'informations sur les noms distinctifs, voir «Noms distinctifs», à la page 11.
11. Dans la zone **Entrez le nom d'un fichier dans lequel stocker la demande de certificat** , acceptez la valeur par défaut `certreq.arm`ou entrez une nouvelle valeur avec un chemin d'accès complet.
12. Cliquez sur **OK**.

    Une fenêtre de confirmation s'affiche.
13. Cliquez sur **OK**.

    La liste **Demandes de certificat personnel** affiche le libellé de la nouvelle demande de certificat personnel que vous avez créée. La demande de certificat est stockée dans le fichier que vous avez choisi à l'étape «11», à la page 131.
14. Demandez le nouveau certificat personnel soit en envoyant le fichier à une autorité de certification, soit en copiant le fichier dans le formulaire de demande sur le site Web de l'autorité de certification.

Utilisation de la ligne de commande

Procédure

Utilisez les commandes suivantes pour demander un certificat personnel à l'aide de la commande **runmqckm** ou **runmqakm** :

- A l'aide de **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -sig_alg algorithm
```

  A la place de `-dn` *distinguished_name* , vous pouvez utiliser `-san_dsname` *DNS_names* , `-san_emailaddr` *email_addresses* ou `-san_ipaddr` *IP_addresses* .

- Utilisation de runmqakm:

```
runmqakm -certreq -create -db filename -pw
password -label label
```

```
        -dn distinguished_name -size key_size
 -file filename -fips
        -sig_alg algorithm
```

où :

-db *nom_fichier*
Indique le nom de fichier qualifié complet d'une base de données de clés CMS.

-pw *mot_de_passe*
Indique le mot de passe de la base de données de clés CMS.

-label *Libellé*
Indique le libellé de clé associé au certificat.

-dn *nom_distinctif*
Indique le nom distinctif X.500 entre guillemets. Au moins un attribut est requis. Vous pouvez fournir plusieurs attributs d'unité organisationnelle et de centre de données.

-size *taille_clé*
Indique la taille de la clé. Si vous utilisez **runmqckm** , la valeur peut être 512 ou 1024. Si vous utilisez **runmqakm**, la valeur peut être 512, 1024ou 2048.

-file *nom fichier*
Indique le nom de fichier de la demande de certificat.

-fips
indique que la commande est exécutée en mode FIPS. Ce mode désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

-sig_alg
Pour **runmqckm**, indique l'algorithme de signature asymétrique utilisé pour la création de la paire de clés de l'entrée. La valeur peut être 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, SHAWithDSAou SHAWithRSA . La valeur par défaut est SHA1WithRSA

-sig_alg
Pour **runmqakm**, indique l'algorithme de hachage utilisé lors de la création d'une demande de certificat. Cet algorithme de hachage est utilisé pour créer la signature associée à la demande de certificat nouvellement créée. La valeur peut être 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. La valeur par défaut est SHA1WithRSA.

-san_dnsname *noms_DNS*
Indique une liste de noms DNS séparés par des virgules ou des espaces pour l'entrée en cours de création.

-san_emailaddr *adresse_e-mail*
Indique une liste d'adresses électroniques séparées par des virgules ou des espaces pour l'entrée en cours de création.

-san_ipaddr *Adresse_IP*
Indique une liste d'adresses IP séparées par des virgules ou des espaces pour l'entrée en cours de création.

Renouvellement d'un certificat personnel existant sur les systèmes UNIX, Linux, and Windows

Vous pouvez renouveler un certificat personnel à l'aide de l'interface utilisateur iKeyman ou à l'aide des commandes **iKeycmd** ou **runmqakm** .

Avant de commencer

Si vous devez utiliser des tailles de clé plus grandes pour vos certificats personnels, les étapes de renouvellement décrites ci-dessous ne fonctionnent pas car la demande de certificat recréée est générée à partir d'une clé existante.

Suivez les étapes décrites dans «Demande d'un certificat personnel sur les systèmes UNIX, Linux, and Windows», à la page 130 pour créer une demande de certificat à l'aide des tailles de clé requises. Ce processus remplace votre clé existante.

Pourquoi et quand exécuter cette tâche

Un certificat personnel a une date d'expiration, après laquelle le certificat ne peut plus être utilisé. Cette tâche explique comment renouveler un certificat personnel existant avant son expiration.

Utilisation de l'interface utilisateur iKeyman

Pourquoi et quand exécuter cette tâche

iKeyman ne fournit pas d'option compatible avec la norme FIPS. Si vous devez gérer les certificats SSL ou TLS d'une manière compatible avec FIPS, utilisez la commande **runmqakm** .

Procédure

Pour appliquer un certificat personnel à l'aide de l'interface utilisateur iKeyman , procédez comme suit:

1. Démarrez l'interface utilisateur iKeyman à l'aide de la commande **strmqikm** sur les systèmes UNIX, Linux, and Windows .
2. Dans le menu **Fichier de base de données de clés** , cliquez sur **Ouvrir**.

   La fenêtre **Ouvrir** s'ouvre.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez générer la demande ; par exemple, `key.kdb`.
6. Cliquez sur **Ouvrir**.

   La fenêtre **Invite de mot de passe** s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**.

   Le nom de votre fichier de base de données de clés est affiché dans la zone **Nom de fichier** .
8. Sélectionnez **Personal Certificates** dans le menu déroulant de sélection, puis sélectionnez le certificat à renouveler dans la liste.
9. Cliquez sur **Recréer la demande ...** bouton.

   Une fenêtre s'ouvre pour que vous puissiez entrer le nom de fichier et les informations d'emplacement de fichier.
10. Dans la zone **nom de fichier**, acceptez la valeur par défaut `certreq.arm`ou entrez une nouvelle valeur, y compris le chemin d'accès complet au fichier.
11. Cliquez sur **OK**. La demande de certificat est stockée dans le fichier que vous avez sélectionné à l'étape «9», à la page 133.
12. Demandez le nouveau certificat personnel soit en envoyant le fichier à une autorité de certification, soit en copiant le fichier dans le formulaire de demande sur le site Web de l'autorité de certification.

Procédure

Utilisez les commandes suivantes pour demander un certificat personnel à l'aide de la commande **iKeycmd** ou **runmqakm** :

- Utilisation de **iKeycmd** sur les systèmes UNIX, Linux, and Windows :

```
runmqckm -certreq -recreate -db filename -pw
password -label label
 -target filename
```

- Utilisation de runmqakm:

```
runmqakm -certreq -recreate -db filename -pw
password -label label
  -target filename
```

où :

-db *nom_fichier*
Indique le nom de fichier qualifié complet d'une base de données de clés CMS.

-pw *mot_de_passe*
Indique le mot de passe de la base de données de clés CMS.

-target *nom_fichier*
Indique le nom de fichier de la demande de certificat.

Que faire ensuite

Une fois que vous avez reçu le certificat personnel signé de l'autorité de certification, vous pouvez l'ajouter à votre base de données de clés en suivant les étapes décrites dans «Réception de certificats personnels dans un référentiel de clés sur les systèmes UNIX, Linux et Windows», à la page 134.

Réception de certificats personnels dans un référentiel de clés sur les systèmes UNIX, Linux et Windows

Utilisez cette procédure pour recevoir un certificat personnel dans le fichier de la base de données de clés. Le référentiel de clés doit être le même que celui dans lequel vous avez créé la demande de certificat.

Une fois que l'autorité de certification vous a envoyé un nouveau certificat personnel, vous l'ajoutez au fichier de base de données de clés à partir duquel vous avez généré la nouvelle demande de certificat. Si l'autorité de certification envoie le certificat dans le cadre d'un message électronique, copiez le certificat dans un fichier distinct.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Vérifiez que le fichier certificat à importer dispose des droits d'accès en écriture pour l'utilisateur en cours, puis utilisez la procédure suivante pour un gestionnaire de files d'attente ou un client WebSphere MQ MQI pour recevoir un certificat personnel dans le fichier de la base de données de clés:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sous Windows UNIX and Linux).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.

5. Sélectionnez le fichier de clés dans lequel vous souhaitez ajouter le certificat, par exemple `key.kdb`.
6. Cliquez sur **Ouvrir**, puis sur **OK**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** . Sélectionnez la vue **Certificats personnels** .
8. Cliquez sur **Receive**. La fenêtre Recevoir un certificat d'un fichier s'affiche.
9. Entrez le nom du fichier de certificat et l'emplacement du nouveau certificat personnel ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
10. Cliquez sur **OK**. Si vous disposez déjà d'un certificat personnel dans votre base de données de clés, une fenêtre s'ouvre pour vous demander si vous souhaitez définir la clé que vous ajoutez comme clé par défaut dans la base de données.
11. Cliquez sur **Oui** ou sur **Non**. La fenêtre Enter a Label s'ouvre.
12. Cliquez sur **OK**. La zone **Certificats personnels** affiche le libellé du nouveau certificat personnel que vous avez ajouté.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour ajouter un certificat personnel à un fichier de base de données de clés à l'aide de iKeycmd :

- Sous UNIX, Linux et Windows, exécutez la commande suivante:

```
runmqckm -cert -receive -file filename -db filename -pw
password
        -format ascii
```

où :

`-file` *`filename`*	est le nom de fichier complet du fichier contenant le certificat personnel.
`-db` *`filename`*	est le nom de fichier qualifié complet d'une base de données de clés CMS.
`-pw` *`password`*	correspond au mot de passe de la base de données de clés CMS.
`-format` *`ascii`*	correspond au format du certificat. La valeur peut être `ascii` pour Base64-encoded ASCII ou `binary` pour les données DER binaires. La valeur par défaut est `ascii` .

Si vous utilisez du matériel de cryptographie, voir «Importation d'un certificat personnel sur votre matériel PKCS #11», à la page 149.

Extraction d'un certificat de l'autorité de certification à partir d'un référentiel de clés

Procédez comme suit pour extraire un certificat d'autorité de certification.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Effectuez les étapes suivantes sur la machine à partir de laquelle vous souhaitez extraire le certificat de l'autorité de certification:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **`strmqikm`** .
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.

5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez extraire, par exemple `key.kdb`.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** .
8. Dans la zone **Contenu de la base de données de clés** , sélectionnez **Certificats de signataire** et sélectionnez le certificat à extraire.
9. Cliquez sur **Extraire**. La fenêtre Extraire un certificat dans un fichier s'ouvre.
10. Sélectionnez le **Type de données** du certificat, par exemple **Base64-encoded codées en Base64** pour un fichier avec l'extension `.arm` .
11. Entrez le nom du fichier de certificat et l'emplacement où vous souhaitez stocker le certificat ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
12. Cliquez sur **OK**. Le certificat est écrit dans le fichier que vous avez spécifié.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour extraire un certificat de l'autorité de certification à l'aide de iKeycmd :

- Sous UNIX, Linux et Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

où :

`-db` *`filename`*	est le nom de chemin qualifié complet d'une base de données de clés CMS.
`-pw` *`password`*	correspond au mot de passe de la base de données de clés CMS.
`-label` *`label`*	correspond au libellé du certificat.
`-target` *`filename`*	est le nom du fichier de destination.
`-format` *`ascii`*	correspond au format du certificat. La valeur peut-être `ascii` pour les données ASCII codées en base 64 ou `binary` pour les données Binary DER. La valeur par défaut est `ascii`.

Extraction de la partie publique d'un certificat autosigné à partir d'un référentiel de clés sur les systèmes UNIX, Linux et Windows

Procédez comme suit pour extraire la partie publique d'un certificat autosigné.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Effectuez les étapes suivantes sur la machine à partir de laquelle vous souhaitez extraire la partie publique d'un certificat autosigné:

1. Démarrez l'interface graphique d' iKeyman à l'aide de la commande **strmqikm** (sous UNIX, Linux et Windows).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.

5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez extraire le certificat, par exemple `key.kdb`.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** .
8. Dans la zone **Contenu de la base de données de clés** , sélectionnez **Certificats personnels** et sélectionnez le certificat.
9. Cliquez sur **Extraire le certificat**. La fenêtre Extraire un certificat dans un fichier s'ouvre.
10. Sélectionnez le **Type de données** du certificat, par exemple **Base64-encoded codées en Base64** pour un fichier avec l'extension `.arm` .
11. Entrez le nom du fichier de certificat et l'emplacement où vous souhaitez stocker le certificat ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
12. Cliquez sur **OK**. Le certificat est écrit dans le fichier que vous avez spécifié. Notez que lorsque vous extrayez (plutôt que d'exporter) un certificat, seule la partie publique du certificat est incluse, de sorte qu'un mot de passe n'est pas requis.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour extraire la partie publique d'un certificat autosigné à l'aide de iKeycmd ou de runmqakm:

- Sous UNIX, Linux et Windows:

```
runmqckm -cert -extract -db filename -pw password -label label -target filename
         -format ascii
```

- Utilisation de runmqakm:

```
runmqakm -cert -extract -db filename -pw password -label label
            -target filename -format ascii -fips
```

où :

`-db` *`filename`*	est le nom de chemin qualifié complet d'une base de données de clés CMS.
`-pw` *`password`*	correspond au mot de passe de la base de données de clés CMS.
`-label` *`label`*	correspond au libellé du certificat.
`-target` *`filename`*	est le nom du fichier de destination.
`-format` *`ascii`*	correspond au format du certificat. La valeur peut-être `ascii` pour les données ASCII codées en base 64 ou `binary` pour les données Binary DER. La valeur par défaut est `ascii`.

Ajout d'un certificat de l'autorité de certification (ou de la partie publique d'un certificat autosigné) dans un référentiel de clés sur les systèmes UNIX, Linux, and Windows

Suivez cette procédure pour ajouter un certificat de l'autorité de certification ou la partie publique d'un certificat autosigné au référentiel principal.

Si le certificat que vous souhaitez ajouter se trouve dans une chaîne de certificats, vous devez également ajouter tous les certificats se trouvant au-dessus de ce dernier dans la chaîne. Vous devez absolument ajouter les certificats dans l'ordre décroissant en commençant par la racine, puis par le certificat de l'autorité de certification situé immédiatement en-dessous dans la chaîne, etc.

Lorsque les instructions suivantes font référence à un certificat de l'autorité de certification, elles s'appliquent également à la partie publique d'un certificat autosigné.

Remarque : Si le certificat que vous souhaitez ajouter se trouve dans une chaîne de certificats, vous devez également ajouter tous les certificats se trouvant au-dessus de ce dernier dans la chaîne. Vous devez vous assurer que le certificat est au format ASCII (UTF-8) ou binaire (DER) car IBM Global Secure Toolkit (GSKit) ne prend pas en charge les certificats avec d'autres types de codage. Vous devez absolument ajouter les certificats dans l'ordre décroissant en commençant par la racine, puis par le certificat de l'autorité de certification situé immédiatement en-dessous dans la chaîne, et ainsi de suite.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Suivez les étapes suivantes sur la machine sur laquelle vous souhaitez ajouter le certificat de l'autorité de certification :

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sur les systèmes UNIX, Linux et Windows).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de clés dans lequel vous souhaitez ajouter le certificat, par exemple `key.kdb`.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de clés s'affiche dans la zone **Nom du fichier**.
8. Dans la zone **Key database content**, sélectionnez **Signer Certificates**.
9. Cliquez sur **Ajouter**. La fenêtre Add CA's Certificate from a File s'ouvre.
10. Entrez le nom et l'emplacement du fichier certificat ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
11. Cliquez sur **OK**. La fenêtre Enter a Label s'ouvre.
12. Dans la fenêtre Enter a Label, entrez le nom du certificat.
13. Cliquez sur **OK**. Le certificat est ajouté à la base de données de clés.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour ajouter un certificat de l'autorité de certification à l'aide de iKeycmd :

- Sous UNIX, Linux et Windows, exécutez la commande suivante:

```
runmqckm -cert -add -db filename -pw password -label label -file filename
        -format ascii
```

où :

`-db` *filename*	correspond au nom de chemin qualifié complet de la base de données de clés CMS.
`-pw` *password*	correspond au mot de passe de la base de données de clés CMS.
`-label` *label*	correspond au libellé du certificat.
`-file` *filename*	correspond au nom du fichier contenant le certificat.

-format *ascii*	correspond au format du certificat. La valeur peut-être `ascii` pour les données ASCII codées en base 64 ou `binary` pour les données Binary DER. La valeur par défaut est `ascii`.

Exportation d'un certificat personnel à partir d'un référentiel de clés

Suivez cette procédure pour exporter un certificat personnel.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Effectuez les étapes suivantes sur la machine à partir de laquelle vous souhaitez exporter le certificat personnel:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sous Windows UNIX and Linux).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez exporter le certificat, par exemple `key.kdb`.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** .
8. Dans la zone **Contenu de la base de données de clés** , sélectionnez **Certificats personnels** et sélectionnez le certificat à exporter.
9. Cliquez sur **Exporter / Importer**. La fenêtre Exportation / Importation de clé s'ouvre.
10. Sélectionnez **Exporter la clé**.
11. Sélectionnez le **Type de fichier de clés** du certificat à exporter, par exemple **PKCS12**.
12. Entrez le nom de fichier et l'emplacement vers lesquels vous souhaitez exporter le certificat ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
13. Cliquez sur **OK**. La fenêtre Password Prompt s'ouvre. Notez que lorsque vous exportez (plutôt que d'extraire) un certificat, les parties publique et privée du certificat sont incluses. C'est pourquoi le fichier exporté est protégé par un mot de passe. Lorsque vous extrayez un certificat, seule la partie publique du certificat est incluse, de sorte qu'un mot de passe n'est pas requis.
14. Entrez un mot de passe dans la zone **Mot de passe** , puis entrez-le à nouveau dans la zone **Confirmer le mot de passe** .
15. Cliquez sur **OK**. Le certificat est exporté dans le fichier que vous avez spécifié.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour exporter un certificat personnel à l'aide de iKeycmd:

- Sous UNIX, Linux et Windows:

```
runmqckm -cert -export -db filename -pw password -label label -type cms
        -target filename -target_pw password -target_type pkcs12
```

où :

-db *filename*	correspond au nom de chemin qualifié complet de la base de données de clés CMS.

-pw *password*	correspond au mot de passe de la base de données de clés CMS.
-label *label*	correspond au libellé du certificat.
-type *cms*	est le type de la base de données.
-target *filename*	est le nom de chemin qualifié complet du fichier de destination.
-target_pw *password*	est le mot de passe utilisé pour le chiffrement du certificat.
-target_type *pkcs12*	est le type du certificat.

Importation d'un certificat personnel dans un référentiel de clés sur des systèmes UNIX, Linux, and Windows

Suivez cette procédure pour importer un certificat personnel

Avant d'importer un certificat personnel au format PKCS #12 dans le fichier de la base de données de clés, vous devez d'abord ajouter la chaîne valide complète d'émission de certificats de l'autorité de certification au fichier de la base de données de clés (voir «Ajout d'un certificat de l'autorité de certification (ou de la partie publique d'un certificat autosigné) dans un référentiel de clés sur les systèmes UNIX, Linux, and Windows», à la page 137).

Les fichiers PKCS #12 doivent être considérés comme temporaires et supprimés après utilisation.

Utilisation d'iKeyman

Si vous devez gérer les certificats SSL d'une manière compatible avec FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

Effectuez les étapes suivantes sur la machine sur laquelle vous souhaitez importer le certificat personnel:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** .
2. Dans le menu **Fichier de base de données de clés** , cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de clés dans lequel vous souhaitez ajouter le certificat, par exemple key.kdb.
6. Cliquez sur **Ouvrir**. La fenêtre d'invite de mot de passe s'affiche.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de clés s'affiche dans la zone **Nom du fichier**.
8. Dans la zone **Contenu de la base de données de clés** , sélectionnez **Certificats personnels**.
9. Si la vue Certificats personnels contient des certificats, procédez comme suit:
   a. Cliquez sur **Exporter / Importer**. La fenêtre Export / Import key s'affiche.
   b. Sélectionnez **Importer la clé**.
10. S'il n'existe aucun certificat dans la vue Certificats personnels, cliquez sur **Importer**.
11. Sélectionnez le **Type de fichier de clés** du certificat à importer, par exemple PKCS12.
12. Entrez le nom et l'emplacement du fichier certificat ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
13. Cliquez sur **OK**. La fenêtre d'invite de mot de passe s'affiche.
14. Dans la zone **Mot de passe** , entrez le mot de passe utilisé lors de l'exportation du certificat.
15. Cliquez sur **OK**. La fenêtre Modifier les libellés s'affiche. Cette fenêtre permet de modifier les libellés des certificats importés si, par exemple, un certificat portant le même libellé existe déjà dans la base de données de clés cible. La modification des libellés de certificat n'a aucun effet sur la validation de la chaîne de certificats. Vous pouvez l'utiliser pour remplacer le libellé de certificat personnel par celui requis par WebSphere MQ afin d'associer le certificat au gestionnaire de files d'attente ou au client particulier (ibmwebspheremqqm1 par exemple).

16. Pour modifier un libellé, sélectionnez-le dans la liste **Sélectionner un libellé à modifier** . Le libellé est copié dans la zone d'entrée **Entrer un nouveau libellé** . Remplacez le texte du libellé par celui du nouveau libellé et cliquez sur **Appliquer**.
17. Le texte de la zone d'entrée **Entrer un nouveau libellé** est recopié dans la zone **Sélectionner un libellé à modifier** , en remplaçant le libellé sélectionné à l'origine et en réétiquetant le certificat correspondant.
18. Une fois que vous avez modifié tous les libellés à modifier, cliquez sur **OK**. La fenêtre Modifier les libellés se ferme et la fenêtre de gestion des clés IBM d'origine réapparaît avec les zones **Certificats personnels** et **Certificats de signataire** mises à jour avec les certificats correctement libellés.
19. Le certificat est importé dans la base de données de clés cible.

Utilisation de la ligne de commande

Pour importer un certificat personnel à l'aide de iKeycmd, utilisez les commandes suivantes:

- Sous UNIX, Linux et Windows:

```
runmqckm -cert -import -file filename -pw password -type pkcs12 -target filename
-target_pw password -target_type cms -label label
```

où :

`-file` *filename*	est le nom de fichier qualifié complet du fichier contenant le certificat PKCS #12 .
`-pw` *password*	est le mot de passe du certificat PKCS #12 .
`-type` *pkcs12*	est le type du fichier.
`-target` *filename*	est le nom de la base de données de clés CMS de destination.
`-target_pw` *password*	correspond au mot de passe de la base de données de clés CMS.
`-target_type` *cms*	est le type de la base de données spécifiée par `-target`
`-label` *label*	est le libellé du certificat à importer à partir de la base de données de clés source.
`-new_label` *label*	est le libellé auquel le certificat sera affecté dans la base de données cible. Si vous omettez l'option `-new_label` , l'option `-label` est utilisée par défaut.

iKeycmd ne fournit pas de commande permettant de modifier directement les libellés de certificat. Pour modifier un libellé de certificat, procédez comme suit:

1. Exportez le certificat dans un fichier PKCS #12 à l'aide de la commande **`-cert -export`** . Indiquez le libellé de certificat existant pour l'option `-label` .
2. Supprimez la copie existante du certificat de la base de données de clés d'origine à l'aide de la commande **`-cert -delete`** .
3. Importez le certificat à partir du fichier PKCS #12 à l'aide de la commande **`-cert -import`** . Spécifiez l'ancien libellé pour l'option `-label` et le nouveau libellé requis pour l'option `-new_label` . Le certificat sera réimporté dans la base de données de clés avec le libellé requis.

Importation à partir d'un fichier Microsoft .pfx

Exécutez cette procédure pour mport à partir d'un fichier Microsoft .pfx à l'aide de iKeyman. Vous ne pouvez pas utiliser runmqakm pour importer un fichier .pfx.

Un fichier .pfx peut contenir deux certificats relatifs à la même clé. L'un est un certificat personnel ou de site (contenant à la fois une clé publique et une clé privée). L'autre est un certificat de l'autorité de certification (signataire) (contenant uniquement une clé publique). Ces certificats ne pouvant pas

coexister dans le même fichier de base de données de clés CMS, un seul d'entre eux peut être importé. En outre, le "nom usuel" ou le libellé est joint uniquement au certificat de signataire.

Le certificat personnel est identifié par un identificateur unique (UUID) généré par le système. Cette section montre l'importation d'un certificat personnel à partir d'un fichier pfx tout en l'étiquetant avec le nom usuel précédemment affecté au certificat de l'autorité de certification (signataire). Les certificats de l'autorité de certification émettrice (signataire) doivent déjà être ajoutés à la base de données de clés cible. Notez que les fichiers PKCS#12 doivent être considérés comme temporaires et supprimés après utilisation.

Pour importer un certificat personnel à partir d'une base de données de clés pfx source, procédez comme suit:

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sous Linux, UNIX ou Windows). La fenêtre de gestion des clés IBM (IBM Key Management) s'affiche.
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Sélectionnez le type de base de données de clés **PKCS12**.
4. **Il est recommandé d'effectuer une sauvegarde de la base de données pfx avant d'effectuer cette étape.** Sélectionnez la base de données de clés pfx à importer. Cliquez sur **Ouvrir**. La fenêtre de saisie de mot de passe s'affiche.
5. Entrez le mot de passe de la base de données de clés et cliquez sur **OK**. La fenêtre de gestion des clés IBM (IBM Key Management) s'affiche. La barre de titre affiche le nom du fichier de base de données de clés pfx sélectionné, indiquant que le fichier est ouvert et prêt.
6. Sélectionnez **Signer Certificates** dans la liste. Le "nom usuel" du certificat requis s'affiche sous la forme d'un libellé dans le panneau Certificats de signataire.
7. Sélectionnez l'entrée de libellé et cliquez sur **Supprimer** pour supprimer le certificat de signataire. La fenêtre de confirmation s'affiche.
8. Cliquez sur **Oui**. Le libellé sélectionné n'est plus affiché dans le panneau Certificats de signataire.
9. Répétez les étapes 6, 7 et 8 pour tous les certificats de signataire.
10. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
11. Sélectionnez la base de données CMS de clés cible dans laquelle le fichier pfx est importé. Cliquez sur **Ouvrir**. La fenêtre de saisie de mot de passe s'affiche.
12. Entrez le mot de passe de la base de données de clés et cliquez sur **OK**. La fenêtre de gestion des clés IBM (IBM Key Management) s'affiche. La barre de titre affiche le nom du fichier de base de données de clés sélectionné, indiquant que le fichier est ouvert et prêt.
13. Sélectionnez **Certificats personnels** dans la liste.
14. Si la vue Certificats personnels contient des certificats, procédez comme suit:
    a. Cliquez sur **Exporter / Importer la clé**. La fenêtre Export / Import key s'affiche.
    b. Sélectionnez **Importer** dans Choisir le type d'action.
15. S'il n'existe aucun certificat dans la vue Certificats personnels, cliquez sur **Importer**.
16. Sélectionnez le fichier PKCS12 .
17. Entrez le nom du fichier pfx tel qu'il est utilisé à l'étape 4. Cliquez sur **OK**. La fenêtre de saisie de mot de passe s'affiche.
18. Indiquez le même mot de passe que celui que vous avez indiqué lorsque vous avez supprimé le certificat de signataire. Cliquez sur **OK**.
19. La fenêtre Modifier les libellés s'affiche (car il ne doit y avoir qu'un seul certificat disponible pour l'importation). Le libellé du certificat doit être un identificateur unique universel au format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.
20. Pour modifier le libellé, sélectionnez l'identificateur unique universel dans le panneau **Sélectionner un libellé à modifier:** . Le libellé sera répliqué dans la zone **Entrez un nouveau libellé:** . Remplacez le texte du libellé par celui du nom usuel qui a été supprimé à l'étape 7 et cliquez sur **Appliquer**. Le

nom usuel doit être au format `ibmwebspheremq`, suivi du nom du gestionnaire de files d'attente ou de l'ID de connexion utilisateur du client WebSphere MQ MQI en minuscules.

21. Cliquez sur **OK**. La fenêtre Modifier les libellés est maintenant supprimée et la fenêtre de gestion des clés IBM d'origine réapparaît avec les panneaux Certificats personnels et Certificats de signataire mis à jour avec le certificat personnel correctement libellé.
22. Le certificat personnel pfx est maintenant importé dans la base de données (cible).

Il n'est pas possible de modifier un libellé de certificat à l'aide de iKeycmd

Importation à partir d'un fichier PKCS #7

Les outils iKeyman et iKeycmd ne prennent pas en charge les fichiers PKCS #7 (.p7b). Utilisez l'outil runmqckm pour importer des certificats à partir d'un fichier PKCS #7 .

Utilisez la commande suivante pour ajouter un certificat d'autorité de certification à partir d'un fichier PKCS #7 :

```
runmqckm -cert -add -db filename -pw password -type cms -file filename
-label label
```

`-db` *`filename`*	est le nom de fichier qualifié complet de la base de données de clés CMS.
`-pw` *`password`*	est le mot de passe de la base de données de clés.
`-type` *`cms`*	est le type de la base de données de clés.
`-file` *`filename`*	est le nom du fichier PKCS #7 .
`-label` *`label`*	est le libellé auquel le certificat est affecté dans la base de données cible. Le premier certificat prend le label donné. Tous les autres certificats, s'ils sont présents, sont libellés avec leur nom de sujet.

Utilisez la commande suivante pour importer un certificat personnel à partir d'un fichier 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`*	est le nom de fichier qualifié complet du fichier contenant le certificat PKCS #7 .
`-pw` *`password`*	est le mot de passe du certificat PKCS #7 .
`-type` *`pkcs7`*	est le type du fichier.
`-target` *`filename`*	est le nom de la base de données de clés de destination.
`-target_pw` *`password`*	est le mot de passe de la base de données de clés de destination.
`-target_type` *`cms`*	est le type de la base de données spécifiée par `-target`
`-label` *`label`*	est le libellé du certificat à importer.
`-new_label` *`label`*	est le libellé auquel le certificat sera affecté dans la base de données cible. Si vous omettez l'option `-new_label` , la valeur par défaut est d'utiliser la même valeur que l'option `-label` .

Suppression d'un certificat d'un référentiel de clés sur des systèmes UNIX, Linux, and Windows

Utilisez cette procédure pour supprimer des certificats personnels ou de l'autorité de certification.

Utilisation d'iKeyman

Si vous devez gérer des certificats SSL conformément à la norme FIPS, utilisez la commande runmqakm. iKeyman ne fournit pas d'option compatible avec la norme FIPS.

1. Démarrez l'interface graphique iKeyman à l'aide de la commande **strmqikm** (sur les systèmes UNIX, Linux et Windows).
2. Dans le menu **Key Database File**, cliquez sur **Ouvrir**. La fenêtre Ouvrir s'affiche.
3. Cliquez sur **Key database type** et sélectionnez **CMS** (système de gestion des certificats).
4. Cliquez sur **Parcourir** pour accéder au répertoire contenant le fichier de clés.
5. Sélectionnez le fichier de base de données de clés à partir duquel vous souhaitez supprimer le certificat, par exemple key.kdb.
6. Cliquez sur **Ouvrir**. La fenêtre Password Prompt s'ouvre.
7. Entrez le mot de passe défini lors de la création de la base de données de clés et cliquez sur **OK**. Le nom de votre fichier de base de données de clés s'affiche dans la zone **Nom de fichier** .
8. Dans la liste déroulante, sélectionnez **Certificats personnels** ou **Certificats de signataire** .
9. Sélectionnez le certificat à supprimer.
10. Si vous ne disposez pas encore d'une copie du certificat et que vous souhaitez l'enregistrer, cliquez sur **Exporter / Importer** et exportez-la (voir «Exportation d'un certificat personnel à partir d'un référentiel de clés», à la page 139).
11. Une fois le certificat sélectionné, cliquez sur **Supprimer**. La fenêtre de confirmation s'ouvre.
12. Cliquez sur **Oui**. La zone **Certificats personnels** n'affiche plus le libellé du certificat que vous avez supprimé.

Utilisation de la ligne de commande

Utilisez les commandes suivantes pour supprimer un certificat à l'aide de iKeycmd ou de runmqakm:

- Sous UNIX, Linux et Windows:

```
runmqckm -cert -delete -db filename -pw password -label label
```

où :

-db *filename*	est le nom de fichier qualifié complet d'une base de données de clés CMS.
-pw *password*	correspond au mot de passe de la base de données de clés CMS.
-label *label*	est le label attaché au certificat personnel.
-fips	indique que la commande est exécutée en mode FIPS. Ce mode désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

Génération de mots de passe fiables pour la protection des référentiels de clés

Vous pouvez générer des mots de passe fiables pour la protection du référentiel de clés à l'aide de la commande **runmqakm** .

Vous pouvez utiliser la commande **runmqakm** avec les paramètres suivants pour générer un mot de passe fiable:

```
runmqakm -random -create -length 14 -strong -fips
```

Lorsque vous utilisez le mot de passe généré dans le paramètre **-pw** des commandes d'administration de certificat suivantes, placez toujours le mot de passe entre guillemets. Sur les systèmes UNIX and Linux , vous devez également utiliser une barre oblique inversée pour échapper les caractères suivants s'ils apparaissent dans la chaîne de mot de passe:

```
!   \   "    '
```

Lorsque vous entrez le mot de passe en réponse à une invite à partir de **runmqckm**, **runmqakm** ou de l'interface graphique iKeyman , il n'est pas nécessaire de le citer ou de le mettre en échappement. Elle n'est pas nécessaire car l'interpréteur de commandes du système d'exploitation n'affecte pas la saisie des données dans ces cas.

Configuration du matériel de cryptographie sur les systèmes UNIX, Linux, and Windows

Vous pouvez configurer le matériel de cryptographie pour un gestionnaire de files d'attente ou un client de plusieurs manières.

Vous pouvez configurer le matériel de cryptographie pour un gestionnaire de files d'attente sur des systèmes UNIX, Linux ou Windows à l'aide de l'une des méthodes suivantes:

- Utilisez la commande ALTER QMGR MQSC avec le paramètre SSLCRYP, comme décrit dans ALTER QMGR.
- Utilisez IBM WebSphere MQ Explorer pour configurer le matériel de chiffrement sur votre système UNIX, Linux ou Windows . Pour plus d'informations, reportez-vous à l'aide en ligne.

Vous pouvez configurer le matériel de cryptographie pour un client WebSphere MQ sur des systèmes UNIX, Linux ou Windows à l'aide de l'une des méthodes suivantes:

- Définissez la variable d'environnement MQSSLCRYP. Les valeurs autorisées pour MQSSLCRYP sont les mêmes que pour le paramètre SSLCRYP, comme décrit dans ALTER QMGR. Si vous utilisez la version GSK_PCS11 du paramètre SSLCRYP, le libellé de jeton PKCS #11 doit être indiqué en minuscules.
- Définissez la zone **CryptoHardware** de la structure des options de configuration SSL, MQSCO, sur un appel MQCONNX. Pour plus d'informations, voir Présentation de MQSCO.

Si vous avez configuré du matériel cryptographique qui utilise l'interface PKCS #11 à l'aide de l'une de ces méthodes, vous devez stocker le certificat personnel à utiliser sur vos canaux dans le fichier de la base de données de clés pour le jeton cryptographique que vous avez configuré. Ceci est décrit dans «Gestion des certificats sur le matériel PKCS #11», à la page 145.

Gestion des certificats sur le matériel PKCS #11

Vous pouvez gérer des certificats numériques sur du matériel de cryptographie qui prend en charge l'interface PKCS #11 .

Pourquoi et quand exécuter cette tâche

Vous devez créer une base de données de clés pour préparer l'environnement IBM WebSphere MQ , même si vous n'avez pas l'intention d'y stocker des certificats d'autorité de certification, mais que vous stockez tous vos certificats sur votre matériel de cryptographie. Une base de données de clés est nécessaire pour que le gestionnaire de files d'attente y fasse référence dans sa zone SSLKEYR ou pour que l'application client y fasse référence dans la variable d'environnement MQSSLKEYR. Cette base de données de clés est également requise si vous créez une demande de certificat.

Vous créez la base de données de clés à l'aide de la ligne de commande ou de l'interface utilisateur **strmqikm** (iKeyman).

Procédure

Créez une base de données de clés à l'aide de la ligne de commande.

1. Exécutez l'une des commandes suivantes:

- Sur les systèmes UNIX, Linux, and Windows :

```
runmqckm -keydb -create -db filename -pw password -type cms -stash
```

- Utilisation de runmqakm:

```
runmqakm -keydb -create -db filename -pw password -type cms
    -stash -fips -strong
```

où :

-db *nom_fichier*
Indique le nom de fichier qualifié complet d'une base de données de clés CMS et doit avoir l'extension de fichier `.kdb`.

-pw *mot_de_passe*
Indique le mot de passe de la base de données de clés CMS.

-type *cms*
Indique le type de base de données. (Pour IBM WebSphere MQ, il doit s'agir de `cms`.)

-stash
Sauvegarde le mot de passe de la base de données de clés dans un fichier.

-fips
Désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

-forte
Vérifie que le mot de passe entré répond aux exigences minimales de puissance de mot de passe. Les exigences minimales pour un mot de passe sont les suivantes:

- Le mot de passe doit avoir une longueur minimale de 14 caractères.
- Le mot de passe doit contenir au moins un caractère minuscule, un caractère majuscule et un chiffre ou un caractère spécial. Les caractères spéciaux incluent l'astérisque (*), le signe dollar ($), le signe nombre (#) et le signe pourcentage (%). Un espace est classé comme un caractère spécial.
- Chaque caractère peut apparaître au maximum trois fois dans un mot de passe.
- Un maximum de deux caractères consécutifs dans le mot de passe peut être identique.
- Tous les caractères se trouvent dans le jeu de caractères ASCII imprimables standard compris entre 0x20 et 0x7E.

Vous pouvez également créer une base de données de clés à l'aide de l'interface utilisateur **strmqikm** (iKeyman).

2. Sur les systèmes UNIX and Linux , connectez-vous en tant que superutilisateur. Sur les systèmes Windows , connectez-vous en tant qu'administrateur ou en tant que membre du groupe MQM.
3. Démarrez l'interface utilisateur iKeyman en exécutant la commande **strmqikm** .
4. Cliquez sur **Fichier de base de données de clés** > **Ouvrir**.
5. Cliquez sur **Type de base de données de clés** et sélectionnez **PKCS11Direct**.
6. Dans la zone **Nom de fichier** , entrez le nom du module de gestion de votre matériel de cryptographie ; par exemple, `PKCS11_API.so`.

   Si vous utilisez des certificats ou des clés stockés sur du matériel de cryptographie PKCS #11, notez que iKeycmd et iKeyman sont des programmes 64 bits. Etant donné que les modules externes requis pour la prise en charge de PKCS #11 seront chargés dans un processus 64 bits, une bibliothèque PKCS #11 64 bits doit être installée pour l'administration du matériel de cryptographie. Les plateformes Windows et Linux x86 32 bits sont les seules exceptions, car les programmes iKeyman et iKeycmd sont 32 bits sur ces plateformes.
7. Dans la zone **Emplacement** , entrez le chemin:

- Sur les systèmes UNIX and Linux , il peut s'agir de `/usr/lib/pksc11`, par exemple.
- Sur les systèmes Windows , vous pouvez entrer le nom de la bibliothèque ; par exemple, `cryptoki`.

Cliquez sur **OK**. La fenêtre Open Cryptographic Token s'ouvre.

8. Dans la zone **Cryptographic Token Password** , entrez le mot de passe que vous avez défini lors de la configuration du matériel cryptographique.
9. Si votre matériel de cryptographie a la capacité de contenir les certificats de signataire requis pour recevoir ou importer un certificat personnel, décochez les deux cases de la base de données de clés secondaire et passez à l'étape «13», à la page 147.

   Si vous avez besoin d'une base de données de clés CMS secondaire pour stocker les certificats de signataire, sélectionnez **Ouvrir un fichier de base de données de clés secondaire existant** ou **Créer un fichier de base de données de clés secondaire**.
10. Dans la zone **Nom de fichier** , entrez un nom de fichier. Cette zone contient déjà le texte `key.kdb`. Si votre nom de radical est `key`, laissez cette zone inchangée. Si vous avez spécifié un autre nom de radical, remplacez `key` par votre nom de radical. Vous ne devez pas modifier le suffixe `.kdb` .
11. Dans la zone **Emplacement** , entrez le chemin, par exemple:
    - Pour un gestionnaire de files d'attente: `/var/mqm/qmgrs/QM1/ssl`
    - Pour un client IBM WebSphere MQ MQI: `/var/mqm/ssl`

    Cliquez sur **OK**. La fenêtre Password Prompt s'ouvre.
12. Entrez un mot de passe.

    Si vous avez sélectionné **Ouvrir un fichier de base de données de clés secondaire existant** à l'étape «9», à la page 147, entrez un mot de passe dans la zone **Mot de passe** .

    Si vous avez sélectionné **Créer un fichier de base de données de clés secondaires** à l'étape «9», à la page 147, effectuez les sous-étapes suivantes:

    a) Entrez un mot de passe dans la zone **Mot de passe** , puis entrez-le à nouveau dans la zone **Confirmer le mot de passe** .

    b) Sélectionnez **Stocker le mot de passe dans un fichier**. Notez que si vous ne stockez pas le mot de passe, les tentatives de démarrage des canaux SSL échouent car ils ne peuvent pas obtenir le mot de passe requis pour accéder au fichier de la base de données de clés.

    c) Cliquez sur **OK**. Une fenêtre s'ouvre, confirmant que le mot de passe se trouve dans le fichier `key.sth` (sauf si vous avez spécifié un nom de radical différent).
13. Cliquez sur **OK**. Le cadre de contenu de la base de données de clés s'affiche.

Demande d'un certificat personnel pour votre matériel PKCS #11
Utilisez cette procédure pour un gestionnaire de files d'attente ou un client IBM WebSphere MQ MQI afin de demander un certificat personnel pour votre matériel de cryptographie.

Utilisation de l'interface utilisateur iKeyman

Pourquoi et quand exécuter cette tâche

Remarque : WebSphere MQ ne prend pas en charge les algorithmes SHA-3 ou SHA-5 . Vous pouvez utiliser les noms d'algorithme de signature numérique SHA384WithRSA et SHA512WithRSA car ces deux algorithmes sont membres de la famille SHA-2 .

Les noms d'algorithme de signature numérique SHA3WithRSA et SHA5WithRSA sont obsolètes car ils sont de forme abrégée SHA384WithRSA et SHA512WithRSA respectivement.

Procédure

Pour demander un certificat personnel à partir de l'interface utilisateur iKeyman , procédez comme suit:

1. Procédez comme suit pour utiliser votre matériel de cryptographie. Voir «Gestion des certificats sur le matériel PKCS #11», à la page 145.
2. Dans le menu **Créer** , cliquez sur **Nouvelle demande de certificat**.

   La fenêtre Créer une nouvelle clé et une nouvelle demande de certificat s'ouvre.
3. Dans la zone **Key Label** , entrez les libellés suivants:
   - Pour un gestionnaire de files d'attente, entrez `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour un gestionnaire de files d'attente appelé `QM1`, entrez `ibmwebspheremqqm1`.
   - Pour un IBM WebSphere MQ MQI client, entrez `ibmwebspheremq` suivi de votre ID utilisateur de connexion, en minuscules ; par exemple, `ibmwebspheremqmyuserid` .
4. Entrez des valeurs pour **Nom usuel** et **Organisation**, puis sélectionnez un **pays** . Pour les autres zones facultatives, acceptez les valeurs par défaut ou entrez ou sélectionnez de nouvelles valeurs.

   Notez que vous ne pouvez indiquer qu'un seul nom dans la zone **Unité organisationnelle** . Pour plus d'informations sur ces zones, voir «Noms distinctifs», à la page 11.
5. Dans la zone **Entrez le nom d'un fichier dans lequel stocker la demande de certificat** , acceptez la valeur par défaut `certreq.arm`ou entrez une nouvelle valeur avec un chemin d'accès complet.
6. Cliquez sur **OK**.

   Une fenêtre de confirmation s'ouvre.
7. Cliquez sur **OK**.

   La liste **Demandes de certificat personnel** affiche le libellé de la nouvelle demande de certificat personnel que vous avez créée. La demande de certificat est stockée dans le fichier que vous avez choisi à l'étape «5», à la page 148.
8. Demandez le nouveau certificat personnel soit en envoyant le fichier à une autorité de certification, soit en copiant le fichier dans le formulaire de demande sur le site Web de l'autorité de certification.

Utilisation de la ligne de commande

Procédure

Utilisez les commandes suivantes pour demander un certificat personnel à l'aide de la commande **runmqckm** ou **runmqakm** :

- A l'aide de **runmqckm**:

```
runmqckm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -sig_alg algorithm
```

  A la place de `-dn` *distinguished_name* , vous pouvez utiliser `-san_dsname` *DNS_names* , `-san_emailaddr` *email_addresses* ou `-san_ipaddr` *IP_addresses* .

- Utilisation de runmqakm:

```
runmqakm -certreq -create -db filename -pw
password -label label
        -dn distinguished_name -size key_size
 -file filename -fips
        -sig_alg algorithm
```

où :

-db ***nom_fichier***
Indique le nom de fichier qualifié complet d'une base de données de clés CMS.

-pw ***mot_de_passe***
Indique le mot de passe de la base de données de clés CMS.

-label ***Libellé***
Indique le libellé de clé associé au certificat.

-dn ***nom_distinctif***
Indique le nom distinctif X.500 entre guillemets. Au moins un attribut est requis. Vous pouvez fournir plusieurs attributs d'unité organisationnelle et de centre de données.

-size ***taille_clé***
Indique la taille de la clé. Si vous utilisez **runmqckm** , la valeur peut être 512 ou 1024. Si vous utilisez **runmqakm**, la valeur peut être 512, 1024ou 2048.

-file ***nom fichier***
Indique le nom de fichier de la demande de certificat.

-fips
indique que la commande est exécutée en mode FIPS. Ce mode désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

-sig_alg
Pour **runmqckm**, indique l'algorithme de signature asymétrique utilisé pour la création de la paire de clés de l'entrée. La valeur peut être 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, SHAWithDSAou SHAWithRSA . La valeur par défaut est SHA1WithRSA

-sig_alg
Pour **runmqakm**, indique l'algorithme de hachage utilisé lors de la création d'une demande de certificat. Cet algorithme de hachage est utilisé pour créer la signature associée à la demande de certificat nouvellement créée. La valeur peut être 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. La valeur par défaut est SHA1WithRSA.

-san_dnsname ***noms_DNS***
Indique une liste de noms DNS séparés par des virgules ou des espaces pour l'entrée en cours de création.

-san_emailaddr ***adresse_e-mail***
Indique une liste d'adresses électroniques séparées par des virgules ou des espaces pour l'entrée en cours de création.

-san_ipaddr ***Adresse_IP***
Indique une liste d'adresses IP séparées par des virgules ou des espaces pour l'entrée en cours de création.

Importation d'un certificat personnel sur votre matériel PKCS #11
Utilisez cette procédure pour un gestionnaire de files d'attente ou un client IBM WebSphere MQ MQI afin d'importer un certificat personnel sur votre matériel de cryptographie.

Utilisation d'iKeyman

Procédure

Pour demander un certificat personnel à partir de l'interface utilisateur iKeyman , procédez comme suit:

1. Procédez comme suit pour utiliser votre matériel de cryptographie. Voir «Gestion des certificats sur le matériel PKCS #11», à la page 145.

2. Cliquez sur **Recevoir**. La fenêtre Recevoir un certificat d'un fichier s'affiche.
3. Sélectionnez le **Type de données** du nouveau certificat personnel ; par exemple, `Base64-encoded ASCII data` pour un fichier avec l'extension `.arm` .
4. Entrez le nom du fichier de certificat et l'emplacement du nouveau certificat personnel ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
5. Cliquez sur **OK**. Si vous disposez déjà d'un certificat personnel dans votre base de données de clés, une fenêtre s'ouvre et vous demande si vous souhaitez définir la clé que vous ajoutez comme clé par défaut dans la base de données.
6. Cliquez sur **Oui** ou sur **Non**. La fenêtre Enter a Label s'ouvre.
7. Entrez un libellé.

   Par exemple, vous pouvez utiliser le même libellé que lorsque vous avez demandé le certificat personnel. Notez que le libellé doit être au format IBM WebSphere MQ correct:

   - Pour un gestionnaire de files d'attente, `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour un gestionnaire de files d'attente appelé QM1, le libellé serait: `ibmwebspheremqqm1`.
   - Pour un client IBM WebSphere MQ MQI, `ibmwebspheremq` suivi de votre ID utilisateur de connexion en minuscules. Par exemple, pour un ID utilisateur `MyUserID`, le libellé serait: `ibmwebspheremqmyuserid`.
8. Cliquez sur **OK**. La liste **Certificats personnels** affiche le libellé du nouveau certificat personnel que vous avez ajouté. Ce libellé est formé en ajoutant le libellé de jeton de chiffrement avant le libellé que vous avez fourni.

Utilisation de la ligne de commande

Procédure

Pour demander un certificat personnel à partir d'une ligne de commande, procédez comme suit:

1. Ouvrez une fenêtre de commande configurée pour votre environnement.
2. Entrez la commande appropriée pour votre système d'exploitation et votre configuration:

   - Sur les systèmes Windows, UNIX and Linux , utilisez l'une des commandes suivantes:

     ```
     runmqckm -cert -receive -file filename -crypto path
     -tokenlabel hardware_token -pw hardware_password -format cert_format
     ```

     ```
     runmqakm -cert -receive -file filename -crypto path
     -tokenlabel hardware_token -pw hardware_password -format cert_format -fips
     ```

   où :

   -file *nom fichier*
   Indique le nom de fichier complet du fichier contenant le certificat personnel.

   -crypto *chemin*
   Indique le chemin d'accès complet à la bibliothèque PKCS #11 fournie avec le matériel.

   -tokenlabel *jeton_matériel*
   Indique le libellé attribué à la partie stockage du matériel de cryptographie lors de l'installation.

   -pw *mot_de_passe_matériel*
   Indique le mot de passe d'accès au matériel.

   -format *format_certificat*
   Indique le format du certificat. La valeur peut-être `ascii` pour les données ASCII codées en base 64 ou `binary` pour les données Binary DER. La valeur par défaut est ASCII.

   -fips
   Indique que la commande est exécutée en mode FIPS. Ce mode désactive l'utilisation de la bibliothèque cryptographique BSafe. Seul le composant ICC est utilisé et ce composant doit être

initialisé en mode FIPS. En mode FIPS, le composant ICC utilise des algorithmes validés par FIPS 140-2. Si le composant ICC ne s'initialise pas en mode FIPS, la commande **runmqakm** échoue.

Identification et authentification des utilisateurs

Vous pouvez identifier et authentifier les utilisateurs à l'aide de la structure MQCSP ou dans plusieurs types de programme d'exit utilisateur.

Utilisation de la structure MQCSP

Vous spécifiez la structure des paramètres de sécurité de connexion MQCSP sur un appel MQCONNX ; cette structure contient un ID utilisateur et un mot de passe. Si nécessaire, vous pouvez modifier le MQCSP dans un exit de sécurité.

Remarque : Le gestionnaire des droits d'accès aux objets (OAM) n'utilise pas le mot de passe. Cependant, l'OAM effectue un travail limité avec l'ID utilisateur, ce qui peut être considéré comme une forme d'authentification triviale. Ces vérifications vous empêchent d'adopter un autre ID utilisateur, si vous utilisez ces paramètres dans vos applications.

Implémentation de l'identification et de l'authentification dans les exits de sécurité

L'objectif principal d'un exit de sécurité est d'activer l'agent MCA à chaque extrémité d'un canal pour authentifier son partenaire. A chaque extrémité d'un canal de transmission de messages et à l'extrémité serveur d'un canal MQI, un agent MCA agit généralement pour le compte du gestionnaire de files d'attente auquel il est connecté. A l'extrémité client d'un canal MQI, un agent MCA agit généralement pour le compte de l'utilisateur de l'application client WebSphere MQ . Dans ce cas, l'authentification mutuelle a lieu entre deux gestionnaires de files d'attente ou entre un gestionnaire de files d'attente et l'utilisateur d'une application client WebSphere MQ MQI.

L'exit de sécurité fourni (l'exit de canal SSPI) illustre comment l'authentification mutuelle peut être implémentée en échangeant des jetons d'authentification qui sont générés, puis vérifiés, par un serveur d'authentification sécurisé tel que Kerberos. Pour plus de détails, voir «Programme d'exit de canal SSPI», à la page 107.

L'authentification mutuelle peut également être mise en oeuvre à l'aide de la technologie PKI (Public Key Infrastructure). Chaque exit de sécurité génère des données aléatoires, les signe à l'aide de la clé privée du gestionnaire de files d'attente ou de l'utilisateur qu'il représente et envoie les données signées à son partenaire dans un message de sécurité. L'exit de sécurité partenaire effectue l'authentification en vérifiant la signature numérique à l'aide de la clé publique du gestionnaire de files d'attente ou de l'utilisateur. Avant d'échanger des signatures numériques, les exits de sécurité peuvent avoir besoin de convenir de l'algorithme de génération d'un résumé de message, si plusieurs algorithmes sont disponibles pour être utilisés.

Lorsqu'un exit de sécurité envoie les données signées à son partenaire, il doit également envoyer un moyen d'identifier le gestionnaire de files d'attente ou l'utilisateur qu'il représente. Il peut s'agir d'un nom distinctif ou même d'un certificat numérique. Si un certificat numérique est envoyé, l'exit de sécurité partenaire peut le valider en utilisant la chaîne de certificats pour le certificat de l'autorité de certification racine. Cela garantit la propriété de la clé publique utilisée pour vérifier la signature numérique.

L'exit de sécurité partenaire ne peut valider un certificat numérique que s'il a accès à un référentiel de clés qui contient les certificats restants dans la chaîne de certificats. Si un certificat numérique pour le gestionnaire de files d'attente ou l'utilisateur n'est pas envoyé, il doit être disponible dans le référentiel de clés auquel l'exit de sécurité partenaire a accès. L'exit de sécurité partenaire ne peut pas vérifier la signature numérique sauf s'il peut trouver la clé publique du signataire.

Les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) utilisent des techniques PKI telles que celles qui viennent d'être décrites. Pour plus d'informations sur la manière dont SSL et TLS effectuent l'authentification, voir «Concepts SSL (Secure Sockets Layer) et TLS (Transport Layer Security)», à la page 15.

Si un serveur d'authentification sécurisé ou une prise en charge de l'infrastructure PKI n'est pas disponible, d'autres techniques peuvent être utilisées. Une technique commune, qui peut être implémentée dans les exits de sécurité, utilise un algorithme de clé symétrique.

L'un des exits de sécurité, l'exit A, génère un nombre aléatoire et l'envoie dans un message de sécurité à son exit de sécurité partenaire, l'exit B. L'exit B chiffre le nombre à l'aide de sa copie d'une clé connue uniquement des deux exits de sécurité. L'exit B envoie le numéro chiffré à l'exit A dans un message de sécurité avec un deuxième nombre aléatoire que l'exit B a généré. L'exit A vérifie que le premier nombre aléatoire a été chiffré correctement, chiffre le deuxième nombre aléatoire à l'aide de sa copie de la clé et envoie le nombre chiffré à l'exit B dans un message de sécurité. La sortie B vérifie alors que le deuxième nombre aléatoire a été chiffré correctement. Lors de cet échange, si l'un des exits de sécurité n'est pas satisfait de l'authenticité d'un autre, il peut demander à l'agent MCA de fermer le canal.

Un avantage de cette technique est qu'aucune clé ou mot de passe n'est envoyé sur la connexion de communication lors de l'échange. Un inconvénient est qu'il ne permet pas de résoudre le problème de la répartition sécurisée de la clé partagée. Une solution à ce problème est décrite dans «Implémentation de la confidentialité dans les programmes d'exit utilisateur», à la page 235. Une technique similaire est utilisée dans SNA pour l'authentification mutuelle de deux unités logiques lorsqu'elles se lient pour former une session. Cette technique est décrite dans «Authentification au niveau de la session», à la page 78.

Toutes les techniques d'authentification mutuelle précédentes peuvent être adaptées pour fournir une authentification unidirectionnelle.

Implémentation de l'identification et de l'authentification dans les exits de message

Lorsqu'une application place un message dans une file d'attente, la zone *UserIdentifier* du descripteur de message contient un ID utilisateur associé à l'application. Toutefois, il n'existe aucune donnée pouvant être utilisée pour authentifier l'ID utilisateur. Ces données peuvent être ajoutées par un exit de message à l'extrémité émettrice d'un canal et vérifiées par un exit de message à l'extrémité réceptrice du canal. Les données d'authentification peuvent être par example un mot de passe chiffré ou une signature numérique.

Ce service peut être plus efficace s'il est implémenté au niveau de l'application. La condition de base est que l'utilisateur de l'application qui reçoit le message puisse identifier et authentifier l'utilisateur de l'application qui a envoyé le message. Il est donc naturel d'envisager la mise en oeuvre de ce service au niveau de l'application. Pour plus d'informations, voir «Mappage d'identité dans l'exit d'API et l'exit de croisement d'API», à la page 156.

Implémentation de l'identification et de l'authentification dans l'exit d'API et l'exit de croisement d'API

Au niveau d'un message individuel, l'identification et l'authentification sont un service qui implique deux utilisateurs, l'expéditeur et le destinataire du message. La condition de base est que l'utilisateur de l'application qui reçoit le message puisse identifier et authentifier l'utilisateur de l'application qui a envoyé le message. Notez que l'exigence concerne l'authentification unidirectionnelle et non bidirectionnelle.

Selon la façon dont il est implémenté, les utilisateurs et leurs applications peuvent avoir besoin d'interfacer, voire d'interagir, avec le service. En outre, le moment et la manière dont le service est utilisé peuvent dépendre de l'emplacement des utilisateurs et de leurs applications, ainsi que de la nature des applications elles-mêmes. Il est donc naturel d'envisager d'implémenter le service au niveau de l'application plutôt qu'au niveau de la liaison.

Si vous envisagez d'implémenter ce service au niveau de la liaison, vous devrez peut-être résoudre les problèmes suivants:

- Sur un canal de transmission de messages, comment appliquer le service uniquement aux messages qui en ont besoin?
- Comment autorisez-vous les utilisateurs et leurs applications à interagir avec le service, si c'est une exigence?

- Dans une situation à plusieurs tronçons, où un message est envoyé via plusieurs canaux de transmission de messages sur le chemin de sa destination, où appelez-vous les composants du service?

Voici quelques exemples de la façon dont le service d'identification et d'authentification peut être implémenté au niveau de l'application. Le terme *exit d'API* signifie un exit d'API ou un exit de croisement d'API.

- Lorsqu'une application place un message dans une file d'attente, un exit API peut acquérir un jeton d'authentification à partir d'un serveur d'authentification sécurisé tel que Kerberos. L'exit API peut ajouter ce jeton aux données d'application dans le message. Lorsque le message est extrait par l'application de réception, un deuxième exit API peut demander au serveur d'authentification d'authentifier l'expéditeur en vérifiant le jeton.
- Lorsqu'une application place un message dans une file d'attente, un exit API peut ajouter les éléments suivants aux données d'application du message:
  - Certificat numérique de l'expéditeur
  - Signature numérique de l'expéditeur

  Si des algorithmes différents sont disponibles pour la génération d'un résumé de message, l'exit d'API peut inclure le nom de l'algorithme qu'il a utilisé.

  Lorsque le message est extrait par l'application de réception, un deuxième exit d'API peut effectuer les vérifications suivantes:

  - L'exit API peut valider le certificat numérique en utilisant la chaîne de certificats pour le certificat de l'autorité de certification racine. Pour ce faire, l'exit API doit avoir accès à un référentiel de clés qui contient les certificats restants dans la chaîne de certificats. Cette vérification garantit que l'expéditeur, identifié par le nom distinctif, est le véritable propriétaire de la clé publique contenue dans le certificat.
  - L'exit API peut vérifier la signature numérique à l'aide de la clé publique contenue dans le certificat. Cette vérification authentifie l'expéditeur.

  Le nom distinctif de l'expéditeur peut être envoyé à la place du certificat numérique complet. Dans ce cas, le référentiel de clés doit contenir le certificat de l'expéditeur pour que le deuxième exit d'API puisse trouver la clé publique de l'expéditeur. Une autre possibilité consiste à envoyer tous les certificats de la chaîne de certificats.
- Lorsqu'une application place un message dans une file d'attente, la zone *UserIdentifier* du descripteur de message contient un ID utilisateur associé à l'application. L'ID utilisateur peut être utilisé pour identifier l'expéditeur. Pour activer l'authentification, un exit d'API peut ajouter des données, telles qu'un mot de passe chiffré, aux données d'application du message. Lorsque le message est extrait par l'application de réception, un deuxième exit API peut authentifier l'ID utilisateur à l'aide des données qui ont été transmises avec le message.

  Cette technique peut être considérée comme suffisante pour les messages provenant d'un environnement contrôlé et sécurisé, et dans les cas où un serveur d'authentification sécurisé ou une prise en charge de l'infrastructure PKI n'est pas disponible.

Utilisateurs privilégiés

Un utilisateur privilégié est un utilisateur disposant de droits d'administration complets pour WebSphere MQ.

Outre les utilisateurs répertoriés dans le tableau suivant, les membres de tout groupe disposant des droits `+crt` sur les files d'attente sont indirectement des administrateurs. De même, tout utilisateur disposant des droits `+set` sur le gestionnaire de files d'attente et des droits `+put` sur la file d'attente de commandes est un administrateur.

Vous ne devez pas accorder ces privilèges à des utilisateurs et des applications ordinaires.

Tableau 13. Utilisateurs privilégiés par plateforme.

Tableau des utilisateurs privilégiés. Sous Windows, SYSTEM, tous les membres du groupe mqm et tous les membres du groupe Administrateurs sont des utilisateurs privilégiés. Sur les systèmes UNIX and Linux , tous les membres du groupe mqm sont des utilisateurs privilégiés. Sous IBM i, les profils (utilisateurs) qmqm et qmqmadm, tous les membres du groupe qmqmadm et tout utilisateur défini avec le paramètre *ALLOBJ sont des utilisateurs privilégiés.

Plateforme	**Utilisateurs privilégiés**
Systèmes Windows	• SYSTEME • Membres du groupe mqm • Membres du groupe Administrateurs
Systèmes UNIX and Linux	• Membres du groupe mqm

Identification et authentification des utilisateurs à l'aide de la structure MQCSP

Vous pouvez spécifier la structure des paramètres de sécurité de connexion MQCSP sur un appel MQCONNX.

La structure des paramètres de sécurité de connexion MQCSP contient un ID utilisateur et un mot de passe que le service d'autorisation peut utiliser pour identifier et authentifier l'utilisateur.

Le composant de service d'autorisation fourni avec IBM WebSphere MQ est appelé Object Authority Manager (OAM). La méthode d'accès aux objets (OAM) autorise les utilisateurs en fonction de l'ID contenu dans le MQCSP, mais ne valide pas le mot de passe. Il est possible d'implémenter la validation de mot de passe dans le service d'autorisation en utilisant des exits chaînés avec la méthode d'accès aux objets (OAM) ou en remplaçant la méthode d'accès aux objets (OAM) par un autre service d'autorisation.

Vous pouvez modifier le MQCSP dans un exit de sécurité.

Implémentation de l'identification et de l'authentification dans les exits de sécurité

Vous pouvez utiliser un exit de sécurité pour implémenter l'authentification unidirectionnelle ou mutuelle.

L'objectif principal d'un exit de sécurité est d'activer l'agent MCA à chaque extrémité d'un canal pour authentifier son partenaire. A chaque extrémité d'un canal de transmission de messages et à l'extrémité serveur d'un canal MQI, un agent MCA agit généralement pour le compte du gestionnaire de files d'attente auquel il est connecté. A l'extrémité client d'un canal MQI, un agent MCA agit généralement pour le compte de l'utilisateur de l'application client WebSphere MQ MQI. Dans ce cas, l'authentification mutuelle a lieu entre deux gestionnaires de files d'attente ou entre un gestionnaire de files d'attente et l'utilisateur d'une application client WebSphere MQ MQI.

L'exit de sécurité fourni (l'exit de canal SSPI) illustre comment l'authentification mutuelle peut être implémentée en échangeant des jetons d'authentification qui sont générés, puis vérifiés, par un serveur d'authentification sécurisé tel que Kerberos. Pour plus de détails, voir «Programme d'exit de canal SSPI», à la page 107.

L'authentification mutuelle peut également être mise en oeuvre à l'aide de la technologie PKI (Public Key Infrastructure). Chaque exit de sécurité génère des données aléatoires, les signe à l'aide de la clé privée du gestionnaire de files d'attente ou de l'utilisateur qu'il représente et envoie les données signées à son partenaire dans un message de sécurité. L'exit de sécurité partenaire effectue l'authentification en vérifiant la signature numérique à l'aide de la clé publique du gestionnaire de files d'attente ou de l'utilisateur. Avant d'échanger des signatures numériques, les exits de sécurité peuvent avoir besoin de convenir de l'algorithme de génération d'un résumé de message, si plusieurs algorithmes sont disponibles pour être utilisés.

Lorsqu'un exit de sécurité envoie les données signées à son partenaire, il doit également envoyer un moyen d'identifier le gestionnaire de files d'attente ou l'utilisateur qu'il représente. Il peut s'agir d'un nom distinctif ou même d'un certificat numérique. Si un certificat numérique est envoyé, l'exit de sécurité partenaire peut le valider en utilisant la chaîne de certificats pour le certificat de l'autorité de certification racine. Cela garantit la propriété de la clé publique utilisée pour vérifier la signature numérique.

L'exit de sécurité partenaire ne peut valider un certificat numérique que s'il a accès à un référentiel de clés qui contient les certificats restants dans la chaîne de certificats. Si un certificat numérique pour le gestionnaire de files d'attente ou l'utilisateur n'est pas envoyé, il doit être disponible dans le référentiel de clés auquel l'exit de sécurité partenaire a accès. L'exit de sécurité partenaire ne peut pas vérifier la signature numérique sauf s'il peut trouver la clé publique du signataire.

Les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) utilisent des techniques PKI telles que celles qui viennent d'être décrites. Pour plus d'informations sur la manière dont la couche Secure Sockets Layer effectue l'authentification, voir «Concepts SSL (Secure Sockets Layer) et TLS (Transport Layer Security)», à la page 15.

Si un serveur d'authentification sécurisé ou une prise en charge de l'infrastructure PKI n'est pas disponible, d'autres techniques peuvent être utilisées. Une technique commune, qui peut être implémentée dans les exits de sécurité, utilise un algorithme de clé symétrique.

L'un des exits de sécurité, l'exit A, génère un nombre aléatoire et l'envoie dans un message de sécurité à son exit de sécurité partenaire, l'exit B. L'exit B chiffre le nombre à l'aide de sa copie d'une clé connue uniquement des deux exits de sécurité. L'exit B envoie le numéro chiffré à l'exit A dans un message de sécurité avec un deuxième nombre aléatoire que l'exit B a généré. L'exit A vérifie que le premier nombre aléatoire a été chiffré correctement, chiffre le deuxième nombre aléatoire à l'aide de sa copie de la clé et envoie le nombre chiffré à l'exit B dans un message de sécurité. La sortie B vérifie alors que le deuxième nombre aléatoire a été chiffré correctement. Lors de cet échange, si l'un des exits de sécurité n'est pas satisfait de l'authenticité d'un autre, il peut demander à l'agent MCA de fermer le canal.

Un avantage de cette technique est qu'aucune clé ou mot de passe n'est envoyé sur la connexion de communication lors de l'échange. Un inconvénient est qu'il ne permet pas de résoudre le problème de la répartition sécurisée de la clé partagée. Une solution à ce problème est décrite dans «Implémentation de la confidentialité dans les programmes d'exit utilisateur», à la page 235. Une technique similaire est utilisée dans SNA pour l'authentification mutuelle de deux unités logiques lorsqu'elles se lient pour former une session. Cette technique est décrite dans «Authentification au niveau de la session», à la page 78.

Toutes les techniques d'authentification mutuelle précédentes peuvent être adaptées pour fournir une authentification unidirectionnelle.

Mappage d'identité dans les exits de message

Vous pouvez utiliser des exits de message pour traiter des informations afin d'authentifier un ID utilisateur, mais il peut être préférable d'implémenter l'authentification au niveau de l'application.

Lorsqu'une application place un message dans une file d'attente, la zone *UserIdentifier* du descripteur de message contient un ID utilisateur associé à l'application. Toutefois, il n'existe aucune donnée pouvant être utilisée pour authentifier l'ID utilisateur. Ces données peuvent être ajoutées par un exit de message à l'extrémité émettrice d'un canal et vérifiées par un exit de message à l'extrémité réceptrice du canal. Les données d'authentification peuvent être par example un mot de passe chiffré ou une signature numérique.

Ce service peut être plus efficace s'il est implémenté au niveau de l'application. La condition de base est que l'utilisateur de l'application qui reçoit le message puisse identifier et authentifier l'utilisateur de l'application qui a envoyé le message. Il est donc naturel d'envisager la mise en oeuvre de ce service au niveau de l'application. Pour plus d'informations, voir «Mappage d'identité dans l'exit d'API et l'exit de croisement d'API», à la page 156.

Mappage d'identité dans l'exit d'API et l'exit de croisement d'API

Une application qui reçoit un message doit être en mesure d'identifier et d'authentifier l'utilisateur de l'application qui a envoyé le message. Ce service est généralement mieux implémenté au niveau de l'application. Les exits API peuvent implémenter le service de différentes manières.

Au niveau d'un message individuel, l'identification et l'authentification sont un service qui implique deux utilisateurs, l'expéditeur et le destinataire du message. La condition de base est que l'utilisateur de l'application qui reçoit le message puisse identifier et authentifier l'utilisateur de l'application qui a envoyé le message. Notez que l'exigence concerne l'authentification unidirectionnelle et non bidirectionnelle.

Selon la façon dont il est implémenté, les utilisateurs et leurs applications peuvent avoir besoin d'interfacer, voire d'interagir, avec le service. En outre, le moment et la manière dont le service est utilisé peuvent dépendre de l'emplacement des utilisateurs et de leurs applications, ainsi que de la nature des applications elles-mêmes. Il est donc naturel d'envisager d'implémenter le service au niveau de l'application plutôt qu'au niveau de la liaison.

Si vous envisagez d'implémenter ce service au niveau de la liaison, vous devrez peut-être résoudre les problèmes suivants:

- Sur un canal de transmission de messages, comment appliquer le service uniquement aux messages qui en ont besoin?
- Comment autorisez-vous les utilisateurs et leurs applications à interagir avec le service, si c'est une exigence?
- Dans une situation à plusieurs tronçons, où un message est envoyé via plusieurs canaux de transmission de messages sur le chemin de sa destination, où appelez-vous les composants du service?

Voici quelques exemples de la façon dont le service d'identification et d'authentification peut être implémenté au niveau de l'application. Le terme *exit d'API* signifie un exit d'API ou un exit de croisement d'API.

- Lorsqu'une application place un message dans une file d'attente, un exit API peut acquérir un jeton d'authentification à partir d'un serveur d'authentification sécurisé tel que Kerberos. L'exit API peut ajouter ce jeton aux données d'application dans le message. Lorsque le message est extrait par l'application de réception, un deuxième exit API peut demander au serveur d'authentification d'authentifier l'expéditeur en vérifiant le jeton.
- Lorsqu'une application place un message dans une file d'attente, un exit API peut ajouter les éléments suivants aux données d'application du message:
  - Certificat numérique de l'expéditeur
  - Signature numérique de l'expéditeur

  Si des algorithmes différents sont disponibles pour la génération d'un résumé de message, l'exit d'API peut inclure le nom de l'algorithme qu'il a utilisé.

  Lorsque le message est extrait par l'application de réception, un deuxième exit d'API peut effectuer les vérifications suivantes:

  - L'exit API peut valider le certificat numérique en utilisant la chaîne de certificats pour le certificat de l'autorité de certification racine. Pour ce faire, l'exit API doit avoir accès à un référentiel de clés qui contient les certificats restants dans la chaîne de certificats. Cette vérification garantit que l'expéditeur, identifié par le nom distinctif, est le véritable propriétaire de la clé publique contenue dans le certificat.
  - L'exit API peut vérifier la signature numérique à l'aide de la clé publique contenue dans le certificat. Cette vérification authentifie l'expéditeur.

  Le nom distinctif de l'expéditeur peut être envoyé à la place du certificat numérique complet. Dans ce cas, le référentiel de clés doit contenir le certificat de l'expéditeur pour que le deuxième exit d'API puisse trouver la clé publique de l'expéditeur. Une autre possibilité consiste à envoyer tous les certificats de la chaîne de certificats.

- Lorsqu'une application place un message dans une file d'attente, la zone *UserIdentifier* du descripteur de message contient un ID utilisateur associé à l'application. L'ID utilisateur peut être utilisé pour identifier l'expéditeur. Pour activer l'authentification, un exit d'API peut ajouter des données, telles qu'un mot de passe chiffré, aux données d'application du message. Lorsque le message est extrait par l'application de réception, un deuxième exit API peut authentifier l'ID utilisateur à l'aide des données qui ont été transmises avec le message.

  Cette technique peut être considérée comme suffisante pour les messages provenant d'un environnement contrôlé et sécurisé, et dans les cas où un serveur d'authentification sécurisé ou une prise en charge de l'infrastructure PKI n'est pas disponible.

Utilisation des certificats révoqués

Les certificats numériques peuvent être révoqués par les autorités de certification. Vous pouvez vérifier le statut de révocation des certificats à l'aide d'OCSP ou de CRL sur les serveurs LDAP, en fonction de la plateforme.

Lors de l'établissement de liaison SSL, les partenaires communicants s'authentifient avec des certificats numériques. L'authentification peut inclure une vérification du certificat reçu. Les autorités de certification révoquent les certificats pour diverses raisons, notamment:

- Le propriétaire a été déplacé vers une autre organisation
- La clé privée n'est plus un secret

Les autorités de certification publient les certificats personnels révoqués dans une liste de révocation de certificat (CRL). Les certificats d'autorités de certification qui ont été révoqués sont publiés dans une liste de révocation des droits d'accès (ARL).

Sur les systèmes UNIX, Linux et Windows , le support SSL de WebSphere MQ vérifie les certificats révoqués à l'aide du protocole OCSP (Online Certificate Status Protocol) ou des listes CRL et ARL sur les serveurs LDAP (Lightweight Directory Access Protocol). OCSP est la méthode préférée. Les classes IBM WebSphere MQ classes for Java et IBM WebSphere MQ classes for JMS ne peuvent pas utiliser les informations OCSP dans un fichier de table de définition de canal du client. Toutefois, vous pouvez configurer OCSP comme indiqué à la section Using Online Certificate Protocol.

Sous z / Os et IBM i WebSphere MQ , la prise en charge SSL vérifie les certificats révoqués à l'aide de listes CRL et ARL sur les serveurs LDAP uniquement.

Pour plus d'informations sur le certificat

Droits d'accès, voir «Certificats numériques», à la page 9.

Certificats révoqués et OCSP

IBM WebSphere MQ détermine le répondeur OCSP (Online Certificate Status Protocol) à utiliser et traite la réponse reçue. Vous pouvez être amené à réaliser certaines étapes pour pouvoir accéder au répondeur OCSP.

Remarque : Ces informations s'appliquent uniquement à WebSphere MQ sur Windows, UNIX and Linux.

Pour vérifier l'état de retrait d'un certificat numérique à l'aide de OCSP, WebSphere MQ peut utiliser deux méthodes pour déterminer quel répondeur OCSP contacter :

- A l'aide de l'extension de certificat AuthorityInfoAccess (AIA) dans le certificat à vérifier.
- A l'aide d'une adresse URL spécifiée dans un objet d'informations d'authentification ou spécifiée par une application client.

Une URL spécifiée dans un objet d'informations d'authentification ou par une application client est prioritaire par rapport à une URL d'une extension de certificat AIA.

Si l'adresse URL du répondeur OCSP se trouve derrière le pare-feu, reconfigurez le pare-feu pour que le répondeur OCSP soit accessible ou configurez un serveur proxy OCSP. Indiquez le nom du serveur proxy en utilisant la variable SSLHTTPProxyName dans la strophe SSL. Sur les systèmes client, vous pouvez

également indiquer le nom du serveur proxy à l'aide de la variable d'environnement MQSSLPROXY. Pour plus de détails, consultez les informations connexes.

Si vous n'êtes pas concerné par la révocation des certificats TLS ou SSL, peut-être parce que vous exécutez un environnement de test, vous pouvez définir OCSPCheckExtensions sur NO dans la strophe SSL. Si vous configurez cette variable, toute extension de certificat AIA est ignorée. Cette solution sera probablement refusée dans un environnement de production, dans lequel vous ne souhaitez sûrement pas autoriser les utilisateurs à accéder aux certificats révoqués.

L'appel d'accès au répondeur OCSP peut entraîner l'un des trois résultats suivants :

Bon
Le certificat est valide.

Révoqué
Le certificat est révoqué.

Inconnu
Ce résultat peut survenir à cause de l'une des trois raisons suivantes :

- IBM WebSphere MQ ne peut pas accéder au répondeur OCSP.
- Le répondeur OCSP a envoyé une réponse, mais WebSphere MQ ne peut pas vérifier la signature numérique de la réponse.
- Le répondeur OCSP a envoyé une réponse qui indique qu'il n'existe pas de données de révocation pour le certificat.

Si IBM WebSphere MQ reçoit un résultat OCSP `Inconnu`, son comportement dépend de la valeur de l'attribut OCSPAuthentication. Pour les gestionnaires de files d'attente, cet attribut se trouve dans la strophe SSL du fichier `qm.ini` sur les systèmes UNIX and Linux ou dans le registre Windows. Il peut être défini à l'aide de l'explorateur IBM WebSphere MQ . Pour les clients, il s'agit de la strophe SSL du fichier de configuration du client.

Si une sortie `Inconnu` est reçue et si l'attribut OCSPAuthentication est défini sur REQUIRED (valeur par défaut), WebSphere MQ rejette la connexion et envoie un message d'erreur de type AMQ9716. Si les messages d'événements SSL de gestionnaire de files d'attente sont activés, un message d'événement SSL de type MQRC_CHANNEL_SSL_ERROR, avec ReasonQualifier défini sur MQRQ_SSL_HANDSHAKE_ERROR, est généré.

Si une sortie `Inconnu` est reçue et si l'attribut OCSPAuthentication est défini sur OPTIONAL, WebSphere MQ permet au canal SSL de démarrer et aucun avertissement ou message d'événement SSL n'est généré.

Si `Inconnu` est reçu et que l'attribut OCSPAuthentication a la valeur WARN, le canal SSL démarre, mais IBM WebSphere MQ génère un message d'avertissement de type AMQ9717 dans le journal des erreurs. Si les messages d'événements SSL de gestionnaire de files d'attente sont activés, un message d'événement SSL de type MQRC_CHANNEL_SSL_WARNING, avec ReasonQualifier défini sur MQRQ_SSL_UNKNOWN_REVOCATION, est généré.

Signature numérique de réponses OCSP

Un répondeur OCSP peut signer ses réponses de trois manières. Votre répondeur vous informe de la méthode à utiliser.

- La réponse OCSP peut être signée numériquement à l'aide du même certificat CA qui a émis le certificat en cours de vérification. Dans ce cas, vous n'avez pas besoin de configurer d'autres certificats ; les étapes que vous avez déjà prises pour établir la connectivité SSL suffisent pour vérifier la réponse OCSP.
- La réponse OCSP peut être signée numériquement à l'aide d'un autre certificat signé par la même autorité de certification que celle ayant émis le certificat en cours de vérification. Le certificat signataire est envoyé avec la réponse OCSP dans ce cas. Le certificat transmis à partir du répondeur OCSP doit avoir une extension d'utilisation clé étendue définie sur `id-kp-OCSPSigning` pour pouvoir être digne de confiance. Etant donné que la réponse OCSP est envoyée avec le certificat signataire (et que ce certificat est signé par une autorité de certification déjà digne de confiance pour la connectivité SSL), aucune configuration supplémentaire n'est requise.

- La réponse OCSP peut être signée numériquement à l'aide d'un autre certificat qui n'est pas directement lié au certificat en cours de vérification. Dans ce cas, la réponse OCSP est signée par un certificat émis par le répondeur OCSP. Vous devez ajouter une copie du certificat de répondeur OCSP à la base de données de clés du client ou du gestionnaire de files d'attente effectuant la vérification OCSP ; voir «Ajout d'un certificat de l'autorité de certification (ou de la partie publique d'un certificat autosigné) dans un référentiel de clés sur les systèmes UNIX, Linux, and Windows», à la page 137. Lors de l'ajout d'un certificat CA, il est ajouté par défaut en racine de confiance, ce qui représente le paramètre requis dans ce contexte. Si ce certificat n'est pas ajouté, WebSphere MQ ne peut pas vérifier la signature numérique sur la réponse OCSP et la vérification OCSP donne un résultat Inconnu, ce qui peut entraîner la fermeture du canal par IBM WebSphere MQ, selon la valeur d'OCSPAuthentication.

Protocole OCSP (Online Certificate Status Protocol) dans des applications client Java et JMS

En raison d'une limitation de l'interface de programme d'application Java, WebSphere MQ ne peut utiliser la vérification de révocation de certificat OCSP pour des connexions sécurisées SSL et TLS que lorsque OCSP est activé pour l'intégralité du processus de la machine virtuelle Java. OCSP peut être activé pour toutes les connexions sécurisées de la machine virtuelle Java de deux manières :

- En modifiant le fichier JRE java.security pour y inclure les paramètres de configuration OCSP affichés dans le tableau 1 et en redémarrant l'application.
- En utilisant l'interface de programme d'application java.security.Security.setProperty(), qui est soumise à toutes les règles Java Security Manager en vigueur.

Vous devez au moins spécifier l'une des valeurs ocsp.enable et ocsp.responderURL.

Nom de la propriété	Description
ocsp.enable	Cette propriété a la valeur `true` ou `false`. Si la valeur est `true`, la vérification OCSP est activée lors de la vérification de révocation de certificat. Si la valeur est `false` (ou non définie), la vérification OCSP est désactivée.
ocsp.responderURL	La valeur de cette propriété est une adresse URL identifiant l'emplacement du canal répondeur OCSP. Par exemple, `ocsp.responderURL=http://ocsp.example.net:80`. Par défaut, l'emplacement du canal répondeur OCSP est déterminé de manière implicite à partir du certificat en cours de validation. La propriété est utilisée lorsque l'extension Authority Information Access (définie dans RFC 3280) n'est pas indiquée dans le certificat ou lorsqu'elle doit être remplacée.
ocsp.responderCertSubjectName	La valeur de cette propriété est le nom du sujet du certificat du canal répondeur OCSP. Par exemple, `ocsp.responderCertSubjectName="CN=OCSP Responder, O=XYZ Corp"`. Par défaut, le certificat du canal répondeur OCSP est celui de l'émetteur du certificat en cours de validation. Cette propriété identifie le certificat du canal répondeur OCSP lorsque la valeur par défaut ne s'applique pas. Sa valeur est un nom distinctif de chaîne (défini dans RFC 2253) qui identifie un certificat dans l'ensemble des certificats fournis lors de la validation du chemin aux certificats. Lorsque le seul nom du sujet ne suffit pas à identifier le certificat, alors les propriétés ocsp.responderCertIssuerName et ocsp.responderCertSerialNumber doivent toutes deux être utilisées. Lorsque cette propriété est définie, les propriétés ocsp.responderCertIssuerName et ocsp.responderCertSerialNumber sont ignorées.
ocsp.responderCertIssuerName	La valeur de cette propriété est le nom de l'émetteur du certificat du canal répondeur OCSP. Par

Nom de la propriété	Description
	exemple, `ocsp.responderCertIssuerName="CN=Enterprise CA, O=XYZ Corp"`. Par défaut, le certificat du canal répondeur OCSP est celui de l'émetteur du certificat en cours de validation. Cette propriété identifie le certificat du canal répondeur OCSP lorsque la valeur par défaut ne s'applique pas. Sa valeur est un nom distinctif de chaîne (défini dans RFC 2253) qui identifie un certificat dans l'ensemble des certificats fournis lors de la validation du chemin aux certificats. Lorsque cette propriété est définie, la propriété ocsp.responderCertSerialNumber doit également être définie. Cette propriété est ignorée lorsque la propriété ocsp.responderCertSubjectName est définie.
ocsp.responderCertSerialNumber	La valeur de cette propriété est le numéro de série du certificat du canal répondeur OCSP. Par exemple, `ocsp.responderCertSerialNumber=2A:FF:00`. Par défaut, le certificat du canal répondeur OCSP est celui de l'émetteur du certificat en cours de validation. Cette propriété identifie le certificat du canal répondeur OCSP lorsque la valeur par défaut ne s'applique pas. Cette valeur est une chaîne de chiffres hexadécimaux (séparés par des signes deux-points ou des espaces) qui identifie un certificat dans l'ensemble des certificats fournis lors de la validation du chemin d'accès aux certificats. Lorsque cette propriété est définie, la propriété ocsp.responderCertIssuerName doit également être définie. Cette propriété est ignorée lorsque la propriété ocsp.responderCertSubjectName est définie.

Avant d'activer OCSP de cette manière, tenez compte des remarques suivantes :

- La définition de la configuration OCSP affecte toutes les connexions sécurisées du processus de la machine virtuelle Java. Dans certains cas, cette configuration peut avoir des effets indésirables lorsque la machine virtuelle Java est partagée avec un autre code d'application utilisant des connexions sécurisées SSL ou TLS. Assurez-vous que la configuration OCSP choisie est appropriée à toutes les applications s'exécutant sur la même machine virtuelle Java.
- L'application de la maintenance à votre environnement d'exécution Java écrase le fichier java.security. Soyez attentif, lorsque vous appliquez des correctifs temporaires Java ou une maintenance produit, à éviter l'écrasement du fichier java.security. Il peut s'avérer nécessaire d'appliquer à nouveau les modifications de votre fichier java.security après la maintenance. Pour cette raison, vous pouvez envisager de définir la configuration OCSP à l'aide de l'interface de programme d'application java.security.Security.setProperty().
- L'activation de la vérification OCSP n'est effective que si la vérification de la révocation est également activée. La vérification de la révocation est activée via la méthode `PKIXParameters.setRevocationEnabled()`.
- Si vous utilisez l'intercepteur AMS Java décrit dans Enabling OCSP checking in native interceptors, évitez d'utiliser une configuration OCSP java.security entrant en conflit avec la configuration OCSP AMS dans le fichier de configuration du magasin de clés.

Utilisation des listes de révocation de certificat et des listes de révocation d'autorité

La prise en charge de WebSphere MQpour les CRL et les ARL varie en fonction de la plateforme.

Le support CRL et ARL sur chaque plateforme est le suivant:

- Sous z/OS, System SSL prend en charge les listes CRL et ARL stockées sur les serveurs LDAP par le produit Tivoli Public Key Infrastructure.

- Sur les autres plateformes, la prise en charge de CRL et ARL est conforme aux recommandations de profil de CRL PKIX X.509 V2 .

WebSphere MQ gère un cache des listes de révocation de certificat et des listes de révocation de certificat qui ont été consultées au cours des 12 dernières heures.

Lorsqu'un gestionnaire de files d'attente ou un client WebSphere MQ MQI reçoit un certificat, il vérifie la liste de révocation de certificat pour confirmer que le certificat est toujours valide. WebSphere MQ effectue d'abord des vérifications dans le cache, s'il existe un cache. Si la liste de révocation de certificat ne figure pas dans le cache, WebSphere MQ interroge les emplacements du serveur de listes de révocation de certificat LDAP dans l'ordre dans lequel ils apparaissent dans la liste de noms des objets d'informations d'authentification spécifiés par l'attribut *SSLCRLNamelist* , jusqu'à ce que WebSphere MQ trouve une liste de révocation de certificat disponible. Si la liste de noms n'est pas spécifiée ou qu'elle est spécifiée avec une valeur vide, les listes de révocation de nom ne sont pas vérifiées.

Pour plus d'informations sur LDAP, voir Utilisation des services LDAP (Lightweight Directory Access Protocol) avec WebSphere MQ for Windows.

Configuration des serveurs LDAP

Configurez la structure de l'arborescence d'informations de l'annuaire LDAP pour refléter la hiérarchie des noms distinctifs des autorités de certification. Pour ce faire, utilisez les fichiers LDAP Data Interchange Format.

Configurez la structure DIT (Directory Information Tree) LDAP pour utiliser la hiérarchie correspondant aux noms distinctifs des autorités de certification qui émettent les certificats et les CRL. Vous pouvez configurer la structure DIT avec un fichier qui utilise le format LDIF (LDAP Data Interchange Format). Vous pouvez également utiliser des fichiers LDIF pour mettre à jour un répertoire.

Les fichiers LDIF sont des fichiers texte ASCII qui contiennent les informations requises pour définir des objets dans un annuaire LDAP. Les fichiers LDIF contiennent une ou plusieurs entrées, dont chacune comprend un nom distinctif, au moins une définition de classe d'objet et, éventuellement, plusieurs définitions d'attribut.

L'attribut `certificateRevocationList;binary` contient une liste, au format binaire, des certificats d'utilisateur révoqués. L'attribut `authorityRevocationList;binary` contient une liste binaire des certificats de l'autorité de certification qui ont été révoqués. Pour une utilisation avec WebSphere MQ SSL, les données binaires de ces attributs doivent être conformes au format DER (règles de codage définies). Pour plus d'informations sur les fichiers LDIF, reportez-vous à la documentation fournie avec votre serveur LDAP.

La Figure 12, à la page 162 illustre un exemple de fichier LDIF que vous pouvez créer en entrée de votre serveur LDAP pour charger les CRL et les ARL émis par CA1, qui est une autorité de certification imaginaire avec le nom distinctif "CN=CA1, OU=Test, O=IBM, C=GB", configuré par l'organisation de test dans 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)
```

Figure 12. Exemple de fichier LDIF pour une autorité de certification. Cela peut varier d'une implémentation à l'autre.

La Figure 13, à la page 162 montre la structure DIT créée par votre serveur LDAP lorsque vous chargez l'exemple de fichier LDIF présenté dans Figure 12, à la page 162 avec un fichier similaire pour CA2, une autorité de certification imaginaire configurée par l'organisation PKI, également dans IBM.

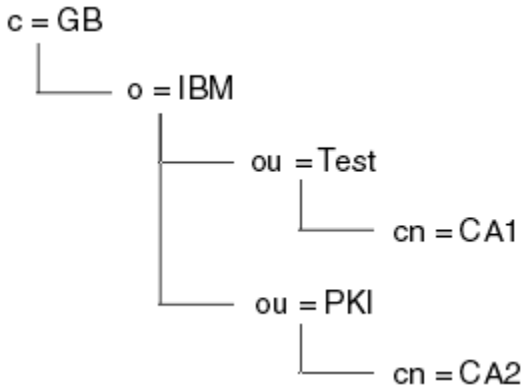


Figure 13. Exemple de structure d'arborescence d'informations d'annuaire LDAP

WebSphere MQ vérifie à la fois les CRL et les ARL.

Remarque : Assurez-vous que la liste de contrôle d'accès de votre serveur LDAP permet aux utilisateurs autorisés de lire, de rechercher et de comparer les entrées qui contiennent les CRL et les ARL. WebSphere MQ accède au serveur LDAP à l'aide des propriétés LDAPUSER et LDAPPWD de l'objet AUTHINFO.

Configuration et mise à jour des serveurs LDAP
Utilisez cette procédure pour configurer ou mettre à jour votre serveur LDAP.

1. Procurez-vous les listes de révocation de certificat et les listes de révocation de certificat au format DER auprès de votre ou de vos autorités de certification.
2. A l'aide d'un éditeur de texte ou de l'outil fourni avec votre serveur LDAP, créez un ou plusieurs fichiers LDIF contenant le nom distinctif de l'autorité de certification et les définitions de classe d'objets requises. Copiez les données au format DER dans le fichier LDIF en tant que valeurs de l'attribut `certificateRevocationList;binary` pour les CRL, de l'attribut `authorityRevocationList;binary` pour les ARL, ou les deux.
3. Démarrez votre serveur LDAP.
4. Ajoutez les entrées du ou des fichiers LDIF que vous avez créés à l'étape «2», à la page 162.

Après avoir configuré votre serveur CRL LDAP, vérifiez qu'il est correctement configuré. Tout d'abord, essayez d'utiliser un certificat qui n'est pas révoqué sur le canal et vérifiez que le canal démarre correctement. Utilisez ensuite un certificat révoqué et vérifiez que le canal ne démarre pas.

Obtenir fréquemment des listes de révocation de certificats mises à jour auprès des autorités de certification. Envisagez de le faire sur vos serveurs LDAP toutes les 12 heures.

Accès aux CRL et aux ARL à l'aide d'un gestionnaire de files d'attente

Un gestionnaire de files d'attente est associé à un ou plusieurs objets d'informations d'authentification, qui contiennent l'adresse d'un serveur CRL LDAP.

Notez que dans cette section, les informations sur les listes de révocation de certificat (CRL) s'appliquent également aux listes de révocation d'autorité (ARL).

Vous indiquez au gestionnaire de files d'attente comment accéder aux listes de révocation de certificat en lui fournissant des objets d'informations d'authentification, chacun contenant l'adresse d'un serveur de listes de révocation de certificat LDAP. Les objets d'informations d'authentification sont conservés dans une liste de noms, qui est spécifiée dans l'attribut de gestionnaire de files d'attente *SSLCRLNamelist* .

Dans l'exemple suivant, MQSC est utilisé pour spécifier les paramètres:

1. Définissez les objets d'informations d'authentification à l'aide de la commande DEFINE AUTHINFO MQSC, avec le paramètre AUTHTYPE défini sur CRLLDAP.

   La valeur CRLLDAP pour le paramètre AUTHTYPE indique que les CRL sont accessibles sur les serveurs LDAP. Chaque objet d'informations d'authentification de type CRLLDAP que vous créez contient l'adresse d'un serveur LDAP. Lorsque vous disposez de plusieurs objets d'informations d'authentification, les serveurs LDAP vers lesquels ils pointent *doivent* contenir des informations identiques. Cela assure la continuité du service en cas d'échec d'un ou de plusieurs serveurs LDAP.

   Sur toutes les plateformes, l'ID utilisateur et le mot de passe sont envoyés au serveur LDAP en clair.
2. A l'aide de la commande DEFINE NAMELIST MQSC, définissez une liste de noms pour les noms de vos objets d'informations d'authentification.
3. A l'aide de la commande ALTER QMGR MQSC, fournissez la liste de noms au gestionnaire de files d'attente. Exemple :

   ```
   ALTER QMGR SSLCRLNL(sslcrlnlname)
   ```

   où `sslcrlnlname` est votre liste de noms d'objets d'informations d'authentification.

   Cette commande définit un attribut de gestionnaire de files d'attente appelé *SSLCRLNamelist*. La valeur initiale du gestionnaire de files d'attente pour cet attribut est vide.

Vous pouvez ajouter jusqu'à 10 connexions à des serveurs LDAP de remplacement à la liste de noms afin d'assurer la continuité du service en cas d'échec d'un ou de plusieurs serveurs LDAP. Notez que les serveurs LDAP *doivent* contenir des informations identiques.

Accès aux CRL et aux ARL à l'aide de IBM WebSphere MQ Explorer

Vous pouvez utiliser IBM WebSphere MQ Explorer pour indiquer à un gestionnaire de files d'attente comment accéder aux listes de révocation de certificat.

Notez que dans cette section, les informations sur les listes de révocation de certificat (CRL) s'appliquent également aux listes de révocation d'autorité (ARL).

Utilisez la procédure suivante pour configurer une connexion LDAP à une CRL:

1. Vérifiez que vous avez démarré votre gestionnaire de files d'attente.
2. Cliquez avec le bouton droit de la souris sur le dossier **Informations d'authentification** , puis cliquez sur **Nouveau-> Informations d'authentification**. Dans la feuille de propriétés qui s'ouvre:

   a. Sur la première page **Créer des informations d'authentification** , entrez un nom pour l'objet CRL (LDAP).

b. Dans la page **Général** de **Modifier les propriétés**, sélectionnez le type de connexion. Vous pouvez éventuellement entrer une description.

c. Sélectionnez la page **CRL (LDAP)** de **Modifier les propriétés**.

d. Entrez le nom du serveur LDAP en tant que nom de réseau ou adresse IP.

e. Si le serveur requiert des détails de connexion, indiquez un ID utilisateur et, si nécessaire, un mot de passe.

f. Cliquez sur **OK**.

3. Cliquez avec le bouton droit de la souris sur le dossier **Listes de noms** , puis cliquez sur **Nouveau-> Liste de noms** . Dans la feuille de propriétés qui s'ouvre:

   a. Entrez un nom pour la liste de noms.

   b. Ajoutez le nom de l'objet CRL (LDAP) (à l'étape «2.a», à la page 163) à la liste.

   c. Cliquez sur **OK**.

4. Cliquez avec le bouton droit de la souris sur le gestionnaire de files d'attente, sélectionnez **Propriétés**, puis sélectionnez la page **SSL** :

   a. Cochez la case **Vérifier les certificats reçus par ce gestionnaire de files d'attente par rapport aux listes de révocation de certification** .

   b. Entrez le nom de la liste de noms (à l'étape «3.a», à la page 164) dans la zone **Liste de noms CRL** .

Accès aux CRL et aux ARL à l'aide d'un client IBM WebSphere MQ MQI

Vous disposez de trois options pour spécifier les serveurs LDAP qui contiennent des listes de révocation de certificat à vérifier par un client IBM WebSphere MQ MQI.

Notez que dans cette section, les informations sur les listes de révocation de certificat (CRL) s'appliquent également aux listes de révocation d'autorité (ARL).

Les trois méthodes de spécification des serveurs LDAP sont les suivantes:

- Utilisation d'une table de définition de canal
- Utilisation de la structure des options de configuration SSL, MQSCO, sur un appel MQCONNX
- Utilisation d' Active Directory (sur les systèmes Windows avec prise en charge d' Active Directory)

Pour plus de détails, reportez-vous aux informations associées.

Vous pouvez inclure jusqu'à 10 connexions à d'autres serveurs LDAP pour assurer la continuité du service en cas d'échec d'un ou de plusieurs serveurs LDAP. Notez que les serveurs LDAP *doivent* contenir des informations identiques.

Vous ne pouvez pas accéder aux CRL LDAP à partir d'un canal client WebSphere MQ MQI s'exécutant sur Linux (plateforme zSeries).

Emplacement d'un répondeur OCSP et des serveurs LDAP qui contiennent des listes CRL
Sur un système client IBM WebSphere MQ MQI, vous pouvez spécifier l'emplacement d'un répondeur OCSP et des serveurs LDAP (Lightweight Directory Access Protocol) qui contiennent des listes de révocation de certificats (CRL).

Vous pouvez spécifier ces emplacements de trois manières, répertoriées ici par ordre de priorité décroissante.

Lorsqu'une application client MQI WebSphere MQ émet un appel MQCONNX

Vous pouvez spécifier un répondeur OCSP ou un serveur LDAP contenant des CRL sur un appel **MQCONNX** .

Sur un appel **MQCONNX** , la structure d'options de connexion, MQCNO, peut faire référence à une structure d'options de configuration SSL, MQSCO. A son tour, la structure MQSCO peut référencer une ou plusieurs structures d'enregistrement d'informations d'authentification, MQAIR. Chaque structure MQAIR contient toutes les informations dont un client WebSphere MQ MQI a besoin pour accéder à un répondeur OCSP ou à un serveur LDAP contenant des CRL. Par exemple, l'une des zones d'une structure MQAIR est

l'URL à laquelle un répondeur peut être contacté. Pour plus d'informations sur la structure MQAIR, voir MQAIR-Enregistrement des informations d'authentification.

Utilisation d'une table de définition de canal du client (ccdt) pour accéder à un répondeur OCSP ou à des serveurs LDAP

Pour qu'un client WebSphere MQ MQI puisse accéder à un répondeur OCSP ou à des serveurs LDAP qui contiennent des CRL, incluez les attributs d'un ou de plusieurs objets d'informations d'authentification dans une table de définition de canal du client.

Sur un gestionnaire de files d'attente de serveur, vous pouvez définir un ou plusieurs objets d'informations d'authentification. Les attributs d'un objet d'authentification contiennent toutes les informations requises pour accéder à un répondeur OCSP (sur les plateformes où OCSP est pris en charge) ou à un serveur LDAP qui contient des CRL. L'un des attributs spécifie l'URL du répondeur OCSP, l'autre l'adresse de l'hôte ou l'adresse IP d'un système sur lequel s'exécute un serveur LDAP.

Un objet d'informations d'authentification avec AUTHTYPE (OCSP) ne s'applique pas aux gestionnaires de files d'attente IBM i ou z/OS , mais il peut être spécifié sur ces plateformes pour être copié dans la table de définition de canal du client (CCDT) à des fins d'utilisation par le client.

Pour permettre à un client WebSphere MQ MQI d'accéder à un répondeur OCSP ou à des serveurs LDAP qui contiennent des CRL, les attributs d'un ou de plusieurs objets d'informations d'authentification peuvent être inclus dans une table de définition de canal du client. Vous pouvez inclure ces attributs de l'une des manières suivantes:

Sur les plateformes serveur AIX, HP-UX, Linux, Solaris et Windows

Vous pouvez définir une liste de noms contenant les noms d'un ou de plusieurs objets d'informations d'authentification. Vous pouvez ensuite définir l'attribut de gestionnaire de files d'attente, **SSLCRLNameList**, sur le nom de cette liste de noms.

Si vous utilisez des listes de révocation de certificat, plusieurs serveurs LDAP peuvent être configurés pour fournir une disponibilité plus élevée. L'objectif est que chaque serveur LDAP dispose des mêmes CRL. Si un serveur LDAP n'est pas disponible lorsqu'il est requis, un client WebSphere MQ MQI peut tenter d'accéder à un autre serveur.

Les attributs des objets d'informations d'authentification identifiés par la liste de noms sont appelés collectivement ici *emplacement de révocation de certificat*. Lorsque vous définissez l'attribut de gestionnaire de files d'attente, **SSLCRLNameList**, sur le nom de la liste de noms, l'emplacement de révocation de certificat est copié dans la table de définition de canal du client associée au gestionnaire de files d'attente. Si la table de définition de canal du client est accessible à partir d'un système client en tant que fichier partagé, ou si la table de définition de canal du client est ensuite copiée sur un système client, le client WebSphere MQ MQI sur ce système peut utiliser l'emplacement de révocation de certificat dans la table de définition de canal du client pour accéder à un répondeur OCSP ou à des serveurs LDAP contenant des listes de révocation de certificat.

Si l'emplacement de révocation de certificat du gestionnaire de files d'attente est modifié ultérieurement, la modification est reflétée dans la table de définition de canal du client associée au gestionnaire de files d'attente. Si l'attribut de gestionnaire de files d'attente, **SSLCRLNameList**, est mis à blanc, l'emplacement de révocation de certificat est supprimé de la table de définition de canal du client. Ces modifications ne sont reflétées dans aucune copie de la table sur un système client.

Si vous souhaitez que l'emplacement de révocation de certificat aux extrémités client et serveur d'un canal MQI soit différent et que le gestionnaire de files d'attente du serveur est celui qui est utilisé pour créer l'emplacement de révocation de certificat, procédez comme suit:

1. Sur le gestionnaire de files d'attente du serveur, créez l'emplacement de révocation de certificat à utiliser sur le système client.
2. Copiez la table de définition de canal du client contenant l'emplacement de révocation de certificat sur le système client.

3. Sur le gestionnaire de files d'attente du serveur, remplacez l'emplacement de révocation de certificat par l'emplacement requis à l'extrémité serveur du canal MQI.

Utilisation d' Active Directory sous Windows

Sur les systèmes Windows , vous pouvez utiliser la commande de contrôle **setmqcrl** pour publier les informations CRL en cours dans Active Directory.

La commande **setmqcrl** ne publie pas les informations OCSP.

Pour plus d'informations sur cette commande et sa syntaxe, voir setmqcrl.

Accès aux CRL et aux ARL avec des classes IBM WebSphere MQ pour Java et des classes IBM WebSphere MQ pour JMS

Les classes IBM WebSphere MQ pour Java et les classes IBM WebSphere MQ pour JMS accèdent aux listes de révocation de certificat différemment des autres plateformes.

Pour plus d'informations sur l'utilisation des CRL et des ARL avec IBM WebSphere MQ classes for Java, voir Utilisation des listes de révocation de certificats.

Pour plus d'informations sur l'utilisation des CRL et des ARL avec IBM WebSphere MQ classes for JMS, voir Propriété d'objet SSLCERTSTORES.

Manipulation des objets d'informations d'authentification

Vous pouvez manipuler des objets d'informations d'authentification à l'aide de commandes MQSC ou PCF ou du IBM WebSphere MQ Explorer.

Les commandes MQSC suivantes agissent sur les objets d'informations d'authentification:

- DEFINE AUTHINFO
- ALTER AUTHINFO
- DELETE AUTHINFO
- INFORMATIONS D'AUTHENTIFICATION D'AFFICHAGE

Pour une description complète de ces commandes, voir Commandes Script (MQSC) .

Les commandes PCF (Programmable Command Format) suivantes agissent sur les objets d'informations d'authentification:

- Créer des informations d'authentification
- Copier des informations d'authentification
- Modifier des informations d'authentification
- Supprimer des informations d'authentification
- Consulter des informations d'authentification
- Consulter des noms d'informations d'authentification

Pour une description complète de ces commandes, voir Définitions des formats de commande programmables .

Sur les plateformes où il est disponible, vous pouvez également utiliser WebSphere MQ Explorer.

Autorisation de l'accès aux objets

Cette section contient des informations sur l'utilisation du gestionnaire de droits d'accès aux objets et des programmes d'exit de canal pour contrôler l'accès aux objets.

Sur les systèmes UNIX, Linux, and Windows . vous contrôlez l'accès aux objets à l'aide du gestionnaire des droits d'accès aux objets (OAM). Cette collection de rubriques contient des informations sur l'utilisation de l'interface de commande de la méthode d'accès aux objets (OAM). Il contient également une liste de contrôle que vous pouvez utiliser pour déterminer les tâches à effectuer pour appliquer la

sécurité à votre système, ainsi que les considérations à prendre en compte pour accorder aux utilisateurs le droit d'administrer IBM WebSphere MQ et d'utiliser des objets IBM WebSphere MQ . Si les mécanismes de sécurité fournis ne répondent pas à vos besoins, vous pouvez développer vos propres programmes d'exit de canal.

Contrôle de l'accès aux objets à l'aide de la méthode d'accès aux objets (OAM) sur les systèmes UNIX, Linux et Windows

Le gestionnaire des droits d'accès aux objets (OAM) fournit une interface de commande pour l'octroi et la révocation des droits d'accès aux objets WebSphere MQ .

Vous devez disposer des droits appropriés pour utiliser ces commandes, comme décrit dans «Droits d'administration de IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows», à la page 206. Les ID utilisateur autorisés à administrer WebSphere MQ disposent des droits *superutilisateur* sur le gestionnaire de files d'attente, ce qui signifie que vous n'avez pas besoin de leur accorder des droits supplémentaires pour émettre des demandes ou des commandes MQI.

Octroi de l'accès à un objet IBM WebSphere MQ sur des systèmes UNIX, Linux, and Windows

Utilisez la commande de contrôle **setmqaut** ou la commande PCF **MQCMD_SET_AUTH_REC** pour accorder aux utilisateurs et aux groupes d'utilisateurs l'accès aux objets IBM WebSphere MQ .

Pour une définition complète de la commande de contrôle **setmqaut** et de sa syntaxe, voir setmqaut, et pour une définition complète de la commande PCF **MQCMD_SET_AUTH_REC** et de sa syntaxe, voir Set Authority Record.

Le gestionnaire de files d'attente doit être en cours d'exécution pour pouvoir utiliser cette commande. Lorsque vous avez modifié l'accès à un principal, les modifications sont reflétées immédiatement par la méthode d'accès aux objets (OAM).

Pour accorder aux utilisateurs l'accès à un objet, vous devez spécifier:

- Nom du gestionnaire de files d'attente qui possède les objets que vous utilisez ; si vous ne spécifiez pas le nom d'un gestionnaire de files d'attente, le gestionnaire de files d'attente par défaut est utilisé.
- Nom et type de l'objet (pour identifier l'objet de manière unique). Vous spécifiez le nom en tant que *profil*; il s'agit soit du nom explicite de l'objet, soit d'un nom générique, y compris les caractères génériques. Pour une description détaillée des profils génériques et de l'utilisation des caractères génériques qu'ils contiennent, voir «Utilisation des profils génériques OAM sur les systèmes UNIX, Linux, and Windows», à la page 168.
- Un ou plusieurs principaux et noms de groupe auxquels les droits s'appliquent.

  Si un ID utilisateur contient des espaces, placez-le entre guillemets lorsque vous utilisez cette commande. Sur les systèmes Windows , vous pouvez qualifier un ID utilisateur avec un nom de domaine. Si l'ID utilisateur réel contient un symbole arobase (@), remplacez-le par @ @ pour indiquer qu'il fait partie de l'ID utilisateur et non du délimiteur entre l'ID utilisateur et le nom de domaine.
- Liste des autorisations. Chaque élément de la liste indique un type d'accès qui doit être accordé à cet objet (ou révoqué). Chaque autorisation de la liste est indiquée en tant que mot clé, précédé d'un signe plus (+) ou d'un signe moins (-). Utilisez un signe plus pour ajouter l'autorisation spécifiée et un signe moins pour supprimer l'autorisation. Il ne doit pas y avoir d'espaces entre le signe + ou-et le mot clé.

  Vous pouvez spécifier n'importe quel nombre d'autorisations dans une seule commande. Par exemple, la liste des autorisations permettant à un utilisateur ou à un groupe de placer des messages dans une file d'attente et de les parcourir, mais de révoquer l'accès pour obtenir des messages est la suivante:

```
+browse -get +put
```

Exemples d'utilisation de la commande setmqaut

Les exemples suivants montrent comment utiliser la commande `setmqaut` pour accorder et révoquer des droits d'utilisation d'un objet:

```
setmqaut -m saturn.queue.manager -t queue -n RED.LOCAL.QUEUE
         -g groupa +browse -get +put
```

Dans cet exemple :

- `saturn.queue.manager` est le nom du gestionnaire de files d'attente
- `queue` est le type d'objet
- `RED.LOCAL.QUEUE` est le nom de l'objet
- `groupa` est l'identificateur du groupe avec les autorisations à modifier
- `+browse -get +put` est la liste d'autorisation pour la file d'attente spécifiée
  - `+browse` ajoute l'autorisation de parcourir les messages dans la file d'attente (pour émettre **MQGET** avec l'option de navigation)
  - `-get` supprime l'autorisation d'obtenir (**MQGET**) des messages de la file d'attente
  - `+put` ajoute l'autorisation d'insertion de messages (**MQPUT**) dans la file d'attente

La commande suivante révoque le droit d'insertion sur la file d'attente MyQueue du principal fvuser et des groupes groupa et groupb. Sur les systèmes UNIX and Linux , cette commande révoque également l'autorisation d'insertion pour tous les principaux du même groupe principal que fvuser.

```
setmqaut -m saturn.queue.manager -t queue -n MyQueue -p fvuser
         -g groupa -g groupb -put
```

Utilisation de la commande avec un service d'autorisation différent

Si vous utilisez votre propre service d'autorisation à la place de la méthode d'accès aux objets (OAM), vous pouvez spécifier le nom de ce service dans la commande **setmqaut** pour diriger la commande vers ce service. Vous devez spécifier ce paramètre si plusieurs composants installables sont en cours d'exécution en même temps ; si ce n'est pas le cas, la mise à jour est effectuée sur le premier composant installable pour le service d'autorisation. Par défaut, il s'agit de la méthode d'accès aux objets (OAM) fournie.

Utilisation des profils génériques OAM sur les systèmes UNIX, Linux, and Windows

Les profils génériques OAM vous permettent de définir les droits d'accès d'un utilisateur à de nombreux objets à la fois, au lieu d'avoir à émettre des commandes **setmqaut** distinctes pour chaque objet individuel lors de sa création.

L'utilisation de profils génériques dans la commande **setmqaut** vous permet de définir des droits génériques pour tous les objets qui correspondent à ce profil.

Cette collection de rubriques décrit plus en détail l'utilisation des profils génériques.

Utilisation de caractères génériques dans les profils OAM

Ce qui rend un profil générique, c'est l'utilisation de caractères spéciaux (caractères génériques) dans le nom du profil. Par exemple, le caractère générique point d'interrogation (?) correspond à n'importe quel caractère unique dans un nom. Par conséquent, si vous spécifiez `ABC.?EF`, l'autorisation que vous accordez à ce profil s'applique à tous les objets portant les noms `ABC.DEF` , `ABC.CEF`, `ABC.BEF`, etc.

Les caractères génériques disponibles sont les suivants:

?

Utilisez le point d'interrogation (?) au lieu de n'importe quel caractère. Par exemple, `AB.?D` s'applique aux objets `AB.CD` , `AB.EDet AB.FD`.

*****

Utilisez l'astérisque (*) comme suit:

- Un *qualificateur* dans un nom de profil pour correspondre à un qualificateur dans un nom d'objet. Le qualificatif est une partie de nom d'objet délimitée par un point. Par exemple, dans `ABC.DEF.GHI`, les qualificateurs sont `ABC`, `DEFet GHI` .

  Par exemple, `ABC.*.JKL` s'applique aux objets `ABC.DEF.JKLet ABC.GHI.JKL`. (Notez qu'il ne s'applique **pas** à `ABC.JKL`; * utilisé dans ce contexte indique toujours un qualificateur.)
- Caractère dans un qualificatif d'un nom de profil qui doit correspondre à zéro ou plusieurs caractères dans le qualificatif d'un nom d'objet.

  Par exemple, `ABC.DE*.JKL` s'applique aux objets `ABC.DE.JKL`, `ABC.DEF.JKLet ABC.DEGH.JKL` .

******

Utilisez le double astérisque (**) **une fois** dans un nom de profil comme suit:

- Nom de profil complet correspondant à tous les noms d'objet. Par exemple, si vous utilisez `-t prcs` pour identifier les processus, puis utilisez ** comme nom de profil, vous modifiez les autorisations pour tous les processus.
- Comme qualificatif de début, de milieu ou de fin dans un nom de profil pour correspondre à zéro ou plusieurs qualificatifs dans un nom d'objet. Par exemple, `**.ABC` identifie tous les objets avec le qualificateur final ABC.

Remarque : Lorsque vous utilisez des caractères génériques sur des systèmes UNIX and Linux , vous **devez** placer le nom de profil entre apostrophes.

Priorités de profil

Un point important à comprendre lors de l'utilisation de profils génériques est la priorité donnée aux profils lors de la détermination des droits à appliquer à un objet en cours de création. Par exemple, supposons que vous ayez émis les commandes suivantes:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

Le premier accorde le droit d'insertion à toutes les files d'attente pour le principal fred dont les noms correspondent au profil AB. * ; La seconde permet d'obtenir des droits sur les mêmes types de file d'attente qui correspondent au profil AB.C*.

Supposons que vous créiez maintenant une file d'attente appelée AB.CD. Selon les règles de correspondance des caractères génériques, setmqaut peut s'appliquer à cette file d'attente. Alors, a-t-elle mis ou obtenu l'autorité?

Pour trouver la réponse, vous appliquez la règle selon laquelle, chaque fois que plusieurs profils peuvent s'appliquer à un objet, **seuls les plus spécifiques s'appliquent**. La façon dont vous appliquez cette règle consiste à comparer les noms de profil de gauche à droite. Lorsqu'ils diffèrent, un caractère non générique est plus spécifique qu'un caractère générique. Ainsi, dans l'exemple ci-dessus, la file d'attente AB.CD dispose du droit **get** (AB.C* est plus spécifique que AB. *).

Lorsque vous comparez des caractères génériques, l'ordre de la *spécificité* est le suivant:

1. ?
2. *
3. **

Vidage des paramètres de profil

Pour une définition complète de la commande de contrôle **dmpmqaut** et de sa syntaxe, voir dmpmqaut, et pour une définition complète de la commande PCF **MQCMD_INQUIRE_AUTH_RECS** et de sa syntaxe, voir Inquire Authority Records .

Les exemples suivants illustrent l'utilisation de la commande de contrôle **dmpmqaut** pour vider des enregistrements de droits d'accès pour des profils génériques:

1. Cet exemple vide tous les enregistrements de droits d'accès dont le profil correspond à la file d'attente a.b.c pour le principal user1.

   ```
   dmpmqaut -m qm1 -n a.b.c -t q -p user1
   ```

   Le vidage résultant se présente comme suit:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```

   Remarque : Bien que les utilisateurs UNIX and Linux puissent utiliser l'option `-p` pour la commande **dmpmqaut** , ils doivent utiliser `-g groupname` à la place lors de la définition des autorisations.
2. Cet exemple vide tous les enregistrements de droits d'accès dont le profil correspond à la file d'attente a.b.c.

   ```
   dmpmqaut -m qmgr1 -n a.b.c -t q
   ```

   Le vidage résultant se présente comme suit:

   ```
   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. Cet exemple vide tous les enregistrements de droits d'accès pour le profil a.b. *, de type file d'attente.

   ```
   dmpmqaut -m qmgr1 -n a.b.* -t q
   ```

   Le vidage résultant se présente comme suit:

   ```
   profile:     a.b.*
   object type: queue
   entity:      user1
   type:        principal
   authority:   get, browse, put, inq
   ```
4. Cet exemple vide tous les enregistrements de droits d'accès pour le gestionnaire de files d'attente qmX.

   ```
   dmpmqaut -m qmX
   ```

Le vidage résultant se présente comme suit:

```
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. Cet exemple vide tous les noms de profil et tous les types d'objet pour le gestionnaire de files d'attente qmX.

```
dmpmqaut -m qmX -l
```

Le vidage résultant se présente comme suit:

```
profile: q1, type: queue
profile: q*, type: queue
profile: name.*, type: namelist
profile: pr1, type: process
```

Remarque : Pour WebSphere MQ for Windows uniquement, tous les principaux affichés incluent des informations de domaine, par exemple:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

Utilisation de caractères génériques dans les profils OAM

Utilisez des caractères génériques dans un nom de profil de gestionnaire des droits d'accès aux objets (OAM) pour rendre ce profil applicable à plusieurs objets.

Ce qui rend un profil générique, c'est l'utilisation de caractères spéciaux (caractères génériques) dans le nom du profil. Par exemple, le caractère générique point d'interrogation (?) correspond à n'importe quel caractère unique dans un nom. Par conséquent, si vous spécifiez `ABC.?EF`, l'autorisation que vous accordez à ce profil s'applique à tous les objets portant les noms `ABC.DEF`, `ABC.CEF`, `ABC.BEF`, etc.

Les caractères génériques disponibles sont les suivants:

?

Utilisez le point d'interrogation (?) au lieu de n'importe quel caractère. Par exemple, `AB.?D` s'applique aux objets `AB.CD`, `AB.EDet AB.FD`.

*****

Utilisez l'astérisque (*) comme suit:

- Un *qualificateur* dans un nom de profil pour correspondre à un qualificateur dans un nom d'objet. Le qualificatif est une partie de nom d'objet délimitée par un point. Par exemple, dans `ABC.DEF.GHI`, les qualificatifs sont `ABC`, `DEF` et `GHI`.

Par exemple, ABC.*.JKL s'applique aux objets ABC.DEF.JKLet ABC.GHI.JKL. (Notez qu'il ne s'applique **pas** à ABC.JKL; * utilisé dans ce contexte indique toujours un qualificateur.)

- Caractère dans un qualificatif d'un nom de profil qui doit correspondre à zéro ou plusieurs caractères dans le qualificatif d'un nom d'objet.

  Par exemple, ABC.DE*.JKL s'applique aux objets ABC.DE.JKL, ABC.DEF.JKLet ABC.DEGH.JKL.

**

Utilisez le double astérisque (**) **une fois** dans un nom de profil comme suit:

- Nom de profil complet correspondant à tous les noms d'objet. Par exemple, si vous utilisez `-t prcs` pour identifier les processus, puis utilisez ** comme nom de profil, vous modifiez les autorisations pour tous les processus.
- Comme qualificatif de début, de milieu ou de fin dans un nom de profil pour correspondre à zéro ou plusieurs qualificatifs dans un nom d'objet. Par exemple, **.ABC identifie tous les objets avec le qualificateur final ABC.

Remarque : Lorsque vous utilisez des caractères génériques sur des systèmes UNIX and Linux , vous **devez** placer le nom de profil entre apostrophes.

Priorités de profil

Plusieurs profils génériques peuvent s'appliquer à un seul objet. Lorsque c'est le cas, la règle la plus spécifique s'applique.

Un point important à comprendre lors de l'utilisation de profils génériques est la priorité donnée aux profils lors de la détermination des droits à appliquer à un objet en cours de création. Par exemple, supposons que vous ayez émis les commandes suivantes:

```
setmqaut -n AB.* -t q +put -p fred
setmqaut -n AB.C* -t q +get -p fred
```

Le premier accorde le droit d'insertion à toutes les files d'attente pour le principal fred dont les noms correspondent au profil AB. * ; La seconde permet d'obtenir des droits sur les mêmes types de file d'attente qui correspondent au profil AB.C*.

Supposons que vous créiez maintenant une file d'attente appelée AB.CD. Selon les règles de correspondance des caractères génériques, setmqaut peut s'appliquer à cette file d'attente. Alors, a-t-elle mis ou obtenu l'autorité?

Pour trouver la réponse, vous appliquez la règle selon laquelle, chaque fois que plusieurs profils peuvent s'appliquer à un objet, **seuls les plus spécifiques s'appliquent**. La façon dont vous appliquez cette règle consiste à comparer les noms de profil de gauche à droite. Lorsqu'ils diffèrent, un caractère non générique est plus spécifique qu'un caractère générique. Ainsi, dans l'exemple ci-dessus, la file d'attente AB.CD dispose du droit **get** (AB.C* est plus spécifique que AB. *).

Lorsque vous comparez des caractères génériques, l'ordre de la *spécificité* est le suivant:

1. ?
2. *
3. **

Vidage des paramètres de profil

Utilisez la commande de contrôle **dmpmqaut** ou la commande PCF **MQCMD_INQUIRE_AUTH_RECS** pour vider les autorisations en cours associées à un profil spécifié.

Pour une définition complète de la commande de contrôle **dmpmqaut** et de sa syntaxe, voir dmpmqaut, et pour une définition complète de la commande PCF **MQCMD_INQUIRE_AUTH_RECS** et de sa syntaxe, voir Inquire Authority Records.

Les exemples suivants illustrent l'utilisation de la commande de contrôle **dmpmqaut** pour vider des enregistrements de droits d'accès pour des profils génériques:

1. Cet exemple vide tous les enregistrements de droits d'accès dont le profil correspond à la file d'attente a.b.c pour le principal user1.

```
dmpmqaut -m qm1 -n a.b.c -t q -p user1
```

Le vidage résultant ressemble à l'exemple suivant:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

Remarque : Les utilisateurs UNIX and Linux ne peuvent pas utiliser l'option `-p` ; ils doivent utiliser `-g groupname` à la place.

2. Cet exemple vide tous les enregistrements de droits d'accès dont le profil correspond à la file d'attente a.b.c.

```
dmpmqaut -m qmgr1 -n a.b.c -t q
```

Le vidage résultant ressemble à l'exemple suivant:

```
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. Cet exemple vide tous les enregistrements de droits d'accès pour le profil a.b. *, de type file d'attente.

```
dmpmqaut -m qmgr1 -n a.b.* -t q
```

Le vidage résultant ressemble à l'exemple suivant:

```
profile:     a.b.*
object type: queue
entity:      user1
type:        principal
authority:   get, browse, put, inq
```

4. Cet exemple vide tous les enregistrements de droits d'accès pour le gestionnaire de files d'attente qmX.

```
dmpmqaut -m qmX
```

Le vidage résultant ressemble à l'exemple suivant:

```
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. Cet exemple vide tous les noms de profil et tous les types d'objet pour le gestionnaire de files d'attente qmX.

   ```
   dmpmqaut -m qmX -l
   ```

   Le vidage résultant ressemble à l'exemple suivant:

   ```
   profile: q1, type: queue
   profile: q*, type: queue
   profile: name.*, type: namelist
   profile: pr1, type: process
   ```

Remarque : Pour WebSphere MQ for Windows uniquement, tous les principaux affichés incluent des informations de domaine, par exemple:

```
profile:     a.b.*
object type: queue
entity:      user1@domain1
type:        principal
authority:   get, browse, put, inq
```

Affichage des paramètres d'accès

Utilisez la commande de contrôle **dspmqaut** ou la commande PCF **MQCMD_INQUIRE_ENTITY_AUTH** pour afficher les autorisations d'un principal ou d'un groupe spécifique pour un objet particulier.

Le gestionnaire de files d'attente doit être en cours d'exécution pour pouvoir utiliser cette commande. Lorsque vous modifiez l'accès à un principal, les modifications sont répercutées immédiatement par la méthode d'accès aux objets (OAM). L'autorisation ne peut être affichée que pour un seul groupe ou principal à la fois. Pour une définition complète de la commande de contrôle **dmpmqaut** et de sa syntaxe, voir dmpmqaut, et pour une définition complète de la commande PCF **MQCMD_INQUIRE_ENTITY_AUTH** et de sa syntaxe, voir Inquire Entity Authority.

L'exemple suivant illustre l'utilisation de la commande de contrôle **dspmqaut** pour afficher les autorisations dont dispose le groupe `GpAdmin` pour une définition de processus nommée `Annuities` qui se trouve sur le gestionnaire de files d'attente `QueueMan1`.

```
dspmqaut -m QueueMan1 -t process -n Annuities -g GpAdmin
```

Modification et révocation de l'accès à un objet IBM WebSphere MQ

Pour modifier le niveau d'accès d'un utilisateur ou d'un groupe à un objet, utilisez la commande **setmqaut** . Pour révoquer l'accès d'un utilisateur particulier qui est membre d'un groupe autorisé, supprimez l'utilisateur du groupe.

Le processus de suppression de l'utilisateur d'un groupe est décrit dans:

- «Création et gestion de groupes sous Windows», à la page 86
- «Création et gestion de groupes sous HP-UX», à la page 89
- «Création et gestion de groupes sous AIX», à la page 90
- «Création et gestion de groupes sous Solaris», à la page 91
- «Création et gestion de groupes sur Linux», à la page 92

.

L'ID utilisateur qui crée un objet IBM WebSphere MQ dispose de droits de contrôle complets sur cet objet. Si vous supprimez cet ID utilisateur du groupe mqm local (ou du groupe Administrateurs sur les systèmes Windows), ces droits ne sont pas révoqués. Utilisez la commande de contrôle **setmqaut** ou la commande PCF **MQCMD_DELETE_AUTH_REC** pour révoquer l'accès à un objet pour l'ID utilisateur qui l'a créé, après l'avoir supprimé du groupe mqm ou Administrateurs. Pour une définition complète de la commande de contrôle setmqaut et de sa syntaxe, voir setmqaut, et pour une définition complète de la commande PCF **MQCMD_INQUIRE_ENTITY_AUTH** et de sa syntaxe, voir Inquire Entity Authority.

Sous Windows, supprimez les entrées OAM correspondant à un compte utilisateur Windows particulier avant de supprimer le profil utilisateur. Il est impossible de supprimer les entrées OAM après la suppression du compte utilisateur.

Prévention des contrôles d'accès de sécurité sur les systèmes UNIX, Linux, and Windows

Pour désactiver toutes les vérifications de sécurité, vous pouvez désactiver la méthode d'accès aux objets (OAM). Cela peut convenir à un environnement de test. Après avoir désactivé ou supprimé la méthode d'accès aux objets (OAM), vous ne pouvez pas ajouter une méthode d'accès aux objets (OAM) à un gestionnaire de files d'attente existant.

Si vous décidez de ne pas effectuer de contrôles de sécurité (par exemple, dans un environnement de test), vous pouvez désactiver la méthode d'accès aux objets (OAM) de l'une des deux manières suivantes:

- Avant de créer un gestionnaire de files d'attente, définissez la variable d'environnement du système d'exploitation MQSNOAUT (dans ce cas, vous ne pouvez pas ajouter de gestionnaire de files d'attente ultérieurement):

  Pour plus d'informations sur les implications de la définition de la variable MQSNOAUT, voir Variables d'environnement .
- Editez le fichier de configuration du gestionnaire de files d'attente pour supprimer le service. (Si vous effectuez cette opération, vous ne pourrez pas ajouter de méthode d'accès aux objets ultérieurement.)

Si vous utilisez setmqaut ou dspmqaut alors que la méthode d'accès aux objets (OAM) est désactivée, notez les points suivants:

- La méthode d'accès aux objets (OAM) ne valide pas le principal ou le groupe spécifié, ce qui signifie que la commande peut accepter des valeurs non valides.
- La méthode d'accès aux objets (OAM) n'effectue pas de contrôles de sécurité et indique que tous les principaux et groupes sont autorisés à effectuer toutes les opérations d'objet applicables.

Avertissement : Lorsqu'une méthode d'accès aux objets (OAM) est supprimée, elle ne peut pas être remise sur un gestionnaire de files d'attente existant. Cela est dû au fait que la méthode d'accès aux objets (OAM) doit être en place au moment de la création de l'objet. Pour utiliser à nouveau le gestionnaire de files d'attente WebSphere MQ après sa suppression, vous devez régénérer le gestionnaire de files d'attente.

Concepts associés

Services optionnels

Octroi de l'accès requis aux ressources

Cette rubrique permet de déterminer les tâches à effectuer pour appliquer la sécurité à votre système WebSphere MQ .

Pourquoi et quand exécuter cette tâche

Au cours de cette tâche, vous décidez des actions nécessaires pour appliquer le niveau de sécurité approprié aux éléments de votre installation WebSphere MQ . Chaque tâche individuelle à qui vous vous référez fournit des instructions étape par étape pour toutes les plateformes.

Procédure

1. Avez-vous besoin de limiter l'accès à votre gestionnaire de files d'attente à certains utilisateurs?
   a) Non: ne prenez aucune autre mesure.
   b) Oui: Passez à la question suivante.
2. Ces utilisateurs ont-ils besoin d'un accès administratif partiel sur un sous-ensemble de ressources de gestionnaire de files d'attente?
   a) Non: Passez à la question suivante.
   b) Oui: voir «Octroi d'un accès administrateur partiel sur un sous-ensemble de ressources de gestionnaire de files d'attente», à la page 176.
3. Ces utilisateurs ont-ils besoin d'un accès administrateur complet sur un sous-ensemble de ressources de gestionnaire de files d'attente?
   a) Non: Passez à la question suivante.
   b) Oui: voir «Octroi d'un accès administrateur complet sur un sous-ensemble de ressources de gestionnaire de files d'attente», à la page 181.
4. Ces utilisateurs ont-ils besoin d'un accès en lecture seule à toutes les ressources du gestionnaire de files d'attente?
   a) Non: Passez à la question suivante.
   b) Oui: voir «Octroi d'un accès en lecture seule à toutes les ressources d'un gestionnaire de files d'attente», à la page 186.
5. Ces utilisateurs ont-ils besoin d'un accès administrateur complet sur toutes les ressources du gestionnaire de files d'attente?
   a) Non: Passez à la question suivante.
   b) Oui: voir «Octroi d'un accès administrateur complet à toutes les ressources d'un gestionnaire de files d'attente», à la page 187.
6. Avez-vous besoin d'applications utilisateur pour vous connecter à votre gestionnaire de files d'attente?
   a) Non: Désactiver la connectivité, comme décrit dans «Suppression de la connectivité au gestionnaire de files d'attente», à la page 188
   b) Oui: voir «Autorisation des applications utilisateur à se connecter à votre gestionnaire de files d'attente», à la page 189.

Octroi d'un accès administrateur partiel sur un sous-ensemble de ressources de gestionnaire de files d'attente

Vous devez accorder à certains utilisateurs un accès administrateur partiel à certaines ressources de gestionnaire de files d'attente, mais pas à toutes. Utilisez ce tableau pour déterminer les actions que vous devez effectuer.

Tableau 14. Octroi d'un accès administrateur partiel à un sous-ensemble de ressources de gestionnaire de files d'attente

Les utilisateurs doivent administrer les objets de ce type	**Effectuer cette action**
Files d'attente	Accordez un accès administrateur partiel aux files d'attente requises, comme décrit dans «Octroi d'un accès administrateur limité à certaines files d'attente», à la page 177
Rubriques	Accordez un accès administrateur partiel aux rubriques requises, comme décrit dans «Octroi d'un accès administrateur limité à certaines rubriques», à la page 178

Tableau 14. Octroi d'un accès administrateur partiel à un sous-ensemble de ressources de gestionnaire de files d'attente (suite)	
Les utilisateurs doivent administrer les objets de ce type	**Effectuer cette action**
Canaux	Accordez un accès administrateur partiel aux canaux requis, comme décrit dans «Octroi d'un accès administratif limité à certains canaux», à la page 178
Gestionnaire de files d'attente	Accordez un accès administrateur partiel au gestionnaire de files d'attente, comme décrit dans «Octroi d'un accès administrateur limité à un gestionnaire de files d'attente», à la page 179
Processus	Accordez un accès administratif partiel aux processus requis, comme décrit dans «Octroi d'un accès administrateur limité à certains processus», à la page 180
Listes de noms	Accordez un accès administrateur partiel aux listes de noms requises, comme décrit dans «Octroi d'un accès administrateur limité à certaines listes de noms», à la page 180
Services	Accordez un accès administrateur partiel aux services requis, comme décrit dans «Octroi d'un accès administratif limité à certains services», à la page 181

Octroi d'un accès administrateur limité à certaines files d'attente

Accordez un accès administrateur partiel à certaines files d'attente d'un gestionnaire de files d'attente, à chaque groupe d'utilisateurs qui en ont besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certaines files d'attente pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName ReqdAction
```

- Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

  ReqdAction
  L'action que vous autorisez le groupe à effectuer:

  – Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + dlt, + dsp. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Remarque : L'octroi + crt pour les files d'attente fait indirectement de l'utilisateur ou du groupe un administrateur. N'utilisez pas le droit + crt pour accorder un accès administrateur limité à certaines files d'attente.

QType

Pour la commande DISPLAY, l'une des valeurs QUEUE, QLOCAL, QALIAS, QMODEL, QREMOTE ou QCLUSTER.

Pour les autres valeurs de *ReqdAction*, l'une des valeurs QLOCAL, QALIAS, QMODEL ou QREMOTE.

Octroi d'un accès administrateur limité à certaines rubriques

Accordez un accès administratif partiel à certaines rubriques d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certaines rubriques pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName ReqdAction
```

- Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

  ReqdAction
  L'action que vous autorisez le groupe à effectuer:

  – Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + dsp. + ctrl. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Octroi d'un accès administratif limité à certains canaux

Accordez un accès administratif partiel à certains canaux d'un gestionnaire de files d'attente, à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certains canaux pour certaines actions, utilisez les commandes appropriées à votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName ReqdAction
```

- Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

ReqdAction
L'action que vous autorisez le groupe à effectuer:

– Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + dsp. + ctrl, + ctrlx. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Octroi d'un accès administrateur limité à un gestionnaire de files d'attente

Accordez un accès administrateur partiel à un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité afin d'effectuer certaines actions sur le gestionnaire de files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName ReqdAction
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Résultats

Pour déterminer les commandes MQSC que l'utilisateur peut exécuter sur le gestionnaire de files d'attente, exécutez les commandes suivantes pour chaque commande MQSC:

```
RDEFINE MQCMDS QMgrName.ReqdAction.QMGR UACC(NONE)
PERMIT QMgrName.ReqdAction.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Pour permettre à l'utilisateur d'utiliser la commande DISPLAY QMGR, exécutez les commandes suivantes:

```
RDEFINE MQCMDS QMgrName.DISPLAY.QMGR UACC(NONE)
PERMIT QMgrName.DISPLAY.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

ReqdAction
L'action que vous autorisez le groupe à effectuer:

- Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + dsp. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

  Bien que + set soit une autorisation MQI et qu'elle ne soit normalement pas considérée comme administrative, l'octroi de + set sur le gestionnaire de files d'attente peut indirectement conduire

à des droits d'administration complets. N'accordez pas + défini aux utilisateurs et aux applications ordinaires.

Octroi d'un accès administrateur limité à certains processus

Accordez un accès administratif partiel à certains processus d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certains processus pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName ReqdAction
```

- Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

  ReqdAction
  L'action que vous autorisez le groupe à effectuer:

  – Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + dsp. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Octroi d'un accès administrateur limité à certaines listes de noms

Accordez un accès administrateur partiel à certaines listes de noms sur un gestionnaire de files d'attente, à chaque groupe d'utilisateurs qui en ont besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certaines listes de noms pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName ReqdAction
```

- Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

  ReqdAction
  L'action que vous autorisez le groupe à effectuer:

– Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Octroi d'un accès administratif limité à certains services

Accordez un accès administratif partiel à certains services d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur limité à certains services pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Remarque : Les objets de service n'existent pas dans z/OS.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName ReqdAction
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(ReqdAction)
MQMNAME('QMgrName')
```

Résultats

Ces commandes permettent d'accéder au service spécifié. Pour déterminer les commandes MQSC que l'utilisateur peut exécuter sur le service, exécutez les commandes suivantes pour chaque commande MQSC:

```
RDEFINE MQCMDS QMgrName.ReqdAction.SERVICE UACC(NONE)
PERMIT QMgrName.ReqdAction.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(ALTER)
```

Pour permettre à l'utilisateur d'utiliser la commande DISPLAY SERVICE, exécutez les commandes suivantes:

```
RDEFINE MQCMDS QMgrName.DISPLAY.SERVICE UACC(NONE)
PERMIT QMgrName.DISPLAY.SERVICE CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

ReqdAction
L'action que vous autorisez le groupe à effectuer:

- Sur les systèmes UNIX, Linux et Windows , toute combinaison des autorisations suivantes: + chg, + clr, + crt, + dlt, + ctrl, + ctrlx, + dsp. L'autorisation + alladm est équivalente à + chg + clr + dlt + dsp.

Octroi d'un accès administrateur complet sur un sous-ensemble de ressources de gestionnaire de files d'attente

Vous devez accorder à certains utilisateurs un accès administrateur complet à certaines ressources de gestionnaire de files d'attente, mais pas à toutes. Utilisez ces tableaux pour déterminer les actions que vous devez effectuer.

Tableau 15. Octroi d'un accès administrateur complet à un sous-ensemble de ressources de gestionnaire de files d'attente

Les utilisateurs doivent administrer les objets de ce type	**Effectuer cette action**
Files d'attente	Accordez un accès administrateur complet aux files d'attente requises, comme décrit dans «Octroi d'un accès administrateur complet à certaines files d'attente», à la page 182
Rubriques	Accordez un accès administrateur complet aux rubriques requises, comme décrit dans «Octroi d'un accès administrateur complet à certaines rubriques», à la page 183
Canaux	Accordez un accès administrateur complet aux canaux requis, comme décrit dans «Octroi d'un accès administrateur complet à certains canaux», à la page 183
Gestionnaire de files d'attente	Accordez un accès administrateur complet au gestionnaire de files d'attente, comme décrit dans «Octroi d'un accès administrateur complet à un gestionnaire de files d'attente», à la page 184
Processus	Accordez un accès administrateur complet aux processus requis, comme décrit dans «Octroi d'un accès administrateur complet à certains processus», à la page 184
Listes de noms	Accordez un accès administrateur complet aux listes de noms requises, comme décrit dans «Octroi d'un accès administrateur complet à certaines listes de noms», à la page 185
Services	Accordez un accès administrateur complet aux services requis, comme décrit dans «Octroi d'un accès administrateur complet à certains services», à la page 186

Octroi d'un accès administrateur complet à certaines files d'attente

Accordez un accès administrateur complet à certaines files d'attente d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certaines files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.QUEUE.ObjectProfile UACC(NONE)
PERMIT QMgrName.QUEUE.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à certaines rubriques

Accordez un accès administrateur complet à certaines rubriques d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certaines rubriques pour certaines actions, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(ALLADM)
MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.TOPIC.ObjectProfile UACC(NONE)
PERMIT QMgrName.TOPIC.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à certains canaux

Accordez un accès administrateur complet à certains canaux d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certains canaux, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t channel -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*CHL) USER(GroupName) AUT(ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.CHANNEL.ObjectProfile UACC(NONE)
PERMIT QMgrName.CHANNEL.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à un gestionnaire de files d'attente

Accordez un accès administrateur complet à un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet au gestionnaire de files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -t qmgr -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.QMGR UACC(NONE)
PERMIT QMgrName.QMGR CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à certains processus

Accordez un accès administrateur complet à certains processus d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certains processus, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.CHANNEL.ObjectProfile UACC(NONE)
PERMIT QMgrName.PROCESS.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à certaines listes de noms

Accordez un accès administrateur complet à certaines listes de noms d'un gestionnaire de files d'attente, à chaque groupe d'utilisateurs qui en ont besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certaines listes de noms, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t namelist -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALLADM)
MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.NAMELIST.ObjectProfile UACC(NONE)
PERMIT QMgrName.NAMELIST.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à certains services

Accordez un accès administrateur complet à certains services d'un gestionnaire de files d'attente à chaque groupe d'utilisateurs qui en ont besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder un accès administrateur complet à certains services, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t service -g GroupName +alladm
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*SVC) USER(GroupName) AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.SERVICE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SERVICE.ObjectProfile CLASS(MQADMIN) ID(GroupName ) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès en lecture seule à toutes les ressources d'un gestionnaire de files d'attente

Accordez un accès en lecture seule à toutes les ressources d'un gestionnaire de files d'attente, à chaque utilisateur ou groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Utilisez l'assistant d'ajout de droits basés sur les rôles ou les commandes appropriées pour votre système d'exploitation.

Procédure

- A l'aide de l'assistant:
  a) Dans la sous-fenêtre WebSphere MQ Explorer Navigator , cliquez avec le bouton droit de la souris sur le gestionnaire de files d'attente, puis cliquez sur **Droits sur les objets** > **Ajouter des droits basés sur les rôles**

  L'assistant Ajout de droits basés sur des rôles s'ouvre.
- Pour les systèmes UNIX et Windows , exécutez les commandes suivantes:

```
setmqaut -m QMgrName -n ** -t queue -g GroupName +browse +dsp
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.MODEL -t queue -g GroupName +dsp +inq +get
setmqaut -m QMgrName -n ** -t topic -g GroupName +dsp
```

```
setmqaut -m QMgrName -n ** -t channel -g GroupName +dsp +inq
setmqaut -m QMgrName -n ** -t clntconn -g GroupName +dsp
setmqaut -m QMgrName -n ** -t authinfo -g GroupName +dsp
setmqaut -m QMgrName -n ** -t listener -g GroupName +dsp
setmqaut -m QMgrName -n ** -t namelist -g GroupName +dsp
setmqaut -m QMgrName -n ** -t process -g GroupName +dsp
setmqaut -m QMgrName -n ** -t service -g GroupName +dsp
setmqaut -m QMgrName -t qmgr -g GroupName +dsp +inq +connect
```

Droits d'accès spécifiques à SYSTEM.ADMIN.COMMAND.QUEUE et SYSTEM.MQEXPLORER.REPLY.MODEL est nécessaire uniquement si vous souhaitez utiliser MQ Explorer.

- Pour IBM i, exécutez les commandes suivantes:

```
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')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQQUEUE QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQQUEUE) ID(GroupName) ACCESS(READ)
RDEFINE MQTOPIC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQTOPIC) ID(GroupName) ACCESS(READ)
RDEFINE MQPROC QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQPROC) ID(GroupName) ACCESS(READ)
RDEFINE MQNLIST QMgrName.** UACC(NONE)
PERMIT QMgrName.** CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
PERMIT QMgrName.BATCH CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
PERMIT QMgrName.CICS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
PERMIT QMgrName.IMS CLASS(MQCONN) ID(GroupName) ACCESS(READ)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
PERMIT QMgrName.CHIN CLASS(MQCONN) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi d'un accès administrateur complet à toutes les ressources d'un gestionnaire de files d'attente

Accordez un accès administrateur complet à toutes les ressources d'un gestionnaire de files d'attente, à chaque utilisateur ou groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Utilisez l'assistant d'ajout de droits basés sur les rôles ou les commandes appropriées pour votre système d'exploitation.

Procédure

- A l'aide de l'assistant:

a) Dans la sous-fenêtre WebSphere MQ Explorer Navigator , cliquez avec le bouton droit de la souris sur le gestionnaire de files d'attente, puis cliquez sur **Droits sur les objets** > **Ajouter des droits basés sur les rôles**

L'assistant Ajout de droits basés sur des rôles s'ouvre.

- Pour les systèmes UNIX and Linux , exécutez les commandes suivantes:

```
setmqaut -m QMgrName -n '**' -t queue -g GroupName +alladm +browse
setmqaut -m QMgrName -n @class -t queue -g GroupName +crt
setmqaut -m QMgrName -n SYSTEM.ADMIN.COMMAND.QUEUE -t queue -g GroupName +dsp +inq +put
setmqaut -m QMgrName -n SYSTEM.MQEXPLORER.REPLY.QUEUE -t queue -g GroupName +dsp +inq +get
setmqaut -m QMgrName -n '**' -t topic -g GroupName +alladm
setmqaut -m QMgrName -n @class -t topic -g GroupName +crt
setmqaut -m QMgrName -n '**' -t channel -g GroupName +alladm
setmqaut -m QMgrName -n @class -t channel -g GroupName +crt
setmqaut -m QMgrName -n '**' -t clntconn -g GroupName +alladm
setmqaut -m QMgrName -n @class -t clntconn -g GroupName +crt
setmqaut -m QMgrName -n '**' -t authinfo -g GroupName +alladm
setmqaut -m QMgrName -n @class -t authinfo -g GroupName +crt
setmqaut -m QMgrName -n '**' -t listener -g GroupName +alladm
setmqaut -m QMgrName -n @class -t listener -g GroupName +crt
setmqaut -m QMgrName -n '**' -t namelist -g GroupName +alladm
setmqaut -m QMgrName -n @class -t namelist -g GroupName +crt
setmqaut -m QMgrName -n '**' -t process -g GroupName +alladm
setmqaut -m QMgrName -n @class -t process -g GroupName +crt
setmqaut -m QMgrName -n '**' -t service -g GroupName +alladm
setmqaut -m QMgrName -n @class -t service -g GroupName +crt
setmqaut -m QMgrName -t qmgr -g GroupName +alladm +conn
```

- Pour les systèmes Windows, exécutez les mêmes commandes que pour les systèmes UNIX and Linux , mais en utilisant le nom de profil @CLASS à la place de @class.
- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ(*ALL) OBJTYPE(*ALL) USER('GroupName') AUT(*ALLADM) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQADMIN QMgrName.*.** UACC(NONE)
PERMIT QMgrName.*.** CLASS(MQADMIN) ID(GroupName) ACCESS(ALTER)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Suppression de la connectivité au gestionnaire de files d'attente

Si vous ne souhaitez pas que les applications utilisateur se connectent à votre gestionnaire de files d'attente, supprimez leurs droits de connexion.

Pourquoi et quand exécuter cette tâche

Révoquez le droit de tous les utilisateurs de se connecter au gestionnaire de files d'attente à l'aide de la commande appropriée pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -t qmgr -g GroupName -connect
```

- Pour IBM i, exécutez la commande suivante:

```
RVKMQMAUT OBJ ('QMgrName') OBJTYPE(*MQM) USER(*ALL) AUT(*CONNECT)
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQCONN QMgrName.BATCH UACC(NONE)
RDEFINE MQCONN QMgrName.CHIN UACC(NONE)
RDEFINE MQCONN QMgrName.CICS UACC(NONE)
RDEFINE MQCONN QMgrName.IMS UACC(NONE)
```

N'émettez aucune commande PERMIT.

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

GroupName
Nom du groupe auquel l'accès doit être refusé.

Autorisation des applications utilisateur à se connecter à votre gestionnaire de files d'attente

Vous souhaitez autoriser l'application utilisateur à se connecter à votre gestionnaire de files d'attente. Utilisez les tableaux de cette rubrique pour déterminer les actions à effectuer.

Tout d'abord, déterminez si les applications client se connecteront à votre gestionnaire de files d'attente.

Si aucune des applications qui se connecteront à votre gestionnaire de files d'attente ne sont des applications client, désactivez l'accès distant comme décrit dans «Désactivation de l'accès distant au gestionnaire de files d'attente», à la page 196.

Si une ou plusieurs des applications qui se connecteront à votre gestionnaire de files d'attente sont des applications client, sécurisez la connectivité à distance comme décrit dans «Sécurisation de la connectivité distante au gestionnaire de files d'attente», à la page 189.

Dans les deux cas, configurez la sécurité de connexion comme décrit dans «Configuration de la sécurité de connexion», à la page 197

Si vous souhaitez contrôler l'accès aux ressources pour chaque utilisateur se connectant au gestionnaire de files d'attente, voir le tableau suivant. Si l'instruction de la première colonne est vraie, effectuez l'action indiquée dans la deuxième colonne.

Instruction	Effectuez cette action
Vous disposez d'applications qui utilisent des files d'attente	Pour plus d'informations, voir «Contrôle de l'accès utilisateur aux files d'attente», à la page 197.
Vous disposez d'applications qui utilisent des rubriques	Voir «Contrôle de l'accès des utilisateurs aux rubriques», à la page 202.
Vous disposez d'applications qui s'interrogent sur l'objet gestionnaire de files d'attente	Voir «Octroi de droits d'interrogation sur un gestionnaire de files d'attente», à la page 204.
Vous disposez d'applications qui utilisent des objets de processus	Pour plus d'informations, voir «Octroi de droits d'accès aux processus», à la page 204.
Vous disposez d'applications qui utilisent des listes de noms	Pour plus d'informations, voir «Octroi de droits d'accès aux listes de noms», à la page 205.

Sécurisation de la connectivité distante au gestionnaire de files d'attente

Vous pouvez sécuriser la connectivité distante au gestionnaire de files d'attente à l'aide de SSL ou TLS, d'un exit de sécurité, d'enregistrements d'authentification de canal ou d'une combinaison de ces méthodes.

Pourquoi et quand exécuter cette tâche

Vous connectez un client au gestionnaire de files d'attente à l'aide d'un canal de connexion client sur le poste de travail client et d'un canal de connexion serveur sur le serveur. Sécurisez ces connexions de l'une des manières suivantes.

Procédure

1. Utilisation de SSL ou TLS avec des enregistrements d'authentification de canal:
   a) Empêchez tout nom distinctif (DN) d'ouvrir un canal en utilisant un enregistrement d'authentification de canal SSLPEERMAP pour mapper tous les noms distinctifs à USERSRC (NOACCESS).
   b) Autoriser des noms distinctifs ou des ensembles de noms distinctifs spécifiques à ouvrir un canal à l'aide d'un enregistrement d'authentification de canal SSLPEERMAP pour les mapper à USERSRC (CHANNEL).
2. Utilisation de SSL ou TLS avec un exit de sécurité:
   a) Définissez MCAUSER sur le canal de connexion serveur sur un identificateur utilisateur sans privilèges.
   b) Ecrivez un exit de sécurité pour affecter une valeur MCAUSER en fonction de la valeur du nom distinctif SSL qu'il reçoit dans les zones SSLPeerNamePtr et SSLPeerNameLength transmises à l'exit dans la structure MQCD.
3. Utilisation de SSL ou TLS avec des valeurs de définition de canal fixes:
   a) Définissez SSLPEER sur le canal de connexion serveur sur une valeur spécifique ou une plage de valeurs étroite.
   b) Définissez MCAUSER sur le canal de connexion serveur sur l'ID utilisateur avec lequel le canal doit s'exécuter.
4. Utilisation des enregistrements d'authentification de canal sur les canaux qui n'utilisent pas SSL ou TLS:
   a) Empêchez toute adresse IP d'ouvrir des canaux en utilisant un enregistrement d'authentification de canal de mappage d'adresse avec ADDRESS (*) et USERSRC (NOACCESS).
   b) Autorisez des adresses IP spécifiques à ouvrir des canaux, en utilisant des enregistrements d'authentification de canal de mappage d'adresse pour ces adresses avec USERSRC (CHANNEL).
5. A l'aide d'un exit de sécurité:
   a) Ecrivez un exit de sécurité pour autoriser les connexions en fonction de la propriété que vous choisissez, par exemple, l'adresse IP d'origine.
6. Il est également possible d'utiliser des enregistrements d'authentification de canal avec un exit de sécurité ou d'utiliser les trois méthodes, si vos circonstances particulières l'exigent.

Blocage d'adresses IP spécifiques

Vous pouvez empêcher un canal spécifique d'accepter une connexion entrante à partir d'une adresse IP ou empêcher l'ensemble du gestionnaire de files d'attente d'autoriser l'accès à partir d'une adresse IP, à l'aide d'un enregistrement d'authentification de canal.

Avant de commencer

Activez les enregistrements d'authentification de canal en exécutant la commande suivante:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Pourquoi et quand exécuter cette tâche

Pour empêcher des canaux spécifiques d'accepter une connexion entrante et s'assurer que les connexions sont uniquement acceptées lors de l'utilisation du nom de canal correct, un type de règle peut être utilisé pour bloquer les adresses IP. Pour interdire l'accès d'une adresse IP à l'ensemble du gestionnaire de files d'attente, vous devez normalement utiliser un pare-feu pour le bloquer

définitivement. Toutefois, un autre type de règle peut être utilisé pour vous permettre de bloquer temporairement quelques adresses, par exemple pendant que vous attendez que le pare-feu soit mis à jour.

Procédure

- Pour empêcher les adresses IP d'utiliser un canal spécifique, définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**.

```
SET CHLAUTH(generic-channel-name) TYPE(ADDRESSMAP) ADDRESS(generic-ip-address)
USERSRC(NOACCESS)
```

La commande comporte trois parties:

SET CHLAUTH (*nom-canal-générique*)
Cette partie de la commande permet de contrôler si vous souhaitez bloquer une connexion pour l'ensemble du gestionnaire de files d'attente, un canal unique ou une plage de canaux. Ce que vous mettez ici détermine les zones qui sont couvertes.

Exemple :

- SET CHLAUTH('*') -bloque tous les canaux d'un gestionnaire de files d'attente, c'est-à-dire l'intégralité du gestionnaire de files d'attente
- SET CHLAUTH ('SYSTEM. *')-bloque chaque canal commençant par SYSTEM.
- SET CHLAUTH ('SYSTEM.DEF.SVRCONN')-bloque le canal SYSTEM.DEF.SVRCONN

Type de règle CHLAUTH
Utilisez cette partie de la commande pour spécifier le type de commande et déterminer si vous souhaitez fournir une adresse unique ou une liste d'adresses.

Exemple :

- TYPE(ADDRESSMAP) -Utilisez ADDRESSMAP si vous souhaitez fournir une adresse unique ou une adresse générique. Par exemple, ADDRESS('192.168.*') bloque toutes les connexions provenant d'une adresse IP à partir de 192.168.

  Pour plus d'informations sur le filtrage des adresses IP à l'aide de modèles, voir Adresses IP génériques.
- TYPE(BLOCKADDR) -Utilisez BLOCKADDR si vous souhaitez fournir une liste d'adresses à bloquer.

Paramètres supplémentaires
Ces paramètres dépendent du type de règle que vous avez utilisé dans la deuxième partie de la commande:

- Pour TYPE(ADDRESSMAP) , vous utilisez ADDRESS
- Pour TYPE(BLOCKADDR) , vous utilisez ADDRLIST

Référence associée
SET CHLAUTH

Blocage temporaire d'adresses IP spécifiques si le gestionnaire de files d'attente n'est pas en cours d'exécution
Vous pouvez bloquer des adresses IP particulières ou des plages d'adresses lorsque le gestionnaire de files d'attente n'est pas en cours d'exécution et que vous ne pouvez donc pas émettre de commandes MQSC. Vous pouvez temporairement bloquer des adresses IP de manière exceptionnelle en modifiant le fichier blockaddr.ini .

Pourquoi et quand exécuter cette tâche

Le fichier `blockaddr.ini` contient une copie des définitions BLOCKADDR utilisées par le gestionnaire de files d'attente. Ce fichier est lu par le programme d'écoute si ce dernier est démarré avant le gestionnaire de files d'attente. Dans ces circonstances, le programme d'écoute utilise toutes les valeurs que vous avez ajoutées manuellement au fichier `blockaddr.ini` .

Toutefois, sachez que lorsque le gestionnaire de files d'attente est démarré, il écrit l'ensemble des définitions BLOCKADDR dans le fichier `blockaddr.ini` , en écrase les modifications manuelles que vous avez éventuellement effectuées. De même, chaque fois que vous ajoutez ou supprimez une définition BLOCKADDR à l'aide de la commande **SET CHLAUTH** , le fichier `blockaddr.ini` est mis à jour. Vous pouvez donc apporter des modifications permanentes aux définitions BLOCKADDR uniquement à l'aide de la commande **SET CHLAUTH** lorsque le gestionnaire de files d'attente est en cours d'exécution.

Procédure

1. Ouvrez le fichier `blockaddr.ini` dans n'importe quel éditeur de texte.

   Le fichier se trouve dans le répertoire de données du gestionnaire de files d'attente.
2. Ajoutez des adresses IP sous forme de paires mot clé-valeur simples, où le mot clé est `Addr`.

   Pour plus d'informations sur le filtrage des adresses IP à l'aide de modèles, voir Adresses IP génériques.

   Exemple :

```
Addr = 192.0.2.0
Addr = 192.0.*
Addr = 192.0.2.1-8
```

Tâches associées

«Blocage d'adresses IP spécifiques», à la page 190
Vous pouvez empêcher un canal spécifique d'accepter une connexion entrante à partir d'une adresse IP ou empêcher l'ensemble du gestionnaire de files d'attente d'autoriser l'accès à partir d'une adresse IP, à l'aide d'un enregistrement d'authentification de canal.

Référence associée

SET CHLAUTH

Blocage d'ID utilisateur spécifiques
Vous pouvez empêcher des utilisateurs spécifiques d'utiliser un canal en spécifiant des ID utilisateur qui, s'ils sont vérifiés, provoquent l'arrêt du canal. Pour cela, définissez un enregistrement d'authentification de canal.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(BLOCKUSER) USERLIST(userID1, userID2)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.

La liste d'utilisateurs fournie sur un TYPE(BLOCKUSER) s'applique uniquement aux canaux SVRCONN et non aux canaux de gestionnaire de files d'attente.

userID1 et *userID2* sont chacun l'ID d'un utilisateur qui doit être empêché d'utiliser le canal. Vous pouvez également spécifier la valeur spéciale `*MQADMIN` pour faire référence aux administrateurs privilégiés. Pour plus d'informations sur les utilisateurs privilégiés, voir «Utilisateurs privilégiés», à la page 153. Pour plus d'informations sur `*MQADMIN`, voir SET CHLAUTH.

Référence associée
SET CHLAUTH

Mappage d'un gestionnaire de files d'attente éloignées à un ID utilisateur MCAUSER
Vous pouvez utiliser un enregistrement d'authentification de canal pour définir l'attribut MCAUSER d'un canal, en fonction du gestionnaire de files d'attente à partir duquel le canal se connecte.

Avant de commencer
Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Pourquoi et quand exécuter cette tâche

Vous pouvez éventuellement restreindre les adresses IP auxquelles la règle s'applique.

Notez que cette technique ne s'applique pas aux canaux de connexion serveur. Si vous indiquez le nom d'un canal de connexion serveur dans les commandes ci-dessous, cela n'a aucun effet.

Procédure

- Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
) USERSRC(MAP) MCAUSER(user)
```

  nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
  generic-partner-qmgr-name est soit le nom du gestionnaire de files d'attente, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du gestionnaire de files d'attente.
  user est l'ID utilisateur à utiliser pour toutes les connexions à partir du gestionnaire de files d'attente spécifié.
- Pour limiter cette commande à certaines adresses IP, incluez le paramètre **ADDRESS** comme suit:

```
SET CHLAUTH('generic-channel-name') TYPE (QMGRMAP) QMNAME(generic-partner-qmgr-name
) USERSRC(MAP) MCAUSER(user) ADDRESS(
generic-ip-address)
```

  nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
  generic-ip-address est soit une adresse unique, soit un modèle incluant l'astérisque (*) comme caractère générique ou le trait d'union (-) pour indiquer une plage, qui correspond à l'adresse. Pour plus d'informations sur les adresses IP génériques, voir Adresses IP génériques .

Référence associée
SET CHLAUTH

Mappage d'un ID utilisateur vérifié par le client à un ID utilisateur MCAUSER
Vous pouvez utiliser un enregistrement d'authentification de canal pour modifier l'attribut MCAUSER d'un canal de connexion serveur, en fonction de l'ID utilisateur d'origine reçu d'un client.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Pourquoi et quand exécuter cette tâche

Notez que cette technique s'applique uniquement aux canaux de connexion serveur. Il n'a aucun effet sur les autres types de canal.

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record** . Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (USERMAP) CLNTUSER(client-user-name) USERSRC(MAP)
MCAUSER(
user)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.

client-user-name est l'ID utilisateur vérifié par le client.

user est l'ID utilisateur à utiliser à la place du nom d'utilisateur du client.

Référence associée

SET CHLAUTH

Mappage d'un nom distinctif SSL ou TLS à un ID utilisateur MCAUSER

Vous pouvez utiliser un enregistrement d'authentification de canal pour définir l'attribut MCAUSER d'un canal, en fonction du nom distinctif (DN) reçu.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE (SSLPEERMAP) SSLPEER(generic-ssl-peer-name
) USERSRC(MAP) MCAUSER(user)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.

generic-ssl-peer-name est une chaîne qui suit les règles IBM WebSphere MQ standard pour les valeurs SSLPEER. Voir WebSphere MQ rules for SSLPEER values.

user est l'ID utilisateur à utiliser pour toutes les connexions utilisant le nom distinctif spécifié.

Référence associée

SET CHLAUTH

Blocage de l'accès à partir d'un gestionnaire de files d'attente éloignées

Vous pouvez utiliser un enregistrement d'authentification de canal pour empêcher un gestionnaire de files d'attente éloignées de démarrer des canaux.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Pourquoi et quand exécuter cette tâche

Notez que cette technique ne s'applique pas aux canaux de connexion serveur. Si vous indiquez le nom d'un canal de connexion serveur dans la commande ci-dessous, cela n'a aucun effet.

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(QMGRMAP) QMNAME('generic-partner-qmgr-name')
USERSRC(NOACCESS)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
generic-partner-qmgr-name est soit le nom du gestionnaire de files d'attente, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du gestionnaire de files d'attente.

Référence associée

SET CHLAUTH

Blocage de l'accès pour un ID utilisateur vérifié par le client

Vous pouvez utiliser un enregistrement d'authentification de canal pour empêcher un ID utilisateur vérifié par le client de démarrer des canaux.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Pourquoi et quand exécuter cette tâche

Notez que cette technique s'applique uniquement aux canaux de connexion serveur. Il n'a aucun effet sur les autres types de canal.

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(USERMAP) CLNTUSER('client-user-name') USERSRC(NOACCESS)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
client-user-name est l'ID utilisateur vérifié par le client.

Référence associée

SET CHLAUTH

Blocage de l'accès pour un nom distinctif SSL

Vous pouvez utiliser un enregistrement d'authentification de canal pour empêcher un nom distinctif SSL de démarrer des canaux.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(SSLPEERMAP) SSLPEER('generic-ssl-peer-name')
USERSRC(NOACCESS)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
generic-ssl-peer-name est une chaîne qui suit les règles IBM WebSphere MQ standard pour les valeurs SSLPEER. Voir WebSphere MQ rules for SSLPEER values.

Référence associée

SET CHLAUTH

Mappage d'une adresse IP à un ID utilisateur MCAUSER

Vous pouvez utiliser un enregistrement d'authentification de canal pour définir l'attribut MCAUSER d'un canal, en fonction de l'adresse IP à partir de laquelle la connexion est reçue.

Avant de commencer

Vérifiez que les enregistrements d'authentification de canal sont activés comme suit:

```
ALTER QMGR CHLAUTH(ENABLED)
```

Procédure

Définissez un enregistrement d'authentification de canal à l'aide de la commande MQSC **SET CHLAUTH**ou de la commande PCF **Set Channel Authentication Record**. Par exemple, vous pouvez émettre la commande MQSC:

```
SET CHLAUTH('generic-channel-name') TYPE(ADDRESSMAP) ADDRESS('generic-ip-address') USERSRC(MAP)
MCAUSER(user)
```

nom-canal-générique est soit le nom d'un canal auquel vous souhaitez contrôler l'accès, soit un modèle incluant l'astérisque (*) comme caractère générique qui correspond au nom du canal.
user est l'ID utilisateur à utiliser pour toutes les connexions utilisant le nom distinctif spécifié.
generic-ip-address est soit l'adresse à partir de laquelle la connexion est établie, soit un modèle incluant l'astérisque (*) comme caractère générique ou le trait d'union (-) pour indiquer une plage qui correspond à l'adresse.

Référence associée

SET CHLAUTH

Désactivation de l'accès distant au gestionnaire de files d'attente

Si vous ne souhaitez pas que les applications client se connectent à votre gestionnaire de files d'attente, désactivez l'accès à distance à ce dernier.

Pourquoi et quand exécuter cette tâche

Empêchez les applications client de se connecter au gestionnaire de files d'attente de l'une des manières suivantes:

Procédure

- Supprimez tous les canaux de connexion serveur à l'aide de la commande MQSC **DELETE CHANNEL**.
- Définissez l'ID utilisateur de l'agent de canal de transmission de messages (MCAUSER) du canal sur un ID utilisateur sans droits d'accès, à l'aide de la commande MQSC **ALTER CHANNEL**.

Configuration de la sécurité de connexion

Accordez le droit de se connecter au gestionnaire de files d'attente à chaque utilisateur ou groupe d'utilisateurs dont l'entreprise a besoin pour le faire.

Pourquoi et quand exécuter cette tâche

Pour configurer la sécurité de la connexion, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

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

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('QMgrName') OBJTYPE(*MQM)  USER('GroupName') AUT(*CONNECT)
```

- Pour z/OS, exécutez les commandes suivantes:

```
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)
```

  Ces commandes donnent le droit de se connecter pour le traitement par lots, CICS, IMS et l'initiateur de canal (CHIN). Si vous n'utilisez pas un type particulier de connexion, omettez les commandes appropriées.

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

Contrôle de l'accès utilisateur aux files d'attente

Vous souhaitez contrôler l'accès des applications aux files d'attente. Cette rubrique permet de déterminer les actions à effectuer.

Pour chaque instruction true de la première colonne, effectuez l'action indiquée dans la deuxième colonne.

Instruction	Action
L'application extrait des messages d'une file d'attente	Pour plus d'informations, voir «Octroi de droits pour l'obtention de messages à partir de files d'attente», à la page 198.

Instruction	Action
L'application définit le contexte	Pour plus d'informations, voir «Octroi de droits d'accès pour définir le contexte», à la page 199.
L'application transmet le contexte	Pour plus d'informations, voir «Octroi de l'autorisation de transmettre le contexte», à la page 199.
L'application insère des messages dans une file d'attente en cluster	Pour plus d'informations, voir «Autorisation d'insertion de messages dans des files d'attente de cluster éloignées», à la page 256.
L'application insère des messages dans une file d'attente locale	Pour plus d'informations, voir «Octroi du droit d'insertion de messages dans une file d'attente locale», à la page 200.
L'application insère des messages dans une file d'attente modèle	Pour plus d'informations, voir «Octroi du droit d'insertion de messages dans une file d'attente modèle», à la page 201.
L'application insère des messages dans une file d'attente éloignée	Pour plus d'informations, voir «Octroi du droit d'insertion de messages dans une file d'attente de cluster éloignée», à la page 201.

Octroi de droits pour l'obtention de messages à partir de files d'attente
Accordez le droit d'extraire des messages d'une file d'attente ou d'un ensemble de files d'attente à chaque groupe d'utilisateurs qui en a besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit d'extraire des messages de certaines files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +get
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*GET) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi de droits d'accès pour définir le contexte
Accordez le droit de définir le contexte d'un message en cours d'insertion à chaque groupe d'utilisateurs qui en ont besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit de définir le contexte sur certaines files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez l'une des commandes suivantes:
  - Pour définir le contexte d'identité uniquement:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setid
    ```

  - Pour définir tous les contextes:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +setall
    ```

- Pour IBM i, exécutez l'une des commandes suivantes:
  - Pour définir le contexte d'identité uniquement:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*SETID) MQMNAME('QMgrName')
    ```

  - Pour définir tous les contextes:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*SETALL)
    MQMNAME('QMgrName')
    ```

- Pour z/OS, exécutez l'un des ensembles de commandes suivants:
  - Pour définir le contexte d'identité uniquement:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
    ```

  - Pour définir tous les contextes:

    ```
    RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
    PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(CONTROL)
    ```

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

Octroi de l'autorisation de transmettre le contexte
Accordez le droit de transmettre le contexte d'un message extrait à un message en cours d'insertion, à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit de transmettre le contexte sur certaines files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez l'une des commandes suivantes:
  - Pour transmettre uniquement le contexte d'identité:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passid
    ```

  - Pour transmettre tous les contextes:

    ```
    setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +passall
    ```

- Pour IBM i, exécutez l'une des commandes suivantes:
  - Pour transmettre uniquement le contexte d'identité:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PASSID)
    MQMNAME('QMgrName')
    ```

  - Pour transmettre tous les contextes:

    ```
    GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PASSALL)
    MQMNAME('QMgrName')
    ```

- Pour z/OS, exécutez les commandes suivantes pour transmettre le contexte d'identité ou tout le contexte:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

Octroi du droit d'insertion de messages dans une file d'attente locale
Accordez le droit d'insérer des messages dans une file d'attente locale ou dans un ensemble de files d'attente, à chaque groupe d'utilisateurs qui en a besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit d'insertion de messages dans certaines files d'attente locales, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

  ```
  setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
  ```

- Pour IBM i, exécutez la commande suivante:

  ```
  GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
  ```

- Pour z/OS, exécutez les commandes suivantes:

  ```
  RDEFINE MQQUEUE QMgrName.ObjectProfile UACC(NONE)
  PERMIT QMgrName.ObjectProfile CLASS(MQQUEUE) ID(GroupName) ACCESS(UPDATE)
  ```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi du droit d'insertion de messages dans une file d'attente modèle
Accordez le droit d'insérer des messages dans une file d'attente modèle ou dans un ensemble de files d'attente modèle, à chaque groupe d'utilisateurs qui en a besoin.

Pourquoi et quand exécuter cette tâche

Les files d'attente modèles sont utilisées pour créer des files d'attente dynamiques. Vous devez donc accorder des droits d'accès au modèle et aux files d'attente dynamiques. Pour accorder ces droits, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez les commandes suivantes:

```
setmqaut -m QMgrName -n ModelQueueName -t queue -g GroupName +put
setmqaut -m QMgrName -n ObjectProfile -t queue -g GroupName +put
```

- Pour IBM i, exécutez les commandes suivantes:

```
GRTMQMAUT OBJ('ModelQueueName') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*Q) USER(GroupName) AUT(*PUT) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
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)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

Nom ModelQueue
Nom de la file d'attente modèle sur laquelle sont basées les files d'attente dynamiques.

ObjectProfile
Nom de la file d'attente dynamique ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi du droit d'insertion de messages dans une file d'attente de cluster éloignée
Accordez le droit d'insérer des messages dans une file d'attente de cluster éloignée ou dans un ensemble de files d'attente, à chaque groupe d'utilisateurs qui en a besoin.

Pourquoi et quand exécuter cette tâche

Pour placer un message dans une file d'attente de cluster éloignée, vous pouvez le placer dans une définition locale d'une file d'attente éloignée ou dans une file d'attente éloignée qualifiée complète. Si vous utilisez une définition locale d'une file d'attente éloignée, vous devez disposer des droits d'accès à

l'objet local: voir «Octroi du droit d'insertion de messages dans une file d'attente locale», à la page 200. Si vous utilisez une file d'attente éloignée qualifiée complète, vous devez disposer des droits nécessaires pour la placer dans la file d'attente éloignée. Accordez ces droits à l'aide des commandes appropriées pour votre système d'exploitation.

Le comportement par défaut consiste à effectuer un contrôle d'accès sur le SYSTEM.CLUSTER.TRANSMIT.QUEUE. Notez que ce comportement s'applique, même si vous utilisez plusieurs files d'attente de transmission.

Le comportement spécifique décrit dans cette rubrique s'applique uniquement lorsque vous avez configuré l'attribut **ClusterQueueAccessControl** dans le fichier qm.ini comme étant *RQMName*, comme décrit dans la rubrique Strophe de sécurité , puis redémarré le gestionnaire de files d'attente.

Sur les systèmes UNIX, Linuxet Windows , vous pouvez également utiliser la commande SET AUTHREC.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

  ```
  setmqaut -m QMgrName -t rqmname -n
  ObjectProfile -g GroupName +put
  ```

  Notez que vous pouvez utiliser l'objet *rqmname* uniquement pour les files d'attente de cluster éloignées.
- Pour IBM i, exécutez la commande suivante:

  ```
  GRTMQMAUT OBJTYPE(*RMTMQMNAME) OBJ('
  ObjectProfile') USER(GroupName) AUT(*PUT) MQMNAME('
  QMgrName')
  ```

  Notez que vous pouvez utiliser l'objet RMTMQMNAME uniquement pour les files d'attente de cluster éloignées.
- Pour z/OS, exécutez les commandes suivantes:

  ```
  RDEFINE MQQUEUE  QMgrNameObjectProfile UACC(NONE)
  PERMIT QMgrNameObjectProfile CLASS(MQADMIN)
  ID(GroupName) ACCESS(UPDATE)
  ```

  Notez que vous pouvez utiliser le nom du gestionnaire de files d'attente éloignées (ou du groupe de partage de files d'attente) pour les files d'attente de cluster éloignées uniquement.

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom du gestionnaire de files d'attente éloignées ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

Contrôle de l'accès des utilisateurs aux rubriques

Vous devez contrôler l'accès des applications aux rubriques. Cette rubrique permet de déterminer les actions à effectuer.

Pour chaque instruction true de la première colonne, effectuez l'action indiquée dans la deuxième colonne.

Tableau 16. Contrôle de l'accès des utilisateurs aux rubriques	
Instruction	**Action**
L'application publie des messages dans un sujet	Pour plus d'informations, voir «Octroi du droit de publier des messages dans une rubrique», à la page 203.
L'application s'abonne à une rubrique	Pour plus d'informations, voir «Octroi de droits d'abonnement à des rubriques», à la page 203.

Octroi du droit de publier des messages dans une rubrique
Accordez le droit de publier des messages dans une rubrique ou un ensemble de rubriques, à chaque groupe d'utilisateurs qui en a besoin.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit de publier des messages dans certaines rubriques, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +pub
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(*PUB) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQTOPIC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

  ObjectProfile
  Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

Octroi de droits d'abonnement à des rubriques
Accordez le droit de s'abonner à une rubrique ou à un ensemble de rubriques, à chaque groupe d'utilisateurs ayant besoin d'une rubrique ou d'un ensemble de rubriques.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit d'abonnement à certaines rubriques, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t topic -g GroupName +sub
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*TOPIC) USER(GroupName) AUT(*SUB) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQTOPIC QMgrName.SUBSCRIBE.ObjectProfile UACC(NONE)
PERMIT QMgrName.SUBSCRIBE.ObjectProfile CLASS(MQTOPIC) ID(GroupName) ACCESS(UPDATE)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi de droits d'interrogation sur un gestionnaire de files d'attente

Accordez les droits d'interrogation sur un gestionnaire de files d'attente à chaque groupe d'utilisateurs ayant besoin d'un gestionnaire de files d'attente.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit d'interrogation sur un gestionnaire de files d'attente, utilisez les commandes appropriées pour votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t qmgr -g GroupName +inq
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*MQM) USER(GroupName) AUT(*INQ) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQCMDS QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName ObjectProfile CLASS(MQCMDS) ID(GroupName ) ACCESS(READ)
```

Ces commandes permettent d'accéder au gestionnaire de files d'attente spécifié. Pour permettre à l'utilisateur d'utiliser la commande MQINQ, exécutez les commandes suivantes:

```
RDEFINE MQCMDS QMgrName.MQINQ.QMGR UACC(NONE)
PERMIT QMgrName.MQINQ.QMGR CLASS(MQCMDS) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi de droits d'accès aux processus

Accordez le droit d'accès à un processus ou à un ensemble de processus à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder le droit d'accès à certains processus, utilisez les commandes appropriées à votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n ObjectProfile -t process -g GroupName +all
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile') OBJTYPE(*PRC) USER(GroupName) AUT(*ALL) MQMNAME('QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQPROC QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile CLASS(MQPROC) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Octroi de droits d'accès aux listes de noms

Accordez le droit d'accéder à une liste de noms ou à un ensemble de listes de noms, à chaque groupe d'utilisateurs ayant un besoin métier.

Pourquoi et quand exécuter cette tâche

Pour accorder les droits d'accès à certaines listes de noms, utilisez les commandes appropriées à votre système d'exploitation.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez la commande suivante:

```
setmqaut -m QMgrName -n
ObjectProfile -t namelist -g GroupName
 +all
```

- Pour IBM i, exécutez la commande suivante:

```
GRTMQMAUT OBJ('ObjectProfile
') OBJTYPE(*NMLIST) USER(GroupName) AUT(*ALL) MQMNAME('
QMgrName')
```

- Pour z/OS, exécutez les commandes suivantes:

```
RDEFINE MQNLIST
QMgrName.ObjectProfile UACC(NONE)
PERMIT QMgrName.ObjectProfile
 CLASS(MQNLIST) ID(GroupName) ACCESS(READ)
```

Les noms de variable ont les significations suivantes:

QMgrName
Nom du gestionnaire de files d'attente. Sous z/OS, cette valeur peut également être le nom d'un groupe de partage de files d'attente.

ObjectProfile
Nom de l'objet ou du profil générique pour lequel modifier les autorisations.

GroupName
Nom du groupe auquel l'accès doit être accordé.

Droits d'administration de IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows

Les administrateurs IBM WebSphere MQ peuvent utiliser toutes les commandes IBM WebSphere MQ et accorder des droits à d'autres utilisateurs. Lorsque les administrateurs émettent des commandes pour les gestionnaires de files d'attente éloignées, ils doivent disposer des droits requis sur le gestionnaire de files d'attente éloignées. D'autres considérations s'appliquent aux systèmes Windows .

Les administrateurs IBM WebSphere MQ ont le droit d'utiliser toutes les commandes WebSphere MQ (y compris les commandes permettant d'accorder des droits WebSphere MQ à d'autres utilisateurs)

Pour être administrateur IBM WebSphere MQ , vous devez être membre d'un groupe spécial appelé *mqm* (ou membre du groupe Administrateurs sur les systèmes Windows). Le groupe mqm est créé automatiquement lorsque WebSphere MQ est installé ; ajoutez d'autres utilisateurs au groupe pour leur permettre d'effectuer l'administration. Tous les membres de ce groupe peuvent accéder à toutes les ressources. Cet accès peut être révoqué uniquement en supprimant un utilisateur du groupe mqm et en émettant la commande REFRESH SECURITY. Les administrateurs peuvent utiliser des commandes de contrôle pour administrer WebSphere MQ. L'une de ces commandes de contrôle est **setmqaut**, qui permet d'accorder des droits à d'autres utilisateurs pour leur permettre d'accéder aux ressources WebSphere MQ ou de les contrôler. Les commandes PCF pour les enregistrements d'autorité de gestion sont disponibles pour les non-administrateurs auxquels des droits dsp et chg ont été accordés sur le gestionnaire de files d'attente. Pour plus d'informations sur la gestion des droits à l'aide des commandes PCF, voir Programmable Command Formats.

Les administrateurs peuvent utiliser la commande de contrôle **runmqsc** pour émettre des commandes IBM WebSphere MQ Script (MQSC). Lorsque **runmqsc** est utilisé en mode indirect pour envoyer des commandes MQSC à un gestionnaire de files d'attente éloignées, chaque commande MQSC est encapsulée dans une commande Escape PCF. Les administrateurs doivent disposer des droits requis pour que les commandes MQSC soient traitées par le gestionnaire de files d'attente éloignées. WebSphere MQ Explorer émet des commandes PCF pour effectuer des tâches d'administration. Les administrateurs n'ont pas besoin de droits supplémentaires pour utiliser WebSphere MQ Explorer afin d'administrer un gestionnaire de files d'attente sur le système local. Lorsque IBM WebSphere MQ Explorer est utilisé pour administrer un gestionnaire de files d'attente sur un autre système, les administrateurs doivent disposer des droits requis pour que les commandes PCF soient traitées par le gestionnaire de files d'attente éloignées.

Pour plus d'informations sur les vérifications des droits d'accès lors du traitement des commandes PCF et MQSC, voir les rubriques suivantes:

- Pour les commandes PCF qui fonctionnent sur les gestionnaires de files d'attente, les files d'attente, les processus, les listes de noms et les objets d'informations d'authentification, voir Droits d'utilisation des objets WebSphere MQ. Reportez-vous à cette section pour connaître les commandes MQSC équivalentes encapsulées dans les commandes Escape PCF.
- Pour les commandes PCF qui fonctionnent sur des canaux, des initiateurs de canal, des programmes d'écoute et des clusters, voir Sécurité des canaux.
- Pour les commandes PCF qui fonctionnent sur des enregistrements de droits d'accès, voir Contrôle des droits d'accès pour les commandes PCF

En outre, sur les systèmes Windows , le compte SYSTEM dispose d'un accès complet aux ressources WebSphere MQ .

Sur les plateformes UNIX and Linux , un ID utilisateur spécial de mqm est également créé, à utiliser uniquement par le produit. Il ne doit jamais être disponible pour les utilisateurs non privilégiés. Tous les objets WebSphere MQ appartiennent à l'ID utilisateur mqm.

Sur les systèmes Windows , les membres du groupe Administrateurs peuvent également administrer n'importe quel gestionnaire de files d'attente, de même que le compte SYSTEM. Vous pouvez également créer un groupe mqm de domaine sur le contrôleur de domaine qui contient tous les ID utilisateur privilégiés actifs dans le domaine et l'ajouter au groupe mqm local. Certaines commandes, par exemple **crtmqm**, manipulent les droits sur les objets IBM WebSphere MQ et ont donc besoin de droits pour utiliser ces objets (comme décrit dans les sections suivantes). Les membres du groupe mqm ont le droit d'utiliser tous les objets, mais il peut exister des cas sur les systèmes Windows où les droits d'accès sont refusés si vous disposez d'un utilisateur local et d'un utilisateur authentifié par le domaine portant le même nom. Ceci est décrit dans «Principaux et groupes», à la page 210.

Les versions de Windows avec une fonction de contrôle de compte d'utilisateur (UAC) limitent les actions que les utilisateurs peuvent effectuer sur certaines fonctions du système d'exploitation, même s'ils sont membres du groupe Administrateurs. Si votre ID utilisateur se trouve dans le groupe Administrateurs mais pas dans le groupe mqm, vous devez utiliser une invite de commande élevée pour émettre des commandes d'administration WebSphere MQ telles que **crtmqm**, sinon l'erreur "AMQ7077: Vous n'êtes pas autorisé à effectuer l'opération demandée" est générée. Pour ouvrir une invite de commande avec des droits élevés, cliquez avec le bouton droit de la souris sur l'élément de menu Démarrer ou sur l'icône correspondant à l'invite de commande, puis sélectionnez "Exécuter en tant qu'administrateur".

Vous n'avez pas besoin d'être membre du groupe mqm pour effectuer les opérations suivantes:

- Emettez des commandes à partir d'un programme d'application qui émet des commandes PCF ou des commandes MQSC dans une commande PCF d'échappement, sauf si les commandes manipulent des initiateurs de canal. (Ces commandes sont décrites dans «Protection des définitions d'initialisateur de canal», à la page 74).
- Emettez des appels MQI à partir d'un programme d'application (sauf si vous souhaitez utiliser les liaisons Fast Path sur l'appel MQCONNX).
- La commande `crtmqcvx` permet de créer un fragment de code qui effectue la conversion des données sur les structures de type de données.
- Utilisez la commande `dspmq` pour afficher les gestionnaires de files d'attente.
- Utilisez la commande `dspmqtrc` pour afficher la sortie de trace formatée WebSphere MQ .

Une limitation de 12 caractères s'applique aux ID groupe et utilisateur.

Les plateformes UNIX and Linux limitent généralement la longueur d'un ID utilisateur à 12 caractères. AIX Version 5.3 a augmenté cette limite, mais WebSphere MQ continue d'observer une restriction de 12 caractères sur toutes les plateformes UNIX and Linux . Si vous utilisez un ID utilisateur de plus de 12 caractères, WebSphere MQ le remplace par la valeur `UNKNOWN`. Ne définissez pas d'ID utilisateur avec la valeur `UNKNOWN`.

Gestion du groupe mqm

Les utilisateurs du groupe mqm bénéficient de privilèges d'administration complets sur WebSphere MQ. Pour cette raison, vous ne devez pas inscrire d'applications et d'utilisateurs ordinaires dans le groupe mqm. Le groupe mqm doit contenir uniquement les comptes des administrateurs WebSphere MQ .

Ces tâches sont décrites dans:

- Création et gestion de groupes sous Windows
- Création et gestion de groupes sous HP-UX
- Création et gestion de groupes sous AIX
- Création et gestion de groupes sous Solaris
- Création et gestion de groupes sur Linux

Si votre contrôleur de domaine s'exécute sous Windows 2000 ou Windows 2003, votre administrateur de domaine devra peut-être configurer un compte spécial pour WebSphere MQ . Ceci est décrit dans la rubrique Configuration des comptes WebSphere MQ.

Droits d'utilisation des objets IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows

Tous les objets sont protégés par IBM WebSphere MQet les principaux doivent disposer des droits appropriés pour y accéder. Les différents principaux ont besoin de droits d'accès différents à des objets différents.

Les gestionnaires de files d'attente, les files d'attente, les définitions de processus, les listes de noms, les canaux, les canaux de connexion client, les programmes d'écoute, les services et les objets d'informations d'authentification sont tous accessibles à partir d'applications qui utilisent des appels MQI ou des commandes PCF. Ces ressources sont toutes protégées par WebSphere MQet les applications doivent être autorisées à y accéder. L'entité qui effectue la demande peut être un utilisateur, un programme d'application qui émet un appel MQI ou un programme d'administration qui émet une commande PCF. L'identificateur du demandeur est appelé *principal*.

Différents groupes de principaux peuvent être accordés à différents types de droits d'accès sur le même objet. Par exemple, pour une file d'attente spécifique, un groupe peut être autorisé à effectuer des opérations d'insertion et d'extraction ; un autre groupe peut être autorisé uniquement à parcourir la file d'attente (MQGET avec l'option d'exploration). De même, certains groupes peuvent avoir des droits d'insertion et d'obtention sur une file d'attente, mais ils ne sont pas autorisés à modifier les attributs de la file d'attente ou à la supprimer.

Certaines opérations sont particulièrement sensibles et doivent être limitées aux utilisateurs privilégiés. Exemple :

- Accès à certaines files d'attente spéciales, telles que les files d'attente de transmission ou la file d'attente de commandes SYSTEM.ADMIN.COMMAND.QUEUE
- Exécution de programmes qui utilisent des options de contexte MQI complètes
- Création et suppression de files d'attente d'application

Les droits d'accès complets à un objet sont automatiquement accordés à l'ID utilisateur qui a créé l'objet et à tous les membres du groupe mqm (ainsi qu'aux membres du groupe Administrateurs locaux sur les systèmes Windows).

Concepts associés

«Droits d'administration de IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows», à la page 206

Les administrateurs IBM WebSphere MQ peuvent utiliser toutes les commandes IBM WebSphere MQ et accorder des droits à d'autres utilisateurs. Lorsque les administrateurs émettent des commandes pour les gestionnaires de files d'attente éloignées, ils doivent disposer des droits requis sur le gestionnaire de files d'attente éloignées. D'autres considérations s'appliquent aux systèmes Windows .

Lorsque des contrôles de sécurité sont effectués sur les systèmes UNIX, Linux, and Windows

Les contrôles de sécurité sont généralement effectués lors de la connexion à un gestionnaire de files d'attente, de l'ouverture ou de la fermeture d'objets et de l'insertion ou de l'obtention de messages.

Les contrôles de sécurité effectués pour une application standard sont les suivants:

Connexion au gestionnaire de files d'attente (appels MQCONN ou MQCONNX)
C'est la première fois que l'application est associée à un gestionnaire de files d'attente particulier. Le gestionnaire de files d'attente interroge l'environnement d'exploitation pour découvrir l'ID utilisateur associé à l'application. WebSphere MQ vérifie ensuite que l'ID utilisateur est autorisé à se connecter au gestionnaire de files d'attente et conserve l'ID utilisateur pour les vérifications ultérieures.

Les utilisateurs n'ont pas besoin de se connecter à WebSphere MQ; WebSphere MQ suppose que les utilisateurs se sont connectés au système d'exploitation sous-jacent et qu'ils ont été authentifiés par celui-ci.

Ouverture de l'objet (appels MQOPEN ou MQPUT1)
Les objets WebSphere MQ sont accessibles en ouvrant l'objet et en émettant des commandes sur celui-ci. Toutes les vérifications de ressources sont effectuées lorsque l'objet est ouvert, plutôt que lorsqu'il est réellement consulté. Cela signifie que la demande **MQOPEN** doit spécifier le type d'accès requis (par exemple, si l'utilisateur souhaite uniquement parcourir l'objet ou effectuer une mise à jour comme placer des messages dans une file d'attente).

WebSphere MQ vérifie la ressource nommée dans la demande **MQOPEN** . Pour un alias ou un objet de file d'attente éloignée, l'autorisation utilisée est celle de l'objet lui-même, et non celle de la file d'attente dans laquelle l'alias ou la file d'attente éloignée est résolu. Cela signifie que l'utilisateur n'a pas besoin de droits pour y accéder. Limitez les droits de création de files d'attente aux utilisateurs privilégiés. Si vous ne le faites pas, les utilisateurs peuvent ignorer le contrôle d'accès normal simplement en créant un alias. Si une file d'attente éloignée est référencée explicitement avec les noms de file d'attente et de gestionnaire de files d'attente, la file d'attente de transmission associée au gestionnaire de files d'attente éloignées est vérifiée.

Les droits d'accès à une file d'attente dynamique sont basés sur ceux de la file d'attente modèle dont elle est dérivée, mais ne sont pas nécessairement les mêmes. Ceci est décrit dans la remarque «1», à la page 95.

L'ID utilisateur utilisé par le gestionnaire de files d'attente pour les contrôles d'accès est l'ID utilisateur obtenu à partir de l'environnement d'exploitation de l'application connectée au gestionnaire de files d'attente. Une application dûment autorisée peut émettre un appel **MQOPEN** en spécifiant un autre ID utilisateur ; des vérifications de contrôle d'accès sont ensuite effectuées sur l'autre ID utilisateur. Cela ne modifie pas l'ID utilisateur associé à l'application, mais uniquement celui utilisé pour les vérifications de contrôle d'accès.

Insertion et obtention de messages (appels MQPUT ou MQGET)
Aucune vérification de contrôle d'accès n'est effectuée.

Fermeture de l'objet (MQCLOSE)
Aucune vérification de contrôle d'accès n'est effectuée, sauf si **MQCLOSE** entraîne la suppression d'une file d'attente dynamique. Dans ce cas, il est vérifié que l'ID utilisateur est autorisé à supprimer la file d'attente.

Abonnement à une rubrique (MQSUB)
Lorsqu'une application s'abonne à une rubrique, elle spécifie le type d'opération qu'elle doit effectuer. Il s'agit soit de créer un nouvel abonnement, soit de modifier un abonnement existant, soit de reprendre un abonnement existant sans le modifier. Pour chaque type d'opération, le gestionnaire de files d'attente vérifie que l'ID utilisateur associé à l'application est autorisé à effectuer l'opération.

Lorsqu'une application s'abonne à une rubrique, les vérifications des droits d'accès sont effectuées sur les objets de rubrique qui se trouvent dans l'arborescence de rubriques au niveau ou au-dessus du point de l'arborescence de rubriques auquel l'application s'est abonnée. Les vérifications des droits d'accès peuvent impliquer des vérifications sur plusieurs objets de rubrique.

L'ID utilisateur utilisé par le gestionnaire de files d'attente pour les vérifications des droits d'accès est l'ID utilisateur obtenu auprès du système d'exploitation lorsque l'application se connecte au gestionnaire de files d'attente.

Le gestionnaire de files d'attente effectue des vérifications des droits d'accès sur les files d'attente d'abonné, mais pas sur les files d'attente gérées.

Comment le contrôle d'accès est implémenté par IBM WebSphere MQ sur les systèmes UNIX, Linux, and Windows

IBM WebSphere MQ utilise les services de sécurité fournis par le système d'exploitation sous-jacent, à l'aide du gestionnaire des droits d'accès aux objets. IBM WebSphere MQ fournit des commandes pour créer et gérer des listes de contrôle d'accès.

Une interface de contrôle d'accès appelée Interface de service d'autorisation fait partie de WebSphere MQ. WebSphere MQ fournit une implémentation d'un gestionnaire de contrôle d'accès (conforme à l'interface de service d'autorisation) appelé *gestionnaire des droits d'accès aux objets (OAM)*. Il est automatiquement installé et activé pour chaque gestionnaire de files d'attente que vous créez, sauf indication contraire (comme décrit dans «Prévention des contrôles d'accès de sécurité sur les systèmes UNIX, Linux, and Windows», à la page 175). La méthode d'accès aux objets (OAM) peut être remplacée par tout composant écrit par un utilisateur ou un fournisseur conforme à l'interface de service d'autorisation.

La méthode d'accès aux objets (OAM) exploite les fonctions de sécurité du système d'exploitation sous-jacent, à l'aide des ID utilisateur et de groupe du système d'exploitation. Les utilisateurs ne peuvent accéder aux objets WebSphere MQ que s'ils disposent des droits appropriés. «Contrôle de l'accès aux objets à l'aide de la méthode d'accès aux objets (OAM) sur les systèmes UNIX, Linux et Windows», à la page 167 décrit comment accorder et révoquer ces droits.

La méthode d'accès aux objets (OAM) gère une liste de contrôle d'accès (ACL) pour chaque ressource qu'elle contrôle. Les données d'autorisation sont stockées dans une file d'attente locale appelée SYSTEM.AUTH.DATA.QUEUE. L'accès à cette file d'attente est limité aux utilisateurs du groupe mqm, ainsi qu'à Windows, aux utilisateurs du groupe Administrateurs et aux utilisateurs connectés avec l'ID SYSTEM. L'accès utilisateur à la file d'attente ne peut pas être modifié.

WebSphere MQ fournit des commandes permettant de créer et de gérer des listes de contrôle d'accès. Pour plus d'informations sur ces commandes, voir «Contrôle de l'accès aux objets à l'aide de la méthode d'accès aux objets (OAM) sur les systèmes UNIX, Linux et Windows», à la page 167.

WebSphere MQ transmet à la méthode d'accès aux objets (OAM) une demande contenant un principal, un nom de ressource et un type d'accès. La méthode d'accès aux objets (OAM) accorde ou rejette l'accès en fonction de la liste de contrôle d'accès qu'elle gère. WebSphere MQ suit la décision de la méthode d'accès aux objets (OAM) ; si la méthode d'accès aux objets (OAM) ne peut pas prendre de décision, WebSphere MQ n'autorise pas l'accès.

Identification de l'ID utilisateur sur les systèmes UNIX, Linux, and Windows

Le gestionnaire des droits d'accès aux objets identifie le principal qui demande l'accès à une ressource. L'ID utilisateur utilisé comme principal varie en fonction du contexte.

Le gestionnaire des droits d'accès aux objets (OAM) doit pouvoir identifier qui demande l'accès à une ressource particulière. IBM WebSphere MQ utilise le terme *principal* pour désigner cet identificateur. Le principal est établi lorsque l'application se connecte pour la première fois au gestionnaire de files d'attente ; il est déterminé par le gestionnaire de files d'attente à partir de l'ID utilisateur associé à l'application de connexion. (Si l'application émet des appels XA sans se connecter au gestionnaire de files d'attente, l'ID utilisateur associé à l'application qui émet l'appel xa_open est utilisé pour les vérifications des droits d'accès par le gestionnaire de files d'attente.)

Sur les systèmes UNIX and Linux , les routines d'autorisation vérifient l'ID utilisateur réel (loggedin) ou l'ID utilisateur effectif associé à l'application. L'ID utilisateur vérifié peut dépendre du type de liaison. Pour plus de détails, voir Services optionnels.

IBM WebSphere MQ propage l'ID utilisateur reçu du système dans l'en-tête de message (structure MQMD) de chaque message en tant qu'identification de l'utilisateur. Cet identificateur fait partie des informations de contexte de message et est décrit dans «Droits de contexte sur les systèmes UNIX, Linux et Windows», à la page 213. Les applications ne peuvent pas modifier ces informations sauf si elles ont été autorisées à modifier les informations de contexte.

Principaux et groupes

Les principaux peuvent appartenir à des groupes. Vous pouvez accorder l'accès à une ressource particulière à des groupes plutôt qu'à des individus, afin de réduire la quantité d'administration requise. Sur les systèmes UNIX and Linux , toutes les listes de contrôle d'accès (ACL) sont basées sur des groupes, mais sur les systèmes Windows , les listes de contrôle d'accès (ACLS) sont basées sur des ID utilisateur et des groupes.

Par exemple, vous pouvez définir un groupe composé d'utilisateurs qui souhaitent exécuter une application particulière. Les autres utilisateurs peuvent avoir accès à toutes les ressources dont ils ont besoin en ajoutant leur ID utilisateur au groupe approprié. Ce processus est décrit dans:

- Création et gestion de groupes sous Windows
- Création et gestion de groupes sous HP-UX
- Création et gestion de groupes sous AIX
- Création et gestion de groupes sous Solaris
- Création et gestion de groupes sur Linux

Un principal peut appartenir à plusieurs groupes (son ensemble de groupes). Il dispose de l'ensemble des droits accordés à chaque groupe de son groupe. Ces droits étant mis en cache, les modifications apportées à l'appartenance au groupe du principal ne sont pas reconnues tant que le gestionnaire de files d'attente n'est pas redémarré, sauf si vous émettez la commande MQSC REFRESH SECURITY (ou l'équivalent PCF).

Systèmes UNIX and Linux

Toutes les listes de contrôle d'accès sont basées sur des groupes. Lorsqu'un utilisateur est autorisé à accéder à une ressource particulière, le groupe principal de l'ID utilisateur est inclus dans la liste de contrôle d'accès. L'ID utilisateur individuel n'est pas inclus et des droits sont accordés à tous les membres de ce groupe. Pour cette raison, sachez que vous pouvez modifier par inadvertance les droits d'un principal en modifiant les droits d'un autre principal du même groupe. Tous les utilisateurs sont nominalement affectés au groupe d'utilisateurs par défaut *personne* et, par défaut, aucune autorisation n'est accordée à ce groupe. Vous pouvez modifier l'autorisation dans le groupe *personne* pour accorder l'accès aux ressources WebSphere MQ aux utilisateurs sans autorisation spécifique.

Ne définissez pas d'ID utilisateur avec la valeur "UNKNOWN". La valeur "UNKNOWN" est utilisée lorsqu'un ID utilisateur est trop long. Par conséquent, les ID utilisateur arbitraires utilisent les droits d'accès de UNKNOWN.

Les ID utilisateur peuvent contenir jusqu'à 12 caractères et les noms de groupe jusqu'à 12 caractères.

Systèmes Windows

Les listes de contrôle d'accès sont basées sur les ID utilisateur et les groupes. Les vérifications sont les mêmes que pour les systèmes UNIX , sauf que des ID utilisateur individuels peuvent également être affichés dans la liste de contrôle d'accès. Vous pouvez avoir différents utilisateurs sur différents domaines avec le même ID utilisateur. WebSphere MQ permet aux ID utilisateur d'être qualifiés par un nom de domaine afin que ces utilisateurs puissent disposer de différents niveaux d'accès.

Le nom de groupe peut éventuellement inclure un nom de domaine, spécifié dans les formats suivants:

```
GroupName@domain
domain\GroupName
```

Les groupes globaux sont vérifiés par la méthode d'accès aux objets (OAM) dans deux cas uniquement:

1. La section de sécurité du gestionnaire de files d'attente inclut le paramètre: `GroupModel=GlobalGroups`; voir Sécurité.
2. Le gestionnaire de files d'attente utilise un autre groupe d'accès de sécurité ; voir **crtmqm**.

Les ID utilisateur peuvent contenir jusqu'à 20 caractères, les noms de domaine jusqu'à 15 caractères et les noms de groupe jusqu'à 64 caractères.

La méthode d'accès aux objets (OAM) vérifie d'abord la base de données de sécurité locale, puis la base de données du domaine principal, et enfin la base de données des domaines de confiance. Le premier ID utilisateur rencontré est utilisé par la méthode d'accès aux objets (OAM) pour la vérification. Chacun de ces ID utilisateur peut avoir des appartenances de groupe différentes sur un ordinateur particulier.

Certaines commandes de contrôle (par exemple, `crtmqm`) modifient les droits sur les objets WebSphere MQ à l'aide du gestionnaire des droits d'accès aux objets (OAM). La méthode d'accès aux objets (OAM) recherche les bases de données de sécurité dans l'ordre indiqué dans le paragraphe précédent afin de déterminer les droits d'accès pour un ID utilisateur particulier. Par conséquent, les droits d'accès déterminés par la méthode d'accès aux objets (OAM) peuvent remplacer le fait qu'un ID utilisateur soit membre du groupe mqm local. Par exemple, si vous émettez la commande `crtmqm` à partir d'un ID utilisateur authentifié par un contrôleur de domaine qui est membre du groupe mqm local via un groupe global, la commande échoue si le système possède un utilisateur local du même nom qui ne fait pas partie du groupe mqm local.

Identificateurs de sécurité (SID) Windows

WebSphere MQ sous Windows utilise le SID où il est disponible. Si un SID Windows n'est pas fourni avec une demande d'autorisation, WebSphere MQ identifie l'utilisateur en fonction du nom d'utilisateur seul, mais cela peut entraîner l'octroi de droits d'accès incorrects.

Sur les systèmes Windows , l'identificateur de sécurité (SID) est utilisé en complément de l'ID utilisateur. Le SID contient des informations qui identifient les détails complets du compte utilisateur sur la base de données du gestionnaire de compte de sécurité (SAM) Windows dans laquelle l'utilisateur est défini. Lorsqu'un message est créé dans WebSphere MQ for Windows, WebSphere MQ stocke le SID dans le descripteur de message. Lorsque WebSphere MQ sous Windows effectue des vérifications d'autorisation, il utilise le SID pour interroger les informations complètes de la base de données SAM. (La base de données SAM dans laquelle l'utilisateur est défini doit être accessible pour que cette requête aboutisse.)

Par défaut, si un SID Windows n'est pas fourni avec une demande d'autorisation, WebSphere MQ identifie l'utilisateur en fonction du nom d'utilisateur uniquement. Pour ce faire, il effectue des recherches dans les bases de données de sécurité dans l'ordre suivant:

1. Base de données de sécurité locale
2. Base de données de sécurité du domaine principal
3. Base de données de sécurité des domaines de confiance

Si le nom d'utilisateur n'est pas unique, des droits WebSphere MQ incorrects peuvent être accordés. Pour éviter ce problème, incluez un SID dans chaque demande d'autorisation ; le SID est utilisé par WebSphere MQ pour établir les données d'identification de l'utilisateur.

Pour indiquer que toutes les demandes d'autorisation doivent inclure un SID, utilisez `regedit`. Définissez SecurityPolicy sur NTSIDsRequired.

Droits d'utilisateur de remplacement sur les systèmes UNIX, Linux et Windows

Vous pouvez indiquer qu'un ID utilisateur peut utiliser les droits d'un autre utilisateur lors de l'accès à un objet WebSphere MQ . Il s'agit du *droit d'utilisateur de remplacement*et vous pouvez l'utiliser sur n'importe quel objet WebSphere MQ .

Les droits d'utilisateur de remplacement sont essentiels lorsqu'un serveur reçoit des demandes d'un programme et souhaite s'assurer que le programme dispose des droits requis pour la demande. Le serveur peut disposer des droits requis, mais il doit savoir si le programme dispose des droits requis pour les actions qu'il a demandées.

Par exemple, supposons qu'un programme serveur s'exécutant sous l'ID utilisateur PAYSERV extrait un message de demande d'une file d'attente qui a été placée dans la file d'attente par l'ID utilisateur USER1. Lorsque le programme serveur obtient le message de demande, il traite la demande et insère la réponse dans la file d'attente de réponse spécifiée dans le message de demande. Au lieu d'utiliser son propre ID utilisateur (PAYSERV) pour autoriser l'ouverture de la file d'attente de réponse, le serveur peut spécifier un ID utilisateur différent, dans ce cas, USER1. Dans cet exemple, vous pouvez utiliser les droits d'utilisateur de remplacement pour contrôler si PAYSERV est autorisé à spécifier USER1 comme ID utilisateur de remplacement lorsqu'il ouvre la file d'attente de réponse.

L'ID utilisateur de remplacement est indiqué dans la zone **`AlternateUserId`** du descripteur d'objet.

Droits de contexte sur les systèmes UNIX, Linux et Windows

Le contexte est une information qui s'applique à un message particulier et qui est contenue dans le descripteur de message, MQMD, qui fait partie du message. Les applications peuvent spécifier les données contextuelles lorsqu'un appel MQOPEN ou MQPUT est effectué.

Les informations contextuelles comportent deux sections :

La section d'identité
D'où vient le message. Il se compose des zones UserIdentifier, AccountingTokenet ApplIdentityData .

Section d'origine
D'où provient le message et quand il a été placé dans la file d'attente. Il se compose des zones PutApplType, PutApplName, PutDate, PutTimeet ApplOriginData .

Les applications peuvent spécifier les données contextuelles lorsqu'un appel MQOPEN ou MQPUT est effectué. Ces données peuvent être générées par l'application, transmises à partir d'un autre message ou générées par le gestionnaire de files d'attente par défaut. Par exemple, les données contextuelles peuvent être utilisées par les programmes serveur pour vérifier l'identité du demandeur, en vérifiant si le message provient d'une application s'exécutant sous un ID utilisateur autorisé.

Un programme serveur peut utiliser le UserIdentifier pour déterminer l'ID utilisateur d'un autre utilisateur. Vous utilisez l'autorisation de contexte pour contrôler si l'utilisateur peut spécifier l'une des options de contexte dans n'importe quel appel MQOPEN ou MQPUT1 .

Voir Contrôle des informations de contexte pour plus d'informations sur les options de contexte et Présentation de MQMD pour obtenir des descriptions des zones de descripteur de message relatives au contexte.

Implémentation du contrôle d'accès dans les exits de sécurité

Vous pouvez implémenter le contrôle d'accès dans un exit de sécurité à l'aide de MCAUserIdentifier ou du gestionnaire des droits d'accès aux objets.

MCAUserIdentifier

Chaque instance d'un canal en cours est associée à une structure de définition de canal, MQCD. Les valeurs initiales des zones dans MQCD sont déterminées par la définition de canal créée par un administrateur WebSphere MQ . En particulier, la valeur initiale de l'une des zones, *MCAUserIdentifier*, est déterminée par la valeur du paramètre MCAUSER dans la commande DEFINE CHANNEL ou par l'équivalent de MCAUSER si la définition de canal est créée d'une autre manière. *MCAUserIdentifier* contient les 12 premiers octets de l'identificateur utilisateur MCA. Si l'ID utilisateur MCA n'est pas vide, il indique l'ID utilisateur à utiliser par l'agent MCA pour l'autorisation d'accès aux ressources MQ . Vérifiez que la valeur de MCAUSER est inférieure à 12 caractères sur la plateforme Windows.

La structure MQCD est transmise à un programme d'exit de canal lorsqu'elle est appelée par un agent MCA. Lorsqu'un exit de sécurité est appelé par un agent MCA, l'exit de sécurité peut modifier la valeur de *MCAUserIdentifier*, en remplaçant toute valeur spécifiée dans la définition de canal.

Sur les systèmes IBM i, UNIX, Linux et Windows , sauf si la valeur de *MCAUserIdentifier* est vide, le gestionnaire de files d'attente utilise la valeur de *MCAUserIdentifier* comme ID utilisateur pour les vérifications des droits d'accès lorsqu'un agent MCA tente d'accéder aux ressources du gestionnaire de files d'attente après s'être connecté au gestionnaire de files d'attente. Si la valeur de *MCAUserIdentifier* est vide, le gestionnaire de files d'attente utilise à la place l'ID utilisateur par défaut de l'agent MCA. Cela s'applique aux canaux RCVR, RQSTR, CLUSRCVR et SVRCONN. Pour l'envoi d'agents MCA, l'ID utilisateur par défaut est toujours utilisé pour les vérifications des droits d'accès, même si la valeur de *MCAUserIdentifier* n'est pas vide.

Sous z/OS, le gestionnaire de files d'attente peut utiliser la valeur de *MCAUserIdentifier* pour les vérifications des droits d'accès, à condition qu'elle ne soit pas vide. Pour la réception des MCM et des MCM de connexion au serveur, le fait que le gestionnaire de files d'attente utilise ou non la valeur de *MCAUserIdentifier* pour les vérifications des droits d'accès dépend des éléments suivants:

- Valeur du paramètre PUTAUT dans la définition de canal
- Profil RACF utilisé pour les vérifications
- Niveau d'accès de l'ID utilisateur de l'espace adresse de l'initiateur de canal au profil RESLEVEL

Pour l'envoi des MCM, il dépend des éléments suivants:

- Indique si l'agent MCA émetteur est un appelant ou un répondeur
- Niveau d'accès de l'ID utilisateur de l'espace adresse de l'initiateur de canal au profil RESLEVEL

L'ID utilisateur stocké par un exit de sécurité dans *MCAUserIdentifier* peut être acquis de différentes manières. Voici quelques exemples :

- S'il n'existe pas d'exit de sécurité à l'extrémité client d'un canal MQI, un ID utilisateur associé à l'application client WebSphere MQ passe de l'agent MCA de la connexion client à l'agent MCA de la connexion serveur lorsque l'application client émet un appel MQCONN.L'agent MCA de connexion serveur stocke cet ID utilisateur dans la zone *RemoteUserIdentifier* de la structure de définition de canal, MQCD. Si la valeur de *MCAUserIdentifier* est vide à ce stade, l'agent MCA stocke le même ID utilisateur dans *MCAUserIdentifier*. Si l'agent MCA ne stocke pas l'ID utilisateur dans *MCAUserIdentifier*, un exit de sécurité peut le faire ultérieurement en affectant à *MCAUserIdentifier* la valeur *RemoteUserIdentifier*.

  Si l'ID utilisateur qui provient du système client entre dans un nouveau domaine de sécurité et n'est pas valide sur le système serveur, l'exit de sécurité peut remplacer l'ID utilisateur par un ID utilisateur valide et stocker l'ID utilisateur remplacé dans *MCAUserIdentifier*.
- L'ID utilisateur peut être envoyé par l'exit de sécurité partenaire dans un message de sécurité.

  Sur un canal de transmission de messages, un exit de sécurité appelé par l'agent MCA émetteur peut envoyer l'ID utilisateur sous lequel l'agent MCA émetteur s'exécute. Un exit de sécurité appelé par l'agent MCA récepteur peut ensuite stocker l'ID utilisateur dans *MCAUserIdentifier*. De même, sur un canal MQI, un exit de sécurité à l'extrémité client du canal peut envoyer l'ID utilisateur associé à l'application client WebSphere MQ MQI. Un exit de sécurité à l'extrémité serveur du canal peut ensuite stocker l'ID utilisateur dans *MCAUserIdentifier*. Comme dans l'exemple précédent, si l'ID utilisateur n'est pas valide sur le système cible, l'exit de sécurité peut remplacer l'ID utilisateur par un ID utilisateur valide et stocker l'ID utilisateur remplacé dans *MCAUserIdentifier*.

  Si un certificat numérique est reçu dans le cadre du service d'identification et d'authentification, un exit de sécurité peut mapper le nom distinctif du certificat à un ID utilisateur valide sur le système cible. Il peut ensuite stocker l'ID utilisateur dans *MCAUserIdentifier*.
- Si SSL est utilisé sur le canal, le nom distinctif (DN) du partenaire est transmis à l'exit dans la zone Ptr SSLPeerNamede MQCD, et le nom distinctif de l'émetteur de ce certificat est transmis à l'exit dans la zone Ptr SSLRemCertIssNamede MQCXP.

Pour plus d'informations sur la zone *MCAUserIdentifier* , la structure de définition de canal, MQCD et la structure de paramètre d'exit de canal, MQCXP, voir Appels d'exit de canal et structures de données. Pour plus d'informations sur l'ID utilisateur qui provient d'un système client sur un canal MQI, voir Contrôle d'accès.

Remarque : Les applications d'exit de sécurité construites avant l'édition de WebSphere MQ v7.1 peuvent nécessiter une mise à jour. Pour plus d'informations, voir Programmes d'exit de sécurité de canal.

WebSphere MQ Authentification des utilisateurs du gestionnaire des droits d'accès aux objets

Sur les connexions client WebSphere MQ MQI, les exits de sécurité peuvent être utilisés pour modifier ou créer la structure MQCSP utilisée dans l'authentification d'utilisateur du gestionnaire des droits d'accès aux objets (OAM). Ceci est décrit dans Programmes d'exit de canal pour les canaux de messagerie

Implémentation du contrôle d'accès dans les exits de message

Vous devrez peut-être utiliser un exit de message pour remplacer un ID utilisateur par un autre.

Prenons l'exemple d'une application client qui envoie un message à une application serveur. L'application serveur peut extraire l'ID utilisateur de la zone *UserIdentifier* du descripteur de message et, à condition qu'elle dispose de droits d'utilisateur de remplacement, demander au gestionnaire de files d'attente d'utiliser cet ID utilisateur pour les vérifications de droits d'accès lorsqu'il accède aux ressources WebSphere MQ pour le compte du client.

Si le paramètre PUTAUT est défini sur CTX (ou ALTMCA sur z/OS) dans la définition de canal, l'ID utilisateur dans la zone *UserIdentifier* de chaque message entrant est utilisé pour les vérifications des droits d'accès lorsque l'agent MCA ouvre la file d'attente de destination.

Dans certains cas, lorsqu'un message de rapport est généré, il est placé à l'aide des droits de l'ID utilisateur dans la zone *UserIdentifier* du message à l'origine du rapport. En particulier, les rapports de confirmation à la livraison (COD) et les rapports d'expiration sont toujours soumis à cette autorité.

En raison de ces situations, il peut être nécessaire de remplacer un ID utilisateur par un autre dans la zone *UserIdentifier* lorsqu'un message entre dans un nouveau domaine de sécurité. Ceci peut être réalisé par un exit de message à l'extrémité réceptrice du canal. Vous pouvez également vous assurer que l'ID utilisateur dans la zone *UserIdentifier* d'un message entrant est défini dans le nouveau domaine de sécurité.

Si un message entrant contient un certificat numérique pour l'utilisateur de l'application qui a envoyé le message, un exit de message peut valider le certificat et mapper le nom distinctif du certificat à un ID utilisateur valide sur le système de réception. Il peut ensuite définir la zone *UserIdentifier* du descripteur de message sur cet ID utilisateur.

S'il est nécessaire qu'un exit de message modifie la valeur de la zone *UserIdentifier* dans un message entrant, il peut être approprié que l'exit de message authentifie l'expéditeur du message en même temps. Pour plus de détails, voir «Mappage d'identité dans les exits de message», à la page 155.

Implémentation du contrôle d'accès dans l'exit d'API et l'exit de croisement d'API

Une API ou un exit de croisement d'API peut fournir des contrôles d'accès pour compléter ceux fournis par WebSphere MQ. En particulier, l'exit peut fournir un contrôle d'accès au niveau du message. L'exit peut s'assurer qu'une application insère dans une file d'attente, ou extrait d'une file d'attente, uniquement les messages qui répondent à certains critères.

Prenons les exemples suivants :

- Un message contient des informations sur une commande. Lorsqu'une application tente d'insérer un message dans une file d'attente, une API ou un exit de croisement d'API peut vérifier que la valeur totale de la commande est inférieure à une limite prescrite.
- Les messages arrivent dans une file d'attente de destination à partir de gestionnaires de files d'attente éloignées. Lorsqu'une application tente d'extraire un message de la file d'attente, une API ou un exit de croisement d'API peut vérifier que l'expéditeur du message est autorisé à envoyer un message à la file d'attente.

Confidentialité des messages

Pour préserver la confidentialité, chiffrez vos messages. Il existe différentes méthodes de chiffrement des messages dans WebSphere MQ en fonction de vos besoins.

Votre choix de CipherSpec détermine le niveau de confidentialité dont vous disposez.

Si vous avez besoin d'une protection des données de bout en bout au niveau de l'application pour votre infrastructure de messagerie point à point, vous pouvez utiliser WebSphere MQ Advanced Message Security pour chiffrer les messages ou écrire votre propre exit d'API ou exit de croisement d'API.

Si vous devez chiffrer les messages uniquement lorsqu'ils sont transportés via un canal, car vous disposez d'une sécurité adéquate sur vos gestionnaires de files d'attente, vous pouvez utiliser SSL ou TLS, ou vous pouvez écrire votre propre exit de sécurité, exit de message, ou envoyer et recevoir des programmes d'exit.

Pour plus d'informations sur WebSphere MQ Advanced Message Security, voir «Planification pour Advanced Message Security», à la page 67.L'utilisation de SSL et TLS avec WebSphere MQ est décrite à l'adresse «Prise en charge de IBM WebSphere MQ pour SSL et TLS», à la page 24. L'utilisation des programmes d'exit dans le chiffrement des messages est décrite à l'adresse «Implémentation de la confidentialité dans les programmes d'exit utilisateur», à la page 235.

Connexion de deux gestionnaires de files d'attente via le protocole SSL ou TLS

Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

Pour configurer votre installation SSL ou TLS, vous devez définir vos canaux pour utiliser les protocoles SSL ou TLS. Vous devez également obtenir et gérer vos certificats numériques. Sur un système de test, vous pouvez utiliser des certificats autosignés ou des certificats émis par une autorité de certification locale. Sur un système de production, n'utilisez pas de certificats autosignés. Pour plus d'informations, voir ..//zs14140_.dita.

Pour plus d'informations sur la création et la gestion des certificats, voir «Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows», à la page 119.

Les rubriques suivantes présentent les tâches de configuration des communications SSL et donnent des instructions détaillées sur la réalisation de ces tâches.

Vous pouvez également vouloir tester l'authentification des clients SSL ou TLS, qui constitue une partie facultative des protocoles. Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation WebSphere MQ , le serveur SSL ou TLS demande toujours un certificat au client.

Remarques :

1. Dans ce contexte, un client SSL se réfère à la connexion initiant l'établissement de liaison.
2. Pour plus d'informations, voir le Glossaire .

Sur les systèmes UNIX, Linux et Windows , le client SSL ou TLS envoie un certificat uniquement s'il en possède un libellé au format WebSphere MQ correct, qui est `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente remplacé par des minuscules. Par exemple, pour `QM1`, `ibmwebspheremqqm1`.

WebSphere MQ utilise le préfixe `ibmwebspheremq` sur un libellé pour éviter toute confusion avec les certificats d'autres produits. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie aucun certificat, l'authentification échoue uniquement si la fin du canal qui agit comme serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur du paramètre SSLPEER déterminée. Pour plus d'informations sur la connexion anonyme d'un gestionnaire de files d'attente, c'est-à-dire lorsque le client SSL ou TLS n'envoie pas de certificat, voir «Connexion de deux gestionnaires de files d'attente à l'aide de l'authentification unidirectionnelle», à la page 220.

Utilisation de certificats autosignés pour l'authentification mutuelle de deux gestionnaires de file d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre deux gestionnaires de files d'attente à l'aide de certificats TLS ou SSL autosignés.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez de deux gestionnaires de files d'attente appelés QM1 et QM2, qui ont besoin de communiquer de façon sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre QM1 et QM2.
- Vous avez décidé de tester votre communication sécurisée en utilisant des certificats autosignés.

La configuration qui en résulte se présente comme suit :

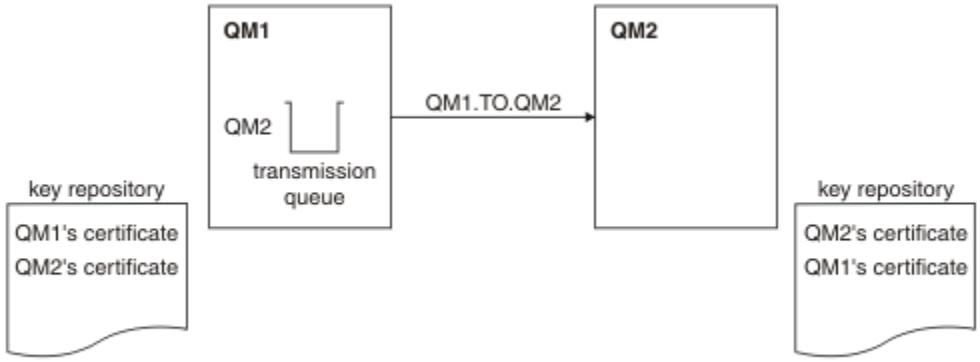


Figure 14. Configuration obtenue

Dans la Figure 14, à la page 217, le référentiel de clés de QM1 contient le certificat de QM1 et le certificat public de QM2. Le référentiel de clés de QM2 contient le certificat de QM2 et le certificat public de QM1.

Procédure

1. Préparez le référentiel de clés de chaque gestionnaire de files d'attente en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Créez un certificat autosigné pour chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
3. Procédez à l'extraction d'une copie de chaque certificat :
   - Sur les systèmes UNIX, Linuxet Windows.
4. Transférez la partie publique du certificat QM1 vers le système QM2 et inversement, à l'aide d'un utilitaire tel que FTP.
5. Ajoutez le certificat partenaire au référentiel de clés de chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
6. Sur QM1, définissez un canal émetteur et une file d'attente de transmission associée en exécutant des commandes similaires à l'exemple suivant :

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
   SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

   DEFINE QLOCAL(QM2) USAGE(XMITQ)
   ```

   Cet exemple utilise CipherSpec RC4_MD5. Le CipherSpec doit être le même à chaque extrémité du canal.
7. Sur QM2, définissez un canal récepteur en émettant une commande similaire à l'exemple suivant :

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
   ```

   Le canal doit porter le même nom que le canal émetteur que vous avez défini à l'étape 6, et utiliser le même CipherSpec.
8. Démarrez le canal.

Résultats

Les référentiels de clés et les canaux sont créés comme illustré dans Figure 14, à la page 217.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

A partir du gestionnaire de files d'attente QM2, entrez la commande suivante :

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Dans chaque cas, la valeur de SSLPEER doit correspondre à celle du nom distinctif dans le certificat partenaire créé à l'étape 2. Le nom de l'émetteur correspond au nom de l'homologue car le certificat est autosigné.

SSLPEER est facultatif. S'il est indiqué, sa valeur doit être définie de telle sorte que le nom distinctif dans le certificat partenaire (créé à l'étape 2) soit autorisé. Pour plus d'informations sur l'utilisation de SSLPEER, voir WebSphere MQ rules for SSLPEER values .

Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle de deux gestionnaires de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre deux gestionnaires de files d'attente à l'aide de certificats TLS ou SSL signés par l'autorité de certification.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez de deux gestionnaires de files d'attente appelés QMA et QMB, qui ont besoin de communiquer de façon sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre QMA et QMB.

- A l'avenir, vous envisagez d'utiliser ce réseau dans un environnement de production et vous avez donc décidé d'employer des certificats signés par l'autorité de certification dès le début.

La configuration qui en résulte se présente comme suit :

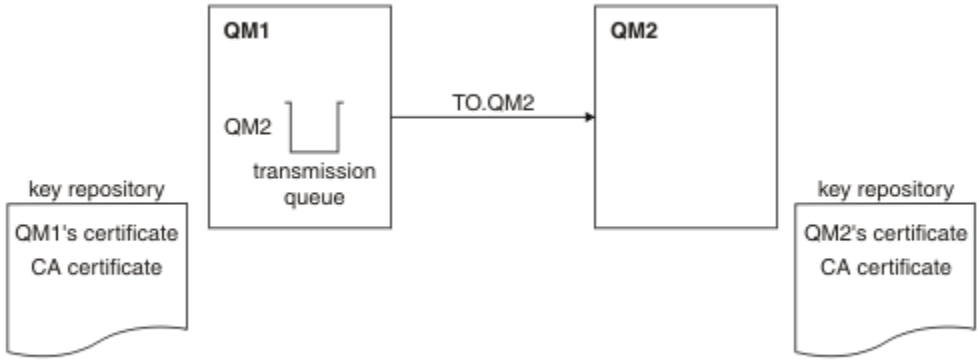


Figure 15. Configuration obtenue

Dans la Figure 15, à la page 219, le référentiel de clés de QMA contient le certificat de QMA et le certificat de l'autorité de certification. Le référentiel de clés de QMB contient le certificat de QMB et le certificat de l'autorité de certification. Dans cet exemple, le certificat de QMA et le certificat de QMB ont été émis par la même autorité de certification. Si le certificat de QMA et le certificat de QMB ont été émis par des autorités de certification différentes, les référentiels de clés de QMA et de QMB doivent contenir les certificats des deux autorités de certification.

Procédure

1. Préparez le référentiel de clés de chaque gestionnaire de files d'attente en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Demandez un certificat signé par l'autorité de certification pour chaque gestionnaire de files d'attente.

   Vous pourriez utiliser des autorités de certification différentes pour les deux gestionnaires de files d'attente.
   - Sur les systèmes UNIX, Linuxet Windows.
3. Ajoutez le certificat de l'autorité de certification au référentiel de clés de chaque gestionnaire de files d'attente :

   Si les gestionnaires de files d'attente utilisent des autorités de certification différentes, le certificat de l'autorité de certification de chaque autorité de certification doit être ajouté dans chacun des référentiels de clés.
   - Sur les systèmes UNIX, Linuxet Windows.
4. Ajoutez le certificat signé par l'autorité de certification au référentiel de clés de chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
5. Sur QMA, définissez un canal émetteur et une file d'attente de transmission associée en exécutant des commandes similaires à l'exemple suivant :

   ```
   DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
   SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

   DEFINE QLOCAL(QMB) USAGE(XMITQ)
   ```

   Cet exemple utilise CipherSpec RC4_MD5. Le CipherSpec doit être le même à chaque extrémité du canal.

6. Sur QMB, définissez un canal récepteur en exécutant une commande similaire à l'exemple suivant :

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
```

   Le canal doit porter le même nom que le canal émetteur que vous avez défini à l'étape 6, et utiliser le même CipherSpec.
7. Démarrez le canal :

Résultats

Les référentiels de clés et les canaux sont créés comme indiqué dans la Figure 15, à la page 219.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QMA, entrez la commande suivante :

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

A partir du gestionnaire de files d'attente QMB, entrez la commande suivante :

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Dans chaque cas, la valeur de SSLPEER doit correspondre à celle du nom distinctif (DN) dans le certificat partenaire créé à l'étape 2. Le nom de l'émetteur correspond au DN de l'objet du certificat de l'autorité de certification qui a signé le certificat personnel ajouté à l'étape 4.

Connexion de deux gestionnaires de files d'attente à l'aide de l'authentification unidirectionnelle

Suivez les instructions de cet exemple pour modifier un système avec l'authentification mutuelle afin d'autoriser un gestionnaire de files d'attente à se connecter à l'aide de l'authentification unidirectionnelle à un autre gestionnaire de files d'attente, à savoir lorsque le client SSL ou TLS n'envoie pas de certificat.

Pourquoi et quand exécuter cette tâche

Scénario :

- Les deux gestionnaires de files d'attente (QM1 et QM2) ont été configurés comme illustré dans la «Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle de deux gestionnaires de files d'attente», à la page 218.
- Vous souhaitez modifier QM1 pour qu'il se connecte à l'aide de l'authentification unidirectionnelle à QM2.

La configuration qui en résulte se présente comme suit :

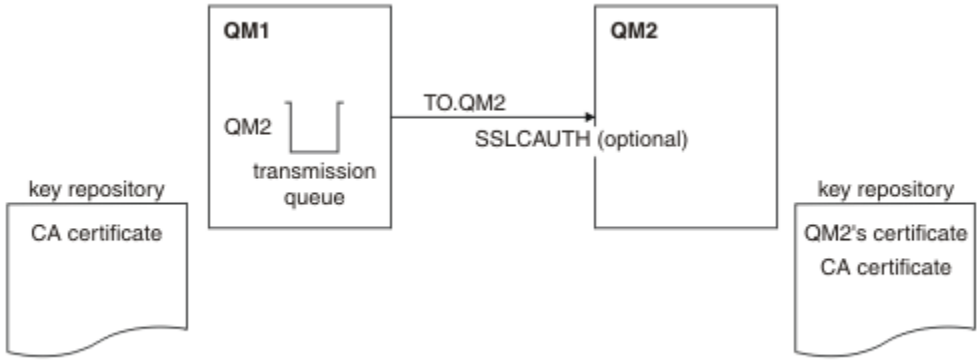


Figure 16. Gestionnaires de files d'attente autorisant l'authentification unidirectionnelle

Procédure

1. Supprimez le certificat personnel de QM1de son référentiel de clés, en fonction du système d'exploitation:
   - Sur les systèmes UNIX, Linuxet Windows. Le certificat est libellé comme suit:
     - `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour `QM1` , `ibmwebspheremqqm1`.
2. Facultatif : Sur QM1, si des canaux SSL ou TLS ont été exécutés précédemment, actualisez l'environnement SSL ou TLS.
3. Autorisez les connexions anonymes sur le récepteur.

Résultats

Les référentiels de clés et les canaux sont modifiés comme illustré dans la Figure 16, à la page 221.

Que faire ensuite

Si le canal émetteur était en cours d'exécution et que vous avez émis la commande REFRESH SECURITY TYPE(SSL) (à l'étape 2), le canal redémarre automatiquement. Si le canal émetteur n'était pas en cours d'exécution, démarrez-le.

A l'extrémité serveur du canal, la présence de la valeur de paramètre du nom d'homologue sur le statut de canal indique qu'un certificat client a été transmis.

Vérifiez que la tâche a abouti en exécutant certaines commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après :

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

A partir du gestionnaire de files d'attente QM2, entrez la commande suivante :

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

Sur QM2, la zone SSLPEER est vide, ce qui indique que QM1 n'a pas envoyé de certificat. Sur QM1, la valeur de SSLPEER correspond à celle du nom distinctif dans le certificat personnel de QM2.

Connexion sécurisée d'un client à un gestionnaire de files d'attente

Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

Pour configurer votre installation SSL ou TLS, vous devez définir vos canaux pour utiliser les protocoles SSL ou TLS. Vous devez également obtenir et gérer vos certificats numériques. Sur un système de test, vous pouvez utiliser des certificats autosignés ou des certificats émis par une autorité de certification locale. Sur un système de production, n'utilisez pas de certificats autosignés. Pour plus d'informations, voir ..//zs14140_.dita.

Pour plus d'informations sur la création et la gestion des certificats, voir «Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows», à la page 119.

Les rubriques suivantes présentent les tâches de configuration des communications SSL et donnent des instructions détaillées sur la réalisation de ces tâches.

Vous pouvez également vouloir tester l'authentification des clients SSL ou TLS, qui constitue une partie facultative des protocoles. Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation WebSphere MQ , le serveur SSL ou TLS demande toujours un certificat au client.

Sur les systèmes UNIX, Linux, and Windows , le client SSL ou TLS envoie un certificat uniquement s'il en a un libellé au format WebSphere MQ correct, qui est `ibmwebspheremq` suivi de votre ID utilisateur de connexion modifié en minuscules, par exemple `ibmwebspheremqmyuserid`.

WebSphere MQ utilise le préfixe `ibmwebspheremq` sur un libellé pour éviter toute confusion avec les certificats d'autres produits. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie aucun certificat, l'authentification échoue uniquement si la fin du canal qui agit comme serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur du paramètre SSLPEER

déterminée. Pour plus d'informations sur la connexion anonyme d'un gestionnaire de files d'attente, voir «Connexion anonyme d'un client à un gestionnaire de files d'attente», à la page 226.

Utilisation de certificats autosignés pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre un client et un gestionnaire de files d'attente à l'aide de certificats SSL ou TLS autosignés.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez d'un client, C1, et d'un gestionnaire de files d'attente, QM1, qui doivent communiquer de manière sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre C1 et QM1.
- Vous avez décidé de tester votre communication sécurisée en utilisant des certificats autosignés.

DCM sur IBM i ne prend pas en charge les certificats autosignés. Cette tâche ne s'applique donc pas aux systèmes IBM i.

La configuration qui en résulte se présente comme suit :

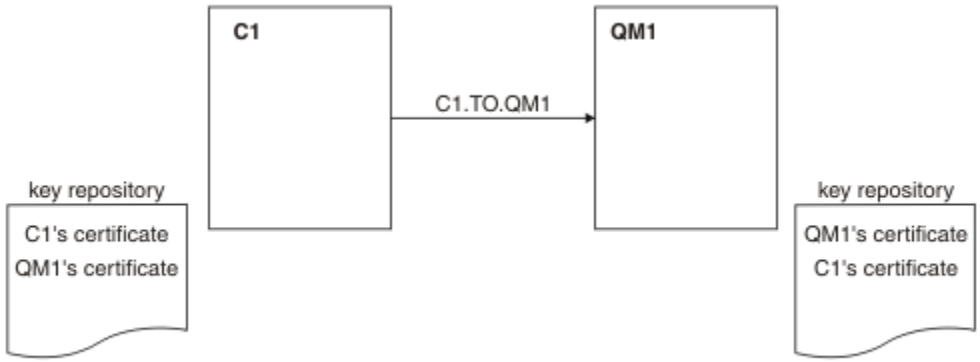


Figure 17. Configuration obtenue

Dans la Figure 17, à la page 223, le référentiel de clés de QM1 contient le certificat de QM1 et le certificat public de C1. Le référentiel de clés de C1 contient le certificat de C1 et le certificat public de QM1.

Procédure

1. Préparez le référentiel de clés sur le client et sur le gestionnaire de files d'attente, en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Créez les certificats autosignés pour le client et le gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
3. Procédez à l'extraction d'une copie de chaque certificat :
   - Sur les systèmes UNIX, Linuxet Windows.
4. Transférez la partie publique du certificat C1 vers le système QM1 et inversement, à l'aide d'un utilitaire tel que FTP.
5. Ajoutez le certificat partenaire dans le référentiel de clés du client et du gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
6. Exécutez la commande REFRESH SECURITY TYPE (SSL) sur le gestionnaire de files d'attente.

7. Définissez un canal de connexion client en procédant de l'une des deux manières suivantes :
   - Utilisation de l'appel MQCONNX avec la structure MQSCO sur C1, comme décrit dans Création d'un canal de connexion client sur le client WebSphere MQ MQI.
   - Utilisation d'une table de définition de canal du client, comme décrit dans Création de définitions de connexion serveur et de connexion client sur le serveur .
8. Sur QM1, définissez un canal de connexion serveur en émettant une commande similaire à l'exemple suivant :

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Le canal doit porter le même nom que le canal de connexion client que vous avez défini à l'étape 6, et utiliser le même CipherSpec.

Résultats

Les référentiels de clés et les canaux sont créés comme illustré dans la Figure 17, à la page 223

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Le paramétrage de l'attribut de filtre SSLPEER des définitions de canal est facultatif. Si la définition de canal SSLPEER est définie, sa valeur doit correspondre au nom distinctif du sujet dans le certificat partenaire créé à l'étape 2. Une fois la connexion établie, la zone SSLPEER de la sortie DISPLAY CHSTATUS affiche le nom distinctif du sujet du certificat client distant.

Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre un client et un gestionnaire de files d'attente à l'aide de certificats SSL ou TLS signés par l'autorité de certification.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez d'un client, C1, et d'un gestionnaire de files d'attente, QM1, qui doivent communiquer de manière sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre C1 et QM1.
- A l'avenir, vous envisagez d'utiliser ce réseau dans un environnement de production et vous avez donc décidé d'employer des certificats signés par l'autorité de certification dès le début.

La configuration qui en résulte se présente comme suit :

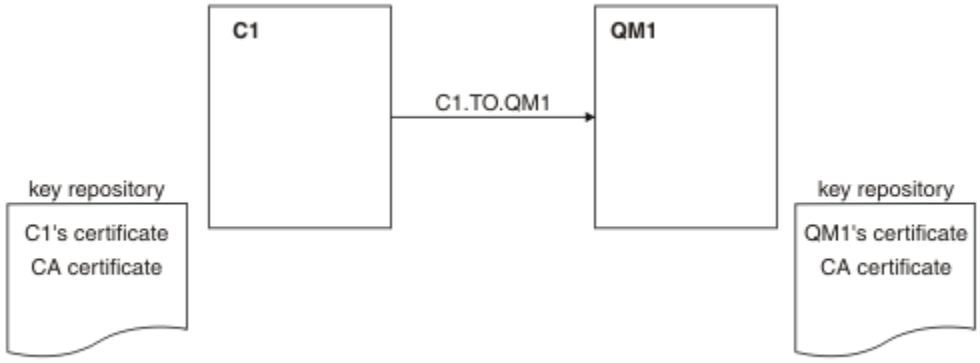


Figure 18. Configuration obtenue

Dans la Figure 18, à la page 225, le référentiel de clés de C1 contient le certificat de C1 et le certificat de l'autorité de certification. Le référentiel de clés de QM1 contient le certificat de QM1 et le certificat de l'autorité de certification. Dans cet exemple, les certificats de C1 et de QM1 ont été émis par la même autorité de certification. S'ils avaient été émis par des autorités de certification différentes, les référentiels de clés de C1 et de QM1 auraient dû inclure les certificats des deux autorités de certification.

Procédure

1. Préparez le référentiel de clés sur le client et sur le gestionnaire de files d'attente, en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Demandez le certificat signé par l'autorité de certification pour le client et le gestionnaire de files d'attente.

   Vous pourriez utiliser des autorités de certification différentes pour le client et le gestionnaire de files d'attente.
   - Sur les systèmes UNIX, Linuxet Windows.
3. Ajoutez le certificat de l'autorité de certification au référentiel de clés du client et du gestionnaire de files d'attente.

   Si le client et le gestionnaire de files d'attente utilisent des autorités de certification différentes, le certificat de chaque autorité de certification doit être ajouté aux deux référentiels de clés.
   - Sur les systèmes UNIX, Linuxet Windows.
4. Ajoutez le certificat signé par l'autorité de certification au référentiel de clés du client et du gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
5. Définissez un canal de connexion client en procédant de l'une des deux manières suivantes :
   - Utilisation de l'appel MQCONNX avec la structure MQSCO sur C1, comme décrit dans Création d'un canal de connexion client sur le client WebSphere MQ MQI.
   - Utilisation d'une table de définition de canal du client, comme décrit dans Création de définitions de connexion serveur et de connexion client sur le serveur .
6. Sur QM1, définissez un canal de connexion serveur en émettant une commande similaire à l'exemple suivant :

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Le canal doit porter le même nom que le canal de connexion client que vous avez défini à l'étape 6, et utiliser le même CipherSpec.

Résultats

Les référentiels de clés et les canaux sont créés comme indiqué dans la Figure 18, à la page 225.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Le champ SSLPEER de la sortie DISPLAY CHSTATUS affiche le DN de sujet du certificat client distant créé à l'étape 2. Le nom de l'émetteur correspond au DN de l'objet du certificat de l'autorité de certification qui a signé le certificat personnel ajouté à l'étape 4.

Connexion anonyme d'un client à un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour modifier un système avec l'authentification mutuelle afin d'autoriser un gestionnaire de files d'attente à se connecter anonymement à un autre gestionnaire de files d'attente.

Pourquoi et quand exécuter cette tâche

Scénario :

- Le gestionnaire de files d'attente et le client (QM1 et C1) ont été configurés comme dans la «Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente», à la page 224.
- Vous souhaitez modifier C1 pour qu'il se connecte de manière anonyme à QM1.

La configuration qui en résulte se présente comme suit :

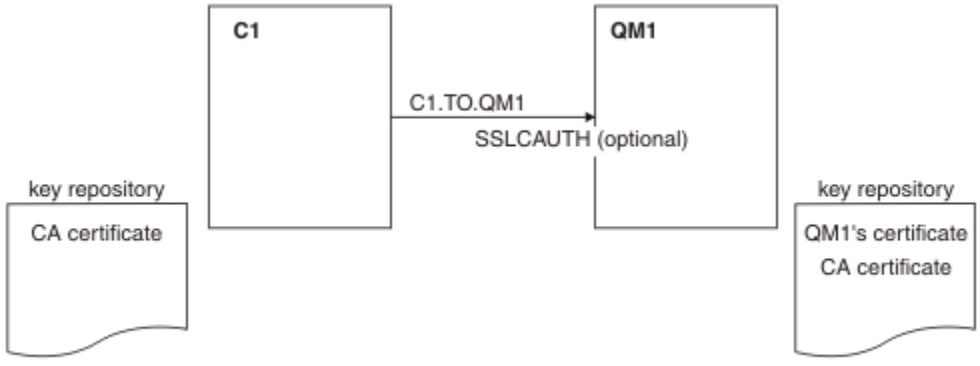


Figure 19. Client et gestionnaire de files d'attente autorisant la connexion anonyme

Procédure

1. Supprimez le certificat personnel du référentiel de clés pour C1, en fonction du système d'exploitation:
   - Sur les systèmes UNIX, Linuxet Windows. Le certificat est libellé comme suit:
     - `ibmwebspheremq` suivi de votre ID utilisateur de connexion en minuscules, par exemple `ibmwebspheremqmyuserid`.
2. Redémarrez l'application client ou faites en sorte qu'elle ferme et rouvre toutes les connexions SSL ou TLS.
3. Autorisez les connexions anonymes sur le gestionnaire de files d'attente en exécutant la commande suivante :

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Résultats

Les référentiels de clés et les canaux sont modifiés comme illustré dans la Figure 19, à la page 226.

Que faire ensuite

A l'extrémité serveur du canal, la présence de la valeur de paramètre du nom d'homologue sur le statut de canal indique qu'un certificat client a été transmis.

Vérifiez que la tâche a abouti en exécutant certaines commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après :

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

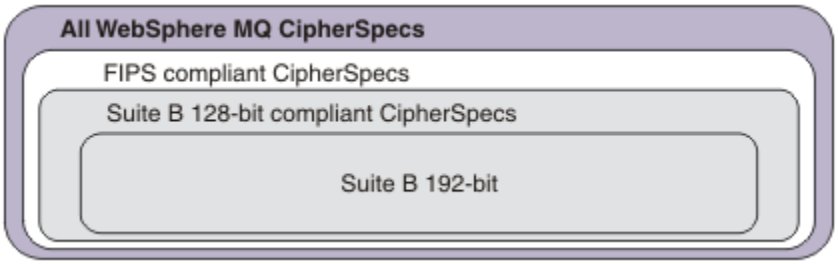
Les zones SSLCERTI et SSLPEER sont vides, indiquant que C1 n'a pas envoyé de certificat.

Définition des spécifications CipherSpec

Spécifiez un CipherSpec à l'aide du paramètre **SSLCIPH** dans la commande **DEFINE CHANNEL** MQSC ou dans la commande **ALTER CHANNEL** MQSC.

Certains CipherSpecs que vous pouvez utiliser avec IBM WebSphere MQ sont conformes à la norme FIPS. D'autres, comme NULL_MD5, ne le sont pas. De même, certains CipherSpecs conformes à la norme FIPS sont également conformes à la norme Suite B, alors que d'autres ne le sont pas. Tous les CipherSpecs conformes à la norme Suite B sont également conformes à la norme FIPS. Tous les CipherSpecs conformes à Suite B appartiennent à deux groupes: 128 bits (par exemple, ECDHE_ECDSA_AES_128_GCM_SHA256) et 192 bits (par exemple, ECDHE_ECDSA_AES_256_GCM_SHA384),

Le diagramme suivant illustre la relation entre ces sous-ensembles:



Les spécifications de chiffrement que vous pouvez utiliser avec le support IBM WebSphere MQ SSL et TLS sont répertoriées dans le tableau ci-dessous. Lorsque vous demandez un certificat personnel, vous définissez une taille de clé pour la paire de clé publique et de clé privée. La taille de clé utilisée lors de l'établissement de liaison SSL est celle qui est stockée dans le certificat à moins qu'elle soit déterminée par la spécification CipherSpec, comme indiqué dans le tableau.

Nom du CipherSpec	**Protocole utilisé**	**Algorithme MAC**	**Algorithme de chiffrement**	**Bits de chiffrement**	**FIPS [1]**	**Suite B 128 bits**	**Suite B 192 bits**
NULL_MD5 [a]	SSL 3.0	MD5	Aucun	0	Non	Non	Non
NULL_SHA [a]	SSL 3.0	SHA-1	Aucun	0	Non	Non	Non
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Non	Non	Non
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Non	Non	Non
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Non	Non	Non
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Non	Non	Non
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Non	Non	Non
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Non	Non	Non
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Non	Non	Non
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Oui	Non	Non
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Non [5]	Non	Non
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Non [6]	Non	Non
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Non
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Oui	Non	Non
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Non	Non	Non
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Non	Non	Non
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non

Nom du CipherSpec	Protocole utilisé	Algorithme MAC	Algorithme de chiffrement	Bits de chiffrement	FIPS [1]	Suite B 128 bits	Suite B 192 bits
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Oui	Non	Non
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Oui	Non	Non
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Oui	Non
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Oui
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Non	Non
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Non
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Aucun	0	Non	Non	Non
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Aucun	0	Non	Non	Non
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Aucun	0	Non	Non	Non
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Aucun	Aucun	0	Non	Non	Non
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Non	Non	Non

Remarques :

1. Indique si le CipherSpec est certifié FIPS sur une plateforme certifiée FIPS. Voir la rubrique sur la norme FIPS (Federal Information Processing Standards) pour une explication de la norme FIPS.
2. La taille de clé d'établissement de liaison maximale est de 512 bits. Si l'un ou l'autre des certificats échangés lors de l'établissement de liaison SSL a une taille de clé supérieure à 512 bit, une clé temporaire de 512 bits est générée pour l'établissement de liaison.
3. La taille de clé d'établissement de liaison maximale est de 1024 bits.
4. Ce CipherSpec ne peut pas être utilisé pour sécuriser une connexion de WebSphere MQ Explorer à un gestionnaire de files d'attente, sauf si les fichiers de règles sans restriction appropriés sont appliqués à l'environnement d'exécution Java utilisé par l'explorateur.
5. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007.
6. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007. Le nom FIPS_WITH_DES_CBC_SHA est historique et reflète le fait que CipherSpec était précédemment (mais n'est plus) conforme à la norme FIPS. Ce CipherSpec est déprécié et son utilisation est déconseillée.
7. Ce CipherSpec permet de transférer jusqu'à 32 Go de données avant que la connexion ne s'arrête avec l'erreur AMQ9288. Pour éviter cette erreur, évitez d'utiliser la norme DES triple ou activez la réinitialisation de clé confidentielle lors de l'utilisation de ce CipherSpec.

Prise en charge des plateformes :

- a Disponible sur toutes les plateformes prises en charge.
- b Disponible uniquement sur les plateformes UNIX, Linux, and Windows .

Concepts associés

«Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36
Cette rubrique fournit des informations sur la façon de choisir les CipherSpecs et les certificats numériques appropriés pour votre règle de sécurité, en soulignant la relation entre les CipherSpecs et les certificats numériques dans IBM WebSphere MQ.

Référence associée

De la définition d'un canal
ALTER CHANNEL

CipherSpecs obsolètes

Liste des CipherSpecs obsolètes que vous pouvez utiliser avec WebSphere MQ si nécessaire.

Voir «CipherSpec valeurs prises en charge dans IBM WebSphere MQ», à la page 41 pour plus d'informations sur la façon dont vous pouvez activer les CipherSpecsobsolètes.

Les CipherSpecs obsolètes que vous pouvez utiliser avec la prise en charge TLS de WebSphere MQ sont répertoriés dans le tableau suivant:

Prise en charge des plateformes «1», à la page 232	Nom du CipherSpec	Protocole utilisé	Intégrité des données	Algorithme de chiffrement	Bits de chiffrement	Norme FIPS «2», à la page 232	Suite B	Mettre à jour si déprécié
Tous	DES_SHA_EXPORT «3», à la page 232	SSL 3.0	SHA-1	DES	56	Non	Non	7.5.0.6
Windows UNIX Linux	DES_SHA_EXPORT1024 «4», à la page 232	SSL 3.0	SHA-1	DES	56	Non	Non	7.5.0.6
Windows UNIX Linux	FIPS_WITH_DES_CBC_SHA	SSL 3.0	SHA-1	DES	56	Non «6», à la page 232	Non	7.5.0.6
Windows UNIX Linux	FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0	SHA-1	3DES	168	Non «7», à la page 232	Non	7.5.0.8
Tous	NULL_MD5	SSL 3.0	MD5	Aucun	0	Non	Non	7.5.0.6
Tous	NULL_SHA	SSL 3.0	SHA-1	Aucun	0	Non	Non	7.5.0.6
Tous	RC2_MD5_EXPORT «3», à la page 232	SSL 3.0	MD5	RC2	40	Non	Non	7.5.0.7
Tous	RC4_MD5_EXPORT «3», à la page 232	SSL 3.0	MD5	RC4	40	Non	Non	7.5.0.7
Tous	RC4_MD5_US	SSL 3.0	MD5	RC4	128	Non	Non	7.5.0.7
Tous	RC4_SHA_US	SSL 3.0	SHA-1	RC4	128	Non	Non	7.5.0.7
Windows UNIX Linux	RC4_56_SHA_EXPORT1024 «4», à la page 232	SSL 3.0	SHA-1	RC4	56	Non	Non	7.5.0.7

Prise en charge des plateformes «1», à la page 232	Nom du CipherSpec	Protocole utilisé	Intégrité des données	Algorithme de chiffrement	Bits de chiffrement	Norme FIPS «2», à la page 232	Suite B	Mettre à jour si déprécié
Tous	TRIPLE_DES_SHA_US	SSL 3.0	SHA-1	3DES	168	Non	Non	7.5.0.8
Tous	TLS_RSA_WITH_DES_CBC_SHA	TLS 1.0	SHA-1	DES	56	Non« 5», à la page 232	Non	7.5.0.6
Windows UNIX Linux	ECDHE_ECDSA_NULL_SHA256	TLS 1.2	SHA-1	Aucun	0	Non	Non	7.5.0.6
Windows UNIX Linux	ECDHE_ECDSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Non	Non	7.5.0.7
Windows UNIX Linux	ECDHE_RSA_NULL_SHA256	TLS 1.2	SHA-1	Aucun	0	Non	Non	7.5.0.6
Windows UNIX Linux	ECDHE_RSA_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Non	Non	7.5.0.7
Windows UNIX Linux	TLS_RSA_WITH_NULL_NULL	TLS 1.2	Aucun	Aucun	0	Non	Non	7.5.0.6
Tous	TLS_RSA_WITH_NULL_SHA256	TLS 1.2	SHA-256	Aucun	0	Non	Non	7.5.0.6
Windows UNIX Linux	TLS_RSA_WITH_RC4_128_SHA256	TLS 1.2	SHA-1	RC4	128	Non	Non	7.5.0.7
Tous	TLS_RSA_WITH_3DES_EDE_CBC_SHA«8», à la page 232	TLS 1.0	SHA-1	3DES	168	Oui	Non	7.5.0.8
Windows UNIX Linux	ECDHE_ECDSA_3DES_EDE_CBC_SHA256«8», à la page 232	TLS 1.2	SHA-1	3DES	168	Oui	Non	7.5.0.8
Windows UNIX Linux	ECDHE_RSA_3DES_EDE_CBC_SHA256«8», à la page 232	TLS 1.2	SHA-1	3DES	168	Oui	Non	7.5.0.8

Prise en charge des plateformes «1», à la page 232	Nom du CipherSpec	Protocole utilisé	Intégrité des données	Algorithme de chiffrement	Bits de chiffrement	Norme FIPS «2», à la page 232	Suite B	Mettre à jour si déprécié

Remarques :

1. Si aucune plateforme spécifique n'est indiquée, le CipherSpec est disponible sur toutes les plateformes.
2. Indique si le CipherSpec est certifié FIPS sur une plateforme certifiée FIPS. Voir la rubrique sur la norme FIPS (Federal Information Processing Standards) pour une explication de la norme FIPS.
3. La taille de clé d'établissement de liaison maximale est de 512 bits. Si l'un ou l'autre des certificats échangés lors de l'établissement de liaison SSL a une taille de clé supérieure à 512 bit, une clé temporaire de 512 bits est générée pour l'établissement de liaison.
4. La taille de clé d'établissement de liaison maximale est de 1024 bits.
5. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007.
6. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007. Le nom `FIPS_WITH_DES_CBC_SHA` est historique et reflète le fait que ce CipherSpec était auparavant conforme FIPS (mais ne l'est plus). Ce CipherSpec est déprécié et son utilisation est déconseillée.
7. Le nom `FIPS_WITH_3DES_EDE_CBC_SHA` est historique et reflète le fait que ce CipherSpec était auparavant conforme FIPS (mais ne l'est plus). L'utilisation de ce CipherSpec a été dépréciée.
8. Ce CipherSpec permet de transférer jusqu'à 32 Go de données avant que la connexion ne s'arrête avec l'erreur AMQ9288. Pour éviter cette erreur, évitez d'utiliser la norme DES triple ou activez la réinitialisation de clé confidentielle lors de l'utilisation de ce CipherSpec.

Obtention d'informations sur les CipherSpecs à l'aide de IBM WebSphere MQ Explorer

Vous pouvez utiliser IBM WebSphere MQ Explorer pour afficher les descriptions des CipherSpecs.

Utilisez la procédure suivante pour obtenir des informations sur les CipherSpecs dans «Définition des spécifications CipherSpec», à la page 227:

1. Ouvrez **IBM WebSphere MQ Explorer** et développez le dossier **Gestionnaires de files d'attente** .
2. Vérifiez que vous avez démarré votre gestionnaire de files d'attente.
3. Sélectionnez le gestionnaire de files d'attente à utiliser et cliquez sur **Canaux**.
4. Cliquez avec le bouton droit de la souris sur le canal que vous souhaitez utiliser et sélectionnez **Propriétés**.
5. Sélectionnez la page de propriétés **SSL** .
6. Dans la liste, sélectionnez le CipherSpec que vous souhaitez utiliser. Une description s'affiche dans la fenêtre située sous la liste.

Alternatives pour la spécification de CipherSpecs

Pour les plateformes sur lesquelles le système d'exploitation fournit la prise en charge SSL, votre système peut prendre en charge de nouveaux CipherSpecs. Vous pouvez spécifier un nouveau CipherSpec avec le paramètre SSLCIPH, mais la valeur que vous fournissez dépend de votre plateforme.

Remarque : Cette section ne s'applique pas aux systèmes UNIX, Linux ou Windows , car les CipherSpecs sont fournis avec le produit WebSphere MQ , de sorte que les nouveaux CipherSpecs ne deviennent pas disponibles après l'expédition.

Pour les plateformes sur lesquelles le système d'exploitation fournit la prise en charge SSL, votre système peut prendre en charge de nouveaux CipherSpecs qui ne sont pas inclus dans «Définition des spécifications CipherSpec», à la page 227. Vous pouvez spécifier un nouveau CipherSpec avec le paramètre SSLCIPH, mais la valeur que vous fournissez dépend de votre plateforme. Dans tous les cas, la spécification *doit* correspondre à un CipherSpec SSL valide et pris en charge par la version de SSL exécutée par votre système.

IBM i
Chaîne de deux caractères représentant une valeur hexadécimale.

Pour plus d'informations sur les valeurs admises, reportez-vous à la documentation du produit appropriée (recherchez *cipher_spec* dans la documentation du produitIBM i).

Vous pouvez utiliser la commande CHGMQMCHL ou CRTMQMCHL pour spécifier la valeur, par exemple:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Vous pouvez également utiliser la commande ALTER QMGR MQSC pour définir le paramètre SSLCIPH .

z/OS
Chaîne de deux caractères représentant une valeur hexadécimale. Les codes hexadécimaux correspondent aux valeurs définies dans le protocole SSL.

Pour plus d'informations, reportez-vous à la description de gsk_environment_open () dans le chapitre de référence de l'API *z/OS Cryptographic Services System SSL Programming*, SC24-5901, où se trouve la liste de toutes les spécifications de chiffrement SSL V3.0 et TLS V1.0 prises en charge, sous la forme de codes hexadécimaux à 2 chiffres.

Remarques relatives aux clusters WebSphere MQ

Avec les clusters WebSphere MQ , il est plus sûr d'utiliser les noms CipherSpec dans «Définition des spécifications CipherSpec», à la page 227. Si vous utilisez une autre spécification, sachez que la spécification peut ne pas être valide sur d'autres plateformes. Pour plus d'informations, voir «SSL et clusters», à la page 259.

Spécification d'un CipherSpec pour un client IBM WebSphere MQ MQI

Vous disposez de trois options pour spécifier un CipherSpec pour un client IBM WebSphere MQ MQI.

Ces options sont les suivantes :

- Utilisation d'une table de définition de canal
- Utilisation de la zone SSLCipherSpec dans la structure MQCD, à l'adresse MQCD_VERSION_7 ou supérieure, sur un appel MQCONNX.
- Utilisation d' Active Directory (sur les systèmes Windows avec prise en charge d' Active Directory)

Spécification d'une CipherSuite avec des classes IBM WebSphere MQ pour Java et des classes IBM WebSphere MQ pour JMS

IBM WebSphere MQ classes for Java et IBM WebSphere MQ classes for JMS spécifient CipherSuites différemment des autres plateformes.

Pour plus d'informations sur la spécification d'une CipherSuite avec des classes IBM WebSphere MQ pour Java, voir Secure Sockets Layer (SSL) support.

Pour plus d'informations sur la spécification d'une CipherSuite avec IBM WebSphere MQ classes for JMS, voir Utilisation de SSL (Secure Sockets Layer) avec WebSphere MQ classes for JMS.

Réinitialisation des clés secrètes SSL et TLS

IBM WebSphere MQ prend en charge la réinitialisation des clés secrètes sur les gestionnaires de files d'attente et les clients.

Les clés secrètes sont réinitialisées lorsqu'un nombre spécifié d'octets chiffrés de données ont transité sur le canal, ou après que le canal a été inactif pendant un certain temps.

La valeur de réinitialisation de clé est toujours définie par le côté initiateur du canal MQ .

Gestionnaire de files d'attente

Pour un gestionnaire de files d'attente, utilisez la commande **ALTER QMGR** avec le paramètre **SSLRKEYC** pour définir les valeurs utilisées lors de la renégociation de clé.

MQI Client

Par défaut, les clients MQI ne renégocient pas la clé secrète. Vous pouvez faire en sorte qu'un client MQI renégocie la clé de trois manières. Dans la liste suivante, les méthodes sont affichées par ordre de priorité. Si vous spécifiez plusieurs valeurs, la valeur de priorité la plus élevée est utilisée.

1. En utilisant la zone KeyResetCount dans la structure MQSCO sur un appel MQCONNX
2. A l'aide de la variable d'environnement MQSSLRESET
3. En définissant l'attribut SSLKeyResetCount dans le fichier de configuration du client MQI

Ces variables peuvent être définies sur un entier compris entre 0 et 999 999 999, représentant le nombre d'octets non chiffrés envoyés et reçus dans une conversation SSL ou TLS avant la renégociation de la clé secrète SSL ou TLS. La valeur 0 indique que les clés secrètes SSL ou TLS ne sont jamais renégociées. Si vous spécifiez un nombre de réinitialisations de clé confidentielle SSL ou TLS compris entre 1 et 32 Ko, les canaux SSL ou TLS utiliseront un nombre de réinitialisations de clé confidentielle de 32 Ko. Cela permet d'éviter un nombre excessif de réinitialisations de clé qui se produiraient pour les petites valeurs de réinitialisation de clé confidentielle SSL ou TLS.

Si une valeur supérieure à zéro est spécifiée et que les pulsations de canal sont activées pour le canal, la clé secrète est également renégociée avant que les données de message ne soient envoyées ou reçues à la suite d'une pulsation de canal.

Nombre d'octets jusqu'à ce que la prochaine renégociation de clé secrète soit réinitialisée après chaque renégociation réussie.

Pour plus de détails sur la structure MQSCO, voir KeyResetCount (MQLONG). Pour plus de détails sur MQSSLRESET, voir MQSSLRESET. Pour plus d'informations sur l'utilisation de SSL ou TLS dans le fichier de configuration du client, voir Strophe SSL du fichier de configuration du client.

Java

Pour IBM WebSphere MQ classes for Java, une application peut réinitialiser la clé secrète de l'une des manières suivantes:

- En définissant la zone sslResetCount dans la classe MQEnvironment.
- En définissant la propriété d'environnement MQC.SSL_RESET_COUNT_PROPERTY dans un objet Hashtable. L'application affecte ensuite la table de hachage à la zone `properties` de la classe MQEnvironment ou transmet la table de hachage à un objet MQQueueManager sur son constructeur.

Si l'application utilise plusieurs de ces méthodes, les règles de priorité habituelles s'appliquent. Voir Class com.ibm.mq.MQEnvironment pour les règles de priorité.

La valeur de la zone sslResetCount ou de la propriété d'environnement MQC.SSL_RESET_COUNT_PROPERTY représente le nombre total d'octets envoyés et reçus par le code client WebSphere MQ classes for Java avant la renégociation de la clé secrète. Le nombre d'octets envoyés est le nombre avant chiffrement et le nombre d'octets reçus est le nombre après déchiffrement.

Le nombre d'octets inclut également les informations de contrôle envoyées et reçues par le client WebSphere MQ classes for Java.

Si le nombre de réinitialisations est égal à zéro, ce qui correspond à la valeur par défaut, la clé secrète n'est jamais renégociée. Le nombre de réinitialisations est ignoré si CipherSuite n'est pas spécifié.

JMS

Pour IBM WebSphere MQ classes for JMS, la propriété SSLRESETCOUNT représente le nombre total d'octets envoyés et reçus par une connexion avant que la clé secrète utilisée pour le chiffrement ne soit renégociée. Le nombre d'octets envoyés est le nombre avant chiffrement et le nombre d'octets reçus est le nombre après déchiffrement. Le nombre d'octets inclut également les informations de contrôle envoyées et reçues par IBM WebSphere MQ classes for JMS. Par exemple, pour configurer un objet ConnectionFactory pouvant être utilisé pour créer une connexion via un canal MQI activé SSL ou TLS avec une clé secrète renégociée après la transmission de 4 Mo de données, exécutez la commande suivante à JMSAdmin:

```
ALTER CF(my.cf) SSLRESETCOUNT(4194304)
```

Si la valeur de SSLRESETCOUNT est zéro, qui est la valeur par défaut, la clé secrète n'est jamais renégociée. La propriété SSLRESETCOUNT est ignorée si SSLCIPHERSUITE n'est pas défini.

.NET

Pour les clients .NET non gérés, la propriété d'entier SSLKeyResetindique le nombre d'octets non chiffrés envoyés et reçus dans une conversation SSL ou TLS avant la renégociation de la clé secrète.

Pour plus d'informations sur l'utilisation des propriétés d'objet dans IBM WebSphere MQ classes for .NET, voir Obtention et définition des valeurs d'attribut.

XMS .NET

Pour les clients XMS .NET non gérés, voir Connexions sécurisées à un gestionnaire de files d'attente IBM WebSphere MQ.

Référence associée
ALTER QMGR
DISPLAY QMGR

Implémentation de la confidentialité dans les programmes d'exit utilisateur

Implémentation de la confidentialité dans les exits de sécurité

Les exits de sécurité peuvent jouer un rôle dans le service de confidentialité en générant et en distribuant la clé symétrique pour le chiffrement et le déchiffrement des données qui circulent sur le canal. Une technique courante pour ce faire utilise la technologie PKI.

Un exit de sécurité génère une valeur de données aléatoire, le chiffre à l'aide de la clé publique du gestionnaire de files d'attente ou de l'utilisateur que l'exit de sécurité partenaire représente et envoie les données chiffrées à son partenaire dans un message de sécurité. L'exit de sécurité partenaire déchiffre la valeur de données aléatoires avec la clé privée du gestionnaire de files d'attente ou de l'utilisateur qu'il représente. Chaque exit de sécurité peut désormais utiliser la valeur de données aléatoires pour dériver la clé symétrique indépendamment l'une de l'autre en utilisant un algorithme connu des deux. Ils peuvent également utiliser la valeur de données aléatoire comme clé.

Si le premier exit de sécurité n'a pas authentifié son partenaire à ce moment-là, le message de sécurité suivant envoyé par le partenaire peut contenir une valeur attendue chiffrée avec la clé symétrique. Le premier exit de sécurité peut désormais authentifier son partenaire en vérifiant que l'exit de sécurité du partenaire a pu chiffrer correctement la valeur attendue.

Les exits de sécurité peuvent également utiliser cette opportunité pour convenir de l'algorithme de chiffrement et de déchiffrement des données qui circulent sur le canal, si plusieurs algorithmes sont disponibles.

Implémentation de la confidentialité dans les exits de message

Un exit de message à l'extrémité émettrice d'un canal peut chiffrer les données d'application dans un message et un autre exit de message à l'extrémité réceptrice du canal peut déchiffrer les données. Pour des raisons de performances, un algorithme de clé symétrique est normalement utilisé à cette fin. Pour plus d'informations sur la façon dont la clé symétrique peut être générée et distribuée, voir «Implémentation de la confidentialité dans les programmes d'exit utilisateur», à la page 235.

Les en-têtes d'un message, tels que l'en-tête de file d'attente de transmission, MQXQH, qui inclut le descripteur de message imbriqué, ne doivent pas être chiffrés par un exit de message. En effet, la conversion des données des en-têtes de message a lieu soit après l'appel d'un exit de message à l'extrémité émettrice, soit avant l'appel d'un exit de message à l'extrémité réceptrice. Si les en-têtes sont chiffrés, la conversion des données échoue et le canal s'arrête.

Implémentation de la confidentialité dans les exits d'envoi et de réception

Les exits d'envoi et de réception peuvent être utilisés pour chiffrer et déchiffrer les données qui circulent sur un canal. Ils sont plus appropriés que les exits de message pour fournir ce service pour les raisons suivantes:

- Sur un canal de message, les en-têtes de message peuvent être chiffrés ainsi que les données d'application dans les messages.
- Les exits d'envoi et de réception peuvent être utilisés sur les canaux MQI ainsi que sur les canaux de message. Les paramètres des appels MQI peuvent contenir des données d'application sensibles qui doivent être protégées alors qu'elles circulent sur un canal MQI. Vous pouvez donc utiliser les mêmes exits d'émission et de réception sur les deux types de canaux.

Implémentation de la confidentialité dans l'exit d'API et l'exit de croisement d'API

Les données d'application d'un message peuvent être chiffrées par une API ou un exit de croisement d'API lorsque le message est inséré par l'application émettrice et déchiffré par un deuxième exit lorsque le message est extrait par l'application réceptrice. Pour des raisons de performances, un algorithme de clé symétrique est généralement utilisé à cette fin. Toutefois, au niveau de l'application, où de nombreux utilisateurs peuvent s'envoyer des messages les uns aux autres, le problème est de s'assurer que seul le destinataire prévu d'un message est en mesure de déchiffrer le message. Une solution consiste à utiliser une clé symétrique différente pour chaque paire d'utilisateurs qui s'envoient des messages. Mais cette solution peut être difficile et longue à administrer, en particulier si les utilisateurs appartiennent à des organisations différentes. Un moyen standard de résoudre ce problème est appelé *enveloppage numérique* et utilise la technologie PKI.

Lorsqu'une application place un message dans une file d'attente, une API ou un exit de croisement d'API génère une clé symétrique aléatoire et utilise la clé pour chiffrer les données d'application dans le message. L'exit chiffre la clé symétrique avec la clé publique du destinataire prévu. Il remplace ensuite les données d'application du message par les données d'application chiffrées et la clé symétrique chiffrée. De cette manière, seul le récepteur visé peut déchiffrer la clé symétrique et donc les données d'application. Si un message chiffré a plus d'un récepteur prévu possible, l'exit peut chiffrer une copie de la clé symétrique pour chaque récepteur prévu.

Si différents algorithmes de chiffrement et de déchiffrement des données d'application sont disponibles, l'exit peut inclure le nom de l'algorithme qu'il a utilisé.

Intégrité des données de messages

Pour préserver l'intégrité des données, vous pouvez utiliser différents types de programme d'exit utilisateur pour fournir des prétraitements de message ou des signatures numériques pour vos messages.

Intégrité des données

Implémentation de l'intégrité des données dans les messages

Lorsque vous utilisez SSL ou TLS, votre choix de CipherSpec détermine le niveau d'intégrité des données dans l'entreprise. Si vous utilisez le service AMS (WebSphere MQ Advanced Message Service), vous pouvez spécifier l'intégrité d'un message unique.

Implémentation de l'intégrité des données dans les exits de message

Un message peut être signé numériquement par un exit de message à l'extrémité émettrice d'un canal. La signature numérique peut alors être vérifiée par une sortie de message à l'extrémité réceptrice d'un canal pour détecter si le message a été volontairement modifié.

Une certaine protection peut être fournie à l'aide d'un résumé de message au lieu d'une signature numérique. Un résumé de message peut être efficace contre les manipulations occasionnelles ou indiscriminées, mais il n'empêche pas l'individu le plus informé de changer ou de remplacer le message, et de générer un résumé complètement nouveau pour lui. Cela est particulièrement vrai si l'algorithme utilisé pour générer le résumé de message est un algorithme bien connu.

Implémentation de l'intégrité des données dans les exits d'envoi et de réception

Sur un canal de message, les exits de message sont plus appropriés pour fournir ce service car un exit de message a accès à l'ensemble d'un message. Sur un canal MQI, les paramètres des appels MQI peuvent contenir des données d'application qui doivent être protégées et seuls les exits d'envoi et de réception peuvent fournir cette protection.

Implémentation de l'intégrité des données dans l'exit API ou l'exit de croisement d'API

Un message peut être signé numériquement par une API ou un exit de croisement d'API lorsque le message est inséré par l'application émettrice. La signature numérique peut alors être vérifiée par une deuxième sortie lorsque le message est récupéré par l'application réceptrice pour détecter si le message a été volontairement modifié.

Une certaine protection peut être fournie à l'aide d'un résumé de message au lieu d'une signature numérique. Un résumé de message peut être efficace contre les manipulations occasionnelles ou indiscriminées, mais il n'empêche pas l'individu le plus informé de changer ou de remplacer le message, et de générer un résumé complètement nouveau pour lui. Ceci est particulièrement vrai si l'algorithme utilisé pour générer le résumé de message est bien connu,

Connexion de deux gestionnaires de files d'attente via le protocole SSL ou TLS

Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

Pour configurer votre installation SSL ou TLS, vous devez définir vos canaux pour utiliser les protocoles SSL ou TLS. Vous devez également obtenir et gérer vos certificats numériques. Sur un système de test, vous pouvez utiliser des certificats autosignés ou des certificats émis par une autorité de certification locale. Sur un système de production, n'utilisez pas de certificats autosignés. Pour plus d'informations, voir ../zs14140_.dita.

Pour plus d'informations sur la création et la gestion des certificats, voir «Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows», à la page 119.

Les rubriques suivantes présentent les tâches de configuration des communications SSL et donnent des instructions détaillées sur la réalisation de ces tâches.

Vous pouvez également vouloir tester l'authentification des clients SSL ou TLS, qui constitue une partie facultative des protocoles. Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation WebSphere MQ , le serveur SSL ou TLS demande toujours un certificat au client.

Remarques :

1. Dans ce contexte, un client SSL se réfère à la connexion initiant l'établissement de liaison.

2. Pour plus d'informations, voir le Glossaire .

Sur les systèmes UNIX, Linux et Windows , le client SSL ou TLS envoie un certificat uniquement s'il en possède un libellé au format WebSphere MQ correct, qui est `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente remplacé par des minuscules. Par exemple, pour `QM1`, `ibmwebspheremqqm1`.

WebSphere MQ utilise le préfixe `ibmwebspheremq` sur un libellé pour éviter toute confusion avec les certificats d'autres produits. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie aucun certificat, l'authentification échoue uniquement si la fin du canal qui agit comme serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur du paramètre SSLPEER déterminée. Pour plus d'informations sur la connexion anonyme d'un gestionnaire de files d'attente, c'est-à-dire lorsque le client SSL ou TLS n'envoie pas de certificat, voir «Connexion de deux gestionnaires de files d'attente à l'aide de l'authentification unidirectionnelle», à la page 220.

Labels de certificat numérique, compréhension des exigences

Lors de la configuration de SSL et TLS pour utiliser des certificats numériques, il peut exister des exigences de libellé spécifiques que vous devez respecter, en fonction de la plateforme utilisée et de la méthode que vous utilisez pour vous connecter.

Pourquoi et quand exécuter cette tâche

Qu'est-ce que le libellé de certificat?

Un label de certificat est un identificateur unique représentant un certificat numérique stocké dans un référentiel de clés et fournit un nom lisible par l'utilisateur qui permet de faire référence à un certificat particulier lors de l'exécution de fonctions de gestion de clés. Vous affectez le libellé de certificat lors de l'ajout d'un certificat à un référentiel de clés pour la première fois.

Le libellé du certificat est distinct des zones *Subject Distinguished Name* ou *Subject Common Name* du certificat. Notez que le *Nom distinctif du sujet* et le *Nom usuel du sujet* sont des zones du certificat lui-même. Elles sont définies lors de la création du certificat et ne peuvent pas être modifiées. Toutefois, vous pouvez modifier le libellé associé à un certificat numérique si nécessaire.

Comment le libellé de certificat est-il utilisé?

IBM WebSphere MQ utilise des libellés de certificat pour localiser un certificat personnel envoyé lors de l'établissement de liaison SSL. Cela élimine l'ambiguïté lorsque plusieurs certificats personnels existent dans le référentiel de clés.

Les libellés de certificat suivent une convention de dénomination ; vous devez vous assurer que vous utilisez la convention de dénomination de libellé correcte correspondant à la plateforme que vous utilisez.

Dans ce contexte, un client SSL ou TLS fait référence au partenaire de connexion qui initie l'établissement de liaison, qui peut être un client IBM WebSphere MQ ou un autre gestionnaire de files d'attente.

Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation IBM WebSphere MQ , le serveur SSL ou TLS demande toujours un certificat au client et ce dernier fournit toujours un certificat au serveur s'il en trouve un. Si le client ne parvient pas à localiser un certificat personnel, il envoie une réponse `no certificate` au serveur.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie pas de certificat, l'authentification échoue si l'extrémité du canal agissant en tant que serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur de paramètre SSLPEER définie.

Pour plus d'informations sur la connexion d'un gestionnaire de files d'attente à l'aide de l'authentification unidirectionnelle, c'est-à-dire lorsque le client SSL ou TLS n'envoie pas de certificat, voir «Connexion de deux gestionnaires de files d'attente à l'aide de l'authentification unidirectionnelle», à la page 220.

, systèmes UNIX, Linux, and Windows

Pourquoi et quand exécuter cette tâche

Sur les systèmes , UNIX, Linux, and Windows , le serveur SSL ou TLS envoie un certificat au client, uniquement si le serveur en trouve un libellé au format IBM WebSphere MQ correct. Sur ces systèmes, le format correct est `ibmwebspheremq`, suivi du nom de votre gestionnaire de files d'attente remplacé par des minuscules.

Par exemple, pour un gestionnaire de files d'attente nommé `QM1`, l'exigence de label de certificat est la suivante:

```
ibmwebspheremqqm1
```

Si aucun certificat n'est trouvé dans le référentiel de clés du gestionnaire de files d'attente, correspondant au libellé requis dans la casse et le format corrects, une erreur se produit et l'établissement de liaison SSL ou TLS échoue.

IBM WebSphere MQ client

Pourquoi et quand exécuter cette tâche

Lors de la connexion à partir d'une application client IBM WebSphere MQ , le client SSL ou TLS envoie un certificat uniquement s'il en possède un avec un libellé au format `ibmwebspheremq`, suivi du nom d'utilisateur de l'utilisateur exécutant le processus d'application client.

Par exemple, pour le nom d'utilisateur `wasadmin`, l'exigence de libellé de certificat est la suivante, pliée en minuscules:

```
  ibmwebspheremqwasadmin
```

L'exigence de libellé ci-dessus s'applique aux clients de service de messagerie pour C, ou C + +, et .NET.

Client IBM WebSphere MQ Java ou IBM WebSphere MQ JMS

Pourquoi et quand exécuter cette tâche

Les clients IBM WebSphere MQ Java ou IBM WebSphere MQ JMS utilisent les fonctions de leur fournisseur JSSE (Java Secure Socket Extension) pour sélectionner un certificat personnel lors de l'établissement de liaison SSL ou TLS et ne sont donc pas soumis aux exigences de libellé de certificat.

Le comportement par défaut est que le client JSSE itère via les certificats du référentiel de clés, en sélectionnant le premier certificat personnel acceptable trouvé. Cependant, ce comportement n'est qu'une valeur par défaut et dépend de l'implémentation du fournisseur JSSE.

En outre, l'interface JSSE est hautement personnalisable via la configuration et l'accès direct lors de l'exécution par l'application. Pour plus de détails, consultez la documentation fournie par votre fournisseur JSSE.

Pour le traitement des incidents ou pour mieux comprendre l'établissement de liaison effectué par l'application client Java IBM WebSphere MQ en association avec votre fournisseur JSSE spécifique, vous pouvez activer le débogage en définissant

```
javax.net.debug=ssl
```

dans l'environnement JVM.

Vous pouvez utiliser `-Djavax.net.debug=ssl` sur la ligne de commande ou définir la variable dans l'application ou via la configuration.

Concepts associés

«Importation d'un certificat personnel dans un référentiel de clés sur des systèmes UNIX, Linux, and Windows», à la page 140
Suivez cette procédure pour importer un certificat personnel

Utilisation de certificats autosignés pour l'authentification mutuelle de deux gestionnaires de file d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre deux gestionnaires de files d'attente à l'aide de certificats TLS ou SSL autosignés.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez de deux gestionnaires de files d'attente appelés QM1 et QM2, qui ont besoin de communiquer de façon sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre QM1 et QM2.
- Vous avez décidé de tester votre communication sécurisée en utilisant des certificats autosignés.

La configuration qui en résulte se présente comme suit :

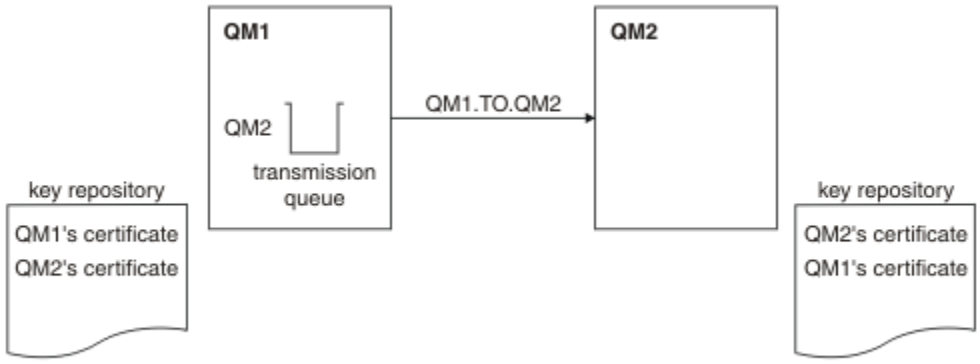


Figure 20. Configuration obtenue

Dans la Figure 14, à la page 217, le référentiel de clés de QM1 contient le certificat de QM1 et le certificat public de QM2. Le référentiel de clés de QM2 contient le certificat de QM2 et le certificat public de QM1.

Procédure

1. Préparez le référentiel de clés de chaque gestionnaire de files d'attente en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Créez un certificat autosigné pour chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
3. Procédez à l'extraction d'une copie de chaque certificat :
   - Sur les systèmes UNIX, Linuxet Windows.
4. Transférez la partie publique du certificat QM1 vers le système QM2 et inversement, à l'aide d'un utilitaire tel que FTP.
5. Ajoutez le certificat partenaire au référentiel de clés de chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
6. Sur QM1, définissez un canal émetteur et une file d'attente de transmission associée en exécutant des commandes similaires à l'exemple suivant :

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QM1.MACH.COM) XMITQ(QM2)
SSLCIPH(RC4_MD5_US) DESCR('Sender channel using SSL from QM1 to QM2')

DEFINE QLOCAL(QM2) USAGE(XMITQ)
```

Cet exemple utilise CipherSpec RC4_MD5. Le CipherSpec doit être le même à chaque extrémité du canal.

7. Sur QM2, définissez un canal récepteur en émettant une commande similaire à l'exemple suivant :

```
DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from QM1 to QM2')
```

Le canal doit porter le même nom que le canal émetteur que vous avez défini à l'étape 6, et utiliser le même CipherSpec.

8. Démarrez le canal.

Résultats

Les référentiels de clés et les canaux sont créés comme illustré dans Figure 14, à la page 217.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM1.TO.QM2)                     CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=QM2,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

A partir du gestionnaire de files d'attente QM2, entrez la commande suivante :

```
DISPLAY CHS(QM1.TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(QM1.TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(QM2.TO.QM1)                     CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QM1)
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QM1,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
   XMITQ( )
```

Dans chaque cas, la valeur de SSLPEER doit correspondre à celle du nom distinctif dans le certificat partenaire créé à l'étape 2. Le nom de l'émetteur correspond au nom de l'homologue car le certificat est autosigné.

SSLPEER est facultatif. S'il est indiqué, sa valeur doit être définie de telle sorte que le nom distinctif dans le certificat partenaire (créé à l'étape 2) soit autorisé. Pour plus d'informations sur l'utilisation de SSLPEER, voir WebSphere MQ rules for SSLPEER values .

Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle de deux gestionnaires de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre deux gestionnaires de files d'attente à l'aide de certificats TLS ou SSL signés par l'autorité de certification.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez de deux gestionnaires de files d'attente appelés QMA et QMB, qui ont besoin de communiquer de façon sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre QMA et QMB.
- A l'avenir, vous envisagez d'utiliser ce réseau dans un environnement de production et vous avez donc décidé d'employer des certificats signés par l'autorité de certification dès le début.

La configuration qui en résulte se présente comme suit :

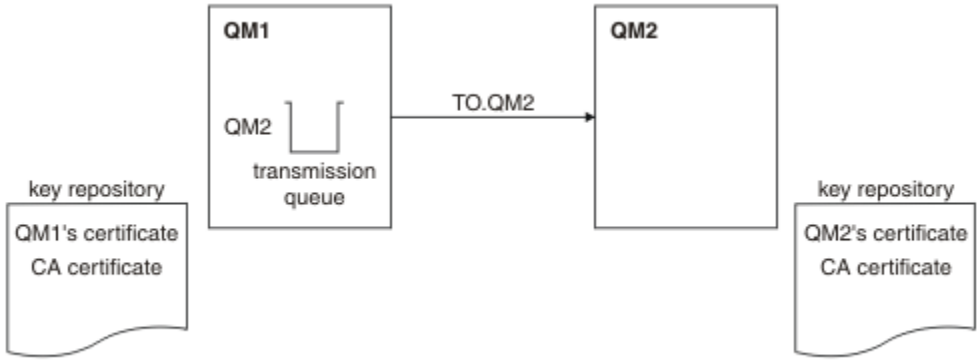


Figure 21. Configuration obtenue

Dans la Figure 15, à la page 219, le référentiel de clés de QMA contient le certificat de QMA et le certificat de l'autorité de certification. Le référentiel de clés de QMB contient le certificat de QMB et le certificat de l'autorité de certification. Dans cet exemple, le certificat de QMA et le certificat de QMB ont été émis par la même autorité de certification. Si le certificat de QMA et le certificat de QMB ont été émis par des autorités de certification différentes, les référentiels de clés de QMA et de QMB doivent contenir les certificats des deux autorités de certification.

Procédure

1. Préparez le référentiel de clés de chaque gestionnaire de files d'attente en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Demandez un certificat signé par l'autorité de certification pour chaque gestionnaire de files d'attente.
   Vous pourriez utiliser des autorités de certification différentes pour les deux gestionnaires de files d'attente.
   - Sur les systèmes UNIX, Linuxet Windows.
3. Ajoutez le certificat de l'autorité de certification au référentiel de clés de chaque gestionnaire de files d'attente :

Si les gestionnaires de files d'attente utilisent des autorités de certification différentes, le certificat de l'autorité de certification de chaque autorité de certification doit être ajouté dans chacun des référentiels de clés.

- Sur les systèmes UNIX, Linuxet Windows.

4. Ajoutez le certificat signé par l'autorité de certification au référentiel de clés de chaque gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
5. Sur QMA, définissez un canal émetteur et une file d'attente de transmission associée en exécutant des commandes similaires à l'exemple suivant :

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(SDR) TRPTYPE(TCP) CONNAME(QMB.MACH.COM) XMITQ(QMB)
SSLCIPH(RC2_MD5_EXPORT) DESCR('Sender channel using SSL from QMA to QMB')

DEFINE QLOCAL(QMB) USAGE(XMITQ)
```

   Cet exemple utilise CipherSpec RC4_MD5. Le CipherSpec doit être le même à chaque extrémité du canal.
6. Sur QMB, définissez un canal récepteur en exécutant une commande similaire à l'exemple suivant :

```
DEFINE CHANNEL(TO.QMB) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL to QMB')
```

   Le canal doit porter le même nom que le canal émetteur que vous avez défini à l'étape 6, et utiliser le même CipherSpec.
7. Démarrez le canal :

Résultats

Les référentiels de clés et les canaux sont créés comme indiqué dans la Figure 15, à la page 219.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QMA, entrez la commande suivante :

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QMB)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QMB)
```

A partir du gestionnaire de files d'attente QMB, entrez la commande suivante :

```
DISPLAY CHS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QMB)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
```

```
   RQMNAME(QMA)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                          SUBSTATE(RECEIVE)
   XMITQ( )
```

Dans chaque cas, la valeur de SSLPEER doit correspondre à celle du nom distinctif (DN) dans le certificat partenaire créé à l'étape 2. Le nom de l'émetteur correspond au DN de l'objet du certificat de l'autorité de certification qui a signé le certificat personnel ajouté à l'étape 4.

Connexion de deux gestionnaires de files d'attente à l'aide de l'authentification unidirectionnelle

Suivez les instructions de cet exemple pour modifier un système avec l'authentification mutuelle afin d'autoriser un gestionnaire de files d'attente à se connecter à l'aide de l'authentification unidirectionnelle à un autre gestionnaire de files d'attente, à savoir lorsque le client SSL ou TLS n'envoie pas de certificat.

Pourquoi et quand exécuter cette tâche

Scénario :

- Les deux gestionnaires de files d'attente (QM1 et QM2) ont été configurés comme illustré dans la «Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle de deux gestionnaires de files d'attente», à la page 218.
- Vous souhaitez modifier QM1 pour qu'il se connecte à l'aide de l'authentification unidirectionnelle à QM2.

La configuration qui en résulte se présente comme suit :

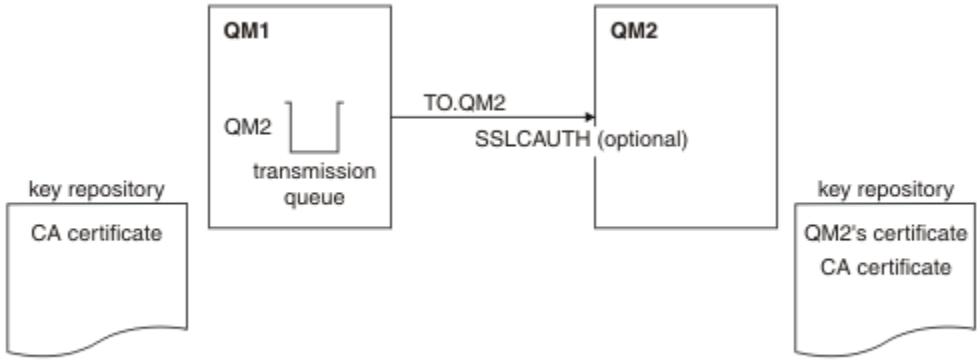


Figure 22. Gestionnaires de files d'attente autorisant l'authentification unidirectionnelle

Procédure

1. Supprimez le certificat personnel de QM1de son référentiel de clés, en fonction du système d'exploitation:
   - Sur les systèmes UNIX, Linuxet Windows. Le certificat est libellé comme suit:
     - `ibmwebspheremq` suivi du nom de votre gestionnaire de files d'attente en minuscules. Par exemple, pour `QM1` , `ibmwebspheremqqm1`.
2. Facultatif : Sur QM1, si des canaux SSL ou TLS ont été exécutés précédemment, actualisez l'environnement SSL ou TLS.
3. Autorisez les connexions anonymes sur le récepteur.

Résultats

Les référentiels de clés et les canaux sont modifiés comme illustré dans la Figure 16, à la page 221.

Que faire ensuite

Si le canal émetteur était en cours d'exécution et que vous avez émis la commande REFRESH SECURITY TYPE(SSL) (à l'étape 2), le canal redémarre automatiquement. Si le canal émetteur n'était pas en cours d'exécution, démarrez-le.

A l'extrémité serveur du canal, la présence de la valeur de paramètre du nom d'homologue sur le statut de canal indique qu'un certificat client a été transmis.

Vérifiez que la tâche a abouti en exécutant certaines commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après :

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
     4 : DISPLAY CHSTATUS(TO.QMB) SSLPEER
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(SDR)
   CONNAME(9.20.25.40)                     CURRENT
   RQMNAME(QM2)
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMB,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(MQGET)
   XMITQ(QM2)
```

A partir du gestionnaire de files d'attente QM2, entrez la commande suivante :

```
DISPLAY CHS(TO.QM2) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(TO.QM2) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(TO.QM2)                         CHLTYPE(RCVR)
   CONNAME(9.20.35.92)                     CURRENT
   RQMNAME(QMA)                            SSLCERTI( )
   SSLPEER( )                              STATUS(RUNNING)
   SUBSTATE(RECEIVE)                       XMITQ( )
```

Sur QM2, la zone SSLPEER est vide, ce qui indique que QM1 n'a pas envoyé de certificat. Sur QM1, la valeur de SSLPEER correspond à celle du nom distinctif dans le certificat personnel de QM2.

Connexion sécurisée d'un client à un gestionnaire de files d'attente

Les communications sécurisées qui font appel aux protocoles de sécurité cryptographiques SSL ou TLS impliquent la configuration des canaux de communication et la gestion des certificats numériques à utiliser à des fins d'authentification.

Pour configurer votre installation SSL ou TLS, vous devez définir vos canaux pour utiliser les protocoles SSL ou TLS. Vous devez également obtenir et gérer vos certificats numériques. Sur un système de test, vous pouvez utiliser des certificats autosignés ou des certificats émis par une autorité de certification locale. Sur un système de production, n'utilisez pas de certificats autosignés. Pour plus d'informations, voir ../zs14140_.dita.

Pour plus d'informations sur la création et la gestion des certificats, voir «Utilisation de SSL ou TLS sur les systèmes UNIX, Linux, and Windows», à la page 119.

Les rubriques suivantes présentent les tâches de configuration des communications SSL et donnent des instructions détaillées sur la réalisation de ces tâches.

Vous pouvez également vouloir tester l'authentification des clients SSL ou TLS, qui constitue une partie facultative des protocoles. Lors de l'établissement de liaison SSL ou TLS, le client SSL ou TLS obtient toujours un certificat numérique du serveur et le valide. Avec l'implémentation WebSphere MQ , le serveur SSL ou TLS demande toujours un certificat au client.

Sur les systèmes UNIX, Linux, and Windows , le client SSL ou TLS envoie un certificat uniquement s'il en a un libellé au format WebSphere MQ correct, qui est `ibmwebspheremq` suivi de votre ID utilisateur de connexion modifié en minuscules, par exemple `ibmwebspheremqmyuserid`.

WebSphere MQ utilise le préfixe `ibmwebspheremq` sur un libellé pour éviter toute confusion avec les certificats d'autres produits. Veillez à spécifier l'intégralité du libellé de certificat en minuscules.

Le serveur SSL ou TLS valide toujours le certificat client si celui-ci est envoyé. Si le client n'envoie aucun certificat, l'authentification échoue uniquement si la fin du canal qui agit comme serveur SSL ou TLS est définie avec le paramètre SSLCAUTH défini sur REQUIRED ou une valeur du paramètre SSLPEER déterminée. Pour plus d'informations sur la connexion anonyme d'un gestionnaire de files d'attente, voir «Connexion anonyme d'un client à un gestionnaire de files d'attente», à la page 226.

Utilisation de certificats autosignés pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre un client et un gestionnaire de files d'attente à l'aide de certificats SSL ou TLS autosignés.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez d'un client, C1, et d'un gestionnaire de files d'attente, QM1, qui doivent communiquer de manière sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre C1 et QM1.
- Vous avez décidé de tester votre communication sécurisée en utilisant des certificats autosignés.

DCM sur IBM i ne prend pas en charge les certificats autosignés. Cette tâche ne s'applique donc pas aux systèmes IBM i.

La configuration qui en résulte se présente comme suit :

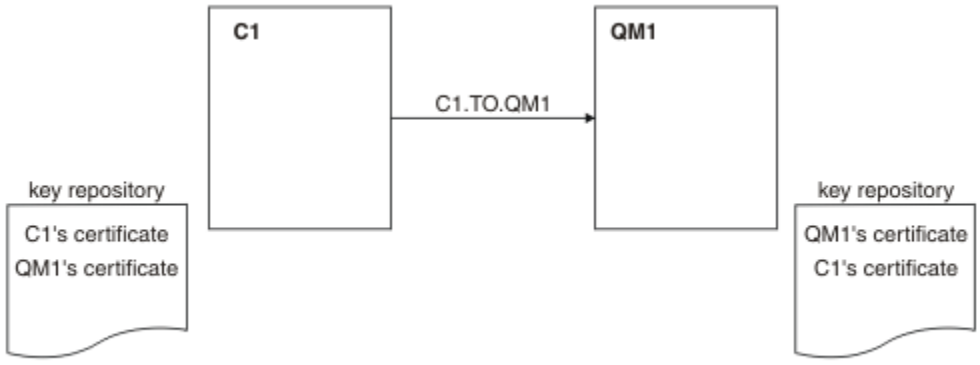


Figure 23. Configuration obtenue

Dans la Figure 17, à la page 223, le référentiel de clés de QM1 contient le certificat de QM1 et le certificat public de C1. Le référentiel de clés de C1 contient le certificat de C1 et le certificat public de QM1.

Procédure

1. Préparez le référentiel de clés sur le client et sur le gestionnaire de files d'attente, en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Créez les certificats autosignés pour le client et le gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
3. Procédez à l'extraction d'une copie de chaque certificat :
   - Sur les systèmes UNIX, Linuxet Windows.
4. Transférez la partie publique du certificat C1 vers le système QM1 et inversement, à l'aide d'un utilitaire tel que FTP.
5. Ajoutez le certificat partenaire dans le référentiel de clés du client et du gestionnaire de files d'attente :
   - Sur les systèmes UNIX, Linuxet Windows.
6. Exécutez la commande REFRESH SECURITY TYPE (SSL) sur le gestionnaire de files d'attente.
7. Définissez un canal de connexion client en procédant de l'une des deux manières suivantes :
   - Utilisation de l'appel MQCONNX avec la structure MQSCO sur C1, comme décrit dans Création d'un canal de connexion client sur le client WebSphere MQ MQI.
   - Utilisation d'une table de définition de canal du client, comme décrit dans Création de définitions de connexion serveur et de connexion client sur le serveur .
8. Sur QM1, définissez un canal de connexion serveur en émettant une commande similaire à l'exemple suivant :

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC4_MD5_US)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Le canal doit porter le même nom que le canal de connexion client que vous avez défini à l'étape 6, et utiliser le même CipherSpec.

Résultats

Les référentiels de clés et les canaux sont créés comme illustré dans la Figure 17, à la page 223

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                       CURRENT
   SSLCERTI("CN=QM1,OU=WebSphere MQ Development,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5E:02,CN=QM2,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

Le paramétrage de l'attribut de filtre SSLPEER des définitions de canal est facultatif. Si la définition de canal SSLPEER est définie, sa valeur doit correspondre au nom distinctif du sujet dans le certificat partenaire créé à l'étape 2. Une fois la connexion établie, la zone SSLPEER de la sortie DISPLAY CHSTATUS affiche le nom distinctif du sujet du certificat client distant.

Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour implémenter une authentification mutuelle entre un client et un gestionnaire de files d'attente à l'aide de certificats SSL ou TLS signés par l'autorité de certification.

Pourquoi et quand exécuter cette tâche

Scénario :

- Vous disposez d'un client, C1, et d'un gestionnaire de files d'attente, QM1, qui doivent communiquer de manière sécurisée. Vous exigez l'établissement d'une authentification mutuelle entre C1 et QM1.
- A l'avenir, vous envisagez d'utiliser ce réseau dans un environnement de production et vous avez donc décidé d'employer des certificats signés par l'autorité de certification dès le début.

La configuration qui en résulte se présente comme suit :

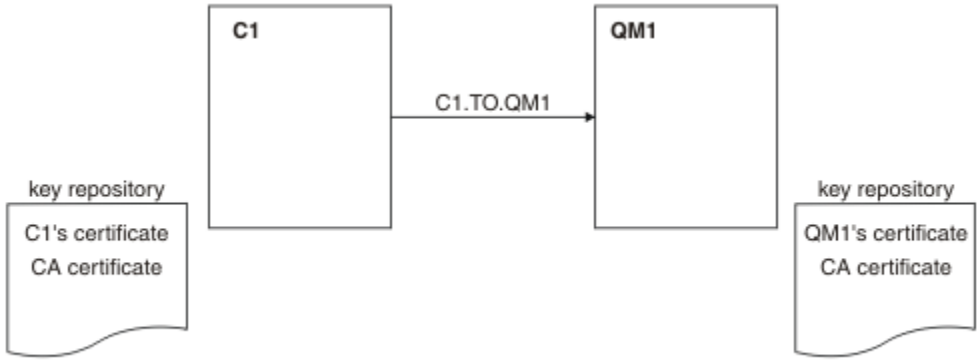


Figure 24. Configuration obtenue

Dans la Figure 18, à la page 225, le référentiel de clés de C1 contient le certificat de C1 et le certificat de l'autorité de certification. Le référentiel de clés de QM1 contient le certificat de QM1 et le certificat de l'autorité de certification. Dans cet exemple, les certificats de C1 et de QM1 ont été émis par la même autorité de certification. S'ils avaient été émis par des autorités de certification différentes, les référentiels de clés de C1 et de QM1 auraient dû inclure les certificats des deux autorités de certification.

Procédure

1. Préparez le référentiel de clés sur le client et sur le gestionnaire de files d'attente, en fonction du système d'exploitation :
   - Sur les systèmes UNIX, Linuxet Windows.
2. Demandez le certificat signé par l'autorité de certification pour le client et le gestionnaire de files d'attente.

   Vous pourriez utiliser des autorités de certification différentes pour le client et le gestionnaire de files d'attente.
   - Sur les systèmes UNIX, Linuxet Windows.
3. Ajoutez le certificat de l'autorité de certification au référentiel de clés du client et du gestionnaire de files d'attente.

   Si le client et le gestionnaire de files d'attente utilisent des autorités de certification différentes, le certificat de chaque autorité de certification doit être ajouté aux deux référentiels de clés.
   - Sur les systèmes UNIX, Linuxet Windows.
4. Ajoutez le certificat signé par l'autorité de certification au référentiel de clés du client et du gestionnaire de files d'attente :

- Sur les systèmes UNIX, Linuxet Windows.

5. Définissez un canal de connexion client en procédant de l'une des deux manières suivantes :
   - Utilisation de l'appel MQCONNX avec la structure MQSCO sur C1, comme décrit dans Création d'un canal de connexion client sur le client WebSphere MQ MQI.
   - Utilisation d'une table de définition de canal du client, comme décrit dans Création de définitions de connexion serveur et de connexion client sur le serveur .
6. Sur QM1, définissez un canal de connexion serveur en émettant une commande similaire à l'exemple suivant :

   ```
   DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) SSLCIPH(RC2_MD5_EXPORT)
   SSLCAUTH(REQUIRED) DESCR('Receiver channel using SSL from C1 to QM1')
   ```

   Le canal doit porter le même nom que le canal de connexion client que vous avez défini à l'étape 6, et utiliser le même CipherSpec.

Résultats

Les référentiels de clés et les canaux sont créés comme indiqué dans la Figure 18, à la page 225.

Que faire ensuite

Vérifiez que la tâche a abouti à l'aide des commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après.

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(TO.QMB) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI("CN=WebSphere MQ CA,OU=WebSphere MQ Devt,O=IBM,ST=Hampshire,C=UK")
   SSLPEER("SERIALNUMBER=4C:D0:49:D5:02:5F:38,CN=QMA,OU=WebSphere MQ
Development,O=IBM,ST=Hampshire,C=UK")
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

Le champ SSLPEER de la sortie DISPLAY CHSTATUS affiche le DN de sujet du certificat client distant créé à l'étape 2. Le nom de l'émetteur correspond au DN de l'objet du certificat de l'autorité de certification qui a signé le certificat personnel ajouté à l'étape 4.

Connexion anonyme d'un client à un gestionnaire de files d'attente

Suivez les instructions de cet exemple pour modifier un système avec l'authentification mutuelle afin d'autoriser un gestionnaire de files d'attente à se connecter anonymement à un autre gestionnaire de files d'attente.

Pourquoi et quand exécuter cette tâche

Scénario :

- Le gestionnaire de files d'attente et le client (QM1 et C1) ont été configurés comme dans la «Utilisation de certificats signés par l'autorité de certification pour l'authentification mutuelle d'un client et d'un gestionnaire de files d'attente», à la page 224.
- Vous souhaitez modifier C1 pour qu'il se connecte de manière anonyme à QM1.

La configuration qui en résulte se présente comme suit :

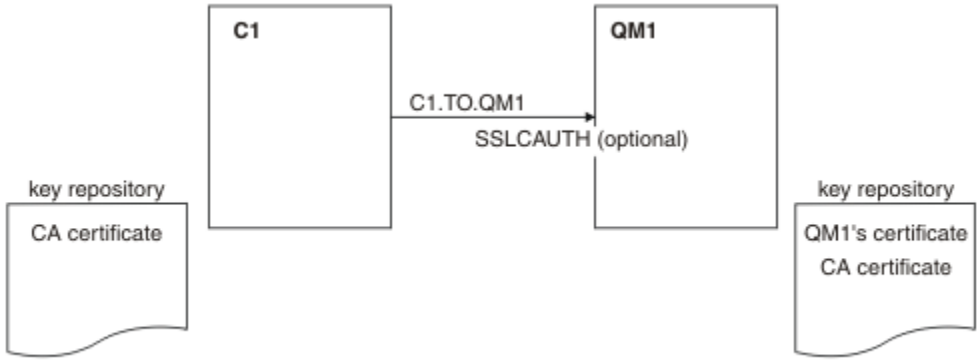


Figure 25. Client et gestionnaire de files d'attente autorisant la connexion anonyme

Procédure

1. Supprimez le certificat personnel du référentiel de clés pour C1, en fonction du système d'exploitation:
   - Sur les systèmes UNIX, Linuxet Windows. Le certificat est libellé comme suit:
     - `ibmwebspheremq` suivi de votre ID utilisateur de connexion en minuscules, par exemple `ibmwebspheremqmyuserid`.
2. Redémarrez l'application client ou faites en sorte qu'elle ferme et rouvre toutes les connexions SSL ou TLS.
3. Autorisez les connexions anonymes sur le gestionnaire de files d'attente en exécutant la commande suivante :

```
ALTER CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) SSLCAUTH(OPTIONAL)
```

Résultats

Les référentiels de clés et les canaux sont modifiés comme illustré dans la Figure 19, à la page 226.

Que faire ensuite

A l'extrémité serveur du canal, la présence de la valeur de paramètre du nom d'homologue sur le statut de canal indique qu'un certificat client a été transmis.

Vérifiez que la tâche a abouti en exécutant certaines commandes DISPLAY. Si la tâche a abouti, la sortie ressemble à l'exemple ci-après :

A partir du gestionnaire de files d'attente QM1, entrez la commande suivante :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
```

La sortie se présente comme suit :

```
DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
     5 : DISPLAY CHSTATUS(C1.TO.QM1) SSLPEER SSLCERTI
AMQ8417: Display Channel Status details.
   CHANNEL(C1.TO.QM1)                      CHLTYPE(SVRCONN)
   CONNAME(9.20.35.92)                     CURRENT
   SSLCERTI( )                             SSLPEER( )
   STATUS(RUNNING)                         SUBSTATE(RECEIVE)
```

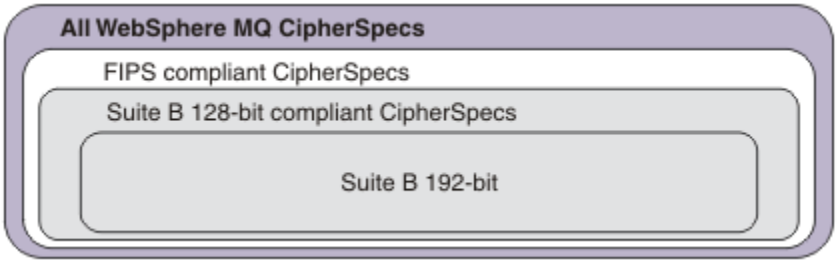
Les zones SSLCERTI et SSLPEER sont vides, indiquant que C1 n'a pas envoyé de certificat.

Définition des spécifications CipherSpec

Spécifiez un CipherSpec à l'aide du paramètre **SSLCIPH** dans la commande **DEFINE CHANNEL** MQSC ou dans la commande **ALTER CHANNEL** MQSC.

Certains CipherSpecs que vous pouvez utiliser avec IBM WebSphere MQ sont conformes à la norme FIPS. D'autres, comme NULL_MD5, ne le sont pas. De même, certains CipherSpecs conformes à la norme FIPS sont également conformes à la norme Suite B, alors que d'autres ne le sont pas. Tous les CipherSpecs conformes à la norme Suite B sont également conformes à la norme FIPS. Tous les CipherSpecs conformes à Suite B appartiennent à deux groupes: 128 bits (par exemple, ECDHE_ECDSA_AES_128_GCM_SHA256) et 192 bits (par exemple, ECDHE_ECDSA_AES_256_GCM_SHA384),

Le diagramme suivant illustre la relation entre ces sous-ensembles:



Les spécifications de chiffrement que vous pouvez utiliser avec le support IBM WebSphere MQ SSL et TLS sont répertoriées dans le tableau ci-dessous. Lorsque vous demandez un certificat personnel, vous définissez une taille de clé pour la paire de clé publique et de clé privée. La taille de clé utilisée lors de l'établissement de liaison SSL est celle qui est stockée dans le certificat à moins qu'elle soit déterminée par la spécification CipherSpec, comme indiqué dans le tableau.

Nom du CipherSpec	Protocole utilisé	Algorithme MAC	Algorithme de chiffrement	Bits de chiffrement	FIPS [1]	Suite B 128 bits	Suite B 192 bits
NULL_MD5 [a]	SSL 3.0	MD5	Aucun	0	Non	Non	Non
NULL_SHA [a]	SSL 3.0	SHA-1	Aucun	0	Non	Non	Non
RC4_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC4	40	Non	Non	Non
RC4_MD5_US [a]	SSL 3.0	MD5	RC4	128	Non	Non	Non
RC4_SHA_US [a]	SSL 3.0	SHA-1	RC4	128	Non	Non	Non
RC2_MD5_EXPORT [2] [a]	SSL 3.0	MD5	RC2	40	Non	Non	Non
DES_SHA_EXPORT [2] [a]	SSL 3.0	SHA-1	DES	56	Non	Non	Non
RC4_56_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	RC4	56	Non	Non	Non
DES_SHA_EXPORT1024 [3] [b]	SSL 3.0	SHA-1	DES	56	Non	Non	Non
TLS_RSA_WITH_AES_128_CBC_SHA [a]	TLS 1.0	SHA-1	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_CBC_SHA [4] [a]	TLS 1.0	SHA-1	AES	256	Oui	Non	Non
TLS_RSA_WITH_DES_CBC_SHA [a]	TLS 1.0	SHA-1	DES	56	Non [5]	Non	Non
FIPS_WITH_DES_CBC_SHA [b]	SSL 3.0	SHA-1	DES	56	Non [6]	Non	Non

Nom du CipherSpec	Protocole utilisé	Algorithme MAC	Algorithme de chiffrement	Bits de chiffrement	FIPS [1]	Suite B 128 bits	Suite B 192 bits
TLS_RSA_WITH_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Non
TLS_RSA_WITH_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non
TLS_RSA_WITH_AES_256_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	256	Oui	Non	Non
ECDHE_ECDSA_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Non	Non	Non
ECDHE_RSA_RC4_128_SHA256 [b]	TLS 1.2	SHA_1	RC4	128	Non	Non	Non
ECDHE_ECDSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non
ECDHE_ECDSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Oui	Non	Non
ECDHE_RSA_AES_128_CBC_SHA256 [b]	TLS 1.2	SHA-256	AES	128	Oui	Non	Non
ECDHE_RSA_AES_256_CBC_SHA384 [b]	TLS 1.2	SHA-384	AES	256	Oui	Non	Non
ECDHE_ECDSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Oui	Non
ECDHE_ECDSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Oui
ECDHE_RSA_AES_128_GCM_SHA256 [b]	TLS 1.2	AEAD AES-128 GCM	AES	128	Oui	Non	Non
ECDHE_RSA_AES_256_GCM_SHA384 [b]	TLS 1.2	AEAD AES-256 GCM	AES	256	Oui	Non	Non
TLS_RSA_WITH_NULL_SHA256 [b]	TLS 1.2	SHA-256	Aucun	0	Non	Non	Non
ECDHE_RSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Aucun	0	Non	Non	Non
ECDHE_ECDSA_NULL_SHA256 [b]	TLS 1.2	SHA-1	Aucun	0	Non	Non	Non
TLS_RSA_WITH_NULL_NULL [b]	TLS 1.2	Aucun	Aucun	0	Non	Non	Non
TLS_RSA_WITH_RC4_128_SHA256 [b]	TLS 1.2	SHA-1	RC4	128	Non	Non	Non

Nom du CipherSpec	Protocole utilisé	Algorithme MAC	Algorithme de chiffrement	Bits de chiffrement	FIPS [1]	Suite B 128 bits	Suite B 192 bits

Remarques :

1. Indique si le CipherSpec est certifié FIPS sur une plateforme certifiée FIPS. Voir la rubrique sur la norme FIPS (Federal Information Processing Standards) pour une explication de la norme FIPS.
2. La taille de clé d'établissement de liaison maximale est de 512 bits. Si l'un ou l'autre des certificats échangés lors de l'établissement de liaison SSL a une taille de clé supérieure à 512 bit, une clé temporaire de 512 bits est générée pour l'établissement de liaison.
3. La taille de clé d'établissement de liaison maximale est de 1024 bits.
4. Ce CipherSpec ne peut pas être utilisé pour sécuriser une connexion de WebSphere MQ Explorer à un gestionnaire de files d'attente, sauf si les fichiers de règles sans restriction appropriés sont appliqués à l'environnement d'exécution Java utilisé par l'explorateur.
5. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007.
6. Ce CipherSpec a été certifié FIPS 140-2 avant le 19 mai 2007. Le nom `FIPS_WITH_DES_CBC_SHA` est historique et reflète le fait que CipherSpec était précédemment (mais n'est plus) conforme à la norme FIPS. Ce CipherSpec est déprécié et son utilisation est déconseillée.
7. Ce CipherSpec permet de transférer jusqu'à 32 Go de données avant que la connexion ne s'arrête avec l'erreur AMQ9288. Pour éviter cette erreur, évitez d'utiliser la norme DES triple ou activez la réinitialisation de clé confidentielle lors de l'utilisation de ce CipherSpec.

Prise en charge des plateformes :

- a Disponible sur toutes les plateformes prises en charge.
- b Disponible uniquement sur les plateformes UNIX, Linux, and Windows .

Concepts associés

«Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36
Cette rubrique fournit des informations sur la façon de choisir les CipherSpecs et les certificats numériques appropriés pour votre règle de sécurité, en soulignant la relation entre les CipherSpecs et les certificats numériques dans IBM WebSphere MQ.

Référence associée

De la définition d'un canal
ALTER CHANNEL

Obtention d'informations sur les CipherSpecs à l'aide de IBM WebSphere MQ Explorer

Vous pouvez utiliser IBM WebSphere MQ Explorer pour afficher les descriptions des CipherSpecs.

Utilisez la procédure suivante pour obtenir des informations sur les CipherSpecs dans «Définition des spécifications CipherSpec», à la page 227:

1. Ouvrez **IBM WebSphere MQ Explorer** et développez le dossier **Gestionnaires de files d'attente** .
2. Vérifiez que vous avez démarré votre gestionnaire de files d'attente.
3. Sélectionnez le gestionnaire de files d'attente à utiliser et cliquez sur **Canaux**.
4. Cliquez avec le bouton droit de la souris sur le canal que vous souhaitez utiliser et sélectionnez **Propriétés**.
5. Sélectionnez la page de propriétés **SSL** .
6. Dans la liste, sélectionnez le CipherSpec que vous souhaitez utiliser. Une description s'affiche dans la fenêtre située sous la liste.

Alternatives pour la spécification de CipherSpecs

Pour les plateformes sur lesquelles le système d'exploitation fournit la prise en charge SSL, votre système peut prendre en charge de nouveaux CipherSpecs. Vous pouvez spécifier un nouveau CipherSpec avec le paramètre SSLCIPH, mais la valeur que vous fournissez dépend de votre plateforme.

Remarque : Cette section ne s'applique pas aux systèmes UNIX, Linux ou Windows , car les CipherSpecs sont fournis avec le produit WebSphere MQ , de sorte que les nouveaux CipherSpecs ne deviennent pas disponibles après l'expédition.

Pour les plateformes sur lesquelles le système d'exploitation fournit la prise en charge SSL, votre système peut prendre en charge de nouveaux CipherSpecs qui ne sont pas inclus dans «Définition des spécifications CipherSpec», à la page 227. Vous pouvez spécifier un nouveau CipherSpec avec le paramètre SSLCIPH, mais la valeur que vous fournissez dépend de votre plateforme. Dans tous les cas, la spécification *doit* correspondre à un CipherSpec SSL valide et pris en charge par la version de SSL exécutée par votre système.

IBM i

Chaîne de deux caractères représentant une valeur hexadécimale.

Pour plus d'informations sur les valeurs admises, reportez-vous à la documentation du produit appropriée (recherchez *cipher_spec* dans la documentation du produitIBM i).

Vous pouvez utiliser la commande CHGMQMCHL ou CRTMQMCHL pour spécifier la valeur, par exemple:

```
CRTMQMCHL CHLNAME('channel name') SSLCIPH('hexadecimal value')
```

Vous pouvez également utiliser la commande ALTER QMGR MQSC pour définir le paramètre SSLCIPH .

z/OS

Chaîne de deux caractères représentant une valeur hexadécimale. Les codes hexadécimaux correspondent aux valeurs définies dans le protocole SSL.

Pour plus d'informations, reportez-vous à la description de gsk_environment_open () dans le chapitre de référence de l'API *z/OS Cryptographic Services System SSL Programming*, SC24-5901, où se trouve la liste de toutes les spécifications de chiffrement SSL V3.0 et TLS V1.0 prises en charge, sous la forme de codes hexadécimaux à 2 chiffres.

Remarques relatives aux clusters WebSphere MQ

Avec les clusters WebSphere MQ , il est plus sûr d'utiliser les noms CipherSpec dans «Définition des spécifications CipherSpec», à la page 227. Si vous utilisez une autre spécification, sachez que la spécification peut ne pas être valide sur d'autres plateformes. Pour plus d'informations, voir «SSL et clusters», à la page 259.

Spécification d'un CipherSpec pour un client IBM WebSphere MQ MQI

Vous disposez de trois options pour spécifier un CipherSpec pour un client IBM WebSphere MQ MQI.

Ces options sont les suivantes :

- Utilisation d'une table de définition de canal
- Utilisation de la zone SSLCipherSpec dans la structure MQCD, à l'adresse MQCD_VERSION_7 ou supérieure, sur un appel MQCONNX.
- Utilisation d' Active Directory (sur les systèmes Windows avec prise en charge d' Active Directory)

Spécification d'une CipherSuite avec des classes IBM WebSphere MQ pour Java et des classes IBM WebSphere MQ pour JMS

IBM WebSphere MQ classes for Java et IBM WebSphere MQ classes for JMS spécifient CipherSuites différemment des autres plateformes.

Pour plus d'informations sur la spécification d'une CipherSuite avec des classes IBM WebSphere MQ pour Java, voir Secure Sockets Layer (SSL) support.

Pour plus d'informations sur la spécification d'une CipherSuite avec IBM WebSphere MQ classes for JMS, voir Utilisation de SSL (Secure Sockets Layer) avec WebSphere MQ classes for JMS.

Audit

Vous pouvez vérifier les intrusions de sécurité ou les tentatives d'intrusion à l'aide de messages d'événement. Vous pouvez également vérifier la sécurité de votre système à l'aide de la IBM WebSphere MQ Explorer.

Pour détecter les tentatives d'exécution d'actions non autorisées, telles que la connexion à un gestionnaire de files d'attente ou l'insertion d'un message dans une file d'attente, examinez les messages d'événement générés par vos gestionnaires de files d'attente, en particulier les messages d'événement de droits d'accès. Pour plus d'informations sur les messages d'événement du gestionnaire de files d'attente, voir Evénements du gestionnaire de files d'attente, et pour plus d'informations sur la surveillance des événements en général, voir Surveillance des événements .

Maintien de la sécurité des clusters

Autorisez ou empêchez les gestionnaires de files d'attente de rejoindre des clusters ou d'insérer des messages dans des files d'attente de cluster. Forcer un gestionnaire de files d'attente à quitter un cluster. Tenez compte de certaines considérations supplémentaires lors de la configuration de SSL pour les clusters.

Arrêt des gestionnaires de files d'attente non autorisés envoyant des messages

Empêchez les gestionnaires de files d'attente non autorisés d'envoyer des messages à votre gestionnaire de files d'attente à l'aide d'un exit de sécurité de canal.

Avant de commencer

La mise en cluster n'a aucun effet sur le fonctionnement des exits de sécurité. Vous pouvez restreindre l'accès à un gestionnaire de files d'attente de la même manière que dans un environnement de mise en file d'attente répartie.

Pourquoi et quand exécuter cette tâche

Empêchez les gestionnaires de files d'attente sélectionnés d'envoyer des messages à votre gestionnaire de files d'attente:

Procédure

1. Définissez un programme d'exit de sécurité de canal sur la définition de canal CLUSRCVR .
2. Ecrivez un programme qui authentifie les gestionnaires de files d'attente en tentant d'envoyer des messages sur votre canal récepteur de cluster et leur refuse l'accès s'ils ne sont pas autorisés.

Que faire ensuite

Les programmes d'exit de sécurité de canal sont appelés au démarrage et à l'arrêt de l'agent MCA.

Arrêt des gestionnaires de files d'attente non autorisés à insérer des messages dans vos files d'attente

Utilisez l'attribut de droit d'insertion de canal sur le canal récepteur de cluster pour arrêter les gestionnaires de files d'attente non autorisés à placer des messages dans vos files d'attente. Autorisez un gestionnaire de files d'attente éloignées en vérifiant l'ID utilisateur dans le message à l'aide de RACF sur z/OSou de la méthode d'accès aux objets (OAM) sur d'autres plateformes.

Pourquoi et quand exécuter cette tâche

Utilisez les fonctions de sécurité d'une plateforme et le mécanisme de contrôle d'accès dans WebSphere MQ pour contrôler l'accès aux files d'attente.

Procédure

1. Pour empêcher certains gestionnaires de files d'attente d'insérer des messages dans une file d'attente, utilisez les fonctions de sécurité disponibles sur votre plateforme.

   Exemple :

   - RACF ou d'autres gestionnaires de sécurité externes sur WebSphere MQ for z/OS
   - Gestionnaire des droits d'accès aux objets (OAM) sur d'autres plateformes.
2. Utilisez les droits d'insertion, PUTAUT, sur l'attribut de la définition de canal CLUSRCVR .

   L'attribut PUTAUT permet de spécifier les identificateurs utilisateur à utiliser pour établir le droit d'insertion d'un message dans une file d'attente.

   Les options de l'attribut PUTAUT sont les suivantes:

   DEF
   Utilisez l'ID utilisateur par défaut. Sous z/OS, la vérification peut impliquer l'utilisation à la fois de l'ID utilisateur reçu du réseau et de l'ID utilisateur dérivé de MCAUSER.

   CTX
   Utilisez l'ID utilisateur dans les informations de contexte associées au message. Sous z/OS , la vérification peut impliquer l'utilisation de l'ID utilisateur reçu du réseau ou de l'ID dérivé de MCAUSER, ou des deux. Utilisez cette option si le lien est sécurisé et authentifié.

   ONLYMCA (z/OS uniquement)
   Comme pour DEF, mais tout ID utilisateur reçu du réseau n'est pas utilisé. Utilisez cette option si le lien n'est pas sécurisé. Vous souhaitez autoriser uniquement un ensemble spécifique d'actions sur celui-ci, qui sont définies pour MCAUSER.

   ALTMCA (z/OS uniquement)
   Comme pour CTX, mais aucun ID utilisateur reçu du réseau n'est utilisé.

Autorisation d'insertion de messages dans des files d'attente de cluster éloignées

Sur votre plateforme, autorisez l'accès à la connexion au gestionnaire de files d'attente et à l'insertion dans la file d'attente de ce gestionnaire de files d'attente.

Pourquoi et quand exécuter cette tâche

Le comportement par défaut consiste à effectuer un contrôle d'accès sur le SYSTEM.CLUSTER.TRANSMIT.QUEUE. Notez que ce comportement s'applique, même si vous utilisez plusieurs files d'attente de transmission.

Le comportement spécifique décrit dans cette rubrique s'applique uniquement lorsque vous avez configuré l'attribut **ClusterQueueAccessControl** dans le fichier qm.ini comme étant *RQMName*, comme décrit dans la rubrique Strophe de sécurité , puis redémarré le gestionnaire de files d'attente.

Procédure

- Pour les systèmes UNIX, Linux et Windows , exécutez les commandes suivantes:

```
setmqaut -m QMgrName -t qmgr -g GroupName +connect
setmqaut -m QMgrName -t queue -n QueueName -g GroupName -all +put
```

  L'utilisateur peut placer des messages uniquement dans la file d'attente de cluster spécifiée, et aucune autre file d'attente de cluster.

  Les noms de variable ont les significations suivantes:

  QMgrName
  Nom du gestionnaire de files d'attente.

  GroupName
  Nom du groupe auquel l'accès doit être accordé.

  QueueName
  Nom de la file d'attente ou du profil générique pour lequel modifier les autorisations.

Que faire ensuite

Si vous indiquez une file d'attente de réponse lorsque vous placez un message dans une file d'attente de cluster, l'application destinataire doit être autorisée à envoyer la réponse. Définissez ces droits en suivant les instructions de la rubrique «Octroi du droit d'insertion de messages dans une file d'attente de cluster éloignée», à la page 201.

Information associée
Section de sécurité dans qm.ini

Empêcher les gestionnaires de files d'attente de rejoindre un cluster

Si un gestionnaire de files d'attente corrompu rejoint un cluster, il est difficile de l'empêcher de recevoir des messages que vous ne souhaitez pas recevoir.

Procédure

Si vous souhaitez vous assurer que seuls certains gestionnaires de files d'attente autorisés rejoignent un cluster, vous avez le choix entre trois techniques:

- A l'aide des enregistrements d'authentification de canal, vous pouvez bloquer la connexion de canal de cluster en fonction de l'adresse IP distante, du nom du gestionnaire de files d'attente distant ou du nom distinctif SSL/TLS fourni par le système distant.
- Ecrire un programme d'exit pour empêcher les gestionnaires de files d'attente non autorisés d'écrire dans SYSTEM.CLUSTER.COMMAND.QUEUE. Ne limitez pas l'accès à SYSTEM.CLUSTER.COMMAND.QUEUE de sorte qu'aucun gestionnaire de files d'attente ne puisse y écrire, sinon vous empêcheriez tout gestionnaire de files d'attente de rejoindre le cluster.
- Un programme d'exit de sécurité sur la définition de canal CLUSRCVR .

Exits de sécurité sur les canaux de cluster

Remarques supplémentaires à prendre en compte lors de l'utilisation des exits de sécurité sur les canaux de cluster.

Pourquoi et quand exécuter cette tâche

Lorsqu'un canal émetteur de cluster est démarré pour la première fois, il utilise les attributs définis manuellement par un administrateur système. Lorsque le canal est arrêté et redémarré, il récupère les attributs de la définition de canal récepteur de cluster correspondante. La définition de canal émetteur de cluster d'origine est remplacée par les nouveaux attributs, y compris l'attribut SecurityExit .

Procédure

1. Vous devez définir un exit de sécurité à la fois sur l'extrémité émettrice du cluster et sur l'extrémité réceptrice du cluster d'un canal.

   La connexion initiale doit être établie avec un établissement de liaison d'exit de sécurité, même si le nom de l'exit de sécurité est envoyé à partir de la définition du récepteur de cluster.
2. Validez `PartnerName` dans la structure `MQCXP` de l'exit de sécurité.

   L'exit doit autoriser le démarrage du canal uniquement si le gestionnaire de files d'attente partenaire est autorisé
3. Concevez l'exit de sécurité sur la définition de récepteur de cluster à lancer.
4. Si vous le concevez comme étant initié par l'expéditeur, un gestionnaire de files d'attente non autorisé sans exit de sécurité peut rejoindre le cluster car aucun contrôle de sécurité n'est effectué.

   Ce n'est que lorsque le canal est arrêté et redémarré que le nom `SCYEXIT` peut être envoyé à partir de la définition du récepteur de cluster et que des contrôles de sécurité complets ont été effectués.
5. Pour afficher la définition de canal émetteur de cluster en cours d'utilisation, utilisez la commande suivante:

   ```
   DISPLAY CLUSQMGR(queue manager) ALL
   ```

   La commande affiche les attributs qui ont été envoyés à partir de la définition du récepteur de cluster.
6. Pour afficher la définition d'origine, utilisez la commande suivante:

   ```
   DISPLAY CHANNEL(channel name) ALL
   ```
7. Vous devrez peut-être définir un exit de définition automatique de canal, `CHADEXIT`, sur le gestionnaire de files d'attente émetteur de cluster, si les gestionnaires de files d'attente se trouvent sur des plateformes différentes.

   Utilisez l'exit de définition automatique de canal pour définir l'attribut `SecurityExit` sur un format approprié pour la plateforme cible.
8. Déployez et configurez l'exit de sécurité.

   Windows UNIX Linux **Windows, systèmes UNIX and Linux**

   - La bibliothèque de liens dynamiques d'exit de sécurité doit se trouver dans le chemin indiqué dans l'attribut `SCYEXIT` de la définition de canal.
   - La bibliothèque de liaison dynamique de l'exit de définition automatique de canal doit se trouver dans le chemin indiqué dans l'attribut `CHADEXIT` de la définition de gestionnaire de files d'attente.

Forcer les gestionnaires de files d'attente indésirables à quitter un cluster

Forcez un gestionnaire de files d'attente non souhaité à quitter un cluster en exécutant la commande `RESET CLUSTER` sur un gestionnaire de files d'attente de référentiel complet.

Pourquoi et quand exécuter cette tâche

Vous pouvez forcer un gestionnaire de files d'attente indésirable à quitter un cluster. Si, par exemple, un gestionnaire de files d'attente est supprimé mais que ses canaux récepteurs de cluster sont toujours définis dans le cluster. Vous voudrez peut-être ranger.

Seuls les gestionnaires de files d'attente de référentiel complet sont autorisés à éjecter un gestionnaire de files d'attente d'un cluster.

Procédez comme suit pour éjecter le gestionnaire de files d'attente `OSLO` du cluster `NORWAY`:

Procédure

1. Sur un gestionnaire de files d'attente de référentiel complet, exécutez la commande suivante:

```
RESET CLUSTER(NORWAY) QMNAME(OSLO) ACTION(FORCEREMOVE)
```

2. Vous pouvez également utiliser QMID à la place de QMNAME dans la commande:

```
RESET CLUSTER(NORWAY) QMID(qmid) ACTION(FORCEREMOVE)
```

Résultats

Le gestionnaire de files d'attente qui est supprimé de force ne change pas: ses définitions de cluster local indiquent qu'il se trouve dans le cluster. Les définitions de tous les autres gestionnaires de files d'attente ne l'affichent pas dans le cluster.

Empêcher les gestionnaires de files d'attente de recevoir des messages

Vous pouvez empêcher un gestionnaire de files d'attente de cluster de recevoir des messages qu'il n'est pas autorisé à recevoir à l'aide de programmes d'exit.

Pourquoi et quand exécuter cette tâche

Il est difficile d'empêcher un gestionnaire de files d'attente membre d'un cluster de définir une file d'attente. Il existe un risque qu'un gestionnaire de files d'attente incontrôlable rejoigne un cluster et définisse sa propre instance de l'une des files d'attente du cluster. Il peut désormais recevoir des messages qu'il n'est pas autorisé à recevoir. Pour empêcher un gestionnaire de files d'attente de recevoir des messages, utilisez l'une des options suivantes fournies dans la procédure.

Procédure

- Un programme d'exit de canal sur chaque canal émetteur de cluster. Le programme d'exit utilise le nom de connexion pour déterminer si le gestionnaire de files d'attente de destination est approprié pour l'envoi des messages.
- Un programme d'exit de charge de travail de cluster, qui utilise les enregistrements de destination pour déterminer l'adéquation de la file d'attente de destination et du gestionnaire de files d'attente pour l'envoi des messages.

SSL et clusters

Lors de la configuration de SSL pour les clusters, sachez qu'une définition de canal CLUSRCVR est propagée à d'autres gestionnaires de files d'attente en tant que canal CLUSSDR défini automatiquement. Si un canal CLUSRCVR utilise SSL, vous devez configurer SSL sur tous les gestionnaires de files d'attente qui communiquent à l'aide du canal.

Pour plus d'informations sur SSL, voir Prise en charge deWebSphere MQ pour SSL et TLS. Les conseils qui s'y appliquent sont généralement applicables aux canaux de cluster, mais vous souhaiterez peut-être accorder une attention particulière aux éléments suivants:

Dans un cluster IBM WebSphere MQ , une définition de canal CLUSRCVR particulière est fréquemment propagée à de nombreux autres gestionnaires de files d'attente où elle est transformée en un CLUSSDRdéfini automatiquement. Par la suite, le CLUSSDR défini automatiquement est utilisé pour démarrer un canal vers CLUSRCVR. Si CLUSRCVR est configuré pour la connectivité SSL, les considérations suivantes s'appliquent:

- Tous les gestionnaires de files d'attente qui souhaitent communiquer avec ce CLUSRCVR doivent avoir accès à la prise en charge SSL. Cette mise à disposition SSL doit prendre en charge le CipherSpec pour le canal.
- Les différents gestionnaires de files d'attente auxquels les canaux émetteurs de cluster définis automatiquement ont été propagés auront chacun un nom distinctif différent associé. Si la vérification

d'homologue de nom distinctif doit être utilisée sur le CLUSRCVR , elle doit être configurée de sorte que tous les noms distinctifs pouvant être reçus soient correctement mis en correspondance.

Par exemple, supposons que tous les gestionnaires de files d'attente qui hébergeront des canaux émetteurs de cluster qui se connecteront à un CLUSRCVRparticulier soient associés à des certificats. Supposons également que les noms distinctifs de tous ces certificats définissent le pays en tant que Royaume-Uni, l'organisation en tant que IBM, l'unité organisationnelle en tant que IBM WebSphere MQ Development, et aient tous des noms communs sous la forme DEVT.QMnnn, où nnn est numérique.

Dans ce cas, la valeur SSLPEER de C=UK, O=IBM, OU=WebSphere MQ Development, CN=DEVT.QM* sur le CLUSRCVR permet à tous les canaux émetteurs de cluster requis de se connecter correctement, mais empêche les canaux émetteurs de cluster indésirables de se connecter.

- Si des chaînes CipherSpec personnalisées sont utilisées, sachez que les formats de chaîne personnalisés ne sont pas autorisés sur toutes les plateformes. Par exemple, la chaîneCipherSpec RC4_SHA_US a la valeur 05 on IBM i mais n'est pas une spécification valide sur les systèmes UNIX, Linux ou Windows . Par conséquent, si des paramètres SSLCIPH personnalisés sont utilisés sur un CLUSRCVR, tous les canaux émetteurs de cluster définis automatiquement doivent résider sur des plateformes sur lesquelles le support SSL sous-jacent implémente ce CipherSpec et sur lesquelles il peut être spécifié avec la valeur personnalisée. Si vous ne pouvez pas sélectionner une valeur pour le paramètre SSLCIPH qui sera comprise dans votre cluster, vous aurez besoin d'un exit de définition automatique de canal pour que les plateformes utilisées puissent la comprendre. Utilisez les chaînes textuelles CipherSpec lorsque cela est possible (par exemple, RC4_MD5_US).

Un paramètre SSLCRLNL s'applique à un gestionnaire de files d'attente individuel et n'est pas propagé à d'autres gestionnaires de files d'attente au sein d'un cluster.

Mise à niveau des gestionnaires de files d'attente en cluster et des canaux vers SSL

Mettez à niveau les canaux de cluster un par un, en modifiant tous les canaux CLUSRCVR avant les canaux CLUSSDR .

Avant de commencer

Tenez compte des considérations suivantes, car elles peuvent affecter votre choix de CipherSpec pour un cluster:

- Certains CipherSpecs ne sont pas disponibles sur toutes les plateformes. Prenez soin de choisir un CipherSpec pris en charge par tous les gestionnaires de files d'attente du cluster.
- Certains CipherSpecs peuvent être nouveaux dans la version actuelle de WebSphere MQ et ne pas être pris en charge dans les versions plus anciennes. Un cluster contenant des gestionnaires de files d'attente s'exécutant dans différentes éditions de MQ ne peut utiliser que les CipherSpecs prises en charge par chaque édition.

  Pour utiliser un nouveau CipherSpec dans un cluster, vous devez d'abord migrer tous les gestionnaires de files d'attente de cluster vers l'édition en cours.
- Certains CipherSpecs nécessitent l'utilisation d'un type spécifique de certificat numérique, notamment ceux qui utilisent la cryptographie Elliptic Curve.

Mettez à niveau tous les gestionnaires de files d'attente du cluster vers WebSphere MQ V6 ou version ultérieure, s'ils ne sont pas déjà à ces niveaux. Distribuez les certificats et les clés pour que SSL fonctionne à partir de chacun d'eux.

Pourquoi et quand exécuter cette tâche

Modifiez un CLUSRCVR à la fois et autorisez les modifications à passer par le cluster avant de modifier le suivant. Veillez à ne pas modifier le chemin inverse tant que les modifications du canal en cours n'ont pas été distribuées dans le cluster.

Procédure

1. Basculez les canaux CLUSRCVR vers SSL dans l'ordre de votre choix.

   Les modifications circulent dans la direction opposée sur les canaux qui ne sont pas remplacés par SSL.
2. Basculez tous les canaux manuels CLUSSDR vers SSL.

   Cela n'a aucun effet sur le fonctionnement du cluster, sauf si vous utilisez la commande REFRESH CLUSTER avec l'option REPOS(YES).

   Remarque : Pour les grands clusters, l'utilisation de la commande **REFRESH CLUSTER** peut affecter le fonctionnement du cluster et à nouveau tous les 27 jours lorsque les objets de cluster envoient automatiquement les mises à jour de statut à tous les gestionnaires de files d'attente intéressés. Voir L'actualisation d'un grand cluster peut affecter les performances et la disponibilité du cluster.

Concepts associés

«Définition des spécifications CipherSpec», à la page 227
Spécifiez un CipherSpec à l'aide du paramètre **SSLCIPH** dans la commande **DEFINE CHANNEL** MQSC ou dans la commande **ALTER CHANNEL** MQSC.

«Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36
Cette rubrique fournit des informations sur la façon de choisir les CipherSpecs et les certificats numériques appropriés pour votre règle de sécurité, en soulignant la relation entre les CipherSpecs et les certificats numériques dans IBM WebSphere MQ.

Information associée

Mise en cluster : meilleures pratiques d'utilisation REFRESH CLUSTER

Désactivation de SSL ou TLS sur les gestionnaires de files d'attente et les canaux de cluster

Pour désactiver SSL ou TLS, définissez le paramètre SSLCIPH sur ' '. Désactivez TLS sur les canaux de cluster individuellement, en modifiant tous les canaux récepteurs de cluster avant les canaux émetteurs de cluster.

Pourquoi et quand exécuter cette tâche

Modifiez un canal récepteur de cluster à la fois et autorisez les modifications à transiter par le cluster avant de modifier le suivant.

Important : Veillez à ne pas modifier le chemin inverse tant que les modifications du canal en cours n'ont pas été distribuées dans le cluster.

Procédure

1. Définissez la valeur du paramètre SSLCIPH sur ' ', une chaîne vide entre apostrophes .

   Vous pouvez désactiver SSL ou TLS sur les canaux récepteurs de cluster dans l'ordre de votre choix.

   Notez que les modifications circulent dans la direction opposée sur les canaux sur lesquels vous laissez SSL ou TLS actif.
2. Vérifiez que la nouvelle valeur est reflétée dans tous les autres gestionnaires de files d'attente à l'aide de la commande **DISPLAY CLUSQMGR(*)** ALL.
3. Désactivez SSL ou TLS sur tous les canaux émetteurs de cluster manuels.

   Cela n'a aucun effet sur le fonctionnement du cluster, sauf si vous utilisez la commande **REFRESH CLUSTER** avec l'option REPOS (YES).

   Pour les clusters de grande taille, l'utilisation de la commande **REFRESH CLUSTER** peut perturber le cluster pendant qu'il est en cours, puis à intervalles réguliers, lorsque les objets de cluster envoient automatiquement des mises à jour de statut à tous les gestionnaires de files d'attente intéressés.

Pour plus d'informations, voir La régénération dans un cluster de grande taille peut affecter les performances et la disponibilité du cluster .

4. Arrêtez et redémarrez les canaux émetteurs de cluster.

Sécurité de publication / abonnement

Les composants et les interactions impliqués dans la publication / l'abonnement sont décrits comme une introduction aux explications et exemples plus détaillés qui suivent.

Un certain nombre de composants sont impliqués dans la publication et l'abonnement à une rubrique. Certaines des relations de sécurité entre eux sont illustrées dans Figure 26, à la page 262 et décrites dans l'exemple suivant.

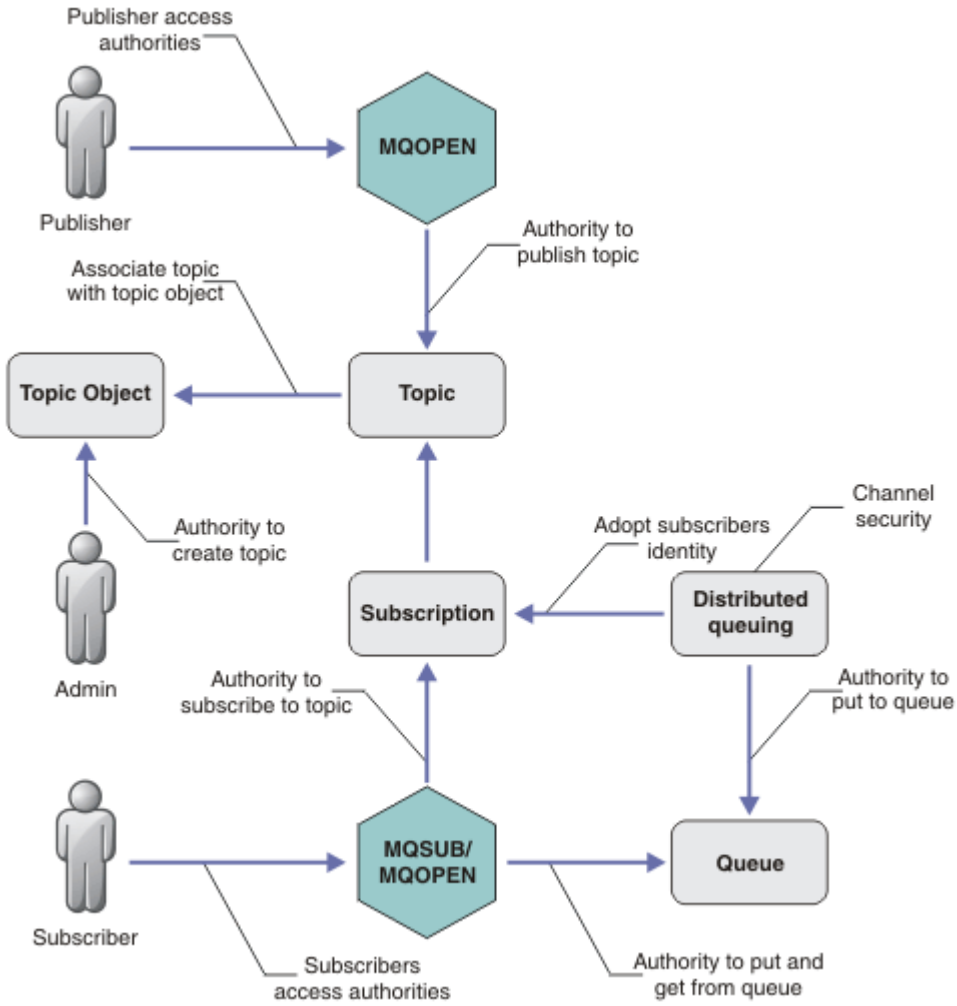


Figure 26. Relations de sécurité de publication / abonnement

Rubriques

Les rubriques sont identifiées par des chaînes de rubrique et sont généralement organisées en arborescences. Voir Arborescences de rubriques. Vous devez associer une rubrique à un objet de rubrique pour contrôler l'accès à la rubrique. «Modèle de sécurité de rubrique», à la page 264 explique comment sécuriser les rubriques à l'aide d'objets de rubrique.

Objets de rubrique d'administration

Vous pouvez contrôler qui a accès à une rubrique et dans quel but, à l'aide de la commande **setmqaut** avec une liste d'objets de rubrique d'administration. Consultez les exemples, «Accorder

l'accès à un utilisateur pour s'abonner à une rubrique», à la page 269 et «Accorder l'accès à un utilisateur pour la publication dans une rubrique», à la page 275.

Abonnements

Abonnez-vous à une ou plusieurs rubriques en créant un abonnement fournissant une chaîne de rubrique, qui peut inclure des caractères génériques, à mettre en correspondance avec les chaînes de rubrique des publications. Pour plus de détails, voir:

S'abonner à l'aide d'un objet de rubrique
«Abonnement à l'aide du nom d'objet de rubrique», à la page 266

S'abonner à l'aide d'une rubrique
«Abonnement à l'aide d'une chaîne de rubrique dans laquelle le noeud de rubrique n'existe pas», à la page 266

S'abonner à l'aide d'une rubrique avec des caractères génériques
«Abonnement à l'aide d'une chaîne de sujet contenant des caractères génériques», à la page 267

Un abonnement contient des informations sur l'identité de l'abonné et sur l'identité de la file d'attente de destination dans laquelle les publications doivent être placées. Il contient également des informations sur la manière dont la publication doit être placée dans la file d'attente de destination.

En plus de définir les abonnés qui ont le droit de s'abonner à certaines rubriques, vous pouvez limiter les abonnements à l'utilisation par un abonné individuel. Vous pouvez également contrôler les informations sur l'abonné qui sont utilisées par le gestionnaire de files d'attente lorsque des publications sont placées dans la file d'attente de destination. Voir «Sécurité des abonnements», à la page 279.

Files d'attente

La file d'attente de destination est une file d'attente importante à sécuriser. Il est local pour l'abonné et les publications qui correspondent à l'abonnement y sont placées. Vous devez envisager d'accéder à la file d'attente de destination à partir de deux perspectives:

1. Insertion d'une publication dans la file d'attente de destination.
2. Extraction de la publication de la file d'attente de destination.

Le gestionnaire de files d'attente place une publication dans la file d'attente de destination à l'aide d'une identité fournie par l'abonné. L'abonné, ou un programme auquel la tâche d'obtention de publications a été déléguée, enlève les messages de la file d'attente. Voir «Droits d'accès aux files d'attente de destination», à la page 267.

Il n'existe pas d'alias d'objet de rubrique, mais vous pouvez utiliser une file d'attente alias comme alias d'un objet de rubrique. Dans ce cas, en plus de vérifier les droits d'utilisation de la rubrique pour la publication ou l'abonnement, le gestionnaire de files d'attente vérifie les droits d'utilisation de la file d'attente.

Sécurité de publication / abonnement entre les gestionnaires de files d'attente

Votre droit de publication ou d'abonnement à une rubrique est vérifié sur le gestionnaire de files d'attente local à l'aide des identités et des autorisations locales. L'autorisation ne dépend pas de la définition ou non de la rubrique, ni de l'endroit où elle est définie. Par conséquent, vous devez effectuer une autorisation de rubrique sur chaque gestionnaire de files d'attente d'un cluster lorsque des rubriques en cluster sont utilisées.

Remarque : Le modèle de sécurité des rubriques diffère du modèle de sécurité des files d'attente. Vous pouvez obtenir le même résultat pour les files d'attente en définissant un alias de file d'attente en local pour chaque file d'attente en cluster.

Les gestionnaires de files d'attente échangent des abonnements dans un cluster. Dans la plupart des configurations de cluster WebSphere MQ , les canaux sont configurés avec PUTAUT=DEF pour placer les messages dans les files d'attente cible en utilisant les droits du processus de canal. Vous pouvez modifier la configuration de canal pour utiliser PUTAUT=CTX afin que l'utilisateur abonné ait le droit de propager un abonnement à un autre gestionnaire de files d'attente dans un cluster.

La sécurité de publication / abonnement entre les gestionnaires de files d'attente décrit comment modifier vos définitions de canal pour contrôler qui est autorisé à propager des abonnements sur d'autres serveurs du cluster.

Authorization

Vous pouvez appliquer une autorisation à des objets de rubrique, tout comme des files d'attente et d'autres objets. Il existe trois opérations d'autorisation, pub, subet `resume` , que vous pouvez appliquer uniquement aux rubriques. Les détails sont décrits dans Spécification des droits pour différents types d'objet.

Appels de fonction

Dans les programmes de publication et d'abonnement, comme dans les programmes en file d'attente, des vérifications d'autorisation sont effectuées lorsque des objets sont ouverts, créés, modifiés ou supprimés. Les vérifications ne sont pas effectuées lorsque des appels `MQPUT` ou `MQGET` `MQI` sont effectués pour placer et obtenir des publications.

Pour publier une rubrique, effectuez un `MQOPEN` sur la rubrique, qui effectue les vérifications d'autorisation. Publiez des messages dans le descripteur de rubrique à l'aide de la commande `MQPUT` , qui n'effectue aucune vérification d'autorisation.

Pour vous abonner à une rubrique, vous exécutez généralement une commande `MQSUB` pour créer ou reprendre l'abonnement, ainsi que pour ouvrir la file d'attente de destination afin de recevoir des publications. Vous pouvez également effectuer un `MQOPEN` distinct pour ouvrir la file d'attente de destination, puis exécuter la commande `MQSUB` pour créer ou reprendre l'abonnement.

Quels que soient les appels que vous utilisez, le gestionnaire de files d'attente vérifie que vous pouvez vous abonner à la rubrique et obtenir les publications résultantes de la file d'attente de destination. Si la file d'attente de destination n'est pas gérée, des vérifications d'autorisation sont également effectuées pour que le gestionnaire de files d'attente puisse placer des publications dans la file d'attente de destination. Il utilise l'identité qu'il a adoptée à partir d'un abonnement correspondant. Il est supposé que le gestionnaire de files d'attente est toujours en mesure de placer des publications dans des files d'attente de destination gérées.

Rôles

Les utilisateurs sont impliqués dans quatre rôles lors de l'exécution d'applications de publication / abonnement:

1. Diffuseur de publications
2. Abonné
3. Administrateur de rubriques
4. WebSphere MQ Administrateur-membre du groupe `mqm`

Définissez des groupes avec les autorisations appropriées correspondant aux rôles de publication, d'abonnement et d'administration de sujet. Vous pouvez ensuite affecter des principaux à ces groupes en les autorisant à effectuer des tâches de publication et d'abonnement spécifiques.

En outre, vous devez étendre les autorisations d'opérations d'administration à l'administrateur des files d'attente et des canaux en charge du déplacement des publications et des abonnements.

Modèle de sécurité de rubrique

Seuls les objets de rubrique définis peuvent être associés à des attributs de sécurité. Pour obtenir une description des objets de rubrique, voir Objets de rubrique d'administration. Les attributs de sécurité indiquent si un ID utilisateur ou un groupe de sécurité spécifié est autorisé à effectuer une opération d'abonnement ou de publication sur chaque objet de rubrique.

Les attributs de sécurité sont associés au noeud d'administration approprié dans l'arborescence de rubriques. Lorsqu'une vérification des droits est effectuée pour un ID utilisateur particulier lors d'une opération d'abonnement ou de publication, les droits accordés sont basés sur les attributs de sécurité du noeud d'arborescence de rubriques associé.

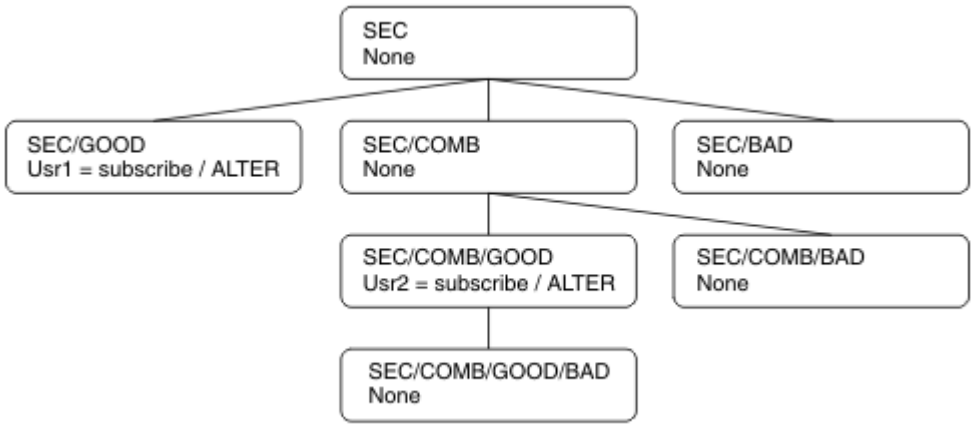
Les attributs de sécurité sont une liste de contrôle d'accès qui indique les droits d'accès d'un ID utilisateur ou d'un groupe de sécurité du système d'exploitation sur l'objet de rubrique.

Prenez l'exemple suivant dans lequel les objets de rubrique ont été définis avec les attributs de sécurité ou les droits affichés:

Tableau 17. Exemples de droits sur les objets de rubrique

Nom de la rubrique	**Chaîne de rubrique**	**Droits-non z/OS**	**Droits z/OS**
SECROOT	SEC	Aucun	Aucun
SECGOOD	SEC/GOOD	usr1+subscribe	ALTER HLQ.SUBSCRIBE.SECGOOD
SECBAD	SEC/BAD	Aucun	Aucun HLQ.SUBSCRIBE.SECBAD
SECCOMB	SEC/COMB	Aucun	Aucun HLQ.SUBSCRIBE.SECCOMB
SECCOMBB	SEC/COMB/ GOOD/BAD	Aucun	Aucun HLQ.SUBSCRIBE.SECCOMBB
SECCOMBG	SEC/COMB/GOOD	usr2+subscribe	ALTER HLQ.SUBSCRIBE.SECCOMBG
SECCOMBN	SEC/COMB/BAD	Aucun	Aucun HLQ.SUBSCRIBE.SECCOMBN

L'arborescence de rubriques avec les attributs de sécurité associés sur chaque noeud peut être représentée comme suit:



Les exemples répertoriés donnent les autorisations suivantes:

- Sur le noeud racine de l'arborescence /SEC, aucun utilisateur n'a de droits sur ce noeud.
- usr1 a reçu le droit d'abonnement à l'objet /SEC/GOOD
- usr2 a reçu le droit d'abonnement à l'objet /SEC/COMB/GOOD

Abonnement à l'aide du nom d'objet de rubrique

Lors de l'abonnement à un objet de rubrique en spécifiant le nom MQCHAR48 , le noeud correspondant dans l'arborescence de rubriques est localisé. Si les attributs de sécurité associés au noeud indiquent que l'utilisateur est autorisé à s'abonner, l'accès est accordé.

Si l'accès n'est pas accordé à l'utilisateur, le noeud parent de l'arborescence détermine si l'utilisateur est autorisé à s'abonner au niveau du noeud parent. Si tel est le cas, l'accès est accordé. Si ce n'est pas le cas, le parent de ce noeud est pris en compte. La récursivité se poursuit jusqu'à ce qu'un noeud soit localisé et accorde le droit d'abonnement à l'utilisateur. La récursivité s'arrête lorsque le noeud racine est pris en compte sans que les droits aient été accordés. Dans ce dernier cas, l'accès est refusé.

En résumé, si un noeud du chemin accorde le droit de s'abonner à cet utilisateur ou à cette application, l'abonné est autorisé à s'abonner à ce noeud ou à n'importe quel emplacement situé en dessous de ce noeud dans l'arborescence de rubriques.

Le noeud racine de l'exemple est SEC.

Le droit d'abonnement est accordé à l'utilisateur si la liste de contrôle d'accès indique que l'ID utilisateur lui-même dispose de droits ou qu'un groupe de sécurité du système d'exploitation dont l'ID utilisateur est membre dispose de droits.

Ainsi, par exemple:

- Si `usr1` tente de s'abonner à l'aide d'une chaîne de rubrique `SEC/GOOD`, l'abonnement est autorisé car l'ID utilisateur a accès au noeud associé à cette rubrique. Toutefois, si `usr1` tente de s'abonner à l'aide de la chaîne de rubrique `SEC/COMB/GOOD` , l'abonnement ne sera pas autorisé car l'ID utilisateur n'a pas accès au noeud qui lui est associé.
- Si `usr2` tente de s'abonner, à l'aide d'une chaîne de rubrique `SEC/COMB/GOOD` , l'abonnement est autorisé car l'ID utilisateur a accès au noeud associé à la rubrique. Toutefois, si `usr2` tentait de s'abonner à `SEC/GOOD` , l'abonnement ne serait pas autorisé car l'ID utilisateur n'a pas accès au noeud qui lui est associé.
- Si `usr2` tente de s'abonner à l'aide d'une chaîne de rubrique `SEC/COMB/GOOD/BAD` , l'abonnement est autorisé car l'ID utilisateur a accès au noeud parent `SEC/COMB/GOOD`.
- Si `usr1` ou `usr2` tente de s'abonner à l'aide d'une chaîne de rubrique `/SEC/COMB/BAD`, aucune n'est autorisée car ils n'ont pas accès au noeud de rubrique qui lui est associé, ni aux noeuds parent de cette rubrique.

Une opération d'abonnement spécifiant le nom d'un objet de rubrique qui n'existe pas génère une erreur MQRC_UNKNOWN_OBJECT_NAME.

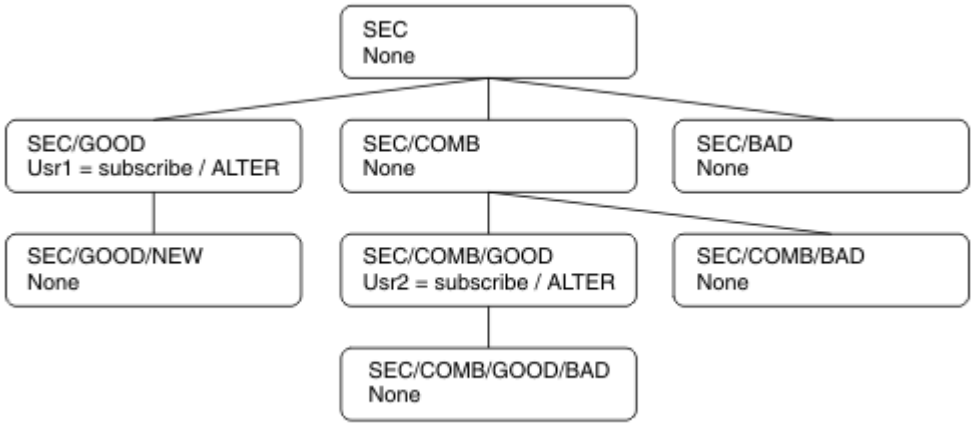
Abonnement à l'aide d'une chaîne de rubrique dans laquelle le noeud de rubrique existe

Le comportement est le même que lors de la spécification de la rubrique par le nom d'objet MQCHAR48 .

Abonnement à l'aide d'une chaîne de rubrique dans laquelle le noeud de rubrique n'existe pas

Prenons le cas d'une application abonnée, en spécifiant une chaîne de rubrique représentant un noeud de rubrique qui n'existe pas actuellement dans l'arborescence de rubriques. La vérification des droits d'accès est effectuée comme indiqué dans la section précédente. La vérification commence par le noeud parent de celui qui est représenté par la chaîne de rubrique. Si les droits sont accordés, un nouveau noeud représentant la chaîne de rubrique est créé dans l'arborescence de rubriques.

Par exemple, `usr1` tente de s'abonner à une rubrique `SEC/GOOD/NEW`. Les droits sont accordés car `usr1` a accès au noeud parent `SEC/GOOD`. Un nouveau noeud de rubrique est créé dans l'arborescence, comme le montre le diagramme suivant. Le nouveau noeud de rubrique n'est pas un objet de rubrique auquel aucun attribut de sécurité n'est directement associé ; les attributs sont hérités de son parent.



Abonnement à l'aide d'une chaîne de sujet contenant des caractères génériques

Prenez en compte le cas de l'abonnement à l'aide d'une chaîne de rubrique contenant un caractère générique. La vérification des droits est réalisée sur le noeud dans l'arborescence de sujets qui correspond à la partie qualifiée complète de la chaîne de sujet.

Par conséquent, si une application s'abonne à SEC/COMB/GOOD/*, une vérification des droits d'accès est effectuée comme indiqué dans les deux sections précédentes sur le noeud SEC/COMB/GOOD dans l'arborescence de rubriques.

De même, si une application doit s'abonner à SEC/COMB/*/GOOD, une vérification des droits d'accès est effectuée sur le noeud SEC/COMB.

Droits d'accès aux files d'attente de destination

Lors de l'abonnement à une rubrique, l'un des paramètres est le descripteur hobj d'une file d'attente qui a été ouverte pour la sortie afin de recevoir les publications.

Si hobj n'est pas spécifié, mais qu'il est vide, une file d'attente gérée est créée si les conditions suivantes s'appliquent:

- L'option MQSO_MANAGED a été spécifiée.
- L'abonnement n'existe pas.
- La création est spécifiée.

Si hobj est vide et que vous modifiez ou reprenez un abonnement existant, la file d'attente de destination précédemment fournie peut être gérée ou non gérée.

L'application ou l'utilisateur qui effectue la demande MQSUB doit avoir le droit d'insérer des messages dans la file d'attente de destination qu'elle a fournie ; en effet, il doit avoir le droit d'insérer des messages publiés dans cette file d'attente. La vérification des droits d'accès suit les règles existantes pour la vérification de la sécurité de la file d'attente.

La vérification de la sécurité inclut un ID utilisateur alternatif et des vérifications de la sécurité du contexte, le cas échéant. Pour pouvoir définir l'une des zones de contexte d'identité, vous devez spécifier l'option MQSO_SET_IDENTITY_CONTEXT ainsi que l'option MQSO_CREATE ou MQSO_ALTER . Vous ne pouvez pas définir de zones de contexte d'identité dans une demande MQSO_RESUME .

Si la destination est une file d'attente gérée, aucun contrôle de sécurité n'est effectué sur la destination gérée. Si vous êtes autorisé à vous abonner à une rubrique, il est supposé que vous pouvez utiliser des destinations gérées.

Publication à l'aide du nom de rubrique ou de la chaîne de rubrique dans laquelle le noeud de rubrique existe

Le modèle de sécurité pour la publication est le même que pour l'abonnement, à l'exception des caractères génériques. Les publications ne contiennent pas de caractères génériques ; il n'y a donc pas de cas d'une chaîne de rubrique contenant des caractères génériques à prendre en compte.

Les droits de publication et d'abonnement sont distincts. Un utilisateur ou un groupe peut avoir le droit d'en effectuer un sans être nécessairement en mesure d'en effectuer un autre.

Lors de la publication dans un objet de rubrique en spécifiant le nom MQCHAR48 ou la chaîne de rubrique, le noeud correspondant dans l'arborescence de rubriques est localisé. Si les attributs de sécurité associés au noeud de rubrique indiquent que l'utilisateur est autorisé à publier, l'accès est accordé.

Si l'accès n'est pas accordé, le noeud parent de l'arborescence détermine si l'utilisateur a le droit de publier à ce niveau. Si tel est le cas, l'accès est accordé. Si ce n'est pas le cas, la récursivité se poursuit jusqu'à ce qu'un noeud soit localisé et accorde le droit de publication à l'utilisateur. La récursivité s'arrête lorsque le noeud racine est pris en compte sans que les droits aient été accordés. Dans ce dernier cas, l'accès est refusé.

En bref, si un noeud du chemin accorde le droit de publier à cet utilisateur ou à cette application, le diffuseur de publications est autorisé à publier sur ce noeud ou n'importe où en dessous de ce noeud dans l'arborescence de rubriques.

Publication à l'aide du nom de rubrique ou de la chaîne de rubrique où le noeud de rubrique n'existe pas

Comme pour l'opération d'abonnement, lorsqu'une application publie, en spécifiant une chaîne de rubrique représentant un noeud de rubrique qui n'existe pas actuellement dans l'arborescence de rubriques, la vérification des droits d'accès est effectuée en commençant par le parent du noeud représenté par la chaîne de rubrique. Si les droits sont accordés, un nouveau noeud représentant la chaîne de rubrique est créé dans l'arborescence de rubriques.

Publication à l'aide d'une file d'attente alias qui se résout en un objet de rubrique

Si vous publiez à l'aide d'une file d'attente alias qui se résout en un objet de rubrique, la vérification de la sécurité est effectuée à la fois sur la file d'attente alias et sur la rubrique sous-jacente à laquelle elle se résout.

Le contrôle de sécurité de la file d'attente alias vérifie que l'utilisateur est autorisé à placer des messages dans cette file d'attente alias et le contrôle de sécurité de la rubrique vérifie que l'utilisateur peut publier des messages dans cette rubrique. Lorsqu'une file d'attente alias est résolue en une autre file d'attente, les vérifications ne sont *pas* effectuées sur la file d'attente sous-jacente. La vérification des droits d'accès est effectuée différemment pour les rubriques et les files d'attente.

Fermeture d'un abonnement

Un contrôle de sécurité supplémentaire est effectué si vous fermez un abonnement à l'aide de l'option MQCO_REMOVE_SUB si vous n'avez pas créé l'abonnement sous ce descripteur.

Un contrôle de sécurité est effectué pour vous assurer que vous disposez des droits appropriés pour effectuer cette opération, car l'action entraîne la suppression de l'abonnement. Si les attributs de sécurité associés au noeud de rubrique indiquent que l'utilisateur dispose de droits d'accès, l'accès est accordé. Si ce n'est pas le cas, le noeud parent de l'arborescence est pris en compte pour déterminer si l'utilisateur a le droit de fermer l'abonnement. La récursivité se poursuit jusqu'à ce que les droits soient accordés ou que le noeud racine soit atteint.

Définition, modification et suppression d'un abonnement

Aucun contrôle de sécurité d'abonnement n'est effectué lorsqu'un abonnement est créé de manière administrative au lieu d'utiliser une demande d'API MQSUB . Ce droit a déjà été accordé à l'administrateur via la commande.

Des contrôles de sécurité sont effectués pour s'assurer que les publications peuvent être placées dans la file d'attente de destination associée à l'abonnement. Les vérifications sont effectuées de la même manière que pour une demande MQSUB .

L'ID utilisateur utilisé pour ces contrôles de sécurité dépend de la commande émise. Si le paramètre **SUBUSER** est spécifié, il affecte la manière dont la vérification est effectuée, comme illustré dans la Tableau 18, à la page 269:

Tableau 18. ID utilisateur utilisés pour les contrôles de sécurité des commandes

Commande	SUBUSER indiqué et vide	SUBUSER indiqué et terminé	SUBUSER non indiqué
	Utiliser l'ID administrateur		Utiliser l'ID administrateur
	Utiliser l'ID administrateur		Utiliser l'ID utilisateur de l'abonnement existant

Le seul contrôle de sécurité effectué lors de la suppression d'abonnements à l'aide de la commande DELETE SUB est le contrôle de sécurité de la commande.

Exemple de configuration de la sécurité de publication / abonnement

Cette section décrit un scénario dans lequel le contrôle d'accès est configuré sur les rubriques de manière à permettre l'application du contrôle de sécurité selon les besoins.

Accorder l'accès à un utilisateur pour s'abonner à une rubrique

Cette rubrique est la première d'une liste de tâches qui vous indique comment accorder l'accès aux rubriques à plusieurs utilisateurs.

Pourquoi et quand exécuter cette tâche

Cette tâche suppose qu'aucun objet de rubrique d'administration n'existe et qu'aucun profil n'a été défini pour l'abonnement ou la publication. Les applications créent de nouveaux abonnements, plutôt que de reprendre des abonnements existants, et utilisent uniquement la chaîne de rubrique.

Une application peut s'abonner en fournissant un objet de rubrique, une chaîne de rubrique ou une combinaison des deux. Quelle que soit la façon dont l'application sélectionne, l'effet est de créer un abonnement à un certain point de l'arborescence de rubriques. Si ce point de l'arborescence de rubriques est représenté par un objet de rubrique d'administration, un profil de sécurité est vérifié en fonction du nom de cet objet de rubrique.

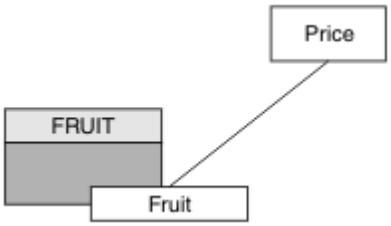


Figure 27. Exemple d'accès à un objet de rubrique

Tableau 19. Exemple d'accès à un objet de rubrique

Topic	Accès à l'abonnement requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun
Prix / Fruits	USER1	fruit

Définissez un nouvel objet de rubrique comme suit:

Procédure

1. Exécutez la commande MQSC `DEF TOPIC(FRUIT) TOPICSTR('Price/Fruit')`.
2. Accordez l'accès comme suit:
   - Autres plateformes:

     Accordez l'accès à USER1 pour vous abonner à la rubrique `"Price/Fruit"` en accordant à l'utilisateur l'accès à l'objet FRUIT . Pour ce faire, utilisez la commande d'autorisation pour la plateforme:

     Windows UNIX Linux **Windows, systèmes UNIX and Linux**

     ```
     setmqaut -t topic -n FRUIT -p USER1 +sub
     ```

Résultats

Lorsque USER1 tente de s'abonner à la rubrique `"Price/Fruit"` , le résultat est un succès.

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit"` , le résultat est un échec avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- Windows UNIX Linux Sur les autres plateformes, l'événement d'autorisation suivant:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

Notez qu'il s'agit d'une illustration de ce que vous voyez ; pas de tous les champs.

Accorder l'accès à un utilisateur pour s'abonner à une rubrique plus en profondeur dans l'arborescence

Cette rubrique est la deuxième d'une liste de tâches qui vous indique comment accorder l'accès aux rubriques à plusieurs utilisateurs.

Avant de commencer

Cette rubrique utilise la configuration décrite dans «Accorder l'accès à un utilisateur pour s'abonner à une rubrique», à la page 269.

Pourquoi et quand exécuter cette tâche

Si le point dans l'arborescence de rubriques où l'application effectue l'abonnement n'est pas représenté par un objet de rubrique d'administration, déplacez l'arborescence vers le haut jusqu'à ce que l'objet de rubrique d'administration parent le plus proche soit localisé. Le profil de sécurité est vérifié en fonction du nom de cet objet de rubrique.

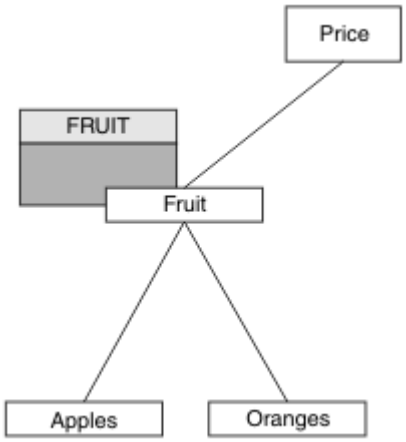


Figure 28. Exemple d'octroi d'accès à une rubrique dans une arborescence de rubriques

Tableau 20. Exigences d'accès pour des exemples de rubriques et d'objets de rubrique

Topic	Accès à l'abonnement requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun
Prix / Fruits	USER1	fruit
Prix / Fruits / Pommes	USER1	
Prix / Fruits / Oranges	USER1	

Dans la tâche précédente, USER1 a été autorisé à s'abonner à la rubrique `"Price/Fruit"` en lui accordant l'accès au profil `hlq.SUBSCRIBE.FRUIT` sur z/OS et l'accès par abonnement au profil FRUIT sur d'autres plateformes. Ce profil unique accorde également à USER1 l'accès pour s'abonner à `"Price/Fruit/Apples"`, `"Price/Fruit/Oranges"` et `"Price/Fruit/#"`.

Lorsque USER1 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le résultat est un succès.

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le résultat est un échec avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- Sous z/OS, les messages suivants s'affichent sur la console et indiquent le chemin de sécurité complet via l'arborescence de rubriques qui a été tentée:

```
ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.FRUIT ...

ICH408I USER(USER2   ) ...
  hlq.SUBSCRIBE.SYSTEM.BASE.TOPIC ...
```

- Sur les autres plateformes, l'événement d'autorisation suivant:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Apples"
```

Notez ce qui suit :

- Les messages que vous recevez sous z/OS sont identiques à ceux reçus lors de la tâche précédente car les mêmes objets de rubrique et les mêmes profils contrôlent l'accès.
- Le message d'événement que vous recevez sur d'autres plateformes est similaire à celui reçu lors de la tâche précédente, mais la chaîne de rubrique réelle est différente.

Accorder à un autre utilisateur l'accès permettant de s'abonner uniquement à la rubrique située plus en profondeur dans l'arborescence

Cette rubrique est la troisième d'une liste de tâches qui vous indique comment accorder l'accès à l'abonnement à des rubriques par plusieurs utilisateurs.

Avant de commencer

Cette rubrique utilise la configuration décrite dans «Accorder l'accès à un utilisateur pour s'abonner à une rubrique plus en profondeur dans l'arborescence», à la page 270.

Pourquoi et quand exécuter cette tâche

Dans la tâche précédente, l'accès à la rubrique `"Price/Fruit/Apples"`a été refusé USER2 . Cette rubrique vous explique comment accorder l'accès à cette rubrique, mais pas à d'autres rubriques.

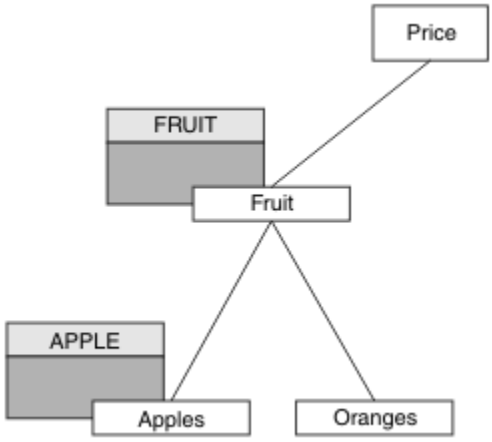


Figure 29. Octroi de l'accès à des rubriques spécifiques dans une arborescence de rubriques

Tableau 21. Exigences d'accès pour des exemples de rubriques et d'objets de rubrique

Topic	Accès à l'abonnement requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun
Prix / Fruits	USER1	fruit
Prix / Fruits / Pommes	USER1 et USER2	Apple

Tableau 21. Exigences d'accès pour des exemples de rubriques et d'objets de rubrique (suite)		
Topic	**Accès à l'abonnement requis**	**Objet de rubrique**
Prix / Fruits / Oranges	USER1	

Définissez un nouvel objet de rubrique comme suit:

Procédure

1. Exécutez la commande MQSC `DEF TOPIC(APPLE) TOPICSTR('Price/Fruit/Apples')`.
2. Accordez l'accès comme suit:
   - Autres plateformes:

     Dans la tâche précédente, USER1 a été autorisé à s'abonner à la rubrique `"Price/Fruit/Apples"` en accordant à l'utilisateur un accès d'abonnement au profil `FRUIT` .

     Ce profil unique a également accordé à USER1 l'accès pour s'abonner à `"Price/Fruit/Oranges"` et `"Price/Fruit/#"`, et cet accès reste même avec l'ajout du nouvel objet de rubrique et des profils qui lui sont associés.

     Accordez l'accès à USER2 pour vous abonner à la rubrique `"Price/Fruit/Apples"` en accordant à l'utilisateur l'accès par abonnement au profil `APPLE` . Pour ce faire, utilisez la commande d'autorisation pour la plateforme:

     
     Windows, systèmes UNIX and Linux

     ```
     setmqaut -t topic -n APPLE -p USER2 +sub
     ```

Résultats

Sous z/OS, lorsque USER1 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le premier contrôle de sécurité du profil `hlq.SUBSCRIBE.APPLE` échoue, mais lorsqu'il remonte l'arborescence, le profil `hlq.SUBSCRIBE.FRUIT` permet à USER1 de s'abonner, de sorte que l'abonnement aboutit et qu'aucun code retour n'est envoyé à l'appel MQSUB. Toutefois, un message RACF `ICH` est généré pour la première vérification:

```
ICH408I USER(USER1   ) ...
  hlq.SUBSCRIBE.APPLE ...
```

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le résultat est un succès car le contrôle de sécurité réussit sur le premier profil.

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit/Oranges"` , le résultat est un échec avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- 
  Sur les plateformes Windows, UNIX et Linux , l'événement d'autorisation suivant:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
  UserIdentifier        USER2
  AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
  TopicString           "Price/Fruit/Oranges"
  ```

L'inconvénient de cette configuration est que sous z/OS, vous recevez des messages `ICH` supplémentaires sur la console. Vous pouvez éviter cela si vous sécurisez l'arborescence de rubriques d'une manière différente.

Modifier le contrôle d'accès pour éviter les messages supplémentaires

Cette rubrique est la quatrième d'une liste de tâches qui vous indique comment accorder à plusieurs utilisateurs l'accès pour s'abonner à des rubriques et éviter des messages RACF ICH408I supplémentaires sur z/OS.

Avant de commencer

Cette rubrique améliore la configuration décrite dans «Accorder à un autre utilisateur l'accès permettant de s'abonner uniquement à la rubrique située plus en profondeur dans l'arborescence», à la page 272 afin d'éviter des messages d'erreur supplémentaires.

Pourquoi et quand exécuter cette tâche

Cette rubrique vous explique comment accorder l'accès à des rubriques plus en profondeur dans l'arborescence et comment supprimer l'accès à la rubrique située en bas de l'arborescence lorsqu'aucun utilisateur n'en a besoin.

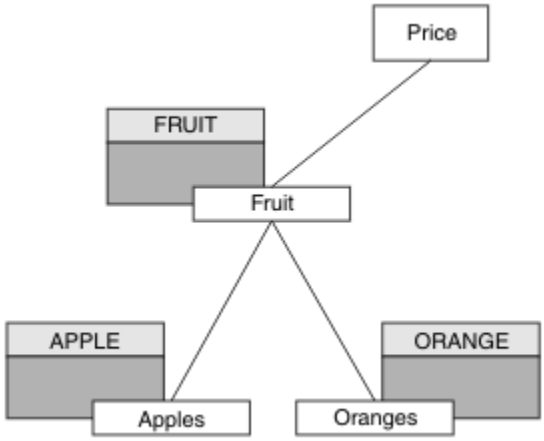


Figure 30. Exemple d'octroi de contrôle d'accès pour éviter des messages supplémentaires.

Définissez un nouvel objet de rubrique comme suit:

Procédure

1. Exécutez la commande MQSC `DEF TOPIC(ORANGE) TOPICSTR('Price/Fruit/Oranges')`.
2. Accordez l'accès comme suit:
   - Autres plateformes:

     Configurez l'accès équivalent à l'aide des commandes d'autorisation pour la plateforme:

     Windows UNIX Linux **Windows, systèmes UNIX and Linux**

     ```
     setmqaut -t topic -n ORANGE -p USER1 +sub
     setmqaut -t topic -n APPLE -p USER1 +sub
     ```

Résultats

Sous z/OS, lorsque USER1 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le premier contrôle de sécurité sur le profil `hlq.SUBSCRIBE.APPLE` aboutit.

De même, lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit/Apples"` , le résultat est un succès car le contrôle de sécurité réussit sur le premier profil.

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Fruit/Oranges"` , le résultat est un échec avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- Windows UNIX Linux Sur les autres plateformes, l'événement d'autorisation suivant:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_SUB_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      ORANGE, FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit/Oranges"
```

Accorder l'accès à un utilisateur pour la publication dans une rubrique

Cette rubrique est la première d'une liste de tâches qui vous indique comment accorder l'accès à la publication de rubriques à plusieurs utilisateurs.

Pourquoi et quand exécuter cette tâche

Cette tâche suppose qu'aucun objet de rubrique d'administration n'existe à droite de l'arborescence de rubriques et qu'aucun profil n'a été défini pour la publication. L'hypothèse utilisée est que les diffuseurs utilisent uniquement la chaîne de rubrique.

Une application peut publier dans une rubrique en fournissant un objet de rubrique, une chaîne de rubrique ou une combinaison des deux. Quel que soit le mode de sélection de l'application, l'effet est la publication à un certain point de l'arborescence de rubriques. Si ce point de l'arborescence de rubriques est représenté par un objet de rubrique d'administration, un profil de sécurité est vérifié en fonction du nom de cet objet de rubrique. Exemple :

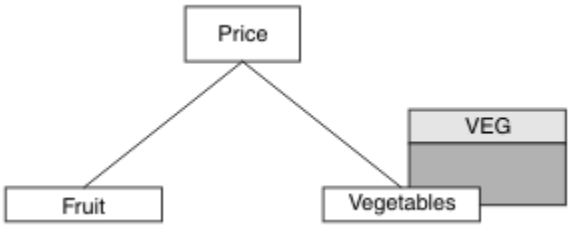


Figure 31. Octroi de l'accès en publication à une rubrique

Tableau 22. Exemple de conditions d'accès à la publication

Topic	Accès à la publication requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun
Prix / Légumes	USER1	VEG

Définissez un nouvel objet de rubrique comme suit:

Procédure

1. Exécutez la commande MQSC `DEF TOPIC(VEG) TOPICSTR('Price/Vegetables')`.
2. Accordez l'accès comme suit:
   - Autres plateformes:

     Accordez l'accès à USER1 pour publier dans la rubrique `"Price/Vegetables"` en accordant à l'utilisateur l'accès au profil VEG . Pour ce faire, utilisez la commande d'autorisation pour la plateforme:

     Windows UNIX Linux **Windows, systèmes UNIX and Linux**

     ```
     setmqaut -t topic -n VEG -p USER1 +pub
     ```

Résultats

Lorsque USER1 tente de publier dans la rubrique `"Price/Vegetables"` , le résultat est un succès, c'est-à-dire que l'appel MQOPEN aboutit.

Lorsque USER2 tente de publier dans la rubrique `"Price/Vegetables"` , l'appel MQOPEN échoue avec un message `MQRC_NOT_AUTHORIZED` et:

- Windows UNIX Linux Sur les autres plateformes, l'événement d'autorisation suivant:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables"
```

Notez qu'il s'agit d'une illustration de ce que vous voyez ; pas de tous les champs.

Accorder l'accès à un utilisateur pour publier dans une rubrique plus en profondeur dans l'arborescence

Cette rubrique est la deuxième d'une liste de tâches qui vous indique comment accorder l'accès à la publication à des rubriques par plusieurs utilisateurs.

Avant de commencer

Cette rubrique utilise la configuration décrite dans «Accorder l'accès à un utilisateur pour la publication dans une rubrique», à la page 275.

Pourquoi et quand exécuter cette tâche

Si le point de l'arborescence de rubriques où l'application publie n'est pas représenté par un objet de rubrique d'administration, déplacez l'arborescence vers le haut jusqu'à ce que l'objet de rubrique d'administration parent le plus proche soit localisé. Le profil de sécurité est vérifié en fonction du nom de cet objet de rubrique.

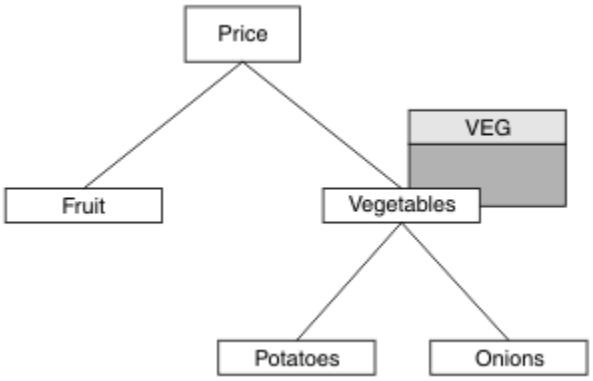


Figure 32. Octroi de l'accès en publication à une rubrique dans une arborescence de rubriques

Tableau 23. Exemple de conditions d'accès à la publication

Topic	Accès à l'abonnement requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun
Prix / Légumes	USER1	VEG
Prix / Légumes / Pommes de terre	USER1	

Tableau 23. Exemple de conditions d'accès à la publication (suite)		
Topic	**Accès à l'abonnement requis**	**Objet de rubrique**
Prix / Légumes / Oignons	USER1	

Dans la tâche précédente, USER1 a été autorisé à publier la rubrique `"Price/Vegetables/Potatoes"` en lui accordant l'accès au profil `hlq.PUBLISH.VEG` sur z/OS ou l'accès en publication au profil `VEG` sur d'autres plateformes. Ce profil unique accorde également à USER1 l'accès à la publication sur `"Price/Vegetables/Onions"`.

Lorsque USER1 tente de publier dans la rubrique `"Price/Vegetables/Potatoes"` , le résultat est un succès, c'est-à-dire que l'appel MQOPEN aboutit.

Lorsque USER2 tente de s'abonner à la rubrique `"Price/Vegetables/Potatoes"` , le résultat est un échec, c'est-à-dire que l'appel MQOPEN échoue avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- Sous z/OS, les messages suivants s'affichent sur la console et indiquent le chemin de sécurité complet via l'arborescence de rubriques qui a été tentée:

```
ICH408I USER(USER2   ) ...
  hlq.PUBLISH.VEG ...

ICH408I USER(USER2   ) ...
  hlq.PUBLISH.SYSTEM.BASE.TOPIC ...
```

- Sur les autres plateformes, l'événement d'autorisation suivant:

```
MQRC_NOT_AUTHORIZED
ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
UserIdentifier        USER2
AdminTopicNames      VEG, SYSTEM.BASE.TOPIC
TopicString           "Price/Vegetables/Potatoes"
```

Notez ce qui suit :

- Les messages que vous recevez sous z/OS sont identiques à ceux reçus lors de la tâche précédente car les mêmes objets de rubrique et les mêmes profils contrôlent l'accès.
- Le message d'événement que vous recevez sur d'autres plateformes est similaire à celui reçu lors de la tâche précédente, mais la chaîne de rubrique réelle est différente.

Accorder l'accès pour la publication et l'abonnement

Cette rubrique est la dernière d'une liste de tâches qui vous indique comment accorder l'accès à la publication et l'abonnement à des rubriques par plusieurs utilisateurs.

Avant de commencer

Cette rubrique utilise la configuration décrite dans «Accorder l'accès à un utilisateur pour publier dans une rubrique plus en profondeur dans l'arborescence», à la page 276.

Pourquoi et quand exécuter cette tâche

Dans une tâche précédente, USER1 a été autorisé à s'abonner à la rubrique `"Price/Fruit"`. Cette rubrique vous indique comment accorder l'accès à cet utilisateur pour publier dans cette rubrique.

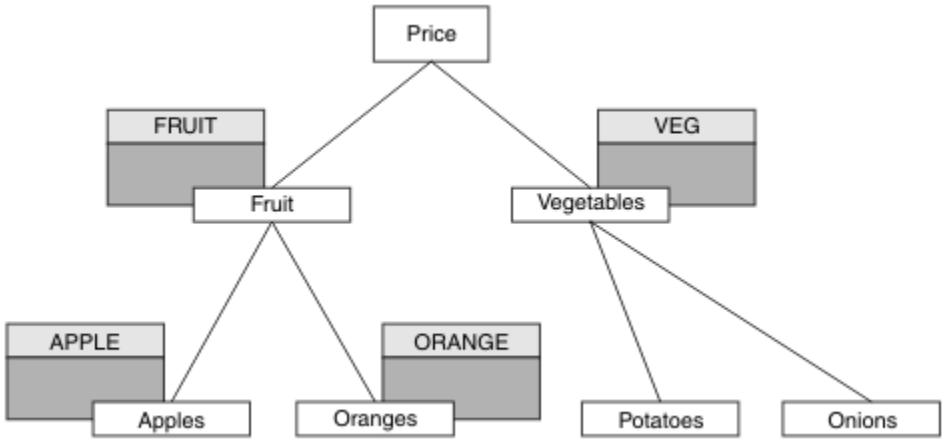


Figure 33. Octroi d'accès pour la publication et l'abonnement

Tableau 24. Exemple de conditions d'accès à la publication et à l'abonnement

Topic	Accès à l'abonnement requis	Accès à la publication requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun utilisateur	Aucun
Prix / Fruits	USER1	USER1	fruit
Prix / Fruits / Pommes	USER1 et USER2		Apple
Prix / Fruits / Oranges	USER1		ORANGE

Procédure

Accordez l'accès comme suit:

- Autres plateformes:

  Accordez l'accès à USER1 pour publier dans la rubrique `"Price/Fruit"` en accordant à l'utilisateur l'accès en publication au profil FRUIT . Pour ce faire, utilisez la commande d'autorisation pour la plateforme:

  Windows UNIX Linux **Windows, systèmes UNIX and Linux**

  ```
  setmqaut -t topic -n FRUIT -p USER1 +pub
  ```

Résultats

Sous z/OS, lorsque USER1 tente de publier dans la rubrique `"Price/Fruit"` , le contrôle de sécurité de l'appel MQOPEN réussit.

Lorsque USER2 tente de publier à la rubrique `"Price/Fruit"` , le résultat est un échec avec un message `MQRC_NOT_AUTHORIZED` , ainsi que:

- Windows UNIX Linux Sur les plateformes Windows, UNIX et Linux , l'événement d'autorisation suivant:

  ```
  MQRC_NOT_AUTHORIZED
  ReasonQualifier      MQRQ_OPEN_NOT_AUTHORIZED
  UserIdentifier        USER2
  ```

```
AdminTopicNames      FRUIT, SYSTEM.BASE.TOPIC
TopicString           "Price/Fruit"
```

En suivant l'ensemble complet de ces tâches, vous attribuez à USER1 et USER2 les droits d'accès suivants pour la publication et l'abonnement aux rubriques répertoriées:

Tableau 25. Liste complète des droits d'accès résultant d'exemples de sécurité

Topic	Accès à l'abonnement requis	Accès à la publication requis	Objet de rubrique
Prix	Aucun utilisateur	Aucun utilisateur	Aucun
Prix / Fruits	USER1	USER1	fruit
Prix / Fruits / Pommes	USER1 et USER2		Apple
Prix / Fruits / Oranges	USER1		ORANGE
Prix / Légumes		USER1	VEG
Prix / Légumes / Pommes de terre			
Prix / Légumes / Oignons			

Lorsque vous avez des exigences différentes en matière d'accès de sécurité à différents niveaux de l'arborescence de rubriques, une planification minutieuse garantit que vous ne recevez pas d'avertissements de sécurité superflus dans le journal de la console z/OS . La configuration de la sécurité au niveau approprié dans l'arborescence permet d'éviter les messages de sécurité trompeurs.

Sécurité des abonnements

MQSO_ALTERNATE_USER_AUTHORITY

La zone ID AlternateUsercontient un identificateur utilisateur à utiliser pour valider cet appel MQSUB. L'appel peut aboutir uniquement si cet ID AlternateUserest autorisé à s'abonner à la rubrique avec les options d'accès spécifiées, que l'ID utilisateur sous lequel l'application s'exécute soit autorisé ou non à le faire.

MQSO_SET_IDENTITY_CONTEXT

L'abonnement permet d'utiliser le jeton de comptabilité et les données d'identité d'application fournies dans les zones PubAccountingToken et PubApplIdentityData .

Si cette option est spécifiée, la même vérification d'autorisation est effectuée comme si la file d'attente de destination était accessible à l'aide d'un appel MQOPEN avec MQOO_SET_IDENTITY_CONTEXT, sauf dans le cas où l'option MQSO_MANAGED est également utilisée, auquel cas aucune vérification d'autorisation n'est effectuée sur la file d'attente de destination.

Si cette option n'est pas spécifiée, les informations de contexte par défaut sont associées aux publications envoyées à cet abonné comme suit:

Tableau 26. Informations de contexte de publication par défaut	
Zone dans MQMD	**Valeur utilisée**
UserIdentifier	ID utilisateur associé à l'abonnement (voir la zone SUBUSER sur DISPLAY SBSTATUS) au moment de la publication.
AccountingToken	Déterminé à partir de l'environnement si possible ; défini sur MQACT_NONE dans le cas contraire.
ApplIdentityData	Mettez à blanc.

Cette option est valide uniquement avec MQSO_CREATE et MQSO_ALTER. Si elles sont utilisées avec MQSO_RESUME, les zones PubAccountingToken et PubApplIdentityData sont ignorées, de sorte que cette option n'a aucun effet.

Si un abonnement est modifié sans utiliser cette option alors que l'abonnement avait précédemment fourni des informations de contexte d'identité, des informations de contexte par défaut sont générées pour l'abonnement modifié.

Si un abonnement permettant à différents ID utilisateur de l'utiliser avec l'option MQSO_ANY_USERID, est repris par un autre ID utilisateur, le contexte d'identité par défaut est généré pour le nouvel ID utilisateur propriétaire de l'abonnement et toutes les publications suivantes sont distribuées contenant le nouveau contexte d'identité.

AlternateSecurityId

Il s'agit d'un identificateur de sécurité qui est transmis avec l'ID AlternateUserau service d'autorisation pour permettre l'exécution des vérifications d'autorisation appropriées. L'ID AlternateSecurityest utilisé uniquement si MQSO_ALTERNATE_USER_AUTHORITY est spécifié et que la zone d'ID AlternateUsern'est pas entièrement vide jusqu'au premier caractère null ou jusqu'à la fin de la zone.

Option d'abonnement MQSO_ANY_USERID

Lorsque MQSO_ANY_USERID est spécifié, l'identité de l'abonné n'est pas limitée à un seul ID utilisateur. Cela permet à tout utilisateur de modifier ou de reprendre l'abonnement lorsqu'il dispose des droits appropriés. Un seul utilisateur peut disposer de l'abonnement à la fois. Une tentative de reprise de l'utilisation d'un abonnement actuellement utilisé par une autre application entraîne l'échec de l'appel avec MQRC_SUBSCRIPTION_IN_USE.

Pour ajouter cette option à un abonnement existant, l'appel MQSUB (à l'aide de MQSO_ALTER) doit provenir du même ID utilisateur que l'abonnement d'origine.

Si un appel MQSUB fait référence à un abonnement existant avec MQSO_ANY_USERID défini et que l'ID utilisateur est différent de l'abonnement d'origine, l'appel aboutit uniquement si le nouvel ID utilisateur est autorisé à s'abonner à la rubrique. Une fois l'opération terminée, les futures publications destinées à cet abonné sont placées dans la file d'attente de l'abonné avec le nouvel ID utilisateur défini dans la publication.

ID_UTILISATEUR_FIXE_MQSO_FIXE

Lorsque MQSO_FIXED_USERID est spécifié, l'abonnement ne peut être modifié ou repris que par un seul ID utilisateur propriétaire. Cet ID utilisateur est le dernier ID utilisateur à modifier l'abonnement qui définit cette option, supprimant ainsi l'option MQSO_ANY_USERID, ou si aucune modification n'a eu lieu, il s'agit de l'ID utilisateur qui a créé l'abonnement.

Si une instruction MQSUB fait référence à un abonnement existant avec MQSO_ANY_USERID défini et modifie l'abonnement (à l'aide de MQSO_ALTER) pour utiliser l'option MQSO_FIXED_USERID, l'ID utilisateur de l'abonnement est désormais corrigé au niveau de ce nouvel ID utilisateur. L'appel aboutit uniquement si le nouvel ID utilisateur est autorisé à s'abonner à la rubrique.

Si un ID utilisateur autre que celui enregistré comme propriétaire d'un abonnement tente de reprendre ou de modifier un abonnement MQSO_FIXED_USERID, l'appel échoue avec MQRC_IDENTITY_MISMATCH. L'ID utilisateur propriétaire d'un abonnement peut être affiché à l'aide de la commande DISPLAY SBSTATUS.

Si ni MQSO_ANY_USERID ni MQSO_FIXED_USERID n'est spécifié, la valeur par défaut est MQSO_FIXED_USERID.

IBM WebSphere MQ Advanced Message Security

IBM WebSphere MQ Advanced Message Security (AMS) est un composant sous licence distincte de IBM WebSphere MQ Advanced Message Security qui offre un niveau de protection élevé pour les données sensibles transitant par le réseau IBM WebSphere MQ Advanced Message Security , sans affecter les applications finales.

IBM WebSphere MQ Advanced Message Security - Généralités

Les applications IBM WebSphere MQ peuvent utiliser IBM WebSphere MQ Advanced Message Security pour envoyer des données sensibles, telles que des transactions financières à valeur élevée et des informations personnelles, avec différents niveaux de protection à l'aide d'un modèle de cryptographie à clé publique.

Référence associée

Codes retour GSKit utilisés dans les messages IBM WebSphere MQ AMS

Comportement modifié entre la version 7.0.1 et la version 7.5

Lorsque IBM Advanced Message Security est devenu un composant dans WebSphere MQ 7.5, certains aspects de la fonctionnalité IBM WebSphere MQ AMS ont changé, ce qui peut affecter les applications existantes, les scripts d'administration ou les procédures de gestion.

Passez en revue la liste de modifications suivante avant de mettre à niveau les gestionnaires de files d'attente vers la version 7.5. Décidez si vous devez prévoir d'apporter des modifications aux applications, scripts et procédures existants avant de commencer à migrer des systèmes vers IBM WebSphere MQ version 7.5:

- L'installation d' IBM WebSphere MQ AMS fait partie du processus d'installation d' WebSphere MQ .
- Les fonctions de sécurité d' IBM WebSphere MQ AMS sont activées avec son installation et contrôlées avec des règles de sécurité. Il n'est pas nécessaire d'activer les intercepteurs pour permettre à IBM WebSphere MQ AMS de démarrer l'interception des données.
- IBM WebSphere MQ AMS dans WebSphere MQ version 7.5 ne nécessite pas l'utilisation de la commande **cfgmqs** comme dans la version autonome de IBM WebSphere MQ AMS.

Caractéristiques et fonctions de IBM WebSphere MQ Advanced Message Security

Advanced Message Security développe les services de sécurité WebSphere MQ pour fournir la signature et le chiffrement des données au niveau des messages. Les services étendus garantissent que les données de message n'ont pas été modifiées entre le moment où elles sont placées à l'origine dans une file d'attente et le moment où elles sont extraites. En outre, IBM WebSphere MQ AMS vérifie qu'un expéditeur de données de message est autorisé à placer des messages signés dans une file d'attente cible.

Voici une liste complète des fonctions IBM WebSphere MQ AMS :

- Sécurise les transactions sensibles ou à valeur élevée traitées par WebSphere MQ.
- Détecte et supprime les messages malveillants ou non autorisés avant qu'ils ne soient traités par une application de réception.
- Vérifie que les messages n'ont pas été modifiés lors de leur passage de la file d'attente à la file d'attente.

- Protège les données non seulement lorsqu'elles circulent sur le réseau, mais également lorsqu'elles sont placées dans une file d'attente.
- Sécurise les applications propriétaires et écrites par le client existantes pour WebSphere MQ.

Traitement des erreurs

Advanced Message Security définit une file d'attente de traitement des erreurs pour gérer les messages qui contiennent des erreurs ou qui ne peuvent pas être protégés.

Les messages défectueux sont traités comme des cas exceptionnels. Si un message reçu ne répond pas aux exigences de sécurité de la file d'attente dans laquelle il se trouve, par exemple, si le message est signé alors qu'il doit être chiffré, ou si le déchiffrement ou la vérification de la signature échoue, le message est envoyé à la file d'attente de traitement des erreurs. Un message peut être envoyé à la file d'attente de traitement des erreurs pour les raisons suivantes:

- Non-concordance de la qualité de protection-Il existe une non-concordance de la qualité de protection (QOP) entre le message reçu et la définition QOP dans la règle de sécurité.
- Erreur de déchiffrement-le message ne peut pas être déchiffré.
- Erreur d'en-tête PDMQ-L'en-tête de message AMS WebSphere MQ est inaccessible.
- Non-concordance de taille-la longueur d'un message après déchiffrement est différente de celle attendue.
- Non-concordance de la force de l'algorithme de chiffrement-l'algorithme de chiffrement du message est plus faible que requis.
- Erreur inconnue-une erreur inattendue s'est produite.

WebSphere MQ AMS utilise SYSTEM.PROTECTION.ERROR.QUEUE comme file d'attente de traitement des erreurs. Tous les messages insérés par IBM WebSphere MQ AMS dans SYSTEM.PROTECTION.ERROR.QUEUE sont précédées de l'en-tête MQDLH.

Votre administrateur WebSphere MQ peut également définir le système SYSTEM.PROTECTION.ERROR.QUEUE en tant que file d'attente alias pointant vers une autre file d'attente.

Concepts clés

Découvrez les concepts clés de Advanced Message Security pour comprendre comment l'outil fonctionne et comment le gérer efficacement.

Infrastructure à clé publique

L'infrastructure à clé publique (ICP) est un système d'installations, de politiques et de services qui appuient l'utilisation de la cryptographie à clé publique pour obtenir des communications sécurisées.

Il n'existe pas de norme unique qui définit les composants d'une infrastructure à clé publique, mais une ICP implique généralement l'utilisation de certificats de clé publique et comprend des autorités de certification (CA) et d'autres autorités d'enregistrement (RA) qui fournissent les services suivants:

- Emission de certificats numériques
- Validation des certificats numériques
- Révocation de certificats numériques
- Distribution de certificats

L'identité des utilisateurs et des applications est représentée par la zone **Nom distinctif (DN)** dans un certificat associé à des messages signés ou chiffrés. Advanced Message Security utilise cette identité pour représenter un utilisateur ou une application. Pour authentifier cette identité, l'utilisateur ou l'application doit avoir accès au magasin de clés dans lequel le certificat et la clé privée associée sont stockés. Chaque certificat est représenté par un libellé dans le magasin de clés.

Concepts associés

«Utilisation de magasins de clés et de certificats», à la page 307

Pour fournir une protection cryptographique transparente aux applications WebSphere MQ , Advanced Message Security utilise le fichier de clés, dans lequel les certificats de clé publique et une clé privée sont stockés.

Certificats numériques

Advanced Message Security associe les utilisateurs et les applications à des certificats numériques standard X.509 . Les certificats X.509 sont généralement signés par une autorité de certification de confiance et impliquent des clés privées et publiques qui sont utilisées pour le chiffrement et le déchiffrement.

Les certificats numériques offrent une protection contre l'usurpation d'identité en liant une clé publique à son propriétaire, qu'il s'agisse d'un individu, d'un gestionnaire de files d'attente ou d'une autre entité. Les certificats numériques sont également appelés certificats de clé publique, car ils vous donnent l'assurance de la propriété d'une clé publique lorsque vous utilisez un schéma de clé asymétrique. Ce schéma requiert la génération d'une clé publique et d'une clé privée pour une application. Les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'à l'aide de la clé privée correspondante, tandis que les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'à l'aide de la clé publique correspondante. La clé privée est stockée dans un fichier de base de données de clés protégé par mot de passe. Seul son propriétaire a accès à la clé privée utilisée pour déchiffrer les messages qui sont chiffrés à l'aide de la clé publique correspondante.

Si les clés publiques sont envoyées directement par leur propriétaire à une autre entité, il existe un risque que le message soit intercepté et que la clé publique soit remplacée par une autre. C'est ce qu'on appelle une attaque de type "man-in-the-middle". La solution consiste à échanger des clés publiques par l'intermédiaire d'un tiers de confiance, ce qui permet à l'utilisateur de s'assurer que la clé publique appartient à l'entité avec laquelle vous communiquez. Au lieu d'envoyer votre clé publique directement, vous demandez à un tiers de confiance de l'incorporer dans un certificat numérique. Le tiers de confiance qui émet des certificats numériques est appelé une autorité de certification (CA).

Pour plus d'informations sur les certificats numériques, voir Qu'est-ce qu'un certificat numérique?.

Un certificat numérique contient la clé publique d'une entité et indique que la clé publique appartient à cette entité:

- lorsqu'un certificat est destiné à une entité individuelle, il est appelé *certificat personnel* ou *certificat d'utilisateur*.
- lorsqu'un certificat est destiné à une autorité de certification, le certificat est appelé *certificat de l'autorité de certification* ou *certificat de signataire*.

Remarque : Advanced Message Security prend en charge les certificats autosignés dans les applications Java et natives

Concepts associés

«Cryptographie», à la page 7
La cryptographie est le processus de conversion entre du texte lisible, appelé *texte en clair*, et un format illisible, appelé *texte chiffré*.

gestionnaire des droits d'accès aux objets

Le gestionnaire des droits d'accès aux objets (OAM) est le composant de service d'autorisation fourni avec les produits WebSphere MQ .

L'accès aux entités Advanced Message Security est contrôlé par les groupes d'utilisateurs WebSphere MQ et la méthode d'accès aux objets (OAM). Les administrateurs peuvent utiliser l'interface de ligne de commande pour accorder ou révoquer des autorisations selon les besoins. Différents groupes d'utilisateurs peuvent avoir différents types de droits d'accès aux mêmes objets. Par exemple, un groupe peut effectuer à la fois des opérations PUT et GET pour une file d'attente spécifique, tandis qu'un autre groupe peut être autorisé uniquement à parcourir la file d'attente. De même, certains groupes peuvent disposer des droits GET et PUT sur une file d'attente, mais ils ne sont pas autorisés à modifier ou à supprimer la file d'attente.

Grâce à la méthode d'accès aux objets (OAM), vous pouvez contrôler:

- Accès aux objets Advanced Message Security via MQI. Lorsqu'un programme d'application tente d'accéder à des objets, la méthode d'accès aux objets (OAM) vérifie si le profil utilisateur à l'origine de la demande possède l'autorisation pour l'opération demandée. Cela signifie que les files d'attente et les messages des files d'attente peuvent être protégés contre tout accès non autorisé.
- Droit d'utilisation des commandes PCF et MQSC.

Concepts associés

gestionnaire des droits d'accès aux objets

Technologie prise en charge

Advanced Message Security dépend de plusieurs composants technologiques pour fournir une infrastructure de sécurité.

Advanced Message Security prend en charge les interfaces de programme d'application (API) WebSphere MQ suivantes:

- interface de file d'attente de messages (MQI)
- WebSphere MQ Java Message Service (JMS) 1.0.2 et 1.1.
- Classes de base WebSphere MQ pour Java
- Classes WebSphere MQ pour. Net en mode non géré

Remarque : Advanced Message Security prend en charge les autorités de certification conformes à X.509 .

Limitations connues

Découvrez les limitations d' IBM WebSphere MQ Advanced Message Security.

- Les options IBM WebSphere MQ suivantes ne sont pas prises en charge:
  - Publication / abonnement.
  - Conversion de données de canal.
  - Listes de distribution.
  - Segmentation des messages d'application
  - Utilisation d'applications sans unités d'exécution à l'aide de l'exit API sur les plateformes HP-UX .
  - IBM WebSphere MQ classes for .NET en mode géré (connexions client ou liaisons).
  - Client Message Service pour les applications .NET (XMS).
  - Client Message Service pour les applications C/C++ (XMS supportPac IA94).
- Toutes les applications Java dépendent de IBM Java Runtime.

  IBM WebSphere MQ Advanced Message Security ne prend pas en charge l'environnement d'exécution Java fourni par d'autres fournisseurs.
- Applications client JMS et Java utilisant IBM WebSphere MQ Advanced Message Security en mode client.

  Toute application client JMS ou Java(y compris les agents IBM WebSphere MQ Explorer et IBM WebSphere MQ Managed File Transfer) ne peut pas utiliser IBM WebSphere MQ Advanced Message Security en mode client avec un gestionnaire de files d'attente WebSphere MQ antérieur à Version 7.5.

  Pour utiliser les règles de protection des messages, ces applications doivent interagir avec un gestionnaire de files d'attente IBM WebSphere MQ Version 7.5 ou se connecter en mode de liaisons locales à un gestionnaire de files d'attente sur la même machine que l'application.
- Vous devez éviter de placer deux ou plusieurs certificats avec les mêmes noms distinctifs, dans un fichier de clés unique, car le fonctionnement de l'interecepteur IBM WebSphere MQ Advanced Message Security avec de tels certificats n'est pas défini.
- L'adaptateur de ressources IBM WebSphere MQ Version 7.5 ne prend pas en charge IBM WebSphere MQ Advanced Message Security. Si la protection des messages doit être utilisée avec des applications

IBM WebSphere MQ classes for JMS ou IBM WebSphere MQ classes for Java s'exécutant dans un environnement de serveur d'applications, procédez comme suit:

– Le serveur d'applications doit être configuré pour utiliser l'adaptateur de ressources Version 8.0 ou version ultérieure.
– Ou l'interception MCA (Message Channel Agent) doit être utilisée.

Scénarios utilisateur

Familiarisez-vous avec les scénarios possibles pour comprendre les objectifs métier que vous pouvez atteindre avec Advanced Message Security.

Guide de démarrage rapide pour les plateformes Windows

Utilisez ce guide pour configurer rapidement IBM Advanced Message Security afin d'assurer la sécurité des messages sur les plateformes Windows . Lorsque vous l'aurez terminé, vous aurez créé une base de données de clés pour vérifier les identités utilisateur et défini des règles de signature / chiffrement pour votre gestionnaire de files d'attente.

Avant de commencer

Au moins les fonctions suivantes doivent être installées sur votre système:

- serveur
- Kit d'outils de développement (pour les exemples de programme)
- Advanced Message Security

Pour plus d'informations, voir FonctionsIBM WebSphere MQ pour les systèmes Windows .

Pour plus d'informations sur l'utilisation de la commande **setmqenv** pour initialiser l'environnement en cours afin que les commandes WebSphere MQ appropriées puissent être localisées et exécutées par le système d'exploitation, voir setmqenv.

1. Création d'un gestionnaire de files d'attente et d'une file d'attente

Pourquoi et quand exécuter cette tâche

Tous les exemples suivants utilisent une file d'attente nommée TEST.Q pour la transmission de messages entre les applications. Advanced Message Security utilise des intercepteurs pour signer et chiffrer les messages lorsqu'ils entrent dans l'infrastructure WebSphere MQ via l'interface WebSphere MQ standard. La configuration de base est effectuée dans WebSphere MQ et est configurée dans les étapes suivantes.

Vous pouvez utiliser WebSphere MQ Explorer pour créer le gestionnaire de files d'attente QM_VERIFY_AMS et sa file d'attente locale appelée TEST.Q à l'aide de tous les paramètres de l'assistant par défaut, ou vous pouvez utiliser les commandes disponibles dans `\WebSphere MQ\bin`. N'oubliez pas que vous devez être membre du groupe d'utilisateurs `mqm` pour exécuter les commandes d'administration suivantes.

Procédure

1. Création d'un gestionnaire de files d'attente

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Démarrer le gestionnaire de files d'attente

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Créez une file d'attente appelée TEST.Q en entrant la commande suivante dans **runmqsc** pour le gestionnaire de files d'attente QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Résultats

Si la procédure est terminée, la commande entrée dans **runmqsc** affiche les détails relatifs à TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Création et autorisation d'utilisateurs

Pourquoi et quand exécuter cette tâche

Deux utilisateurs apparaissent dans cet exemple: alice, l'expéditeur et bob, le destinataire. Pour utiliser la file d'attente d'application, ces utilisateurs doivent être autorisés à l'utiliser. De même, pour utiliser correctement les règles de protection que nous définirons, ces utilisateurs doivent être autorisés à accéder à certaines files d'attente du système. Pour plus d'informations sur la commande **setmqaut** , voir **setmqaut** .

Procédure

1. Créez les deux utilisateurs et assurez-vous que HOMEPATH et HOMEDRIVE sont définis pour ces deux utilisateurs.
2. Autoriser les utilisateurs à se connecter au gestionnaire de files d'attente et à utiliser la file d'attente

```
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. Vous devez également autoriser les deux utilisateurs à parcourir la file d'attente de règles système et à placer des messages dans la file d'attente d'erreurs.

```
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
```

Résultats

Les utilisateurs sont maintenant créés et les droits requis leur sont accordés.

Que faire ensuite

Pour vérifier si les étapes ont été effectuées correctement, utilisez les exemples amqsput et amqsget comme décrit dans la section «7. Test de la configuration», à la page 289.

3. Création d'une base de données de clés et de certificats

Pourquoi et quand exécuter cette tâche

L'intercepteur requiert la clé publique des utilisateurs qui l'envoient pour chiffrer le message. Par conséquent, la base de données de clés des identités utilisateur mappées aux clés publiques et privées doit être créée. Dans le système réel, où les utilisateurs et les applications sont dispersés sur plusieurs ordinateurs, chaque utilisateur dispose de son propre magasin de clés privé. De même, dans ce guide, nous créons des bases de données de clés pour alice et bob et nous partageons les certificats d'utilisateur entre eux.

Remarque : Dans ce guide, nous utilisons des exemples d'applications écrits en C se connectant à l'aide de liaisons locales. Si vous prévoyez d'utiliser des applications Java à l'aide de liaisons client, vous devez créer un magasin de clés JKS et des certificats à l'aide de la commande **keytool** , qui fait partie de l'environnement d'exécution Java (voir «Guide de démarrage rapide pour les clients Java», à la page 296 pour plus de détails). Pour tous les autres langages et pour les applications Java utilisant des liaisons locales, les étapes de ce guide sont correctes.

Procédure

1. Utilisez l'interface graphique IBM Key Management (`strmqikm.exe`) pour créer une nouvelle base de données de clés pour l'utilisateur `alice`.

```
Type:       CMS
Filename:   alicekey.kdb
Location:   C:/Documents and Settings/alice/AMS
```

   Remarque :

   - Il est conseillé d'utiliser un mot de passe fiable pour sécuriser la base de données.
   - Vérifiez que la case **Stocker le mot de passe dans un fichier** est cochée.
2. Remplacez la vue de contenu de la base de données de clés par **Certificats personnels**.
3. Sélectionnez **Nouveau certificat autosigné**; les certificats autosignés sont utilisés dans ce scénario.
4. Créez un certificat identifiant l'utilisateur `alice` à utiliser dans le chiffrement, à l'aide des zones suivantes:

```
Key label: Alice_Cert
Common Name: alice
Organisation: IBM
Country: GB
```

   Remarque :

   - Pour les besoins de ce guide, nous utilisons un certificat autosigné qui peut être créé sans utiliser d'autorité de certification. Pour les systèmes de production, il est conseillé de ne pas utiliser de certificats autosignés, mais de s'appuyer sur des certificats signés par une autorité de certification.
   - Le paramètre **`Key label`** indique le nom du certificat, que les intercepteurs recherchent pour recevoir les informations nécessaires.
   - Le paramètre **`Common Name`** et les paramètres facultatifs spécifient les détails du **nom distinctif** (DN), qui doit être unique pour chaque utilisateur.
5. Répétez les étapes 1 à 4 pour l'utilisateur bob

Résultats

Les deux utilisateurs `alice` et bob possèdent chacun un certificat autosigné.

4. Création de keystore.conf

Pourquoi et quand exécuter cette tâche

Vous devez pointer les intercepteurs Advanced Message Security vers le répertoire dans lequel se trouvent les bases de données de clés et les certificats located.This est effectuée via le fichier `keystore.conf` , qui contient ces informations sous forme de texte en clair. Chaque utilisateur doit disposer d'un fichier `keystore.conf` distinct. Cette étape doit être effectuée pour `alice` et bob.

Le contenu de `keystore.conf` doit être au format suivant:

```
cms.keystore = <dir>/keystore_file
cms.certificate = certificate_label
```

Exemple

Pour ce scénario, le contenu de `keystore.conf` sera le suivant:

```
cms.keystore = C:/Documents and Settings/alice/AMS/alicekey
cms.certificate = Alice_Cert
```

Remarque :

- Le chemin d'accès au fichier de clés doit être fourni sans inclure l'extension de fichier.

- Le label de certificat peut inclure des espaces, ainsi "Alice_Cert" et "Alice_Cert" par exemple, sont reconnus comme des libellés de deux certificats différents. Cependant, pour éviter toute confusion, il est préférable de ne pas utiliser d'espaces dans le nom de l'étiquette.
- Il existe les formats de fichier de clés suivants: CMS (Cryptographic Message Syntax), JKS (Java Keystore) et JCEKS (Java Cryptographic Extension Keystore). Pour plus d'informations, voir «Structure du fichier de configuration du magasin de clés (keystore.conf)», à la page 307.
- *%HOMEDRIVE%\%HOMEPATH%*\.mqs\keystore.conf (par exemple, C:\Documents and Settings\alice\.mqs\keystore.conf) est l'emplacement par défaut où Advanced Message Security recherche le fichier keystore.conf . Pour plus d'informations sur l'utilisation d'un emplacement autre que celui par défaut pour le keystore.conf, voir «Utilisation de magasins de clés et de certificats», à la page 307.
- Pour créer le répertoire .mqs , vous devez utiliser l'invite de commande.

5. Partage de certificats

Pourquoi et quand exécuter cette tâche

Partagez les certificats entre les deux bases de données de clés afin que chaque utilisateur puisse identifier l'autre. Cette opération est effectuée en extrayant le certificat public de chaque utilisateur dans un fichier, qui est ensuite ajouté à la base de données de clés de l'autre utilisateur.

Remarque : Prenez soin d'utiliser l'option *extract* et non l'option *export* . *Extract* obtient la clé publique de l'utilisateur, tandis que *export* obtient à la fois la clé publique et la clé privée. L'utilisation de *export* par erreur compromettrait complètement votre application en transmettant sa clé privée.

Procédure

1. Extrayez le certificat identifiant alice dans un fichier externe:

```
runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/alicekey.kdb" -pw passw0rd
-label Alice_Cert -target alice_public.arm
```

2. Ajoutez le certificat au magasin de clés bob's :

```
runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/bobkey.kdb" -pw passw0rd -label
Alice_Cert -file alice_public.arm
```

3. Répétez les étapes pour bob:

```
runmqakm -cert -extract -db "C:/Documents and Settings/alice/AMS/bobkey.kdb" -pw passw0rd
-label Bob_Cert -target bob_public.arm

runmqakm -cert -add -db "C:/Documents and Settings/bob/AMS/alicekey.kdb" -pw passw0rd -label
Bob_Cert -file bob_public.arm
```

Résultats

Les deux utilisateurs alice et bob sont désormais en mesure de s'identifier mutuellement en ayant créé et partagé des certificats autosignés.

Que faire ensuite

Vérifiez qu'un certificat se trouve dans le magasin de clés en le parcourant à l'aide de l'interface graphique ou en exécutant les commandes suivantes qui impriment ses détails:

```
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. Définition de la règle de file d'attente

Pourquoi et quand exécuter cette tâche

Avec le gestionnaire de files d'attente créé et les intercepteurs préparés pour intercepter les messages et les clés de chiffrement d'accès, nous pouvons commencer à définir des règles de protection sur QM_VERIFY_AMS à l'aide de la commande `setmqspl` . Pour plus d'informations sur cette commande, voir setmqspl . Chaque nom de règle doit être identique au nom de la file d'attente à laquelle il doit être appliqué.

Exemple

Voici un exemple de règle définie pour la file d'attente `TEST.Q` . Dans l'exemple, les messages sont signés avec l'algorithme SHA1 et chiffrés avec l'algorithme AES256 . `alice` est le seul émetteur valide et bob est le seul récepteur des messages de cette file d'attente:

```
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"
```

Remarque : Les noms distinctifs correspondent exactement à ceux spécifiés dans le certificat de l'utilisateur respectif de la base de données de clés.

Que faire ensuite

Pour vérifier la règle que vous avez définie, exécutez la commande suivante:

```
dspmqspl -m QM_VERIFY_AMS
```

Pour imprimer les détails de la règle sous la forme d'un ensemble de commandes `setmqspl` , utilisez l'indicateur `-export` . Cela permet de stocker des règles déjà définies:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Test de la configuration

Pourquoi et quand exécuter cette tâche

En exécutant différents programmes sous différents utilisateurs, vous pouvez vérifier si l'application a été correctement configurée.

Procédure

1. Changez d'utilisateur pour qu'il s'exécute en tant qu'utilisateur `alice`

   Cliquez avec le bouton droit de la souris sur `cmd.exe` et sélectionnez **Exécuter en tant que ...**. Lorsque vous y êtes invité, connectez-vous en tant que `alice`.
2. En tant qu'utilisateur `alice` , placez un message à l'aide d'un exemple d'application:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```
3. Entrez le texte du message, puis appuyez sur Entrée.
4. Changez d'utilisateur pour qu'il s'exécute en tant qu'utilisateur bob

   Ouvrez une autre fenêtre en cliquant avec le bouton droit de la souris sur `cmd.exe` et en sélectionnant **Exécuter en tant que ...**. Lorsque vous y êtes invité, connectez-vous en tant que bob.
5. En tant qu'utilisateur Bob , obtenez un message à l'aide d'un exemple d'application:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Résultats

Si l'application a été correctement configurée pour les deux utilisateurs, le message de l'utilisateur `alice`s'affiche lorsque bob exécute l'application d'obtention.

8. Test du chiffrement

Pourquoi et quand exécuter cette tâche

Pour vérifier que le chiffrement est effectué comme prévu, créez une file d'attente alias qui fait référence à la file d'attente d'origine TEST.Q. Cette file d'attente alias n'ayant pas de règle de sécurité, aucun utilisateur ne dispose des informations permettant de déchiffrer le message. Par conséquent, les données chiffrées sont affichées.

Procédure

1. A l'aide de la commande **runmqsc** sur le gestionnaire de files d'attente QM_VERIFY_AMS, créez une file d'attente alias.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```

2. Accordez à bob l'accès pour parcourir la file d'attente alias

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```

3. En tant qu'utilisateur `alice`, placez un autre message à l'aide d'un exemple d'application comme précédemment:

   ```
   amqsput TEST.Q QM_VERIFY_AMS
   ```

4. En tant qu'utilisateur bob, parcourez le message à l'aide d'un exemple d'application via la file d'attente alias cette fois:

   ```
   amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```

5. En tant qu'utilisateur bob, obtenez le message à l'aide d'un exemple d'application à partir de la file d'attente locale:

   ```
   amqsget TEST.Q QM_VERIFY_AMS
   ```

Résultats

La sortie de l'application `amqsbcg` affiche les données chiffrées qui se trouvent dans la file d'attente prouvant que le message a été chiffré.

Guide de démarrage rapide pour les plateformes UNIX

Utilisez ce guide pour configurer rapidement IBM Advanced Message Security afin d'assurer la sécurité des messages sur les plateformes UNIX . Lorsque vous l'aurez terminé, vous aurez créé une base de données de clés pour vérifier les identités utilisateur et défini des règles de signature / chiffrement pour votre gestionnaire de files d'attente.

Avant de commencer

Au moins les composants suivants doivent être installés sur votre système:

- MQ Light
- serveur
- Exemples de programme
- IBM Global Security Kit
- MQ Advanced Message Security

Reportez-vous aux rubriques suivantes pour connaître les noms de composant sur chaque plateforme spécifique:

- ComposantsIBM WebSphere MQ pour les systèmes Linux
- ComposantsIBM WebSphere MQ pour les systèmes HP-UX
- ComposantsIBM WebSphere MQ pour les systèmes AIX
- ComposantsIBM WebSphere MQ pour les systèmes Solaris

1. Création d'un gestionnaire de files d'attente et d'une file d'attente

Pourquoi et quand exécuter cette tâche

Tous les exemples suivants utilisent une file d'attente nommée TEST.Q pour la transmission de messages entre les applications. Advanced Message Security utilise des intercepteurs pour signer et chiffrer les messages lorsqu'ils entrent dans l'infrastructure WebSphere MQ via l'interface WebSphere MQ standard. La configuration de base est effectuée dans WebSphere MQ et est configurée dans les étapes suivantes.

Vous pouvez utiliser WebSphere MQ Explorer pour créer le gestionnaire de files d'attente QM_VERIFY_AMS et sa file d'attente locale appelée TEST.Q à l'aide de tous les paramètres de l'assistant par défaut, ou vous pouvez utiliser les commandes disponibles dans <MQ_INSTALL_PATH>/bin. N'oubliez pas que vous devez être membre du groupe d'utilisateurs mqm pour exécuter les commandes d'administration suivantes.

Procédure

1. Création d'un gestionnaire de files d'attente

   ```
   crtmqm QM_VERIFY_AMS
   ```

2. Démarrer le gestionnaire de files d'attente

   ```
   strmqm QM_VERIFY_AMS
   ```

3. Créez une file d'attente appelée TEST.Q en entrant la commande suivante dans **runmqsc** pour le gestionnaire de files d'attente QM_VERIFY_AMS

   ```
   DEFINE QLOCAL(TEST.Q)
   ```

Résultats

Si la procédure a abouti, la commande suivante entrée dans **runmqsc** affiche les détails relatifs à TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Création et autorisation d'utilisateurs

Pourquoi et quand exécuter cette tâche

Deux utilisateurs apparaissent dans cet exemple: alice, l'expéditeur et bob, le destinataire. Pour utiliser la file d'attente d'application, ces utilisateurs doivent être autorisés à l'utiliser. De même, pour utiliser correctement les règles de protection que nous définirons, ces utilisateurs doivent être autorisés à accéder à certaines files d'attente du système. Pour plus d'informations sur la commande **setmqaut** , voir **setmqaut** .

Procédure

1. Créer les deux utilisateurs

```
useradd alice
useradd bob
```

2. Autoriser les utilisateurs à se connecter au gestionnaire de files d'attente et à utiliser la file d'attente

```
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. Vous devez également autoriser les deux utilisateurs à parcourir la file d'attente de règles système et à placer des messages dans la file d'attente d'erreurs.

```
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
```

Résultats

Des groupes d'utilisateurs sont maintenant créés et les droits requis leur sont accordés. Ainsi, les utilisateurs affectés à ces groupes auront également le droit de se connecter au gestionnaire de files d'attente et d'insérer et d'extraire de la file d'attente.

Que faire ensuite

Pour vérifier si les étapes ont été effectuées correctement, utilisez les exemples `amqsput` et `amqsget` comme décrit dans la section «8. Test du chiffrement», à la page 296.

3. Création d'une base de données de clés et de certificats

Pourquoi et quand exécuter cette tâche

Pour chiffrer le message, l'intercepteur requiert la clé privée de l'utilisateur émetteur et la ou les clés publiques du ou des destinataires. Par conséquent, la base de données de clés des identités utilisateur mappées aux clés publiques et privées doit être créée. Dans le système réel, où les utilisateurs et les applications sont dispersés sur plusieurs ordinateurs, chaque utilisateur dispose de son propre magasin de clés privé. De même, dans ce guide, nous créons des bases de données de clés pour `alice` et bob et nous partageons les certificats d'utilisateur entre eux.

Remarque : Dans ce guide, nous utilisons des exemples d'applications écrits en C se connectant à l'aide de liaisons locales. Si vous prévoyez d'utiliser des applications Java à l'aide de liaisons client, vous devez créer un magasin de clés JKS et des certificats à l'aide de la commande **keytool** , qui fait partie de l'environnement d'exécution Java (voir «Guide de démarrage rapide pour les clients Java», à la page 296 pour plus de détails). Pour tous les autres langages et pour les applications Java utilisant des liaisons locales, les étapes de ce guide sont correctes.

Procédure

1. Créer une nouvelle base de données de clés pour l'utilisateur `alice`

```
mkdir /home/alice/.mqs -p
runmqakm -keydb -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -stash
```

Remarque :

- Il est conseillé d'utiliser un mot de passe fiable pour sécuriser la base de données.
- Le paramètre `stash` stocke le mot de passe dans le fichier `key.sth` , que les intercepteurs peuvent utiliser pour ouvrir la base de données.

2. Vérifiez que la base de données de clés est lisible

```
chmod +r /home/alice/.mqs/alicekey.kdb
```

3. Créez un certificat identifiant l'utilisateur `alice` à utiliser dans le chiffrement

```
runmqakm -cert -create -db /home/alice/.mqs/alicekey.kdb -pw passw0rd
-label Alice_Cert -dn "cn=alice,o=IBM,c=GB" -default_cert yes
```

Remarque :

- Pour les besoins de ce guide, nous utilisons un certificat autosigné qui peut être créé sans utiliser d'autorité de certification. Pour les systèmes de production, il est conseillé de ne pas utiliser de certificats autosignés, mais de s'appuyer sur des certificats signés par une autorité de certification.
- Le paramètre `label` indique le nom du certificat, que les intercepteurs recherchent pour recevoir les informations nécessaires.
- Le paramètre `DN` spécifie les détails du **nom distinctif** (DN), qui doit être unique pour chaque utilisateur.

4. Maintenant que nous avons créé la base de données de clés, nous devons en définir la propriété et nous assurer qu'elle est illisible par tous les autres utilisateurs.

```
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. Répétez les étapes 1 à 4 pour l'utilisateur bob

Résultats

Les deux utilisateurs `alice` et bob possèdent chacun un certificat autosigné.

4. Création de keystore.conf

Pourquoi et quand exécuter cette tâche

Vous devez pointer les intercepteurs Advanced Message Security vers le répertoire dans lequel se trouvent les bases de données de clés et les certificats. Cette opération est effectuée via le fichier `keystore.conf` , qui contient ces informations sous forme de texte en clair. Chaque utilisateur doit disposer d'un fichier `keystore.conf` distinct dans le dossier `.mqs` . Cette étape doit être effectuée pour `alice` et bob.

Le contenu de `keystore.conf` doit être au format suivant:

```
cms.keystore = <dir>/keystore_file
cms.certificate = certificate_label
```

Exemple

Pour ce scénario, le contenu de `keystore.conf` sera le suivant:

```
cms.keystore = /home/alice/.mqs/alicekey
cms.certificate = Alice_Cert
```

Remarque :

- Le chemin d'accès au fichier de clés doit être fourni sans inclure l'extension de fichier.
- Il existe les formats de fichier de clés suivants: `CMS` (Cryptographic Message Syntax), `JKS` (Java Keystore) et `JCEKS` (Java Cryptographic Extension Keystore). Pour plus d'informations, voir «Structure du fichier de configuration du magasin de clés (keystore.conf)», à la page 307.
- `HOME/.mqs/keystore.conf` est l'emplacement par défaut où Advanced Message Security recherche le fichier `keystore.conf` . Pour plus d'informations sur l'utilisation d'un emplacement autre que celui par défaut pour le `keystore.conf`, voir «Utilisation de magasins de clés et de certificats», à la page 307.

5. Partage de certificats

Pourquoi et quand exécuter cette tâche

Partagez les certificats entre les deux bases de données de clés afin que chaque utilisateur puisse identifier l'autre. Cette opération est effectuée en extrayant le certificat public de chaque utilisateur dans un fichier, qui est ensuite ajouté à la base de données de clés de l'autre utilisateur.

Remarque : Prenez soin d'utiliser l'option *extract* et non l'option *export* . *Extract* obtient la clé publique de l'utilisateur, tandis que *export* obtient à la fois la clé publique et la clé privée. L'utilisation de *export* par erreur compromettrait complètement votre application en transmettant sa clé privée.

Procédure

1. Extrayez le certificat identifiant `alice` dans un fichier externe:

```
runmqakm -cert -extract -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Alice_Cert
-target alice_public.arm
```

2. Ajoutez le certificat au magasin de clés `bob's` :

```
runmqakm -cert -add -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Alice_Cert -file
alice_public.arm
```

3. Répétez l'étape pour bob:

```
 runmqakm -cert -extract -db /home/bob/.mqs/bobkey.kdb -pw passw0rd -label Bob_Cert -target
bob_public.arm
```

4. Ajoutez le certificat pour bob au magasin de clés `alice's` :

```
runmqakm -cert -add -db /home/alice/.mqs/alicekey.kdb -pw passw0rd -label Bob_Cert -file
bob_public.arm
```

Résultats

Les deux utilisateurs `alice` et bob sont désormais en mesure de s'identifier mutuellement en ayant créé et partagé des certificats autosignés.

Que faire ensuite

Vérifiez qu'un certificat se trouve dans le magasin de clés en exécutant les commandes suivantes qui impriment ses détails:

```
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. Définition de la règle de file d'attente

Pourquoi et quand exécuter cette tâche

Avec le gestionnaire de files d'attente créé et les intercepteurs préparés pour intercepter les messages et les clés de chiffrement d'accès, nous pouvons commencer à définir des règles de protection sur `QM_VERIFY_AMS` à l'aide de la commande `setmqspl` . Pour plus d'informations sur cette commande, voir setmqspl . Chaque nom de règle doit être identique au nom de la file d'attente à laquelle il doit être appliqué.

Exemple

Voici un exemple de règle définie pour la file d'attente TEST.Q . Dans cet exemple, les messages sont signés par l'utilisateur `alice` à l'aide de l'algorithme SHA1 et chiffrés à l'aide de l'algorithme AES 256 bits.`alice` est le seul émetteur valide et bob est le seul récepteur des messages de cette file d'attente:

```
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"
```

Remarque : Les noms distinctifs correspondent exactement à ceux spécifiés dans le certificat de l'utilisateur respectif de la base de données de clés.

Que faire ensuite

Pour vérifier la règle que vous avez définie, exécutez la commande suivante:

```
dspmqspl -m QM_VERIFY_AMS
```

Pour imprimer les détails de la règle sous la forme d'un ensemble de commandes `setmqspl` , utilisez l'indicateur `-export` . Cela permet de stocker des règles déjà définies:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Test de la configuration

Pourquoi et quand exécuter cette tâche

En exécutant différents programmes sous différents utilisateurs, vous pouvez vérifier si l'application a été correctement configurée.

Procédure

1. Accédez au répertoire contenant les exemples. Si MQ est installé dans un emplacement autre que celui par défaut, il se peut qu'il se trouve à un autre emplacement.

   ```
   cd /opt/mqm/samp/bin
   ```

2. Changez d'utilisateur pour qu'il s'exécute en tant qu'utilisateur `alice`

   ```
   su alice
   ```

3. En tant qu'utilisateur `alice`, placez un message à l'aide d'un exemple d'application:

   ```
   ./amqsput TEST.Q QM_VERIFY_AMS
   ```

4. Entrez le texte du message, puis appuyez sur Entrée.
5. Arrêt de l'exécution en tant qu'utilisateur `alice`

   ```
   exit
   ```

6. Changez d'utilisateur pour qu'il s'exécute en tant qu'utilisateur bob

   ```
   su bob
   ```

7. En tant qu'utilisateur bob, obtenez un message à l'aide d'un exemple d'application:

   ```
   ./amqsget TEST.Q QM_VERIFY_AMS
   ```

Résultats

Si l'application a été correctement configurée pour les deux utilisateurs, le message de l'utilisateur `alice`s'affiche lorsque bob exécute l'application d'obtention.

8. Test du chiffrement

Pourquoi et quand exécuter cette tâche

Pour vérifier que le chiffrement est effectué comme prévu, créez une file d'attente alias qui fait référence à la file d'attente d'origine TEST.Q. Cette file d'attente alias n'ayant pas de règle de sécurité, aucun utilisateur ne dispose des informations permettant de déchiffrer le message. Par conséquent, les données chiffrées sont affichées.

Procédure

1. A l'aide de la commande **runmqsc** sur le gestionnaire de files d'attente QM_VERIFY_AMS, créez une file d'attente alias.

   ```
   DEFINE QALIAS(TEST.ALIAS) TARGET(TEST.Q)
   ```

2. Accordez à bob l'accès pour parcourir la file d'attente alias

   ```
   setmqaut -m QM_VERIFY_AMS -n TEST.ALIAS -t queue -p bob +browse
   ```

3. En tant qu'utilisateur alice, placez un autre message à l'aide d'un exemple d'application comme précédemment:

   ```
   ./amqsput TEST.Q QM_VERIFY_AMS
   ```

4. En tant qu'utilisateur bob, parcourez le message à l'aide d'un exemple d'application via la file d'attente alias cette fois:

   ```
   ./amqsbcg TEST.ALIAS QM_VERIFY_AMS
   ```

5. En tant qu'utilisateur bob, obtenez le message à l'aide d'un exemple d'application à partir de la file d'attente locale:

   ```
   ./amqsget TEST.Q QM_VERIFY_AMS
   ```

Résultats

La sortie de l'application amqsbcg affichera les données chiffrées qui se trouvent dans la file d'attente prouvant que le message a été chiffré.

Guide de démarrage rapide pour les clients Java

Utilisez ce guide pour configurer rapidement IBM Advanced Message Security afin de garantir la sécurité des messages pour les applications Java qui se connectent à l'aide de liaisons client. Lorsque vous l'aurez terminé, vous aurez créé un magasin de clés pour vérifier les identités des utilisateurs et défini des règles de signature / chiffrement pour votre gestionnaire de files d'attente.

Avant de commencer

Vérifiez que les composants appropriés sont installés, comme décrit dans le **Guide de démarrage rapide** (Windows ou UNIX).

1. Création d'un gestionnaire de files d'attente et d'une file d'attente

Pourquoi et quand exécuter cette tâche

Tous les exemples suivants utilisent une file d'attente nommée TEST.Q pour la transmission de messages entre les applications. Advanced Message Security utilise des intercepteurs pour signer et chiffrer les messages lorsqu'ils entrent dans l'infrastructure WebSphere MQ via l'interface WebSphere MQ standard. La configuration de base est effectuée dans WebSphere MQ et est configurée dans les étapes suivantes.

Procédure

1. Création d'un gestionnaire de files d'attente

```
crtmqm QM_VERIFY_AMS
```

2. Démarrer le gestionnaire de files d'attente

```
strmqm QM_VERIFY_AMS
```

3. Créez et démarrez un programme d'écoute en entrant les commandes suivantes dans **runmqsc** pour le gestionnaire de files d'attente QM_VERIFY_AMS

```
DEFINE LISTENER(AMS.LSTR) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
START LISTENER(AMS.LSTR)
```

4. Créez un canal via lequel nos applications se connectent en entrant la commande suivante dans **runmqsc** pour le gestionnaire de files d'attente QM_VERIFY_AMS

```
DEFINE CHANNEL(AMS.SVRCONN) CHLTYPE(SVRCONN)
```

5. Créez une file d'attente appelée TEST.Q en entrant la commande suivante dans **runmqsc** pour le gestionnaire de files d'attente QM_VERIFY_AMS

```
DEFINE QLOCAL(TEST.Q)
```

Résultats

Si la procédure a abouti, la commande suivante entrée dans **runmqsc** affiche les détails relatifs à TEST.Q:

```
DISPLAY Q(TEST.Q)
```

2. Création et autorisation d'utilisateurs

Pourquoi et quand exécuter cette tâche

Deux utilisateurs apparaissent dans notre scénario: alice, l'expéditeur et bob, le destinataire. Pour utiliser la file d'attente d'application, ces utilisateurs doivent être autorisés à l'utiliser. De même, pour utiliser correctement les règles de protection que nous définirons, ces utilisateurs doivent être autorisés à accéder à certaines files d'attente du système. Pour plus d'informations sur la commande **setmqaut** , voir **setmqaut** .

Procédure

1. Créez les deux utilisateurs comme décrit dans le **Guide de démarrage rapide** (Windows ou UNIX) pour votre plateforme.
2. Autoriser les utilisateurs à se connecter au gestionnaire de files d'attente et à utiliser la file d'attente

```
setmqaut -m QM_VERIFY_AMS -t qmgr -p alice -p bob +connect +inq
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p alice +put
setmqaut -m QM_VERIFY_AMS -n TEST.Q -t queue -p bob +get +inq
```

3. Vous devez également autoriser les deux utilisateurs à parcourir la file d'attente de règles système et à placer des messages dans la file d'attente d'erreurs.

```
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
```

Résultats

Les utilisateurs sont maintenant créés et les droits requis leur sont accordés.

Que faire ensuite

Pour vérifier si les étapes ont été effectuées correctement, utilisez les exemples `JmsProducer` et `JmsConsumer` comme décrit dans la section «7. Test de la configuration», à la page 300.

3. Création d'une base de données de clés et de certificats

Pourquoi et quand exécuter cette tâche

Pour chiffrer le message à l'intercepteur, la clé publique des utilisateurs qui l'envoient est requise. Par conséquent, la base de données de clés des identités utilisateur mappées aux clés publiques et privées doit être créée. Dans le système réel, où les utilisateurs et les applications sont dispersés sur plusieurs ordinateurs, chaque utilisateur dispose de son propre magasin de clés privé. De même, dans ce guide, nous créons des bases de données de clés pour `alice` et bob et nous partageons les certificats d'utilisateur entre eux.

Remarque : Dans ce guide, nous utilisons des exemples d'application écrits en Java se connectant à l'aide de liaisons client. Si vous prévoyez d'utiliser des applications Java à l'aide de liaisons locales ou d'applications C, vous devez créer un magasin de clés CMS et des certificats à l'aide de la commande **`runmqakm`** . Cela est indiqué dans le **Guide de démarrage rapide** (Windows ou UNIX).

Procédure

1. Créez un répertoire dans lequel créer votre magasin de clés, par exemple `/home/alice/.mqs`. Vous souhaiterez peut-être le créer dans le même répertoire que celui utilisé par le **Guide de démarrage rapide** (Windows ou UNIX) pour votre plateforme.

   Remarque : Ce répertoire sera appelé *keystore-dir* dans les étapes suivantes
2. Création d'un fichier de clés et d'un certificat identifiant l'utilisateur `alice` à utiliser dans le chiffrement

   Remarque : La commande **`keytool`** fait partie de l'environnement d'exécution Java.

   ```
   keytool -genkey -alias Alice_Java_Cert -keyalg RSA -keystore keystore-dir/keystore.jks
   -storepass passw0rd
   -dname "CN=alice, O=IBM, C=GB" -keypass passw0rd
   ```

   Remarque :

   - Si votre *keystore-dir* contient des espaces, vous devez placer des guillemets autour du nom complet de votre magasin de clés
   - Il est conseillé d'utiliser un mot de passe fiable pour sécuriser le magasin de clés.
   - Pour les besoins de ce guide, nous utilisons un certificat autosigné qui peut être créé sans utiliser d'autorité de certification. Pour les systèmes de production, il est conseillé de ne pas utiliser de certificats autosignés, mais de s'appuyer sur des certificats signés par une autorité de certification.
   - Le paramètre `alias` indique le nom du certificat, que les intercepteurs recherchent pour recevoir les informations nécessaires.
   - Le paramètre dname spécifie les détails du **nom distinctif** (DN), qui doit être unique pour chaque utilisateur.
3. Sous UNIX, vérifiez que le magasin de clés est lisible

   ```
   chmod +r keystore-dir/keystore.jks
   ```
4. Répétez l' step1-4 pour l'utilisateur bob

Résultats

Les deux utilisateurs `alice` et bob possèdent chacun un certificat autosigné.

4. Création de keystore.conf

Pourquoi et quand exécuter cette tâche

Vous devez pointer les intercepteurs Advanced Message Security vers le répertoire dans lequel se trouvent les bases de données de clés et les certificats. Cette opération est effectuée via le fichier `keystore.conf` , qui contient ces informations sous forme de texte en clair. Chaque utilisateur doit disposer d'un fichier `keystore.conf` distinct. Cette étape doit être effectuée pour `alice` et bob.

Exemple

Pour ce scénario, le contenu de `keystore.conf` for `alice` sera le suivant:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Alice_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Pour ce scénario, le contenu de `keystore.conf` for bob sera le suivant:

```
JKS.keystore = keystore-dir/keystore
JKS.certificate = Bob_Java_Cert
JKS.encrypted = no
JKS.keystore_pass = passw0rd
JKS.key_pass = passw0rd
JKS.provider = IBMJCE
```

Remarque :

- Le chemin d'accès au fichier de clés doit être fourni sans inclure l'extension de fichier.
- Si vous disposez déjà d'un `keystore.conf` car vous avez suivi le **Guide de démarrage rapide** (Windows ou UNIX), vous pouvez éditer le fichier existant à ajouter aux lignes ci-dessus.
- Pour plus d'informations, voir «Structure du fichier de configuration du magasin de clés (keystore.conf)», à la page 307.

5. Partage de certificats

Pourquoi et quand exécuter cette tâche

Partagez les certificats entre les deux magasins de clés afin que chaque utilisateur puisse identifier l'autre. Cette opération est effectuée en extrayant le certificat de chaque utilisateur et en l'important dans le magasin de clés de l'autre utilisateur.

Remarque : Les termes *extraire* et *exporter* sont utilisés différemment par les différents outils de certificat. Par exemple, l'outil IBM GSKit Keyman (ikeyman) distingue que vous *extrayez* des certificats (clés publiques) et que vous *exportez* des clés privées. Cette distinction est extrêmement importante pour les outils qui offrent les deux options, car l'utilisation de *export* par erreur compromettrait complètement votre application en transmettant sa clé privée. Etant donné que la distinction est si importante, la documentation WebSphere MQ s'efforce d'utiliser ces termes de manière cohérente. Toutefois, l'outil de clé Java fournit une option de ligne de commande appelée *exportcert* qui extrait uniquement la clé publique. Pour ces raisons, la procédure suivante fait référence à l' *extraction de certificats* à l'aide de l'option *exportcert* .

Procédure

1. Extrayez le certificat identifiant `alice`.

   ```
   keytool -exportcert -keystore alice-keystore-dir/keystore.jks -storepass passw0rd
   -alias Alice_Java_Cert -file alice-keystore-dir/Alice_Java_Cert.cer
   ```

2. Importez le certificat identifiant `alice` dans le magasin de clés que bob utilisera. Lorsque vous y êtes invité, indiquez que vous ferez confiance à ce certificat.

```
keytool -importcert -file alice-keystore-dir/Alice_Java_Cert.cer -alias Alice_Java_Cert
-keystore bob-keystore-dir/keystore.jks -storepass passw0rd
```

3. Répétez les étapes pour bob

Résultats

Les deux utilisateurs `alice` et bob sont désormais en mesure de s'identifier mutuellement en ayant créé et partagé des certificats autosignés.

Que faire ensuite

Vérifiez qu'un certificat se trouve dans le magasin de clés en exécutant les commandes suivantes qui impriment ses détails:

```
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. Définition de la règle de file d'attente

Pourquoi et quand exécuter cette tâche

Avec le gestionnaire de files d'attente créé et les intercepteurs préparés pour intercepter les messages et les clés de chiffrement d'accès, nous pouvons commencer à définir des règles de protection sur `QM_VERIFY_AMS` à l'aide de la commande `setmqspl` . Pour plus d'informations sur cette commande, voir setmqspl . Chaque nom de règle doit être identique au nom de la file d'attente à laquelle il doit être appliqué.

Exemple

Voici un exemple de règle définie dans la file d'attente `TEST.Q` , signée par l'utilisateur `alice` à l'aide de l'algorithme SHA1 et chiffrée à l'aide de l'algorithme AES 256 bits pour l'utilisateur 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"
```

Remarque : Les noms distinctifs correspondent exactement à ceux spécifiés dans le certificat de l'utilisateur respectif de la base de données de clés.

Que faire ensuite

Pour vérifier la règle que vous avez définie, exécutez la commande suivante:

```
dspmqspl -m QM_VERIFY_AMS
```

Pour imprimer les détails de la règle sous la forme d'un ensemble de commandes `setmqspl` , utilisez l'indicateur `-export` . Cela permet de stocker des règles déjà définies:

```
dspmqspl -m QM_VERIFY_AMS -export >restore_my_policies.bat
```

7. Test de la configuration

Avant de commencer

Vérifiez que les fichiers de règles JCE sans restriction sont installés dans la version de Java que vous utilisez.

Remarque : La version de Java fournie dans l'installation WebSphere MQ contient déjà ces fichiers de règles. Il se trouve dans *MQ_INSTALLATION_PATH*`/java/bin`.

Pourquoi et quand exécuter cette tâche

En exécutant différents programmes sous différents utilisateurs, vous pouvez vérifier si l'application a été correctement configurée. Reportez-vous au **Guide de démarrage rapide** (Windows ou UNIX) de votre plateforme pour plus de détails sur l'exécution de programmes sous différents utilisateurs.

Procédure

1. Pour exécuter ces modèles d'application JMS, utilisez le paramètre CLASSPATH pour votre plateforme, comme indiqué dans la rubrique Variables d'environnement utilisées par IBM WebSphere MQ classes for JMS pour vous assurer que le répertoire des exemples est inclus.
2. En tant qu'utilisateur `alice`, placez un message à l'aide d'un exemple d'application, en vous connectant en tant que client:

   ```
   java JMSProducer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
   ```

3. En tant qu'utilisateur bob, obtenez un message à l'aide d'un exemple d'application, en vous connectant en tant que client:

   ```
   java JMSConsumer -m QM_VERIFY_AMS -d TEST.Q -h localhost -p 1414 -l AMS.SVRCONN
   ```

Résultats

Si l'application a été correctement configurée pour les deux utilisateurs, le message de l'utilisateur `alice`s'affiche lorsque bob exécute l'application d'obtention.

Protection des files d'attente éloignées

Pour protéger complètement les connexions de file d'attente éloignée, la même règle doit être définie sur la file d'attente éloignée et la file d'attente locale à laquelle les messages sont transmis.

Lorsqu'un message est inséré dans une file d'attente éloignée, Advanced Message Security intercepte l'opération et traite le message conformément à un ensemble de règles pour la file d'attente éloignée. Par exemple, pour une règle de chiffrement, le message est chiffré avant d'être transmis à WebSphere MQ pour le gérer. Une fois que Advanced Message Security a traité le message inséré dans une file d'attente éloignée, WebSphere MQ le place dans la file d'attente de transmission associée et le transmet au gestionnaire de files d'attente cible et à la file d'attente cible.

Lorsqu'une opération GET est effectuée sur la file d'attente locale, Advanced Message Security tente de décoder le message en fonction de l'ensemble de règles de la file d'attente locale. Pour que l'opération aboutisse, la règle utilisée pour déchiffrer le message doit être identique à celle utilisée pour le chiffrer. Toute différence provoquera le rejet du message.

Si, pour une raison quelconque, les deux règles ne peuvent pas être définies en même temps, une prise en charge du déploiement par étapes est fournie. La règle peut être définie sur une file d'attente locale avec l'indicateur de tolérance activé, qui indique qu'une règle associée à une file d'attente peut être ignorée lorsqu'une tentative d'extraction d'un message de la file d'attente implique un message pour lequel la règle de sécurité n'est pas définie. Dans ce cas, GET tente de déchiffrer le message, mais autorise la distribution de messages non chiffrés. De cette manière, les règles des files d'attente éloignées peuvent être définies une fois que les files d'attente locales ont été protégées (et testées).

A faire : Supprimez l'indicateur de tolérance une fois le déploiement de Advanced Message Security terminé.

Référence associée

setmqspl (définition de la règle de sécurité)

Routage des messages protégés à l'aide de WebSphere Message Broker

IBM Advanced Message Security peut protéger les messages dans une infrastructure où WebSphere Message Broker version 8.0.0.1 (ou ultérieure) est installé. Vous devez comprendre la nature des deux produits avant d'appliquer la sécurité dans l'environnement WebSphere Message Broker.

Pourquoi et quand exécuter cette tâche

Advanced Message Security fournit une sécurité de bout en bout de la charge de message. Cela signifie que seules les parties spécifiées comme expéditeurs et destinataires valides d'un message sont capables de le produire ou de le recevoir. Cela implique que pour sécuriser les messages transitant par WebSphere Message Broker, vous pouvez soit autoriser WebSphere Message Broker à traiter les messages sans connaître leur contenu (scénario 1), soit permettre à un utilisateur autorisé de recevoir et d'envoyer des messages (scénario 2).

Scénario 1-Message Broker ne peut pas voir le contenu des messages

Avant de commencer

WebSphere Message Broker doit être connecté à un gestionnaire de files d'attente existant. Remplacez *QMgrName* par ce nom de gestionnaire de files d'attente existant dans les commandes qui suivent.

Pourquoi et quand exécuter cette tâche

Dans ce scénario, Alice place un message protégé dans une file d'attente d'entrée `QIN`. En fonction de la propriété de message `routeTo`, le message est acheminé vers *Bob's* (`QBOB`),[1](`QCECIL`) ou la file d'attente par défaut (`QDEF`). Le routage est possible car Advanced Message Security protège uniquement la charge de message et non ses en-têtes et propriétés qui restent non protégés et peuvent être lus par WebSphere Message Broker. Advanced Message Security est utilisé uniquement par *alice*, *bob* et *cecil*. Il n'est pas nécessaire de l'installer ou de le configurer pour WebSphere Message Broker.

WebSphere Message Broker reçoit le message protégé de la file d'attente des alias non protégés afin d'éviter toute tentative de déchiffrement du message. S'il devait utiliser directement la file d'attente protégée, le message serait placé dans la file d'attente DEAD LETTER comme impossible à déchiffrer. Le message est acheminé par WebSphere Message Broker et arrive dans la file d'attente cible sans modification. Par conséquent, il est toujours signé par l'auteur d'origine (*bob* et *cecil* n'acceptent que les messages envoyés par *alice*) et protégé comme auparavant (seuls *bob* et *cecil* peuvent le lire). WebSphere Message Broker place le message acheminé vers un alias non protégé. Les destinataires extraient le message d'une file d'attente en sortie protégée dans laquelle IBM WebSphere MQ AMS déchiffre le message de manière transparente.

Procédure

1. Configurez *alice*, *bob* et *cecil* pour utiliser Advanced Message Security comme décrit dans le **Guide de démarrage rapide** (Windows ou UNIX).

   Vérifiez que les étapes suivantes sont effectuées:

   - Création et autorisation d'utilisateurs
   - Création de la base de données de clés et des certificats
   - Création de keystore.conf
2. Fournissez le certificat *alice* à *bob* et *cecil*, de sorte que *alice* puisse être identifié par eux lors de la vérification des signatures numériques sur les messages.

   Pour ce faire, extrayez le certificat identifiant *alice* dans un fichier externe, puis ajoutez le certificat extrait aux magasins de clés *Bob's* et *Cecil's* . Il est important d'utiliser la méthode décrite dans la tâche 5 de **. Partage de certificats** dans le **Guide de démarrage rapide** (Windows ou UNIX).
3. Fournissez les certificats *bob* et *cecil* à *alice*, de sorte que *alice* puisse envoyer des messages chiffrés pour *bob* et *cecil*.

   Effectuez cette opération à l'aide de la méthode spécifiée à l'étape précédente.
4. Sur votre gestionnaire de files d'attente, définissez des files d'attente locales appelées `QIN`, `QBOB`, `QCECIL` et `QDEF`.

   ```
   DEFINE QLOCAL(QIN)
   ```

[1] Cecil's

5. Définissez la règle de sécurité pour la file d'attente QIN dans une configuration éligible. Utilisez la configuration identique pour les files d'attente QBOB, QCECIL et 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"
```

   Ce scénario suppose la règle de sécurité dans laquelle *alice* est le seul expéditeur autorisé et *bob* et *cecil* sont les destinataires.
6. Définissez des files d'attente alias AIN, ABOB et ACECIL référençant des files d'attente locales QIN, QBOB et QCECIL respectivement.

```
DEFINE QALIAS(AIN) TARGET(QIN)
```

7. Vérifiez que la configuration de sécurité pour les alias spécifiés à l'étape précédente n'est pas présente ; sinon, définissez sa règle sur NONE.

```
dspmqspl -m QMgrName -p AIN
```

8. Dans WebSphere Message Broker, créez un flux de messages pour acheminer les messages arrivant dans la file d'attente alias AIN vers le noeud BOB, CECIL ou DEF en fonction de la propriété routeTo du message. Pour ce faire, procédez comme suit :
   a) Créez un noeud MQInput appelé IN et affectez l'alias AIN comme nom de file d'attente.
   b) Créez des noeuds MQOutput appelés BOB, CECIL et DEF et affectez des files d'attente alias ABOB, ACECIL et ADEF comme noms de file d'attente respectifs.
   c) Créez un noeud de route et appelez-le TEST.
   d) Connectez le noeud IN au terminal d'entrée du noeud TEST .
   e) Créez des terminaux de sortie bobet cecil pour le noeud TEST .
   f) Connectez le terminal de sortie bob au noeud BOB .
   g) Connectez le terminal de sortie cecil au noeud CECIL .
   h) Connectez le noeud DEF au terminal de sortie par défaut.
   i) Appliquez les règles suivantes:

```
$Root/MQRFH2/usr/routeTo/text()="bob"
$Root/MQRFH2/usr/routeTo/text()="cecil"
```

9. Déployez le flux de messages dans le composant d'exécution WebSphere Message Broker.
10. L'exécution en tant qu'utilisateur Alice a inséré un message qui contient également une propriété de message appelée routeTo avec la valeur bob ou cecil. L'exécution du modèle d'application **amqsstm** vous permet d'effectuer cette opération.

```
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. L'exécution en tant qu'utilisateur *bob* extrait le message de la file d'attente QBOB à l'aide du modèle d'application **amqsget**.

Résultats

Lorsque *alice* place un message dans la file d'attente QIN , le message est protégé. Il est extrait sous forme protégée par WebSphere Message Broker à partir de la file d'attente alias AIN . WebSphere Message Broker décide où acheminer le message en lisant la propriété routeTo qui est, comme

toutes les propriétés, non chiffrée. WebSphere Message Broker place le message sur l'alias non protégé approprié, ce qui évite une protection supplémentaire. Lorsqu'il est reçu par *bob* ou *cecil* de la file d'attente, le message est déchiffré et la signature numérique est vérifiée.

Scénario 2-Message Broker peut voir le contenu des messages

Pourquoi et quand exécuter cette tâche

Dans ce scénario, un groupe de personnes est autorisé à envoyer des messages à WebSphere Message Broker. Un autre groupe est autorisé à recevoir des messages créés par WebSphere Message Broker. La transmission entre les parties et WebSphere Message Broker ne peut pas être espionner.

N'oubliez pas que WebSphere Message Broker lit les règles de protection et les certificats uniquement lorsqu'une file d'attente est ouverte. Vous devez donc recharger le groupe d'exécution après avoir mis à jour les règles de protection pour que les modifications soient prises en compte.

```
mqsireload execution-group-name
```

Si WebSphere Message Broker est considéré comme une partie autorisée à lire ou à signer le contenu du message, vous devez configurer Advanced Message Security pour l'utilisateur qui démarre le service WebSphere Message Broker. Sachez que ce n'est pas nécessairement le même utilisateur qui insère / extrait les messages dans les files d'attente ni l'utilisateur qui crée et déploie les applications WebSphere Message Broker.

Procédure

1. Configurez *alice*, *bob*, *cecil* et *dave* et l'utilisateur de service WebSphere Message Broker, pour utiliser Advanced Message Security comme décrit dans le **Guide de démarrage rapide** (Windows ou UNIX).

   Vérifiez que les étapes suivantes sont effectuées:

   - Création et autorisation d'utilisateurs
   - Création de la base de données de clés et des certificats
   - Création de keystore.conf
2. Fournissez les certificats *alice*, *bob*, *cecil* et *dave* à l'utilisateur du service WebSphere Message Broker.

   Procédez à cette opération en extrayant dans des fichiers externes chacun des certificats identifiant *alice*, *bob*, *cecil* et *dave*, puis en ajoutant les certificats extraits au magasin de clés WebSphere Message Broker. Il est important d'utiliser la méthode décrite dans la tâche 5 de **. Partage de certificats** dans le **Guide de démarrage rapide** (Windows ou UNIX).
3. Fournissez le certificat de l'utilisateur du service WebSphere Message Broker à *alice*, *bob*, *cecil* et *dave*.

   Effectuez cette opération à l'aide de la méthode spécifiée à l'étape précédente.

   Remarque : *Alice* et *bob* ont besoin du certificat de l'utilisateur du service WebSphere Message Broker pour chiffrer correctement les messages. L'utilisateur du service WebSphere Message Broker a besoin des certificats *alice* et *bob* pour vérifier les auteurs des messages. L'utilisateur du service WebSphere Message Broker a besoin des certificats *cecil* et *dave* pour chiffrer les messages pour eux. *cecil* et *dave* ont besoin du certificat de l'utilisateur du service WebSphere Message Broker pour vérifier si le message provient de WebSphere Message Broker.
4. Définissez une file d'attente locale nommée IN et définissez la règle de sécurité avec *alice* et *bob* spécifiés comme auteurs et l'utilisateur de service WebSphere Message Broker spécifié comme destinataire:

   ```
   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. Définissez une file d'attente locale nommée OUT et définissez la règle de sécurité avec l'utilisateur de service WebSphere Message Broker spécifié comme auteur et *cecil* et *dave* spécifié comme destinataires:

```
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. Dans WebSphere Message Broker, créez un flux de messages avec un noeud `MQInput` et `MQOutput` . Configurez le noeud `MQInput` pour qu'il utilise la file d'attente `IN` et le noeud `MQOutput` pour qu'il utilise la file d'attente `OUT` .
7. Déployez le flux de messages dans le composant d'exécution WebSphere Message Broker.
8. L'exécution en tant qu'utilisateur *alice* ou *bob* a inséré un message dans la file d'attente `IN` à l'aide du modèle d'application **amqsput**.
9. L'exécution en tant qu'utilisateur *cecil* ou *dave* extrait le message de la file d'attente `OUT` à l'aide du modèle d'application **amqsget**.

Résultats

Les messages envoyés par *alice* ou *bob* à la file d'entrée `IN` sont chiffrés, ce qui permet uniquement à WebSphere Message Broker de les lire. WebSphere Message Broker n'accepte que les messages provenant de *alice* et de *bob* et rejette les autres messages. Les messages acceptés seront traités de manière appropriée, puis signés et chiffrés avec les clés *cecil* et *dave* avant d'être placés dans la file d'attente de sortie `OUT`. Seuls *cecil* et *dave* sont capables de le lire, les messages non signés par WebSphere Message Broker sont rejetés.

Utilisation de IBM WebSphere MQ Advanced Message Security avec IBM WebSphere MQ Managed File Transfer

Ce scénario explique comment configurer Advanced Message Security pour fournir la confidentialité des messages pour les données envoyées via un IBM WebSphere MQ Managed File Transfer.

Avant de commencer

Vérifiez que le composant Advanced Message Security est installé sur l'installation WebSphere MQ hébergeant les files d'attente utilisées par IBM WebSphere MQ Managed File Transfer que vous souhaitez protéger.

Si vos agents IBM WebSphere MQ Managed File Transfer se connectent en mode liaisons, assurez-vous que le composant GSKit est également installé sur leur installation locale.

Pourquoi et quand exécuter cette tâche

Lorsque le transfert de données entre deux agents IBM WebSphere MQ Managed File Transfer est interrompu, il est possible que des données confidentielles restent non protégées dans les files d'attente WebSphere MQ sous-jacentes utilisées pour gérer le transfert. Ce scénario explique comment configurer et utiliser Advanced Message Security pour protéger ces données dans les files d'attente IBM WebSphere MQ Managed File Transfer .

Dans ce scénario, nous considérons une topologie simple comprenant une machine avec deux files d'attente IBM WebSphere MQ Managed File Transfer et deux agents, `AGENT1` et `AGENT2`, partageant un seul gestionnaire de files d'attente, `hubQM`, comme décrit dans le scénario Transfert de fichiers de base à l'aide des scripts. Les deux agents se connectent de la même manière, soit en mode liaisons, soit en mode client.

1. Création de certificats

Avant de commencer

Ce scénario utilise un modèle simple dans lequel un utilisateur `ftagent` d'un groupe `FTAGENTS` est utilisé pour exécuter les processus d'agent IBM WebSphere MQ Managed File Transfer . Si vous utilisez vos propres noms d'utilisateur et de groupe, modifiez les commandes en conséquence.

Pourquoi et quand exécuter cette tâche

Advanced Message Security utilise la cryptographie à clé publique pour signer et / ou chiffrer les messages dans les files d'attente protégées.

Remarque :

- Si vos agents IBM WebSphere MQ Managed File Transfer s'exécutent en mode liaisons, les commandes que vous utilisez pour créer un magasin de clés CMS (Cryptographic Message Syntax) sont détaillées dans le **Guide de démarrage rapide** (Windows ou UNIX) pour votre plateforme.
- Si vos agents IBM WebSphere MQ Managed File Transfer s'exécutent en mode client, les commandes dont vous aurez besoin pour créer un fichier de clés JKS (Java Keystore) sont détaillées dans «Guide de démarrage rapide pour les clients Java», à la page 296.

Procédure

1. Créez un certificat autosigné pour identifier l'utilisateur `ftagent` comme indiqué dans le guide de démarrage rapide approprié.
   Utilisez un nom distinctif (DN) comme suit:

   ```
   CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB
   ```

2. Créez un fichier `keystore.conf` pour identifier l'emplacement du magasin de clés et le certificat qu'il contient, comme indiqué dans le guide de démarrage rapide approprié.

2. Configuration de la protection des messages

Pourquoi et quand exécuter cette tâche

Vous devez définir une règle de sécurité pour la file d'attente de données utilisée par AGENT2, à l'aide de la commande **setmqspl** . Dans ce scénario, le même utilisateur est utilisé pour démarrer les deux agents et, par conséquent, le nom distinctif du signataire et du récepteur sont identiques et correspondent au certificat que nous avons généré.

Procédure

1. Arrêtez les agents IBM WebSphere MQ Managed File Transfer en vue de leur protection à l'aide de la commande **fteStopAgent** .
2. Créez une règle de sécurité pour protéger la file d'attente SYSTEM.FTE.DATA.AGENT2 .

   ```
   setmqspl -m hubQM -p SYSTEM.FTE.DATA.AGENT2 -s SHA1 -a "CN=ftagent, OU=MFT, O=IBM,
   L=Hursley, ST=Hampshire, C=GB"
   -e AES128 -r "CN=ftagent, OU=MFT, O=IBM, L=Hursley, ST=Hampshire, C=GB"
   ```

3. Vérifiez que l'utilisateur exécutant le processus d'agent IBM WebSphere MQ Managed File Transfer a accès à la file d'attente des règles système et qu'il y a des messages dans la file d'attente des erreurs.

   ```
   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. Redémarrez vos agents IBM WebSphere MQ Managed File Transfer à l'aide de la commande **fteStartAgent** .
5. Confirmez que vos agents ont été redémarrés avec succès à l'aide de la commande **fteListAgents** et vérifiez qu'ils sont à l'état READY .

Résultats

Vous pouvez maintenant soumettre des transferts depuis AGENT1 vers AGENT2et le contenu du fichier sera transmis de manière sécurisée entre les deux agents.

InstallationIBM WebSphere MQ Advanced Message Security

Installez le composant IBM WebSphere MQ Advanced Message Security sur différentes plateformes.

Pourquoi et quand exécuter cette tâche

Pour connaître les procédures d'installation complètes, voir Installation de IBM WebSphere MQ Advanced Message Security.

Tâches associées

désinstallationIBM WebSphere MQ Advanced Message Security

Utilisation de magasins de clés et de certificats

Pour fournir une protection cryptographique transparente aux applications WebSphere MQ , Advanced Message Security utilise le fichier de clés, dans lequel les certificats de clé publique et une clé privée sont stockés.

Dans Advanced Message Security, les utilisateurs et les applications sont représentés par des identités PKI (Public Key Infrastructure). Ce type d'identité est utilisé pour signer et chiffrer les messages. L'identité PKI est représentée par la zone **Nom distinctif (DN)** du sujet dans un certificat associé à des messages signés et chiffrés. Pour qu'un utilisateur ou une application puisse chiffrer ses messages, il doit avoir accès au fichier de clés dans lequel sont stockés les certificats et les clés privées et publiques associées.

L'emplacement du magasin de clés est fourni dans le fichier de configuration du magasin de clés, qui est `keystore.conf` par défaut. Chaque utilisateur Advanced Message Security doit disposer du fichier de configuration de magasin de clés qui pointe vers un fichier de magasin de clés. Advanced Message Security accepte le format suivant pour les fichiers de clés: `.kdb`, `.jceks`, `.jks`.

L'emplacement par défaut du fichier `keystore.conf` est:

- Sur les plateformes UNIX : `$HOME/.mqs/keystore.conf`
- Sur les plateformes Windows : *%HOMEDRIVE%%HOMEPATH%*`\.mqs\keystore.conf`

Si vous utilisez un nom de fichier de clés et un emplacement spécifiés, vous devez utiliser les commandes suivantes:

- Pour Java: `java -D` *`MQS_KEYSTORE_CONF=path/filename app_name`*
- Pour le client et le serveur C:
  - Sous UNIX and Linux : `export MQS_KEYSTORE_CONF=`*`path/filename`*
  - Sous Windows : `set MQS_KEYSTORE_CONF=`*`path\filename`*

    Remarque : Le chemin d'accès sous Windows peut et doit spécifier l'identificateur d'unité si plusieurs lettres d'unité sont disponibles.

Concepts associés

«Noms distinctifs des expéditeurs», à la page 321

Les noms distinctifs d'expéditeur identifient les utilisateurs autorisés à placer des messages dans une file d'attente.

«Noms distinctifs des destinataires», à la page 322

Les noms distinctifs des destinataires identifient les utilisateurs qui sont autorisés à extraire des messages d'une file d'attente.

Structure du fichier de configuration du magasin de clés (keystore.conf)

Le fichier de configuration du magasin de clés (`keystore.conf`) pointe Advanced Message Security vers l'emplacement du magasin de clés approprié.

Il existe deux types de configuration CMS et Java (JKS et JCEKS). Les entrées de configuration CMS sont préfixées avec `cms.` et Java avec `jks.` ou `jceks.` en fonction du type de magasin de clés.

Le fichier de configuration, en fonction du type de fichier de configuration, peut avoir l'une des structures suivantes:

```
cms.keystore = /<dir>/<keystore_file>
cms.certificate = certificate_label
```

```
jceks.keystore = <dir>/Keystore
jceks.certificate = <certificate_label>
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE

jks.keystore = <dir>/Keystore
jks.certificate = <certificate_label>
jks.encrypted = no
jks.keystore_pass = <password>
jks.key_pass = <password>
jks.provider = IBMJCE
```

Les paramètres du fichier de configuration sont définis comme suit:

keystore
Chemin d'accès au fichier de clés.

Important :

- Le chemin d'accès au fichier de clés ne doit pas inclure l'extension de fichier.
- Pour les fichiers de clés Java, IBM WebSphere MQ AMS prend en charge les formats de fichier suivants: `.jks`, `.jceks`, `.jck`.

certificate
Label de certificat

encrypted
Statut du mot de passe.

keystore_pass
Mot de passe du fichier de clés.

Remarque :

- Pour le magasin de clés CMS, IBM WebSphere MQ AMS s'appuie sur les fichiers de dissimulation (`.sth`), alors que JKS et JCEKS peuvent nécessiter un mot de passe pour le certificat et la clé privée de l'utilisateur.
- Le stockage des mots de passe en texte en clair représente un risque pour la sécurité.

key_pass
Mot de passe de la clé privée de l'utilisateur.

Important : Le stockage des mots de passe sous forme de texte en clair peut présenter un risque pour la sécurité.

provider
Fournisseur de sécurité Java qui implémente les algorithmes de cryptographie requis par le certificat du magasin de clés.

Remarque : Actuellement, IBMJCE est le seul fournisseur pris en charge par Advanced Message Security.

Important : Les informations stockées dans le magasin de clés sont cruciales pour le flux sécurisé des données envoyées à l'aide de WebSphere MQ, c'est pourquoi les administrateurs de sécurité doivent accorder une attention particulière lors de l'affectation de droits d'accès aux fichiers à ces fichiers.

Voici un exemple de fichier `keystore.conf` :

```
cms.keystore = c:\Documents and Settings\Alice\AliceKeystore
cms.certificate = AliceCert

jceks.keystore = c:/Documents and Settings/Alice/AliceKeystore
jceks.certificate = AliceCert
jceks.encrypted = no
jceks.keystore_pass = <password>
jceks.key_pass = <password>
jceks.provider = IBMJCE
```

Tâches associées

«Protection des mots de passe dans Java», à la page 319
Le stockage des mots de passe de clés et de clés privées sous forme de texte en clair représente un risque pour la sécurité. Par conséquent, Advanced Message Security fournit un outil qui peut brouiller ces mots de passe à l'aide de la clé d'un utilisateur, qui est disponible dans le fichier de clés.

Interception MCA (Message Channel Agent)

L'interception MCA permet à un gestionnaire de files d'attente exécuté sous IBM WebSphere MQ d'activer de manière sélective les règles à appliquer pour les canaux de connexion serveur.

L'interception MCA permet aux clients qui restent en dehors de IBM WebSphere MQ AMS d'être toujours connectés à un gestionnaire de files d'attente et de chiffrer et déchiffrer leurs messages.

L'interception MCA est destinée à fournir une fonction IBM WebSphere MQ AMS lorsque IBM WebSphere MQ AMS ne peut pas être activé sur le client. Notez que l'utilisation de l'interception MCA et d'un client compatible avec IBM WebSphere MQ AMSentraîne une double protection des messages qui peut être problématique pour la réception des applications.

Si une erreur `2085 (MQRC_UNKNOWN_OBJECT_NAME)` est signalée si vous utilisez un client Version 7.5 ou version ultérieure pour vous connecter à un gestionnaire de files d'attente à partir d'une version antérieure du produit, vous devez désactiver IBM WebSphere MQ Advanced Message Security sur le client. Pour plus d'informations, voir «Désactivation de IBM WebSphere MQ Advanced Message Security sur le client», à la page 311.

Fichier de configuration du magasin de clés

Par défaut, le fichier de configuration du magasin de clés pour l'interception MCA est `keystore.conf` et se trouve dans le répertoire `.mqs` du répertoire HOME de l'utilisateur qui a démarré le gestionnaire de files d'attente ou le programme d'écoute. Le magasin de clés peut également être configuré à l'aide de la variable d'environnement MQS_KEYSTORE_CONF. Pour plus d'informations sur la configuration du magasin de clés IBM WebSphere MQ AMS , voir «Utilisation de magasins de clés et de certificats», à la page 307.

Pour activer l'interception MCA, vous devez fournir le nom d'un canal que vous souhaitez utiliser dans le fichier de configuration du magasin de clés. Pour l'interception MCA, seul un type de magasin de clés CMS peut être utilisé.

Pour un exemple de configuration de l'interception MCA, voir «Exemple d'interception MCA IBM WebSphere MQ AMS», à la page 309.

Avertissement : Vous devez effectuer l'authentification et le chiffrement des clients sur les canaux sélectionnés, par exemple, en utilisant SSL et SSLPEER ou CHLAUTH TYPE (SSLPEERMAP), pour vous assurer que seuls les clients autorisés peuvent se connecter et utiliser cette fonction.

Exemple d'interception MCA IBM WebSphere MQ AMS

Exemple de tâche de configuration d'une interception MCA IBM WebSphere MQ AMS .

Avant de commencer

Avertissement : Vous devez effectuer l'authentification et le chiffrement des clients sur les canaux sélectionnés, par exemple, en utilisant SSL et SSLPEER ou CHLAUTH TYPE (SSLPEERMAP), pour vous assurer que seuls les clients autorisés peuvent se connecter et utiliser cette fonction.

Pourquoi et quand exécuter cette tâche

Cette tâche vous guide tout au long du processus de configuration de votre système pour utiliser l'interception MCA, puis de vérification de la configuration.

Remarque : Avant IBM WebSphere MQ Version 7.5, IBM WebSphere MQ AMS était un produit complémentaire qui devait être installé séparément et des intercepteurs configurés pour protéger les

applications. A partir de Version 7.5 , les intercepteurs sont automatiquement inclus et activés de manière dynamique dans les environnements d'exécution client et serveur MQ . Dans cet exemple d'interception MCA, les intercepteurs sont fournis à l'extrémité serveur du canal et un environnement d'exécution client plus ancien est utilisé (à l'étape 12) pour placer des messages non protégés sur le canal afin qu'ils puissent être considérés comme protégés par les intercepteurs MCA. Si cet exemple avait utilisé un client Version 7.5 ou ultérieur, le message serait protégé deux fois, car l'intercepteur d'exécution du client MQ et l'intercepteur MCA protégeraient le message lorsqu'il arrive dans MQ.

Avertissement : Remplacez `userID` dans le code par votre ID utilisateur.

Procédure

1. Créez la base de données de clés et les certificats à l'aide des commandes suivantes pour créer un script shell.

   Modifiez également les paramètres **INSTLOC** et **KEYSTORELOC** ou exécutez les commandes requises. Notez que vous n'avez peut-être pas besoin de créer le certificat pour bob.

```
INSTLOC=/opt/mq75
KEYSTORELOC=/home/testusr/ssl/ams1
mkdir -p $KEYSTORELOC
chmod -R 777 $KEYSTORELOC
chown -R mqm:mqm $KEYSTORELOC
export PATH=$PATH:$INSTLOC/gskit8/bin
echo "PATH = $PATH"
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$INSTLOC/gskit8/lib64

gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd -stash
gsk8capicmd_64 -keydb -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd -stash
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/alicekey.kdb -pw passw0rd
-label alice_cert -dn "cn=alice,O=IBM,c=IN" -default_cert yes
gsk8capicmd_64 -cert -create -db $KEYSTORELOC/bobkey.kdb -pw passw0rd
-label bob_cert  -dn "cn=bob,O=IBM,c=IN"  -default_cert yes
```

2. Partagez les certificats entre les deux bases de données de clés afin que chaque utilisateur puisse identifier l'autre.

   Il est important d'utiliser la méthode décrite dans la tâche 5 de **. Partage de certificats** dans le **Guide de démarrage rapide** (Windows ou UNIX).

3. Créez `keystore.conf` avec la configuration suivante: `Keystore.conf location: /home/userID/ssl/ams1/`

```
cms.keystore = /home/userID/ssl/ams1/alicekey
cms.certificate.channel.SYSTEM.DEF.SVRCONN = alice_cert
```

4. Création et démarrage du gestionnaire de files d'attente AMSQMGR1
5. Définissez un programme d'écoute avec *port* 14567 et *contrôle* QMGR
6. Désactivez les droits d'accès au canal ou définissez les règles relatives aux droits d'accès au canal.

   Pour plus d'informations, voir SET CHLAUTH .

7. Arrêtez le gestionnaire de files d'attente.
8. Définissez le magasin de clés:

```
export MQS_KEYSTORE_CONF=/home/userID/ssl/ams1/keystore.conf
```

9. Démarrez le gestionnaire de files d'attente sur le même interpréteur de commandes.
10. Définissez la stratégie de sécurité et vérifiez:

```
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
```

    Pour plus d'informations, voir setmqspl et dspmqspl .

11. Définissez la configuration de canal:

```
export MQSERVER='SYSTEM.DEF.SVRCONN/TCP/127.0.0.1(14567)'
```

12. Exécutez **amqsputc** à partir d'un client MQ qui n'active pas automatiquement un intercepteur MCA ; par exemple, un client IBM WebSphere MQ Version 7.1 ou antérieur. Insérez les deux messages suivants:

```
/opt/mqm/samp/bin/amqsputc TESTQ TESTQMGR
```

13. Supprimez la règle de sécurité et vérifiez le résultat:

```
setmqspl -m AMSQMGR1 -p TESTQ -remove
dspmqspl -m AMSQMGR1
```

14. Parcourez la file d'attente à partir de votre installation IBM WebSphere MQ Version 7.5 :

```
/opt/mq75/samp/bin/amqsbcg TESTQ AMSQMGR1
```

La sortie de navigation affiche les messages au format chiffré.

15. Définissez la règle de sécurité et vérifiez le résultat:

```
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. Exécutez **amqsgetc** à partir de votre installation IBM WebSphere MQ Version 7.5 :

```
/opt/mqm/samp/bin/amqsgetc TESTQ TESTQMGR
```

Tâches associées

«Guide de démarrage rapide pour les clients Java», à la page 296
Utilisez ce guide pour configurer rapidement IBM Advanced Message Security afin de garantir la sécurité des messages pour les applications Java qui se connectent à l'aide de liaisons client. Lorsque vous l'aurez terminé, vous aurez créé un magasin de clés pour vérifier les identités des utilisateurs et défini des règles de signature / chiffrement pour votre gestionnaire de files d'attente.

Référence associée

«Limitations connues», à la page 284
Découvrez les limitations d' IBM WebSphere MQ Advanced Message Security.

Désactivation de IBM WebSphere MQ Advanced Message Security sur le client

Vous devez désactiver IBM WebSphere MQ Advanced Message Security (AMS) sur le client si vous utilisez un client Version 7.5 ou version ultérieure pour vous connecter à un gestionnaire de files d'attente à partir d'une version antérieure du produit et qu'une erreur 2085 (MQRC_UNKNOWN_OBJECT_NAME) est signalée.

Pourquoi et quand exécuter cette tâche

Depuis la Version 7.5, IBM WebSphere MQ Advanced Message Security (AMS) est automatiquement activé dans un client IBM WebSphere MQ . Par conséquent, par défaut, le client tente de vérifier les règles de sécurité pour les objets du gestionnaire de files d'attente. Toutefois, AMS n'est pas activé sur les serveurs des versions antérieures du produit, par exemple Version 7.1, ce qui entraîne le signalement d'une erreur 2085 (MQRC_UNKNOWN_OBJECT_NAME) .

Si cette erreur est signalée, lorsque vous tentez de vous connecter à un gestionnaire de files d'attente à partir d'une version antérieure du produit, vous pouvez désactiver AMS sur le client comme suit:

- Pour les clients Java, de l'une des façons suivantes :
  - V7.5.0.4 En définissant une variable d'environnement AMQ_DISABLE_CLIENT_AMS.
  - V7.5.0.4 En définissant la propriété système Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS.

  - V 7.5.0.5 En utilisant la propriété DisableClientAMS sous la strophe **Security** dans le fichier `mqclient.ini`.
- Pour les clients C, de l'une des façons suivantes :
  - V 7.5.0.4 En définissant une variable d'environnement AMQ_DISABLE_CLIENT_AMS.
  - V 7.5.0.5 En utilisant la propriété DisableClientAMS sous la strophe **Security** dans le fichier `mqclient.ini`.

Procédure

- Pour désactiver AMS sur le client, utilisez l'une des options suivantes:

  V 7.5.0.4 Variable d'environnement AMQ_DISABLE_CLIENT_AMS

  Vous devez définir cette variable dans les cas suivants:
  - Si vous utilisez un environnement d'exécution Java (JRE) autre que l'environnement d'exécution IBM Java (JRE)
  - Si vous utilisez Version 7.5ou une version ultérieure, le client IBM WebSphere MQ classes for Java ou IBM WebSphere MQ classes for JMS .

  Vous pouvez également utiliser AMQ_DISABLE_CLIENT_AMS pour désactiver la fonctionnalité AMS pour les clients C.

  Créez la variable d'environnement AMQ_DISABLE_CLIENT_AMS et définissez-la sur TRUE dans l'environnement où l'application s'exécute. Exemple :

  ```
  export AMQ_DISABLE_CLIENT_AMS=TRUE
  ```

  V 7.5.0.4 Propriété système com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS

  Pour les clients IBM WebSphere MQ classes for JMS et IBM WebSphere MQ classes for Java , définissez la propriété système Java com.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS sur la valeur TRUE pour l'application Java .

  Par exemple, vous pouvez définir la propriété système Java en tant qu'option `-D` lorsque la commande Java est appelée:

  ```
  java -Dcom.ibm.mq.cfg.AMQ_DISABLE_CLIENT_AMS=TRUE -cp <MQ_INSTALLATION_PATH>/java/lib/
  com.ibm.mqjms.jar  my.java.applicationClass
  ```

  Vous pouvez également spécifier la propriété système Java dans un fichier de configuration JMS , `jms.config`, si l'application utilise ce fichier.

  V 7.5.0.5 Propriété `DisableClientAMS` dans le fichier `mqclient.ini`

  Pour les clients IBM WebSphere MQ classes for JMS et IBM WebSphere MQ classes for Java et pour les clients C, ajoutez le nom de propriété `DisableClientAMS` sous la section **Security** du fichier `mqclient.ini` , comme illustré dans l'exemple suivant:

  ```
  Security:
  DisableClientAMS=Yes
  ```

  Vous pouvez également activer AMS comme illustré dans l'exemple suivant:

  ```
  Security:
  DisableClientAMS=No
  ```

Que faire ensuite

Pour plus d'informations sur les problèmes liés à l'ouverture de files d'attente protégées par AMS , voir «Problèmes d'ouverture des files d'attente protégées lors de l'utilisation de JMS», à la page 337.

Concepts associés

«Interception MCA (Message Channel Agent)», à la page 309
L'interception MCA permet à un gestionnaire de files d'attente exécuté sous IBM WebSphere MQ d'activer de manière sélective les règles à appliquer pour les canaux de connexion serveur.

Tâches associées

Configuration d'un client à l'aide d'un fichier de configuration

Référence associée

Le fichier de configuration IBM WebSphere MQ classes for JMS

Exigences de certificat pour AMS

Les certificats doivent disposer d'une clé publique RSA pour pouvoir être utilisés avec Advanced Message Security.

Pour plus d'informations sur les différents types de clé publique et pour savoir comment les créer, voir «Certificats numériques et compatibilité CipherSpec dans IBM WebSphere MQ», à la page 36.

Extensions d'utilisation de clé

Les extensions d'utilisation de clé imposent des restrictions supplémentaires sur la façon dont un certificat peut être utilisé.

Dans Advanced Message Security, l'utilisation de la clé doit être définie comme suit: pour les certificats de la norme X.509 V3 ou ultérieure qui sont utilisés pour la qualité de l'intégrité de la protection, si les extensions d'utilisation de la clé sont définies, elles doivent inclure au moins l'un des deux éléments suivants:

- **nonRepudiation**
- **digitalSignature**

Pour la qualité de la confidentialité de la protection, si les extensions d'utilisation de clé sont définies, elles doivent également inclure l'extension **keyEncipherment** .

Concepts associés

«Qualité de protection», à la page 324
Les règles de protection des données Advanced Message Security impliquent une qualité de protection (QOP).

Méthodes de validation de certificat dans IBM WebSphere MQ Advanced Message Security

Vous pouvez utiliser IBM WebSphere MQ Advanced Message Security pour détecter et rejeter les certificats révoqués afin que les messages de vos files d'attente ne soient pas protégés à l'aide de certificats qui ne répondent pas aux normes de sécurité.

IBM WebSphere MQ AMS vous permet de vérifier la validité d'un certificat à l'aide du protocole OCSP (Online Certificate Status Protocol) ou de la liste de révocation de certificat (CRL).

IBM WebSphere MQ AMS peut être configuré pour la vérification OCSP et/ou CRL. Si les deux méthodes sont activées, pour des raisons de performances, IBM WebSphere MQ AMS utilise d'abord le protocole OCSP pour le statut de révocation. Si le statut de révocation d'un certificat est indéterminé après la vérification OCSP, IBM WebSphere MQ AMS utilise la vérification CRL.

Concepts associés

«Protocole OCSP (Online Certificate Status Protocol)», à la page 314
Le protocole OCSP (Online Certificate Status Protocol) détermine si un certificat a été révoqué et, par conséquent, permet de déterminer si le certificat est digne de confiance.

«Listes de révocation de certificats (CRL)», à la page 316

Les listes CRL contiennent une liste de certificats qui ont été marqués par l'autorité de certification comme n'étant plus dignes de confiance pour diverses raisons, par exemple, la clé privée a été perdue ou compromise.

Protocole OCSP (Online Certificate Status Protocol)

Le protocole OCSP (Online Certificate Status Protocol) détermine si un certificat a été révoqué et, par conséquent, permet de déterminer si le certificat est digne de confiance.

Activation de la vérification OCSP dans des intercepteurs natifs

Pour activer la vérification OCSP (Online Certificate Status Protocol) dans Advanced Message Security, vous devez modifier le fichier de configuration du magasin de clés.

Procédure

Ajoutez les options suivantes au fichier de configuration du magasin de clés :

Remarque : Les valeurs des options individuelles fournies dans le tableau sont des valeurs par défaut.

Vous devez spécifier l'une des valeurs suivantes :

- `ocsp.enable=on`
- `ocsp.url=<`*`reposnder_URL`*`>`
- `ocsp.http.proxy.host=<`*`OCSP_proxy`*`>`

Option	Description
`ocsp.enable=off`	Activez la vérification OCSP si le certificat en cours de vérification a une extension Authority Info Access avec une méthode d'accès PKIX_AD_OCSP contenant l'identificateur URI de l'emplacement du canal répondeur OCSP. Les valeur admises sont `on`/`off`.
`ocsp.url=<`*`reposnder_URL`*`>`	Adresse URL du canal répondeur OCSP.
`ocsp.http.proxy.host=<`*`OCSP_proxy`*`>`	Adresse URL du serveur proxy OCSP.
`ocsp.http.proxy.port=<`*`port_number`*`>`	Numéro de port du serveur proxy OCSP.
`ocsp.nonce.generation=on/off`	Génère une valeur nonce lors de l'interrogation d'OCSP. La valeur par défaut est `off`.
`ocsp.nonce.check=on/off`	Vérifie la valeur nonce après la réception d'une réponse d'OCSP. La valeur par défaut est `off`.
`ocsp.nonce.size=8`	Taille de la valeur nonce en octets.
`ocsp.http.get=on/off`	Spécifie HTTP GET comme méthode d'interrogation. Si cette option est définie sur `off`, HTTP POST est utilisé.
`ocsp.max_response_size=20480`	Taille maximale de la réponse (en octets) du canal répondeur OCSP fourni.
`ocsp.cache_size=100`	Active la mise en cache de la réponse OCSP interne et définit la limite du nombre d'entrées du cache.

Option	Description
`ocsp.timeout=30`	Temps d'attente d'une réponse serveur (en secondes) après laquelle Advanced Message Security expire.

Activation de la vérification OCSP dans Java
Pour activer la restitution OCSP pour Java dans Advanced Message Security, modifiez le fichier `java.security` ou le fichier de configuration du magasin de clés.

Pourquoi et quand exécuter cette tâche

Il existe deux façons d'activer la vérification OCSP dans Advanced Message Security:

Utilisation de java.security
Vérifiez si l'accès aux informations de l'autorité (AIA) est configuré pour votre certificat.

Procédure

1. Si AIA n'est pas configuré ou si vous souhaitez remplacer votre certificat, éditez le fichier `$JAVA_HOME/lib/security/java.security` avec les propriétés suivantes:

   ```
   ocsp.responderURL=http://url.to.responder:port
   ocsp.responderCertSubjectName=CN=Example CA,O=IBM,C=US
   ```

   et activez la vérification OCSP en éditant le fichier `$JAVA_HOME/lib/security/java.security` avec la ligne suivante:

   ```
   ocsp.enable=true
   ```

2. Si AIA est configuré, activez la vérification OCSP en éditant le fichier `$JAVA_HOME/lib/security/java.security` avec la ligne suivante:

   ```
   ocsp.enable=true
   ```

Que faire ensuite

Si vous utilisez Java Security Manager, terminez également la configuration et ajoutez les droits Java suivants à `lib/security/java.policy`

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
```

Utilisation de keystore.conf

Procédure

Ajoutez l'attribut suivant au fichier de configuration:

```
ocsp.enable=true
```

Important : La définition de cet attribut dans le fichier de configuration remplace les paramètres java.security .

Que faire ensuite

Pour terminer la configuration, ajoutez les droits Java suivants à `lib/security/java.policy`:

```
permission java.security.SecurityPermission "getProperty.ocsp.enable";
permission java.security.SecurityPermission "setProperty.ocsp.enable";
```

Listes de révocation de certificats (CRL)

Les listes CRL contiennent une liste de certificats qui ont été marqués par l'autorité de certification comme n'étant plus dignes de confiance pour diverses raisons, par exemple, la clé privée a été perdue ou compromise.

Pour valider les certificats, Advanced Message Security construit une chaîne de certificats qui se compose du certificat du signataire et de la chaîne de certificats de l'autorité de certification jusqu'à un point d'ancrage digne de confiance. Un point d'ancrage digne de confiance est un fichier de clés certifiées qui contient un certificat digne de confiance ou un certificat racine digne de confiance utilisé pour vérifier la confiance d'un certificat.IBM WebSphere MQ AMS vérifie le chemin du certificat à l'aide d'un algorithme de validation PKIX. Lorsque la chaîne est créée et vérifiée, IBM WebSphere MQ AMS effectue la validation de certificat qui inclut la validation de la date d'émission et d'expiration de chaque certificat de la chaîne par rapport à la date en cours, en vérifiant si l'extension d'utilisation de clé est présente dans le certificat d'entité finale. Si l'extension est ajoutée au certificat, IBM WebSphere MQ AMS vérifie si **digitalSignature** ou **nonRepudiation** sont également définis. Si ce n'est pas le cas, le `MQRC_SECURITY_ERROR` est signalé et consigné. Ensuite, IBM WebSphere MQ AMS télécharge les listes de révocation de certificat à partir de fichiers ou de LDAP en fonction des valeurs spécifiées dans le fichier de configuration. Seules les listes de révocation de certificat codées au format DER sont prises en charge par IBM WebSphere MQ AMS. Si aucune configuration liée à la liste de révocation de certificat n'est trouvée dans le fichier de configuration du magasin de clés, IBM WebSphere MQ AMS n'effectue aucune vérification de validité de la liste de révocation de certificat. Pour chaque certificat de l'autorité de certification, IBM WebSphere MQ AMS demande à LDAP des listes de révocation de certificat à l'aide des noms distinctifs d'une autorité de certification pour trouver sa liste de révocation de certificat. Les attributs suivants sont inclus dans la requête LDAP:

```
certificateRevocationList,
certificateRevocationList;binary,
authorityRevocationList,
authorityRevocationList;binary
deltaRevocationList
deltaRevocationList;binary,
```

Remarque : `deltaRevocationList` est pris en charge uniquement lorsqu'il est spécifié en tant que points de distribution.

Activation de la prise en charge de la validation de certificat et de la liste de révocation de certificat dans les intercepteurs natifs

Vous devez modifier le fichier de configuration du magasin de clés afin que Advanced Message Security puisse télécharger des CLR à partir du serveur LDAP (Lightweight Directory Access Protocol).

Procédure

Ajoutez les options suivantes au fichier de configuration:

Remarque : Les valeurs des options individuelles fournies dans le tableau sont des valeurs par défaut.

Option	Description
`crl.ldap.host=<`*`host_name`*`>`	Nom d'hôte du serveur LDAP.

Option	Description
`crl.ldap.port=<port_number>`	Numéro de port du serveur LDAP. Vous pouvez spécifier jusqu'à 11 serveurs. Plusieurs hôtes LDAP sont utilisés pour garantir une reprise en ligne transparente en cas d'échec de la connexion LDAP. Tous les serveurs LDAP doivent être des répliques et contenir les mêmes données. Lorsque l'intercepteur Java IBM WebSphere MQ AMS parvient à se connecter à un serveur LDAP, il ne tente pas de télécharger des listes de révocation de certificat à partir des serveurs restants fournis.
`crl.cdp=off`	Utilisez cette option pour vérifier ou utiliser les extensions CRLDistributionPoints dans les certificats.
`crl.ldap.version=3`	Numéro de version du protocole LDAP. Valeurs possibles: 2 ou 3.
`crl.ldap.user=cn=<username>`	Connectez-vous au serveur LDAP. Si cette valeur n'est pas spécifiée, les attributs CRL dans LDAP doivent être lisibles par tous
`crl.ldap.pass=<password>`	Mot de passe du serveur LDAP.
`crl.ldap.cache_lifetime=0`	Durée de vie du cache LDAP en secondes. Valeurs possibles: 0 à 86400.
`crl.ldap.cache_size=50`	Taille du cache LDAP. Cette option ne peut être spécifiée que si la valeur `crl.ldap.cache_lifetime` est supérieure à `0`.
`crl.http.proxy.host=some.host.com`	Port du serveur proxy HTTP pour l'extraction de la liste de révocation de certificat CDP.
`crl.http.proxy.port=8080`	Numéro de port du serveur proxy HTTP.
`crl.http.max_response_size=204800`	Taille maximale de la CRL , en octets, qui peut être extraite d'un serveur HTTP accepté par GSKit.
`crl.http.timeout=30`	Délai d'attente d'une réponse du serveur, en secondes, après lequel le délai d'attente de IBM WebSphere MQ AMS est écoulé.
`crl.http.cache_size=0`	Taille du cache HTTP, en octets.

Activation de la prise en charge de la liste de révocation de certificat dans Java
Pour activer la prise en charge des listes de révocation de certificat dans Advanced Message Security, vous devez modifier le fichier de configuration du magasin de clés afin de permettre à IBM WebSphere MQ AMS de télécharger des listes de révocation de certificat à partir du serveur LDAP (Lightweight Directory Access Protocol) et de configurer le fichier java.security .

Procédure

1. Ajoutez les options suivantes au fichier de configuration:

En-tête	Description
`crl.ldap.host=<host_name>`	Nom d'hôte LDAP.

En-tête	Description
`crl.ldap.port=<port_number>`	Numéro de port du serveur LDAP. Vous pouvez spécifier jusqu'à 11 serveurs. Plusieurs hôtes LDAP sont utilisés pour garantir une reprise en ligne transparente en cas d'échec de la connexion LDAP. Tous les serveurs LDAP doivent être des répliques et contenir les mêmes données. Lorsque l'intercepteur Java IBM WebSphere MQ AMS parvient à se connecter à un serveur LDAP, il ne tente pas de télécharger des listes de révocation de certificat à partir des serveurs restants fournis. Java n'utilise pas les valeurs `crl.ldap.user` et crl.ldaworldp.pass . Il n'utilise pas d'utilisateur ni de mot de passe lors de la connexion à un serveur LDAP. Par conséquent, les attributs CRL dans LDAP doivent être lisibles par tous.
`crl.cdp=on/off`	Utilisez cette option pour vérifier ou utiliser les extensions CRLDistributionPoints dans les certificats.

2. Modifiez le fichier `JRE/lib/security/java.security` avec les propriétés suivantes:

Nom de la propriété	Description
`com.ibm.security.enableCRLDP`	Cette propriété prend les valeurs suivantes: `true`, `false`. Si la valeur est `true`, lors de la vérification de la révocation de certificat, les listes de révocation de certificat sont localisées à l'aide de l'URL de l'extension des points de distribution de liste de révocation de certificat du certificat. S'il est défini sur `false` ou s'il n'est pas défini, la vérification de la liste de révocation de certificat à l'aide de l'extension des points de distribution de liste de révocation de certificat est désactivée.
`ibm.security.certpath.ldap.cache.lifetime`	Cette propriété peut être utilisée pour définir la durée de vie des entrées dans le cache mémoire de CertStore LDAP sur une valeur en secondes. La valeur 0 désactive le cache ; -1 signifie une durée de vie illimitée. S'il n'est pas défini, la durée de vie par défaut est de 30 secondes.

Nom de la propriété	Description
com.ibm.security.enableAIAEXT	Cette propriété prend les valeurs suivantes: true, false. Si la valeur est true, toutes les extensions d'accès aux informations d'autorité trouvées dans les certificats du chemin de certificat en cours de génération sont examinées afin de déterminer si elles contiennent des URI LDAP. Pour chaque URI LDAP trouvé, un objet LDAPCertStore est créé et ajouté à la collection CertStores qui est utilisée pour localiser les autres certificats requis pour générer le chemin de certificat. S'il est défini sur false ou s'il n'est pas défini, des objets LDAPCertStore supplémentaires ne sont pas créés.

Protection des mots de passe dans Java

Le stockage des mots de passe de clés et de clés privées sous forme de texte en clair représente un risque pour la sécurité. Par conséquent, Advanced Message Security fournit un outil qui peut brouiller ces mots de passe à l'aide de la clé d'un utilisateur, qui est disponible dans le fichier de clés.

Avant de commencer

Le propriétaire du fichier keystore.conf doit s'assurer que seul le propriétaire du fichier est autorisé à lire le fichier. La protection par mot de passe décrite dans ce chapitre n'est qu'une mesure de protection supplémentaire.

Procédure

1. Editez les fichiers keystore.conf pour inclure le chemin d'accès au magasin de clés et le libellé des utilisateurs.

   ```
   jceks.keystore = c:/Documents and Setting/Alice/AliceKeystore
   jceks.certificate = AliceCert
   jceks.provider = IBMJCE
   ```

2. Pour exécuter l'outil, exécutez:

   ```
   java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
   private_key_password
   ```

   Une sortie avec des mots de passe chiffrés est générée et peut être copiée dans le fichier keystore.conf .

   Pour copier automatiquement la sortie dans le fichier keystore.conf , exécutez:

   ```
   java -cp com.ibm.mq.jmqi.jar com.ibm.mq.ese.config.KeyStoreConfigProtector keystore_password
   private_key_password >> ~/<path_to_keystore>/keystore.conf
   ```

   Remarque :

   Pour obtenir la liste des emplacements par défaut de keystore.conf sur différentes plateformes, voir «Utilisation de magasins de clés et de certificats», à la page 307.

Exemple

Voici un exemple de sortie de ce type:

```
#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
```

Administration des règles de sécurité IBM WebSphere MQ Advanced Message Security

IBM WebSphere MQ Advanced Message Security utilise des règles de sécurité pour spécifier les algorithmes de chiffrement cryptographique et de signature pour le chiffrement et l'authentification des messages qui transitent par les files d'attente.

Présentation des stratégies de sécurité

Les règles de sécurité IBM Advanced Message Security sont des objets conceptuels qui décrivent la façon dont un message est chiffré et signé de manière cryptographique.

Pour plus de détails sur les attributs de stratégie de sécurité, voir les sous-rubriques suivantes:

Concepts associés

«Qualité de protection», à la page 324
Les règles de protection des données Advanced Message Security impliquent une qualité de protection (QOP).

«Attributs de stratégie de sécurité», à la page 323
Vous pouvez utiliser Advanced Message Security pour sélectionner un algorithme ou une méthode spécifique afin de protéger les données.

Nom de la règle

Le nom de règle est un nom unique qui identifie une règle Advanced Message Security spécifique et la file d'attente à laquelle elle s'applique.

Le nom de la règle doit être identique au nom de la file d'attente à laquelle elle s'applique. Il existe un mappage un à un entre une règle Advanced Message Security (IBM WebSphere MQ AMS) et une file d'attente.

En créant une règle portant le même nom qu'une file d'attente, vous activez la règle pour cette file d'attente. Les files d'attente sans noms de règle correspondants ne sont pas protégées par IBM WebSphere MQ AMS.

La portée de la règle est pertinente pour le gestionnaire de files d'attente local et ses files d'attente. Les gestionnaires de files d'attente éloignées doivent disposer de leurs propres règles définies en local pour les files d'attente qu'ils gèrent.

Algorithme de signature

L'algorithme de signature indique l'algorithme qui doit être utilisé lors de la signature des messages de données.

Les valeurs valides sont les suivantes :

- MD5
- SHA-1
- SHA-2 Famille :
  - SHA256
  - SHA384 (longueur de clé minimale acceptable-768 bits)
  - SHA512 (longueur de clé minimale acceptable-768 bits)

Une règle qui ne spécifie pas d'algorithme de signature, ou qui spécifie un algorithme de NONE, implique que les messages placés dans la file d'attente associée à la règle ne sont pas signés.

Remarque : La qualité de protection utilisée pour les fonctions d'insertion et d'obtention de message doit correspondre. S'il existe une non-concordance de la qualité de protection de la règle entre la file d'attente et le message dans la file d'attente, le message n'est pas accepté et est envoyé à la file d'attente de traitement des erreurs. Cette règle s'applique aux files d'attente locales et éloignées.

Algorithme de chiffrement

L'algorithme de chiffrement indique l'algorithme qui doit être utilisé lors du chiffrement des messages de données placés dans la file d'attente associée à la règle.

Les valeurs valides sont les suivantes :

- RC2
- DES
- 3DES
- AES128
- AES256

Une règle qui ne spécifie pas d'algorithme de chiffrement ou qui spécifie un algorithme de NONE implique que les messages placés dans la file d'attente associée à la règle ne sont pas chiffrés.

Notez qu'une règle qui spécifie un algorithme de chiffrement autre que NONE doit également spécifier au moins un nom distinctif de destinataire et un algorithme de signature car les messages chiffrés Advanced Message Security sont également signés.

Important : La qualité de protection utilisée pour les fonctions d'insertion et d'obtention de message doit correspondre. S'il existe une non-concordance de la qualité de protection de la règle entre la file d'attente et le message dans la file d'attente, le message n'est pas accepté et est envoyé à la file d'attente de traitement des erreurs. Cette règle s'applique aux files d'attente locales et éloignées.

Tolérance

L'attribut toleration indique si IBM Advanced Message Security peut accepter des messages sans règle de sécurité spécifiée.

Lors de l'extraction d'un message d'une file d'attente avec une règle de chiffrement des messages, si le message n'est pas chiffré, il est renvoyé à l'application appelante. Les valeurs valides sont les suivantes :

0
Non (**par défaut**).

1
Oui.

Une règle qui ne spécifie pas de valeur de tolérance ou qui indique 0 implique que les messages placés dans la file d'attente associée à la règle doivent correspondre aux règles de la règle.

La tolérance est facultative et existe pour faciliter le déploiement de la configuration, où les règles ont été appliquées aux files d'attente, mais ces dernières contiennent déjà des messages pour lesquels aucune règle de sécurité n'est spécifiée.

Noms distinctifs des expéditeurs

Les noms distinctifs d'expéditeur identifient les utilisateurs autorisés à placer des messages dans une file d'attente.

IBM Advanced Message Security (IBM WebSphere MQ AMS) ne vérifie pas si un message a été placé dans une file d'attente protégée par des données par un utilisateur valide tant que le message n'a pas été extrait. A ce stade, si la règle indique un ou plusieurs expéditeurs valides et que l'utilisateur qui a placé le message dans la file d'attente ne figure pas dans la liste des expéditeurs valides, IBM WebSphere MQ AMS renvoie une erreur à l'application d'extraction et place le message dans sa file d'attente des erreurs.

Une règle peut avoir zéro ou plusieurs noms distinctifs d'expéditeurs spécifiés. Si aucun nom distinctif d'expéditeur n'est spécifié pour la règle, tous les utilisateurs peuvent placer des messages de protection des données dans la file d'attente, à condition que le certificat de l'utilisateur soit sécurisé.

Les noms distinctifs des expéditeurs se présentent sous la forme suivante :

```
CN=Common Name,O=Organization,C=Country
```

Important :

- Tous les noms distinctifs doivent être en majuscules. Tous les identificateurs de nom de composant du nom distinctif doivent être indiqués dans l'ordre indiqué dans le tableau suivant:

Nom de composant	Valeur
CN	Nom usuel de l'objet de ce nom distinctif, tel qu'un nom complet ou la finalité prévue d'un périphérique.
OU	Unité au sein de l'organisation à laquelle l'objet du nom distinctif est affilié, telle qu'une division d'entreprise ou un nom de produit.
O	Organisation à laquelle l'objet du nom distinctif est affilié, telle qu'une société.
L	La localité (ville ou municipalité) où se trouve l'objet du nom distinctif.
ST	Nom de l'état ou de la province où se trouve l'objet du nom distinctif.
C	Pays dans lequel se trouve l'objet du nom distinctif (DN).

- Si un ou plusieurs noms distinctifs d'expéditeur sont spécifiés pour la règle, seuls ces utilisateurs peuvent placer des messages dans la file d'attente associée à la règle.
- Les noms distinctifs d'expéditeur, lorsqu'ils sont spécifiés, doivent correspondre exactement aux noms distinctifs contenus dans le certificat numérique associé à l'utilisateur plaçant le message.
- IBM WebSphere MQ AMS prend en charge les noms distinctifs dont les valeurs proviennent uniquement du jeu de caractères Latin-1 . Pour créer des noms distinctifs avec des caractères de l'ensemble, vous devez d'abord créer un certificat avec un nom distinctif créé en UTF-8 à l'aide des plateformes UNIX avec le codage UTF-8 activé ou avec l'utilitaire iKeyman . Vous devez ensuite créer une règle à partir d'une plateforme UNIX avec le codage UTF-8 activé ou utiliser le plug-in IBM WebSphere MQ AMS dans WebSphere MQ.

Concepts associés

«Noms distinctifs des destinataires», à la page 322
Les noms distinctifs des destinataires identifient les utilisateurs qui sont autorisés à extraire des messages d'une file d'attente.

Noms distinctifs des destinataires

Les noms distinctifs des destinataires identifient les utilisateurs qui sont autorisés à extraire des messages d'une file d'attente.

Une règle peut avoir zéro ou plusieurs noms distinctifs de destinataires spécifiés. Les noms distinctifs des destinataires se présentent sous la forme suivante:

```
CN=Common Name,O=Organization,C=Country
```

Important :

- Tous les noms distinctifs doivent être en majuscules. Tous les identificateurs de nom de composant du nom distinctif doivent être indiqués dans l'ordre indiqué dans le tableau suivant:

Nom de composant	Valeur
CN	Nom usuel de l'objet de ce nom distinctif, tel qu'un nom complet ou la finalité prévue d'un périphérique.
OU	Unité au sein de l'organisation à laquelle l'objet du nom distinctif est affilié, telle qu'une division d'entreprise ou un nom de produit.
O	Organisation à laquelle l'objet du nom distinctif est affilié, telle qu'une société.
L	La localité (ville ou municipalité) où se trouve l'objet du nom distinctif.
ST	Nom de l'état ou de la province où se trouve l'objet du nom distinctif.
C	Pays dans lequel se trouve l'objet du nom distinctif (DN).

- Si aucun nom distinctif de destinataire n'est spécifié pour la règle, tous les utilisateurs peuvent récupérer des messages de la file d'attente associée aux règles.
- Si un ou plusieurs noms distinctifs de destinataire est (sont) spécifié(s) pour la règle, seuls ces utilisateurs peuvent récupérer des messages de la file d'attente associée aux règles.
- Les noms distinctifs de destinataire, lorsqu'ils sont spécifiés, doivent correspondre exactement au nom distinctif contenu dans le certificat numérique associé à l'utilisateur récupérant le message.
- Advanced Message Security prend en charge les noms distinctifs dont les valeurs proviennent uniquement du jeu de caractères Latin-1 . Pour créer des noms distinctifs avec des caractères de l'ensemble, vous devez d'abord créer un certificat avec un nom distinctif créé en UTF-8 à l'aide des plateformes UNIX avec le codage UTF-8 activé ou avec l'utilitaire iKeyman . Vous devez ensuite créer une règle à partir d'une plateforme UNIX avec le codage UTF-8 activé ou utiliser le plug-in Advanced Message Security dans WebSphere MQ.

Concepts associés

«Noms distinctifs des expéditeurs», à la page 321
Les noms distinctifs d'expéditeur identifient les utilisateurs autorisés à placer des messages dans une file d'attente.

Attributs de stratégie de sécurité

Vous pouvez utiliser Advanced Message Security pour sélectionner un algorithme ou une méthode spécifique afin de protéger les données.

Une règle de sécurité est un objet conceptuel qui décrit la façon dont un message est chiffré et signé de manière cryptographique. Le tableau suivant présente les attributs de stratégie de sécurité dans Advanced Message Security:

Attribut	Description
Nom de la règle	Nom unique de la règle d'un gestionnaire de files d'attente.
Algorithme de signature	Algorithme de cryptographie utilisé pour signer les messages avant l'envoi.
Algorithme de chiffrement	Algorithme de cryptographie utilisé pour chiffrer les messages avant leur envoi.
Liste des destinataires	Liste des noms distinctifs (DN) de certificats des destinataires potentiels d'un message.

Attribut	Description
Liste de contrôle Nom distinctif de signature	Liste des noms distinctifs de signature à valider lors de l'extraction de message.

Dans Advanced Message Security, les messages sont chiffrés avec une clé symétrique et la clé symétrique est chiffrée avec les clés publiques des destinataires. Les clés publiques sont chiffrées avec l'algorithme RSA, avec des clés d'une longueur effective jusqu'à 2048 bits. Le chiffrement de la clé asymétrique dépend de la longueur de la clé de certificat.

Les algorithmes de clé symétrique pris en charge sont les suivants:

- RC2
- DES
- 3DES
- AES128
- AES256

Advanced Message Security prend également en charge les fonctions de hachage cryptographique suivantes:

- MD5
- SHA-1
- SHA-2 Famille :
  - SHA256
  - SHA384 (longueur de clé minimale acceptable-768 bits)
  - SHA512 (longueur de clé minimale acceptable-768 bits)

Remarque : La qualité de protection utilisée pour les fonctions d'insertion et d'obtention de message doit correspondre. S'il existe une non-concordance de la qualité de protection de la règle entre la file d'attente et le message dans la file d'attente, le message n'est pas accepté et est envoyé à la file d'attente de traitement des erreurs. Cette règle s'applique aux files d'attente locales et éloignées.

Qualité de protection

Les règles de protection des données Advanced Message Security impliquent une qualité de protection (QOP).

Les trois niveaux de qualité de protection dans Advanced Message Security dépendent des algorithmes de cryptographie utilisés pour signer et chiffrer le message:

- Les messages de confidentialité placés dans la file d'attente doivent être signés et chiffrés.
- Intégrité-Les messages placés dans la file d'attente doivent être signés par l'expéditeur.
- Aucune-aucune protection des données n'est applicable.

Une règle qui stipule que les messages doivent être signés lorsqu'ils sont placés dans une file d'attente possède un QOP INTEGRITY. Une QOP d'INTEGRITY signifie qu'une règle stipule un algorithme de signature, mais pas un algorithme de chiffrement. Les messages protégés contre l'intégrité sont également appelés "SIGNED".

Une règle qui stipule que les messages doivent être signés et chiffrés lorsqu'ils sont placés dans une file d'attente a un QOP de type PRIVACY. Une QOP de PRIVACY signifie que lorsqu'une règle stipule un algorithme de signature et un algorithme de chiffrement. Les messages protégés par la protection de la vie privée sont également appelés "SCELLÉS".

Une règle qui ne stipule pas d'algorithme de signature ou de chiffrement a un QOP de NONE. Advanced Message Security ne fournit aucune protection des données pour les files d'attente ayant une règle avec un QOP de NONE.

Gestion des politiques de sécurité

Une règle de sécurité est un objet conceptuel qui décrit la façon dont un message est chiffré et signé de manière cryptographique.

Toutes les tâches d'administration liées aux règles de sécurité sont exécutées à partir de l'emplacement suivant:

- Sur les plateformes UNIX : `<MQInstallRoot>/bin`
- Sur les plateformes Windows , les tâches d'administration peuvent être exécutées à partir de n'importe quel emplacement car la variable d'environnement PATH est mise à jour lors de l'installation.

Tâches associées

«Création de règles de sécurité», à la page 325
Les stratégies de sécurité définissent la façon dont un message est protégé lorsque le message est inséré, ou la façon dont un message doit avoir été protégé lorsqu'un message est reçu.

«Modification des règles de sécurité», à la page 326
Vous pouvez utiliser Advanced Message Security pour modifier les détails des règles de sécurité que vous avez déjà définies.

«Affichage et vidage des règles de sécurité», à la page 326
La commande `dspmqspl` permet d'afficher la liste de toutes les règles de sécurité ou les détails d'une règle nommée en fonction des paramètres de ligne de commande que vous indiquez.

«Suppression des règles de sécurité», à la page 328
Pour supprimer des règles de sécurité dans Advanced Message Security, vous devez utiliser la commande `setmqspl` .

Création de règles de sécurité

Les stratégies de sécurité définissent la façon dont un message est protégé lorsque le message est inséré, ou la façon dont un message doit avoir été protégé lorsqu'un message est reçu.

Avant de commencer

Certaines conditions d'entrée doivent être remplies lors de la création de règles de sécurité:

- Il doit être en cours d'exécution.
- Le nom d'une règle de sécurité doit respecter les règles de dénomination des objets WebSphere MQ.
- Vous devez disposer des droits `+connect +inq +chg` nécessaires pour créer une règle de sécurité. Pour obtenir la syntaxe complète de la commande de changement d'autorisation, voir **`setmqaut`** .
- Vérifiez que vous disposez des droits nécessaires pour effectuer des opérations sur les files d'attente et les gestionnaires de files d'attente WebSphere MQ . Pour plus d'informations, voir «Octroi de droits OAM», à la page 329

Exemple

Voici un exemple de création d'une règle sur le gestionnaire de files d'attente `QMGR`. La règle spécifie que les messages doivent être signés à l'aide de l'algorithme `SHA1` et chiffrés à l'aide de l'algorithme `AES256` pour les certificats avec le nom distinctif: `CN=joe, O=IBM, C=US` et DN: `CN=jane, O=IBM, C = US`. Cette règle est associée à `MY.QUEUE`:

```
$ setmqspl -m QMGR -p MY.QUEUE -s SHA1 -e AES256 -r CN=joe,O=IBM,C=US -r CN=jane,O=IBM,C=US
```

Voici un exemple de création de règles sur le gestionnaire de files d'attente `QMGR`. La règle indique que les messages doivent être chiffrés à l'aide de l'algorithme `DES` pour les certificats avec DN: `CN=john, O=IBM, C=US` et `CN=jeff, O=IBM, C=US` et signés avec l'algorithme `MD5` pour les certificats avec DN: `CN=phil, O=IBM, C=US`

```
$ setmqspl -m QMGR -p MY.OTHER.QUEUE -s MD5 -e DES -r CN=john,O=IBM,C=US -r CN=jeff,O=IBM,C=US
-a CN=phil,O=IBM,C=US
```

Remarque :

- La qualité de la protection utilisée pour l'insertion et l'extraction de message doit correspondre. Si la qualité de protection de la règle définie pour le message est plus faible que celle définie pour une file d'attente, le message est envoyé à la file d'attente de traitement des erreurs. Cette règle est valide pour les files d'attente locales et éloignées.

Référence associée

Liste complète des attributs de la commande setmqspl

Modification des règles de sécurité

Vous pouvez utiliser Advanced Message Security pour modifier les détails des règles de sécurité que vous avez déjà définies.

Avant de commencer

- Le gestionnaire de files d'attente sur lequel vous souhaitez travailler doit être en cours d'exécution.
- Vous devez disposer des droits `+connect +inq +chg` nécessaires pour créer des règles de sécurité. Pour obtenir la syntaxe complète de la commande de changement d'autorisation, voir **`setmqaut`** .

Pourquoi et quand exécuter cette tâche

Pour modifier les règles de sécurité, appliquez la commande `setmqspl` à une règle existante fournissant de nouveaux attributs.

Exemple

Voici un exemple de création d'une règle nommée MYQUEUE sur un gestionnaire de files d'attente nommé QMGR spécifiant que les messages seront chiffrés à l'aide de l'algorithme RC2 pour les certificats avec DN:CN=bob, O=IBM, C=US et signés avec l'algorithme SHA1 pour les certificats avec DN:CN=jeff, O=IBM, C = US.

```
setmqspl -m QMGR -p MYQUEUE -e RC2 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Pour modifier cette règle, exécutez la commande `setmqspl` avec tous les attributs de l'exemple en modifiant uniquement les valeurs que vous souhaitez modifier. Dans cet exemple, la règle créée précédemment est associée à une nouvelle file d'attente et son algorithme de chiffrement est remplacé par AES256:

```
setmqspl -m QMGR -p MYQUEUE -e AES256 -s SHA1 -a CN=jeff,O=IBM,C=US -r CN=alice,O=IBM,C=US
```

Référence associée

setmqspl

Affichage et vidage des règles de sécurité

La commande `dspmqspl` permet d'afficher la liste de toutes les règles de sécurité ou les détails d'une règle nommée en fonction des paramètres de ligne de commande que vous indiquez.

Avant de commencer

- Pour afficher les détails des règles de sécurité, le gestionnaire de files d'attente doit exister et être en cours d'exécution.
- Vous devez disposer des droits `+connect +inq +dsp` nécessaires appliqués à un gestionnaire de files d'attente pour afficher et vider les règles de sécurité. Pour obtenir la syntaxe complète de la commande de changement d'autorisation, voir **`setmqaut`** .

Pourquoi et quand exécuter cette tâche

Voici la liste des indicateurs de commande `dspmqspl` :

Tableau 27. Indicateurs de commande dspmqspl .	
Indicateur de commande	**Explication**
-m	Nom du gestionnaire de files d'attente (**obligatoire**).
-p	Nom de la règle.
-export	L'ajout de cet indicateur génère une sortie qui peut facilement être appliquée à un autre gestionnaire de files d'attente.

Exemple

Dans cet exemple, nous allons créer deux règles de sécurité pour venus.queue.manager:

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE
setmqspl -m venus.queue.manager -p AMS_POL_06_THREE -s MD5 -a "CN=another signer,O=IBM,C=US" -e
NONE
```

Cet exemple illustre une commande qui affiche les détails de toutes les règles définies pour venus.queue.manager et la sortie qu'elle génère:

```
dspmqspl -m  venus.queue.manager

Policy Details:
Policy name: AMS_POL_04_ONE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=signer1,O=IBM,C=US
Recipient DNs: -
Toleration: 0
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

Cet exemple illustre une commande qui affiche les détails d'une règle de sécurité sélectionnée définie pour venus.queue.manager et la sortie qu'elle génère:

```
dspmqspl -m venus.queue.manager -p AMS_POL_06_THREE

Policy Details:
Policy name: AMS_POL_06_THREE
Quality of protection: INTEGRITY
Signature algorithm: MD5
Encryption algorithm: NONE
Signer DNs:
  CN=another signer,O=IBM,C=US
Recipient DNs: -
Toleration: 0
```

Dans l'exemple suivant, nous créons d'abord une règle de sécurité, puis nous exportons la règle à l'aide de l'indicateur -export :

```
setmqspl -m venus.queue.manager -p AMS_POL_04_ONE -s MD5 -a "CN=signer1,O=IBM,C=US" -e NONE

dspmqspl -m venus.queue.manager -export > policies.[bat|sh]
```

Pour importer une règle de sécurité:

- Sur les plateformes Windows , exécutez policies.bat

- Sur les plateformes UNIX :
  1. Connectez-vous en tant qu'utilisateur appartenant au groupe d'administration `mqm` WebSphere MQ .
  2. Exécutez `. policies.sh`.

Référence associée
Liste complète des attributs de la commande dspmqspl

Suppression des règles de sécurité
Pour supprimer des règles de sécurité dans Advanced Message Security, vous devez utiliser la commande `setmqspl` .

Avant de commencer
Certaines conditions d'entrée doivent être remplies lors de la gestion des règles de sécurité:

- Il doit être en cours d'exécution.
- Vous devez disposer des droits `+connect +inq +chg` nécessaires pour créer des règles de sécurité. Pour obtenir la syntaxe complète de la commande de changement d'autorisation, voir **`setmqaut`** .

Pourquoi et quand exécuter cette tâche
Utilisez la commande `setmqspl` avec l'option `-remove` .

Exemple

Voici un exemple de suppression d'une règle:

```
$ setmqspl -m QMGR -remove -p MY.OTHER.QUEUE
```

Référence associée
Liste complète des attributs de la commande setmqspl

Protection des files d'attente système

Les files d'attente système permettent la communication entre WebSphere MQ et ses applications auxiliaires. Chaque fois qu'un gestionnaire de files d'attente est créé, une file d'attente système est également créée pour stocker les messages et les données internes WebSphere MQ . Vous pouvez protéger les files d'attente système avec Advanced Message Security afin que seuls les utilisateurs autorisés puissent y accéder ou les déchiffrer.

La protection des files d'attente système suit le même modèle que la protection des files d'attente standard. Voir «Création de règles de sécurité», à la page 325.

Pour utiliser la protection des files d'attente système sur les plateformes Windows , copiez le fichier `keystore.conf` dans le répertoire suivant:

```
c:\Documents and Settings\Default User\.mqs\keystore.conf
```

Pour protéger `SYSTEM.ADMIN.COMMAND.QUEUE`, le serveur de commandes doit avoir accès à `keystore` et à `keystore.conf`, qui contiennent des clés et une configuration permettant au serveur de commandes d'accéder aux clés et aux certificats. Toutes les modifications apportées à la règle de sécurité de `SYSTEM.ADMIN.COMMAND.QUEUE` nécessitent le redémarrage du serveur de commandes.

Tous les messages envoyés et reçus à partir de la file d'attente de commandes sont signés ou signés et chiffrés en fonction des paramètres de règle. Si un administrateur définit des signataires autorisés, les messages de commande qui ne passent pas la vérification du nom distinctif (DN) du signataire ne sont pas exécutés par le serveur de commandes et ne sont pas acheminés vers la file d'attente de traitement des erreurs Advanced Message Security . Les messages envoyés en tant que réponses à des files d'attente dynamiques temporaires WebSphere MQ Explorer ne sont pas protégés par WebSphere MQ AMS.

Les modifications apportées aux règles de sécurité Advanced Message Security nécessitent le redémarrage du serveur de commandes WebSphere MQ

Les règles de sécurité n'ont pas d'effet sur les files d'attente SYSTEM suivantes:

- SYSTEM.ADMIN.ACCOUNTING.QUEUE
- SYSTEM.ADMIN.ACTIVITY.QUEUE
- SYSTEM.ADMIN.CHANNEL.EVENT
- SYSTEM.ADMIN.COMMAND.EVENT
- SYSTEM.ADMIN.CONFIG.EVENT
- SYSTEM.ADMIN.LOGGER.EVENT
- SYSTEM.ADMIN.PERFM.EVENT
- SYSTEM.ADMIN.PUBSUB.EVENT
- SYSTEM.ADMIN.QMGR.EVENT
- SYSTEM.ADMIN.STATISTICS.QUEUE
- SYSTEM.ADMIN.TRACE.ROUTE.QUEUE
- SYSTEM.AUTH.DATA.QUEUE
- SYSTEM.BROKER.ADMIN.STREAM
- SYSTEM.BROKER.CONTROL.QUEUE
- SYSTEM.BROKER.DEFAULT.STREAM
- SYSTEM.BROKER.INTER.BROKER.COMMUNICATIONS
- SYSTEM.CHANNEL.INITQ
- SYSTEM.CHANNEL.SYNCQ
- SYSTEM.CICS.INITIATION.QUEUE
- SYSTEM.CLUSTER.COMMAND.QUEUE
- SYSTEM.CLUSTER.HISTORY.QUEUE
- SYSTEM.CLUSTER.REPOSITORY.QUEUE
- SYSTEM.CLUSTER.TRANSMIT.QUEUE
- SYSTEM.DEAD.LETTER.QUEUE
- SYSTEM.DURABLE.SUBSCRIBER.QUEUE
- SYSTEM.HIERARCHY.STATE
- SYSTEM.INTER.QMGR.CONTROL
- SYSTEM.INTER.QMGR.FANREQ
- SYSTEM.INTER.QMGR.PUBS
- SYSTEM.INTERNAL.REPLY.QUEUE
- SYSTEM.PENDING.DATA.QUEUE
- SYSTEM.PROTECTION.ERROR.QUEUE
- SYSTEM.PROTECTION.POLICY.QUEUE
- SYSTEM.RETAINED.PUB.QUEUE
- SYSTEM.SELECTION.EVALUATION.QUEUE
- SYSTEM.SELECTION.VALIDATION.QUEUE

Octroi de droits OAM

Les droits d'accès aux fichiers autorisent tous les utilisateurs à exécuter les commandes `setmqspl` et `dspmqspl` . Toutefois, IBM Advanced Message Security s'appuie sur le gestionnaire des droits d'accès aux objets (OAM) et chaque tentative d'exécution de ces commandes par un utilisateur qui n'appartient

pas au groupe mqm, qui est le groupe d'administration WebSphere MQ , ou qui ne dispose pas des droits permettant de lire les paramètres de règles de sécurité accordés, génère une erreur.

Procédure

Pour accorder les droits nécessaires à un utilisateur, exécutez:

```
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
```

Evénements de commande et de configuration

Avec Advanced Message Security, vous pouvez générer des messages d'événement de commande et de configuration, qui peuvent être consignés et servir d'enregistrement des changements de règles à des fins d'audit.

Les événements de commande et de configuration générés par WebSphere MQ sont des messages au format PCF envoyés aux files d'attente dédiées.

Les messages d'événements de configuration sont envoyés à SYSTEM.ADMIN.CONFIG.EVENT EVENT sur le gestionnaire de files d'attente où l'événement se produit.

Les messages d'événements de commande sont envoyés à SYSTEM.ADMIN.COMMAND.EVENT EVENT sur le gestionnaire de files d'attente où l'événement se produit.

Les événements sont générés quels que soient les outils que vous utilisez pour gérer les règles de sécurité Advanced Message Security .

Dans Advanced Message Security, il existe quatre types d'événements générés par différentes actions sur les règles de sécurité:

- «Création de règles de sécurité», à la page 325, qui génère deux messages d'événement WebSphere MQ :
  - Un événement de configuration
  - Un événement de commande
- «Modification des règles de sécurité», à la page 326, qui génère trois messages d'événement WebSphere MQ :
  - Evénement de configuration contenant d'anciennes valeurs de règles de sécurité
  - Evénement de configuration contenant de nouvelles valeurs de règle de sécurité
  - Un événement de commande
- «Affichage et vidage des règles de sécurité», à la page 326, qui génère un message d'événement WebSphere MQ :
  - Un événement de commande
- «Suppression des règles de sécurité», à la page 328, qui génère deux messages d'événement WebSphere MQ :
  - Un événement de configuration
  - Un événement de commande

Activation et désactivation de la journalisation des événements

Vous pouvez contrôler les événements de commande et de configuration à l'aide des attributs de gestionnaire de files d'attente CONFIGEV et CMDEV. Pour activer ces événements, définissez l'attribut de gestionnaire de files d'attente approprié sur ENABLED. Pour désactiver ces événements, définissez l'attribut de gestionnaire de files d'attente approprié sur DISABLED.

Procédure

Evénements de configuration

Pour activer les événements de configuration, définissez CONFIGEV sur ENABLED. Pour désactiver les événements de configuration, définissez CONFIGEV sur DISABLED. Par exemple, vous pouvez activer des événements de configuration à l'aide de la commande MQSC suivante:

```
ALTER QMGR CONFIGEV (ENABLED)
```

Evénements Commande

Pour activer les événements de commande, définissez CMDEV sur ENABLED. Pour activer les événements de commande pour les commandes, à l'exception des commandes DISPLAY MQSC et Inquire PCF, définissez CMDEV sur NODISPLAY. Pour désactiver les événements de commande, définissez CMDEV sur DISABLED. Par exemple, vous pouvez activer des événements de commande à l'aide de la commande MQSC suivante:

```
ALTER QMGR CMDEV (ENABLED)
```

Tâches associées

Contrôle des événements de configuration, de commande et de consignateur dans Websphere MQ

Format de message d'événement de commande

Le message d'événement de commande se compose de la structure MQCFH et des paramètres PCF qui la suivent.

Voici les valeurs MQCFH sélectionnées:

```
Type = MQCFT_EVENT;
Command = MQCMD_COMMAND_EVENT;
MsgSeqNumber = 1;
Control = MQCFC_LAST;
ParameterCount = 2;
CompCode = MQCC_WARNING;
Reason = MQRC_COMMAND_PCF;
```

Remarque : La valeur de ParameterCount est deux car il existe toujours deux paramètres de type MQCFGR (groupe). Chaque groupe est constitué de paramètres appropriés. Les données d'événement se composent de deux groupes, CommandContext et CommandData.

CommandContext contient:

EventUserID

Description :	ID utilisateur qui a émis la commande ou l'appel qui a généré l'événement. (Il s'agit du même ID utilisateur que celui utilisé pour vérifier les droits d'émission de la commande ou de l'appel ; pour les commandes reçues d'une file d'attente, il s'agit également de l'ID utilisateur (UserIdentifier) du MD du message de commande).
Identificateur :	MQCACF_EVENT_USER_ID.
Type de données :	MQCFST.
Longueur maximale :	MQ_USER_ID_LENGTH.
Renvoyé:	Toujours.

EventOrigin

Description :	Origine de l'action à l'origine de l'événement.
Identificateur :	MQIACF_EVENT_ORIGIN.

Type de données : MQCFIN.

Valeurs :

MQEVO_CONSOLE
Ligne de commande de la console.

MSG MQEVO_MQ
Message de commande du plug-in WebSphere MQ Explorer.

Renvoyé: Toujours.

EventQMgr

Description : Gestionnaire de files d'attente dans lequel la commande ou l'appel a été entré. (Le gestionnaire de files d'attente dans lequel la commande est exécutée et qui génère l'événement se trouve dans le descripteur du message d'événement).

Identificateur : MQCACF_EVENT_Q_MGR.

Type de données : MQCFST.

Longueur maximale : MQ_Q_MGR_NAME_LENGTH.

Renvoyé: Toujours.

EventAccountingToken

Description : Pour les commandes reçues sous forme de message (MQEVO_MSG), jeton de comptabilité (AccountingToken) provenant du descripteur de message de commande.

Identificateur : MQBACF_EVENT_ACCOUNTING_TOKEN.

Type de données : MQCFBS.

Longueur maximale : MQ_ACCOUNTING_TOKEN_LENGTH.

Renvoyé: Uniquement si EventOrigin est MQEVO_MSG.

EventIdentityData

Description : Pour les commandes reçues sous forme de message (MQEVO_MSG), données d'identité d'application (donnéesApplIdentity) provenant du descripteur de message de commande.

Identificateur : MQCACF_EVENT_APPL_IDENTITY.

Type de données : MQCFST.

Longueur maximale : MQ_APPL_IDENTITY_DATA_LENGTH.

Renvoyé: Uniquement si EventOrigin est MQEVO_MSG.

EventApplType

Description : Pour les commandes reçues sous forme de message (MQEVO_MSG), type d'application (PutApplType) à partir du descripteur de message du message de commande.

Identificateur : MQIACF_EVENT_APPL_TYPE.

Type de données : MQCFIN.

Renvoyé: Uniquement si EventOrigin est MQEVO_MSG.

EventApplName

Description :	Pour les commandes reçues sous forme de message (MQEVO_MSG), nom de l'application (nomPutAppl) à partir du descripteur de message du message de commande.
Identificateur :	MQCACF_EVENT_APPL_NAME.
Type de données :	MQCFST.
Longueur maximale :	MQ_APPL_NAME_LENGTH.
Renvoyé:	Uniquement si EventOrigin est MQEVO_MSG.

EventApplOrigin

Description :	Pour les commandes reçues sous forme de message (MQEVO_MSG), les données d'origine de l'application (donnéesApplOrigin) provenant du descripteur de message de commande.
Identificateur :	MQCACF_EVENT_APPL_ORIGIN.
Type de données :	MQCFST.
Longueur maximale :	MQ_APPL_ORIGIN_DATA_LENGTH.
Renvoyé:	Uniquement si EventOrigin est MQEVO_MSG.

Command

Description :	Code de la commande.
Identificateur :	MQIACF_COMMAND.
Type de données :	MQCFIN.
Valeurs :	**Valeur numérique MQCMD_INQUIRE_PROT_POLICY 205** **Valeur numérique 206 de MQCMD_CREATE_PROT_POLICY** **Valeur numérique 207 de MQCMD_DELETE_PROT_POLICY** **Valeur numérique 208 de MQCMD_CHANGE_PROT_POLICY** Ils sont définis dans WebSphere MQ 7.5 `cmqcfc.h`
Renvoyé:	Toujours.

CommandData contient des éléments PCF qui composent la commande PCF.

Format de message d'événement de configuration

Les événements de configuration sont des messages PCF au format Advanced Message Security standard.

Pour connaître les valeurs possibles pour le descripteur de message MQMD, voir Message d'événement MQMD (descripteur de message).

Voici les valeurs MQMD sélectionnées:

```
Format = MQFMT_EVENT
Peristence = MQPER_PERSISTENCE_AS_Q_DEF
PutApplType = MQAT_QMGR                      //for both CLI and command server
```

La mémoire tampon de messages est constituée de la structure MQCFH et de la structure de paramètres qui la suit. Pour connaître les valeurs MQCFH possibles, voir Message d'événement MQCFH (en-tête PCF).

Voici les valeurs MQCFH sélectionnées:

```
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}
```

Les paramètres suivants de MQCFH sont:

EventUserID

Description : ID utilisateur qui a émis la commande ou l'appel qui a généré l'événement. (Il s'agit du même ID utilisateur que celui utilisé pour vérifier les droits d'émission de la commande ou de l'appel ; pour les commandes reçues d'une file d'attente, il s'agit également de l'ID utilisateur (UserIdentifier) du MD du message de commande).

Identificateur : **MQCACF_EVENT_USER_ID**

Type de données : MQCFST.

Longueur maximale : MQ_USER_ID_LENGTH.

Renvoyé: Toujours.

SecurityId

Description : Valeur de MQMD.AccountingToken dans le cas d'un message du serveur de commandes ou Windows SID pour la commande locale.

Identificateur : **ID_SÉCURITÉ_ÉVÉNEMENT_MQBACF**

Type de données : MQCBS.

Longueur maximale : MQ_SECURITY_ID_LENGTH.

Renvoyé: Toujours.

EventOrigin

Description : Origine de l'action à l'origine de l'événement.

Identificateur : **MQIACF_EVENT_ORIGIN**

Type de données : MQCFIN.

Valeurs :

MQEVO_CONSOLE
Ligne de commande de la console.

MSG MQEVO_MQ
Message de commande du plug-in WebSphere MQ Explorer.

Renvoyé: Toujours.

EventQMgr

Description : Gestionnaire de files d'attente dans lequel la commande ou l'appel a été entré. (Le gestionnaire de files d'attente dans lequel la commande est exécutée et qui génère l'événement se trouve dans le descripteur du message d'événement).

Identificateur : **MQCACF_EVENT_Q_MGR**

Type de données : MQCFST

Longueur maximale : MQ_Q_MGR_NAME_LENGTH

Renvoyé: Toujours.

ObjectType

Description : Type d'objet.

Identificateur : **MQIACF_OBJECT_TYPE**

Type de données : MQCFIN

Valeur : **POLITIQUE MQOT_PROT_DE**
Règle de protection Advanced Message Security . **1019** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Renvoyé: Toujours.

PolicyName

Description : Nom de la règle Advanced Message Security .

Identificateur : **MQCA_POLICY_NAME**.

Type de données : MQCFST.

Valeur : **2112** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Longueur maximale : MQ_OBJECT_NAME_LENGTH.

Renvoyé: Toujours.

PolicyVersion

Description : Version de la règle Advanced Message Security .

Identificateur : **MQIA_POLICY_VERSION**

Type de données : MQCFIN

Valeur **238** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Renvoyé: Toujours

TolerateFlag

Description : Indicateur de tolérance de la règle Advanced Message Security .

Identificateur : **MQIA_TOLERATE_NON protégé**

Type de données : MQCFIN

Valeur **235** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Renvoyé: Toujours.

SignatureAlgorithm

Description : Algorithme de signature de règle Advanced Message Security .

Identificateur : **Algorithme de signature (MQIA_SIGNATURE_ALGORITHM)**

Type de données : MQCFIN

Valeur : **236** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Renvoyé: Chaque fois qu'un algorithme de signature est défini dans la règle Advanced Message Security

EncryptionAlgorithm

Description : Algorithme de chiffrement de la règle Advanced Message Security .

Identificateur : **Algorithme de chiffrement MQIA_ENCRYPTION_ALGORITHM**

Type de données : MQCFIN

Valeur : **237** -valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Renvoyé: Chaque fois qu'un algorithme de chiffrement est défini dans la règle WebSphere MQ

SignerDNs

Description : Sujet DistinguishedName des signataires autorisés.

Identificateur : **MQCA_SIGNER_DN**

Type de données : MQCFSL

Valeur : **2113** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Longueur maximale : Nom distinctif de signataire le plus long dans la règle, mais pas plus long que MQ_DISTINGUISHED_NAME_LENGTH

Renvoyé: Chaque fois qu'il est défini dans la règle WebSphere MQ .

RecipientDNs

Description : Sujet DistinguishedName des signataires autorisés.

Identificateur : **MQCA_RECIPIENT_DN**

Type de données : MQCFSL

Valeur : **2114** -Valeur numérique définie dans WebSphere MQ 7.5 ou dans le fichier `cmqc.h` .

Longueur maximale : Nom distinctif du destinataire le plus long dans la règle, mais pas MQ_DISTINGUISHED_NAME_LENGTH.

Renvoyé: Chaque fois qu'il est défini dans la règle WebSphere MQ .

Problèmes et solutions

Cette section explique comment résoudre les problèmes pouvant survenir lors de l'installation d' IBM . Ces informations permettent d'identifier et de résoudre les problèmes liés à Advanced Message Security.

com.ibm.security.pkcsutil.PKCSException: Erreur lors du chiffrement du contenu

L'erreur `com.ibm.security.pkcsutil.PKCSException: Error encrypting contents` suggère que IBM Advanced Message Security a des difficultés à accéder aux algorithmes de cryptographie.

Si l'erreur suivante est renvoyée par Advanced Message Security:

```
DRQJP0103E   The IBM WebSphere MQ Advanced Message Security Java interceptor failed to protect
message.
```

```
  com.ibm.security.pkcsutil.PKCSException: Error encrypting contents
(java.security.InvalidKeyException: Illegal key size or default parameters)
```

vérifier si la règle de sécurité JCE dans `JAVA_HOME/lib/security/local_policy.jar/*.policy` accorde l'accès aux algorithmes de signature utilisés dans la règle AMS MQ .

Si l'algorithme de signature que vous souhaitez utiliser n'est pas spécifié dans votre règle de sécurité en cours, téléchargez le fichier de règles Java correct à partir des emplacements suivants:

- IBM pour Java 1.4.2.
- IBM pour Java 5.0.
- IBM pour Java 6.0.
- IBM pour Java 7.0.

Prise en charge d'OSGi

Pour utiliser le bundle OSGi avec IBM Advanced Message Security , des paramètres supplémentaires sont requis.

Exécutez le paramètre suivant lors du démarrage du bundle OSGi:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7
```

Lorsque vous utilisez un mot de passe chiffré dans votre fichier keystore.conf, l'instruction suivante doit être ajoutée lorsque le bundle OSGi est en cours d'exécution:

```
-Dorg.osgi.framework.system.packages.extra=com.ibm.security.pkcs7,com.ibm.misc
```

Restriction : IBM WebSphere MQ AMS prend en charge la communication en utilisant uniquement les classes Java de base MQ pour les files d'attente protégées à partir du bundle OSGi.

Problèmes d'ouverture des files d'attente protégées lors de l'utilisation de JMS

Divers problèmes peuvent se produire lorsque vous ouvrez des files d'attente protégées lors de l'utilisation de IBM WebSphere MQ Advanced Message Security.

Vous exécutez JMS et vous recevez l'erreur 2085 (MQRC_UNKNOWN_OBJECT_NAME) avec l'erreur JMSMQ2008.

Vous avez vérifié que vous avez configuré votre IBM WebSphere MQ Advanced Message Security comme décrit dans «Guide de démarrage rapide pour les clients Java», à la page 296.

Il est possible que vous utilisiez un environnement d'exécution nonIBM Java . Il s'agit d'une limitation connue décrite dans «Limitations connues», à la page 284.

Vous n'avez pas défini la variable d'environnement AMQ_DISABLE_CLIENT_AMS.

Résolution du problème

Il existe quatre options pour contourner ce problème:

1. Démarrez votre application JMS dans un environnement d'exécution IBM Java (JRE) pris en charge.
2. Déplacez votre application sur la même machine que celle sur laquelle votre gestionnaire de files d'attente s'exécute et faites en sorte qu'elle se connecte à l'aide d'une connexion en mode liaisons.

   Une connexion en mode liaisons utilise des bibliothèques natives de plateforme pour effectuer les appels d'API IBM WebSphere MQ . Par conséquent, l'intercepteur AMS natif est utilisé pour effectuer les opérations AMS et les capacités de l'environnement d'exécution Java (JRE) ne sont pas utilisées.
3. Utilisez un intercepteur MCA, car cela permet la signature et le chiffrement des messages dès qu'ils arrivent sur le gestionnaire de files d'attente, sans que le client ait besoin d'effectuer un traitement AMS.

Etant donné que la protection est appliquée au niveau du gestionnaire de files d'attente, un autre mécanisme doit être utilisé pour protéger les messages en transit du client vers le gestionnaire de files d'attente. Le plus souvent, cela est réalisé en configurant le chiffrement SSL/TLS sur le canal de connexion serveur utilisé par l'application.

4. Définissez la variable d'environnement AMQ_DISABLE_CLIENT_AMS si vous ne souhaitez pas utiliser IBM WebSphere MQ Advanced Message Security.

Pour plus d'informations, voir «Interception MCA (Message Channel Agent)», à la page 309.

Remarque : Une règle de sécurité doit être mise en place pour chaque file d'attente dans laquelle l'intercepteur MCA va distribuer des messages. En d'autres termes, la file d'attente cible doit disposer d'une stratégie de sécurité AMS avec le nom distinctif (DN) du signataire et du destinataire correspondant à celui du certificat affecté à l'intercepteur MCA. Il s'agit du nom distinctif du certificat désigné par la propriété `cms.certificate.channel.SYSTEM.DEF.SVRCONN` dans le fichier `keystore.conf` utilisé par le gestionnaire de files d'attente.

Remarques

:NONE.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Corporation
Tour Descartes
Armonk, NY 10504-1785
U.S.A.

Pour toute demande d'informations relatives au jeu de caractères codé sur deux octets, contactez le service de propriété intellectuelle IBM ou envoyez vos questions par courrier à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s’applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
Coordinateur d'interopérabilité logicielle, département 49XA
3605 Autoroute 52 N

Rochester, MN 55901
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans le présent document et tous les éléments sous disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Contrat sur les produits et services IBM, aux Conditions Internationales d'Utilisation de Logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Licence sur les droits d'auteur :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Documentation sur l'interface de programmation

Les informations d'interface de programmation, si elles sont fournies, sont destinées à vous aider à créer un logiciel d'application à utiliser avec ce programme.

Ce manuel contient des informations sur les interfaces de programmation prévues qui permettent au client d'écrire des programmes pour obtenir les services de IBM WebSphere MQ.

Toutefois, lesdites informations peuvent également contenir des données de diagnostic, de modification et d'optimisation. Ces données vous permettent de déboguer votre application.

Important : N'utilisez pas ces informations de diagnostic, de modification et d'optimisation en tant qu'interface de programmation car elles sont susceptibles d'être modifiées.

Marques

IBM, le logo IBM , ibm.com, sont des marques d' IBM Corporation dans de nombreux pays. La liste actualisée de toutes les marques d' IBM est disponible sur la page Web "Copyright and trademark

information"www.ibm.com/legal/copytrade.shtml. Les autres noms de produits et de services peuvent être des marques d'IBM ou d’autres sociétés.

Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans d'autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Ce produit inclut des logiciels développés par le projet Eclipse (http://www.eclipse.org/).

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Référence :

(1P) P/N: