Red Hat AMQ 2021.Q3

AMQ Broker の設定

AMQ Broker 7.9 での使用について

Last Updated: 2023-02-23

Red Hat AMQ 2021.Q3 AMQ Broker の設定

AMQ Broker 7.9 での使用について

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書では、AMQ Broker の設定方法について説明します。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社 の CTO、Chris Wright のメッセージ を参照してください。

第1章 概要

AMQ Broker 設定ファイルは、ブローカーインスタンスの重要な設定を定義します。ブローカーの設定ファイルを編集することにより、ブローカーが環境で動作する方法を制御できます。

1.1. AMQ BROKER の設定ファイルおよび場所

ブローカーの設定ファイルはすべて **<broker_instance_dir>/etc** に保存されます。これらの設定ファイルで設定を編集すると、ブローカーを設定できます。

各ブローカーインスタンスは以下の設定ファイルを使用します。

broker.xml

主要設定ファイル。このファイルを使用して、ネットワーク接続、セキュリティー設定、メッセージアドレスなどのブローカーのほとんどの側面を設定します。

bootstrap.xml

AMQ Broker がブローカーインスタンスを起動するために使用するファイル。これは、**broker.xml** の場所を変更し、Web サーバーを設定し、セキュリティー設定を行います。

logging.properties

このファイルを使用して、ブローカーインスタンスのロギングプロパティーを設定します。

artemis.profile

このファイルを使用して、ブローカーインスタンスの実行中に使用される環境変数を設定します。

login.config, artemis-users.properties, artemis-roles.properties

セキュリティー関連ファイル。これらのファイルを使用して、ブローカーインスタンスへのユーザーアクセスの認証を設定します。

1.2. デフォルトブローカー設定について

broker.xml 設定ファイルを編集して、ブローカーの機能の大半を設定します。このファイルにはデフォルト設定が含まれています。これはブローカーを起動し、操作するには十分です。ただし、デフォルト設定の一部を変更し、お使いの環境にブローカーを設定するために新しい設定を追加する必要があります。

デフォルトでは、**broker.xml** には、以下の機能のデフォルト設定が含まれます。

- メッセージの永続性
- アクセプター
- セキュリティー
- メッセージアドレス

デフォルトのメッセージ永続性設定
デフォルトでは、AMQ Broker の永続性は、ディスク上のファイルセットで設定される追加のみのファイルジャーナルを使用します。ジャーナルは、メッセージ、トランザクション、およびその他の情報を保存します。

```
<configuration ...>

  <core ...>
```

```
...

<persistence-enabled>true</persistence-enabled>

<!-- this could be ASYNCIO, MAPPED, NIO
     ASYNCIO: Linux Libaio
     MAPPED: mmap files
     NIO: Plain Java Files
 -->
<journal-type>ASYNCIO</journal-type>

<paging-directory>data/paging</paging-directory>

<bindings-directory>data/bindings</bindings-directory>

<journal-directory>data/journal</journal-directory>

<large-messages-directory>data/large-messages</large-messages-directory>

<journal-datasync>true</journal-datasync>

<journal-min-files>2</journal-min-files>

<journal-pool-files>10</journal-pool-files>

<journal-file-size>10M</journal-file-size>

<!--
 This value was determined through a calculation.
 Your system could perform 8.62 writes per millisecond
 on the current journal configuration.
 That translates as a sync write every 115999 nanoseconds.

 Note: If you specify 0 the system will perform writes directly to the disk.
       We recommend this to be 0 if you are using journalType=MAPPED and journal-
datasync=false.
-->
<journal-buffer-timeout>115999</journal-buffer-timeout>

<!--
  When using ASYNCIO, this will determine the writing queue depth for libaio.
 -->
<journal-max-io>4096</journal-max-io>

<!-- how often we are looking for how many bytes are being used on the disk in ms -->
<disk-scan-period>5000</disk-scan-period>

<!-- once the disk hits this limit the system will block, or close the connection in certain protocols
     that won't support flow control. -->
<max-disk-usage>90</max-disk-usage>

<!-- should the broker detect dead locks and other issues -->
<critical-analyzer>true</critical-analyzer>

<critical-analyzer-timeout>120000</critical-analyzer-timeout>
```

```
      <critical-analyzer-check-period>60000</critical-analyzer-check-period>

      <critical-analyzer-policy>HALT</critical-analyzer-policy>

      ...

   </core>

</configuration>
```

デフォルトのアクセプター設定

ブローカーは、**acceptor** 設定要素を使用して受信クライアント接続をリッスンし、クライアントが接続を作成するためにポートおよびプロトコルを定義します。デフォルトでは、AMQ Broker には以下のように、サポートされる各メッセージングプロトコルのアクセプターが含まれます。

```
<configuration ...>

   <core ...>

      ...

      <acceptors>

         <!-- Acceptor for every supported protocol -->
         <acceptor name="artemis">tcp://0.0.0.0:61616?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=CORE,AMQP,STOMP,HORNETQ,MQTT,OPENWIRE;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

         <!-- AMQP Acceptor. Listens on default AMQP port for AMQP traffic -->
         <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

         <!-- STOMP Acceptor -->
         <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true</acceptor>

         <!-- HornetQ Compatibility Acceptor. Enables HornetQ Core and STOMP for legacy HornetQ clients. -->
         <acceptor name="hornetq">tcp://0.0.0.0:5445?
anycastPrefix=jms.queue.;multicastPrefix=jms.topic.;protocols=HORNETQ,STOMP;useEpoll=true</acceptor>

         <!-- MQTT Acceptor -->
         <acceptor name="mqtt">tcp://0.0.0.0:1883?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=MQTT;useEpoll=true</acceptor>

      </acceptors>

      ...

   </core>

</configuration>
```

デフォルトのセキュリティー設定
AMQ Broker には、アドレスに基づいてキューにセキュリティーを適用するための柔軟なロールベースのセキュリティーモデルが含まれています。デフォルト設定ではワイルドカードを使用して **amq** ロールをすべてのアドレスに適用します (数値記号 **#** で表されます)。

```
<configuration ...>

  <core ...>

    ...

    <security-settings>
      <security-setting match="#">
        <permission type="createNonDurableQueue" roles="amq"/>
        <permission type="deleteNonDurableQueue" roles="amq"/>
        <permission type="createDurableQueue" roles="amq"/>
        <permission type="deleteDurableQueue" roles="amq"/>
        <permission type="createAddress" roles="amq"/>
        <permission type="deleteAddress" roles="amq"/>
        <permission type="consume" roles="amq"/>
        <permission type="browse" roles="amq"/>
        <permission type="send" roles="amq"/>
        <!-- we need this otherwise ./artemis data imp wouldn't work -->
        <permission type="manage" roles="amq"/>
      </security-setting>
    </security-settings>

    ...

  </core>

</configuration>
```

デフォルトのメッセージアドレス設定
AMQ Broker には、作成されたキューまたはトピックに適用されるデフォルトの設定セットを確立するデフォルトアドレスが含まれています。

さらに、デフォルト設定では、**DLQ** (Dead Letter Queue) の 2 つのキューが、既知の宛先で到達するメッセージを処理します。また、**Expiry Queue** は有効期限を過ぎたメッセージを保持しているため、元の宛先にルーティングしないでください。

```
<configuration ...>

  <core ...>

    ...

    <address-settings>
      ...
      <!--default for catch all-->
      <address-setting match="#">
        <dead-letter-address>DLQ</dead-letter-address>
        <expiry-address>ExpiryQueue</expiry-address>
        <redelivery-delay>0</redelivery-delay>
```

```
            <!-- with -1 only the global-max-size is in use for limiting -->
            <max-size-bytes>-1</max-size-bytes>
            <message-counter-history-day-limit>10</message-counter-history-day-limit>
            <address-full-policy>PAGE</address-full-policy>
            <auto-create-queues>true</auto-create-queues>
            <auto-create-addresses>true</auto-create-addresses>
            <auto-create-jms-queues>true</auto-create-jms-queues>
            <auto-create-jms-topics>true</auto-create-jms-topics>
         </address-setting>
      </address-settings>

      <addresses>
         <address name="DLQ">
            <anycast>
               <queue name="DLQ" />
            </anycast>
         </address>
         <address name="ExpiryQueue">
            <anycast>
               <queue name="ExpiryQueue" />
            </anycast>
         </address>
      </addresses>

   </core>

</configuration>
```

1.3. 設定の更新のリロード

デフォルトでは、ブローカーは 5000 ミリ秒ごとに設定ファイルの変更をチェックします。ブローカーが設定ファイルの最後の変更されたタイムスタンプの変更を検出する場合、ブローカーは設定変更の実行を決定します。この場合、ブローカーは設定ファイルを再読み込みして変更を有効にします。

ブローカーが **broker.xml** 設定ファイルを再読み込みすると、以下のモジュールを再読み込みします。

- アドレス設定およびキュー
  設定ファイルを再読み込みすると、アドレス設定が、設定ファイルから削除されたアドレスおよびキューを処理する方法を決定します。これは、**config-delete-addresses** および **config-delete-queues** プロパティーで設定できます。詳細は、付録B *アドレス設定設定要素* を参照してください。

- セキュリティー設定
  既存のアクセプターの SSL/TLS キーストアおよびトラストストアをリロードすると、既存のクライアントに影響を与えずに新しい証明書を確立できます。接続されているクライアントは、古い証明書または異なる証明書を持つクライアントであっても、メッセージの送受信を継続できます。

- Diverts
  設定の再読み込みにより、追加した **新しい** 迂回をデプロイします。ただし、設定から迂回を削除したり、**<divert>** 要素内のサブ要素に変更しても、ブローカーを再起動するまで反映されません。

以下の手順では、ブローカーが **broker.xml** 設定ファイルへの変更をチェックする間隔を変更する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<core>** 要素内に **<configuration-file-refresh-period> 要素を追加** し、更新期間 (ミリ秒単位) を設定します。
   以下の例では、設定の更新の期間を 60000 ミリ秒に設定します。

```
<configuration>
  <core>
    ...
    <configuration-file-refresh-period>60000</configuration-file-refresh-period>
    ...
  </core>
</configuration>
```

設定ファイルへの何らかの理由でアクセスできない場合は、管理 API またはコンソールを使用して設定ファイルのリロードを強制することもできます。設定ファイルは、**ActiveMQServerControl** で管理操作 **reloadConfigurationFile()** を使用してリロードできます (**ObjectName org.apache.activemq.artemis:broker="BROKER_NAME"** またはリソース ネーム **server** を使用)。

関連情報

- 管理 API の使用方法は、Managing AMQ Broker の Using the Management API を参照してください。

1.4. ブローカー設定ファイルのモジュラー

共通の設定設定を共有する複数のブローカーがある場合は、個別のファイルに共通設定を定義し、各ブローカーの **broker.xml** 設定ファイルにこれらのファイルを含めることができます。

ブローカー間で共有できる最も一般的な設定には、以下が含まれます。

- アドレス
- アドレス設定
- セキュリティー設定

手順

1. 共有する **broker.xml** セクションごとに個別の XML ファイルを作成します。
   各 XML ファイルには、**broker.xml** の単一のセクションのみを含めることができます (例: アドレス設定またはアドレス設定のどちらかですが、両方ではありません)。top-level 要素は、要素名前空間 (**xmlns="urn:activemq:core"**) も定義する必要があります。

   以下の例は、**my-security-settings.xml** で定義されたセキュリティー設定を示しています。

   my-security-settings.xml

```
<security-settings xmlns="urn:activemq:core">
  <security-setting match="a1">
    <permission type="createNonDurableQueue" roles="a1.1"/>
  </security-setting>
  <security-setting match="a2">
```

```
      <permission type="deleteNonDurableQueue" roles="a2.1"/>
    </security-setting>
  </security-settings>
```

2. 共通の設定を使用する各ブローカーの **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

3. 開かれた **broker.xml** ファイルごとに、以下を行います。

   a. **broker.xml** の最初の **<configuration>** 要素で、以下の行が表示されることを確認します。

   ```
   xmlns:xi="http://www.w3.org/2001/XInclude"
   ```

   b. 共有設定設定が含まれる各 XML ファイルに対して XML 包含を追加します。
   この例には **my-security-settings.xml** ファイルが含まれます。

   broker.xml

   ```
   <configuration ...>
     <core ...>
       ...
       <xi:include href="/opt/my-broker-config/my-security-settings.xml"/>
       ...
     </core>
   </configuration>
   ```

   c. 必要に応じて、**broker.xml** を検証し、XML がスキーマに対して有効であることを確認します。
   任意の XML バリデータープログラムを使用できます。この例では、**xmllint** を使用して、**artemis-server.xsl** スキーマに対して **broker.xml** を検証します。

   ```
   $ xmllint --noout --xinclude --schema /opt/redhat/amq-broker/amq-broker-
   7.2.0/schema/artemis-server.xsd /var/opt/amq-broker/mybroker/etc/broker.xml
   /var/opt/amq-broker/mybroker/etc/broker.xml validates
   ```

関連情報

- XML 包含 (XIncludes) の詳細は、https://www.w3.org/TR/xinclude/ を参照してください。

1.4.1. モジュール設定ファイルのリロード

ブローカーが設定変更を定期的にチェックすると (**configuration-file-refresh-period** で指定される頻度)、**xi:include** を使用して **broker.xml** 設定ファイルに含まれる設定ファイルへの変更を自動的に**検出しません**。たとえば、**broker.xml** に **my-address-settings.xml** が含まれ、**my-address-settings.xml** に加えられると、ブローカーは **my-address-settings.xml** の変更を自動的に検出せず、設定を再読み込みしません。

broker.xml 設定ファイルのリロードと、それに含まれる変更された設定ファイルを **強制**するには、**broker.xml** 設定ファイルの last modified タイムスタンプが変更されたことを確認する必要があります。標準の Linux **touch** コマンドを使用して、他の変更を加えずに **broker.xml** の最終変更のタイムスタンプを更新できます。以下は例になります。

```
$ touch -m <broker_instance_dir>/etc/broker.xml
```

または、管理 API を使用して Broker のリロードを強制的に実行することもできます。設定ファイルは、**ActiveMQServerControl** で管理操作 **reloadConfigurationFile()** を使用してリロードできます (**ObjectName org. apache.activemq.artemis:broker="BROKER_NAME"** またはリソース ネーム **server** を使用)。

関連情報

- 管理 API の使用方法は、Managing AMQ Broker の Using the Management API を参照してください。

1.5. 本書の表記慣例

本書では、**sudo** コマンド、ファイルパス、および置き換え可能な値について、以下の規則を使用します。

sudo コマンド
本書では、root 権限を必要とするすべてのコマンドに対して **sudo** が使用されています。何らかの変更がシステム全体に影響を与える可能性があるため、**sudo** を使用する場合は、常に注意が必要です。

sudo の使用の詳細は、**sudo** コマンド を参照してください。

本書におけるファイルパスの使用
本書では、すべてのファイルパスは Linux、UNIX、および同様のオペレーティングシステムで有効です (例: **/home/...**)。Microsoft Windows を使用している場合は、同等の Microsoft Windows パスを使用する必要があります (例: **C:\Users\...**)。

交換可能な値
このドキュメントでは、お客様の環境に合わせた値に置き換える必要のある置換可能な値を使用している場合があります。置き換え可能な値は小文字で、角括弧 (**< >**) で囲まれ、イタリックおよび **monospace** フォントを使用してスタイルされます。単語が複数になる場合は、アンダースコア (_) で区切ります。

たとえば、**<install_dir>** を独自のディレクトリー名に置き換えます。

```
$ <install_dir>/bin/artemis create mybroker
```

第2章 ネットワーク接続でのアクセプターおよびコネクターの設定

AMQ Broker で使用される接続には、ネットワーク接続と**in-VM**接続の 2 種類があります。ネットワーク接続は、同じサーバーまたは物理的にリモート上に関係なく、2 つの当事者が異なる仮想マシンにある場合に使用されます。in-VM 接続は、クライアント (アプリケーションかサーバーかに関係なく) がブローカーと同じ仮想マシンにある場合に使用されます。

ネットワーク接続は Netty を使用します。Netty は、複数の方法でネットワーク接続を設定できるようにする、高パフォーマンスの低レベルネットワークライブラリーです。Java IO または NIO、TCP ソケット、SSL/TLS、または HTTP または HTTPS でのトンネリングの使用。Netty は、すべてのメッセージングプロトコルに単一のポートを使用することもできます。ブローカーは、使用されているプロトコルを自動的に検出し、さらに処理するために受信メッセージを適切なハンドラーに送ります。

ネットワーク接続の URI で、そのタイプを決定します。たとえば、URI で **vm** を指定すると、イン VM 接続が作成されます。

```
<acceptor name="in-vm-example">vm://0</acceptor>
```

また、URI に **tcp** を指定すると、ネットワーク接続が行われます。以下は例になります。

```
<acceptor name="network-example">tcp://localhost:61617</acceptor>
```

以降のセクションでは、ネットワーク接続と VM の接続に必要な 2 つの設定要素 (**acceptors**および**connectors**) を説明します。ここでは、TCP、HTTP、および SSL/TLS ネットワーク接続のアクセプターおよびコネクター、および VM 接続の設定方法を説明します。

2.1. アクセプターについて

アクセプター はブローカーへの接続方法を定義します。各アクセプターは、クライアントが接続を確立するために使用できるポートおよびプロトコルを定義します。簡単なアクセプター設定を以下に示します。

```
<acceptors>
  <acceptor name="example-acceptor">tcp://localhost:61617</acceptor>
</acceptors>
```

ブローカー設定で定義する各 **acceptor** 要素は単一の **acceptors** 要素に含まれます。ブローカーに定義できるアクセプターの数の上限はありません。デフォルトでは、AMQ Broker には以下のように、サポートされる各メッセージングプロトコルのアクセプターが含まれます。

```
<configuration ...>
  <core ...>
    ...
    <acceptors>
      ...
      <!-- Acceptor for every supported protocol -->
      <acceptor name="artemis">tcp://0.0.0.0:61616?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=CORE,AMQP,STOMP,HORNETQ,MQTT,OPENWIRE;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

      <!-- AMQP Acceptor. Listens on default AMQP port for AMQP traffic -->
      <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>
```

```
        <!-- STOMP Acceptor -->
        <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true</acce
ptor>

        <!-- HornetQ Compatibility Acceptor. Enables HornetQ Core and STOMP for legacy HornetQ
clients. -->
        <acceptor name="hornetq">tcp://0.0.0.0:5445?
anycastPrefix=jms.queue.;multicastPrefix=jms.topic.;protocols=HORNETQ,STOMP;useEpoll=true</a
cceptor>

        <!-- MQTT Acceptor -->
        <acceptor name="mqtt">tcp://0.0.0.0:1883?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=MQTT;useEpoll=true</accept
or>
      </acceptors>
      ...
  </core>
</configuration>
```

2.2. アクセプターの設定

以下の例は、アクセプターを設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **acceptors** 要素に、新しい **acceptor** 要素を追加します。ブローカーのプロトコルおよびポートを指定します。以下は例になります。

```
<acceptors>
  <acceptor name="example-acceptor">tcp://localhost:61617</acceptor>
</acceptors>
```

   上記の例では、TCP プロトコルのアクセプターを定義します。ブローカーは TCP を使用するクライアント接続用にポート 61617 でリッスンします。

3. アクセプターに定義された URI にキーと値のペアを追加します。セミコロン (**;**) を使用して複数のキーと値のペアを区切ります。以下は例になります。

```
<acceptor name="example-acceptor">tcp://localhost:61617?sslEnabled=true;key-store-
path=</path/to/key_store></acceptor>
```

   この設定は、TLS/SSL を使用し、必要なキーストアへのパスを定義するアクセプターを定義するようになりました。

関連情報

- アクセプターおよびコネクターで使用できる設定オプションの詳細は、付録A *アクセプターおよびコネクター設定パラメーター* を参照してください。

2.3. コネクター

アクセプターはブローカーが接続を**受け入れる** 方法を定義しますが、コネクターはクライアントによってブローカーへの**接続方法**を定義します。

ブローカー自体がクライアントとして動作する場合、コネクターはブローカーに設定されます。以下は例になります。

- ブローカーが別のブローカーにブリッジされている場合
- ブローカーがクラスターの一部である場合

以下は、簡単なコネクター設定になります。

```
<connectors>
  <connector name="example-connector">tcp://localhost:61617</connector>
</connectors>
```

2.4. コネクターの設定

以下の例は、コネクターの設定方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **connectors** 要素に、新しい **connector** 要素を追加します。ブローカーのプロトコルおよびポートを指定します。以下は例になります。

   ```
   <connectors>
     <connector name="example-connector">tcp://localhost:61617</connector>
   </connectors>
   ```

   上記の例では、TCP プロトコルのコネクターを定義します。クライアントはコネクター設定を使用して、TCP プロトコルを使用してポート 61617 のブローカーに接続できます。ブローカー自体は、送信接続にこのコネクターを使用することもできます。
3. コネクターに定義された URI にキーと値のペアを追加します。セミコロン (**;**) を使用して複数のキーと値のペアを区切ります。以下は例になります。

   ```
   <connector name="example-connector">tcp://localhost:61616?tcpNoDelay=true</connector>
   ```

   この設定は、**tcpNoDelay** プロパティーの値を **true** に設定するコネクターを定義するようになりました。このプロパティーの値を **true** に設定すると、接続の Nagle アルゴリズムがオフになります。Nagle のアルゴリズムは、小さなデータパケットの送信を遅延させ、それを大きなパケットに統合することで、TCP 接続の効率を向上させるために使用するアルゴリズムです。

関連情報

- アクセプターおよびコネクターで使用できる設定オプションの詳細は、付録A *アクセプターおよびコネクター設定パラメーター* を参照してください。
- AMQ Core Protocol JMS クライアントでブローカーコネクターを設定する方法は、AMQ Core Protocol JMS ドキュメントの Configuring a broker connector を参照してください。

2.5. TCP 接続の設定

AMQ Broker は Netty を使用して基本的な、暗号化されていない TCP ベースの接続を提供します。この接続は、ブロッキング Java IO または新しい非ブロッキング Java NIO を使用するように設定できます。多くの同時接続でスケーラビリティーを向上させるために、Java NIO が推奨されます。ただし、古い IO を使用すると、何万もの同時接続のサポートを受けても NIO より優れたレイテンシーが発生することがあります。

信頼できないネットワーク全体で接続を実行している場合は、TCP ネットワーク接続が暗号化されないことを認識する必要があります。セキュリティーが優先度であれば、SSL または HTTPS 設定を使用して、この接続で送信されたメッセージを暗号化することを検討してください。詳細は、「接続のセキュリティー保護」 を参照してください。

TCP 接続を使用すると、すべての接続がクライアントによって開始されます。ブローカーはクライアントへの接続を開始しません。これは、ファイアウォールポリシーと、強制的に接続を一方向から開始するように機能します。

TCP 接続では、コネクター URI のホストおよびポートは接続に使用されるアドレスを定義します。

以下の例は、TCP 接続を設定する方法を示しています。

前提条件

- アクセプターおよびコネクターの設定を理解する必要があります。詳細は以下を参照してください。
  - 「アクセプターの設定」
  - 「コネクターの設定」

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 新しいアクセプターを追加するか、既存のアクセプターを変更します。接続 URI で、**tcp** をプロトコルとして指定します。IP アドレスまたはホスト名とブローカーのポートの両方を含めます。以下は例になります。

```
<acceptors>
  <acceptor name="tcp-acceptor">tcp://10.10.10.1:61617</acceptor>
  ...
</acceptors>
```

   前述の例に基づいて、ブローカーは IP アドレス **10.10.10.1** でポート **61617** に接続するクライアントからの TCP 通信を受け入れます。

3. (任意設定): 同様の方法でコネクターを設定できます。以下は例になります。

```
<connectors>
  <connector name="tcp-connector">tcp://10.10.10.2:61617</connector>
  ...
</connectors>
```

   前述の例のコネクターは、指定された IP およびポート **10.10.10.2:61617** に TCP 接続を確立する場合、クライアントまたはブローカー自体によって参照されます。

関連情報

- TCP 接続に使用できる設定オプションの詳細は、付録A *アクセプターおよびコネクター設定パラメーター* を参照してください。

2.6. HTTP 接続の設定

HTTP プロトコルを介した HTTP 接続トンネルは、ファイアウォールが HTTP トラフィックのみを許可する場合に便利です。AMQ Broker は HTTP が使用されているかどうかを自動的に検出するため、HTTP のネットワーク接続の設定は TCP の接続の設定と同じです。

前提条件

- アクセプターおよびコネクターの設定を理解する必要があります。詳細は以下を参照してください。
  - 「アクセプターの設定」
  - 「コネクターの設定」

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 新しいアクセプターを追加するか、既存のアクセプターを変更します。接続 URI で、**tcp** をプロトコルとして指定します。IP アドレスまたはホスト名とブローカーのポートの両方を含めます。以下は例になります。

```
<acceptors>
  <acceptor name="http-acceptor">tcp://10.10.10.1:80</acceptor>
  ...
</acceptors>
```

   前述の例に基づいて、ブローカーは IP アドレス **10.10.10.1** でポート **80** に接続するクライアントからの HTTP 通信を受け入れます。ブローカーは HTTP プロトコルが使用中であることを自動的に検出し、それに応じてクライアントと通信します。

3. (任意設定): 同様の方法でコネクターを設定できます。以下は例になります。

```
<connectors>
  <connector name="http-connector">tcp://10.10.10.2:80</connector>
  ...
</connectors>
```

   前述の例に記載されているコネクターを使用すると、ブローカーは IP アドレス **10.10.10.2** のポート **80** にアウトバウンド HTTP 接続を作成します。

関連情報

- HTTP 接続は TCP と同じ設定パラメーターを使用しますが、いくつかの設定パラメーターもあります。HTTP 接続で利用可能なすべての設定オプションについては、付録A *アクセプターおよびコネクター設定パラメーター* を参照してください。
- HTTP の使用方法を示す完全な作業例は、ブローカーインストールの **<install_dir>/examples/features/standard/** ディレクトリーにある **http-transport** の例を参照してください。

2.7. セキュアな接続の設定

TLS/SSL を使用してネットワーク接続をセキュアにすることができます。詳細は、「接続のセキュリティー保護」 を参照してください。

2.8. イン仮想マシン接続の設定

複数のブローカーが同じ仮想マシンに共存する場合 (HA) 設定の一部として、VM 内の接続を使用できます。イン仮想マシン接続は、ブローカーと同じ JVM で実行されているローカルクライアントでも使用できます。

前提条件

- アクセプターおよびコネクターの設定を理解する必要があります。詳細は以下を参照してください。
  - 「アクセプターの設定」
  - 「コネクターの設定」

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 新しいアクセプターを追加するか、既存のアクセプターを変更します。接続 URI で、**vm** をプロトコルとして指定します。以下は例になります。

```
<acceptors>
  <acceptor name="in-vm-acceptor">vm://0</acceptor>
  ...
</acceptors>
```

   前述の例のアクセプターに基づいて、ブローカーは ID が **0** のブローカーからの接続を受け入れます。他のブローカーは、同じ仮想マシンで実行している必要があります。

3. (任意設定): 同様の方法でコネクターを設定できます。以下は例になります。

```
<connectors>
  <connector name="in-vm-connector">vm://0</connector>
  ...
</connectors>
```

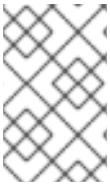
   前述の例の connector は、クライアントがクライアントと同じ仮想マシンで実行している ID が **0** のブローカーにイン VM 接続を確立する方法を定義します。クライアントはアプリケーションまたは別のブローカーになります。

第3章 ネットワーク接続でのメッセージングプロトコルの設定

AMQ Broker にはプラグ可能なプロトコルアーキテクチャーがあるため、ネットワーク接続に 1 つ以上のプロトコルを簡単に有効化できます。

ブローカーは以下のプロトコルをサポートします。

- AMQP
- MQTT
- OpenWire
- STOMP



注記

上記のプロトコルのほかに、ブローカーは Core と呼ばれる独自のネイティブプロトコルもサポートします。このプロトコルの以前のバージョンは HornetQ と呼ばれ、Red Hat JBoss Enterprise Application Platform によって使用されていました。

3.1. メッセージングプロトコルを使用するためのネットワーク接続の設定

使用する前に、プロトコルをネットワーク接続に関連付ける必要があります。ネットワーク接続の作成および設定方法は、Configuring acceptors and connectors in network connections を参照してください。 **<broker_instance_dir>/etc/broker.xml** ファイルにあるデフォルト設定には、すでに定義された接続が複数含まれています。便宜上、AMQ Broker にはサポートされる各プロトコルのアクセプターと、すべてのプロトコルをサポートするデフォルトのアクセプターが含まれます。

デフォルトのアクセプターの概要
以下は、**broker.xml** 設定ファイルにデフォルトで含まれるアクセプターです。

```
<configuration>
  <core>
    ...
    <acceptors>

      <!-- All-protocols acceptor -->
      <acceptor name="artemis">tcp://0.0.0.0:61616?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=CORE,AMQP,STOMP,HORNETQ,MQTT,OPENWIRE;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

      <!-- AMQP Acceptor. Listens on default AMQP port for AMQP traffic -->
      <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;amqpCredits=1000;amqpLowCredits=300</acceptor>

      <!-- STOMP Acceptor -->
      <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true</acceptor>

      <!-- HornetQ Compatibility Acceptor. Enables HornetQ Core and STOMP for legacy HornetQ clients. -->
      <acceptor name="hornetq">tcp://0.0.0.0:5445?
```

```
anycastPrefix=jms.queue.;multicastPrefix=jms.topic.;protocols=HORNETQ,STOMP;useEpoll=true</a
cceptor>

    <!-- MQTT Acceptor -->
    <acceptor name="mqtt">tcp://0.0.0.0:1883?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=MQTT;useEpoll=true</accept
or>

  </acceptors>
  ...
 </core>
</configuration>
```

特定のネットワーク設定でプロトコルを有効にする唯一の要件は、**protocols** パラメーターを アクセプターの URI に追加することです。パラメーターの値は、プロトコル名のコンマ区切りリストである必要があります。protocol パラメーターが URI から省略される場合、すべてのプロトコルが有効になります。

たとえば、AMQP プロトコルを使用して 3232 番ポートでメッセージを受信するためにアクセプターを作成するには、以下の手順に従います。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以下の行を **<acceptors>** スタンザに追加します。

```
<acceptor name="ampq">tcp://0.0.0.0:3232?protocols=AMQP</acceptor>
```

デフォルトのアクセプターの追加パラメーター

最小限のアクセプター設定では、接続 URI の一部としてプロトコルを指定します。ただし、**broker.xml** 設定ファイルのデフォルトのアクセプターには追加のパラメーターが設定されています。以下の表は、デフォルトのアクセプターに設定された追加パラメーターの詳細を示しています。

Acceptor(s)	パラメーター	説明
All-protocols acceptor AMQP STOMP	tcpSendBufferSize	TCP 送信バッファーのサイズ (バイト単位)。デフォルト値は **32768** です。
	tcpReceiveBufferSize	TCP 受信バッファーのサイズ (バイト単位)。デフォルト値は **32768** です。 TCP バッファーサイズは、ネットワークの帯域幅およびレイテンシーに従って調整する必要があります。 つまり、TCP の送信/受信バッファーサイズは以下のように計算する必要があります。 buffer_size = bandwidth * RTT 帯域幅とは秒単位で、ネットワークラウンドトリップタイム (RTT) は秒単位になります。RTT は、**ping** ユーティリティーを使用して簡単に測定できます。 高速ネットワークでは、デフォルトからバッファーサイズを増やす必要がある場合があります。

Acceptor(s)	パラメーター	説明
All-protocols acceptor AMQP STOMP HornetQ MQTT	useEpoll	サポートするシステム (Linux) を使用する場合は Netty epoll を使用します。Netty ネイティブトランスポートは NIO トランスポートよりも優れたパフォーマンスを提供します。このオプションのデフォルト値は **true** です。オプションを **false** に設定すると、OIO が使用されます。
All-protocols acceptor AMQP	amqpCredits	メッセージの合計サイズに関係なく、AMQP プロデューサーが送信できるメッセージの最大数。デフォルト値は **1000** です。 AMQP メッセージのブロックにクレジットが使用される方法は、「AMQP プロデューサーのブロック」 を参照してください。
All-protocols acceptor AMQP	amqpLowCredits	ブローカーによってプロデューサーのクレジットが返送される低いしきい値。デフォルト値は **300** です。プロデューサーがこのしきい値に達すると、ブローカーはプロデューサーに十分なクレジットを送信し、**amqpCredits** 値を復元します。 AMQP メッセージのブロックにクレジットが使用される方法は、「AMQP プロデューサーのブロック」 を参照してください。
HornetQ 互換性アクセプター	anycastPrefix	anycast および **multicast** の両方を使用するアドレスに接続するときに、クライアントが **anycast** および **anycast** ルーティングタイプを指定するために使用する接頭辞。デフォルト値は **jms.queue** です。 アドレスへの接続時にクライアントがルーティングタイプを指定できるように接頭辞を設定する方法は、「アクセプター設定へのルーティングタイプの追加」 を参照してください。
	multicastPrefix	**anycast** および **multicast** の両方を使用するアドレスへの接続時に **multicast** ルーティングタイプを指定するためにクライアントが使用する接頭辞。デフォルト値は **jms.topic** です。 アドレスへの接続時にクライアントがルーティングタイプを指定できるように接頭辞を設定する方法は、「アクセプター設定へのルーティングタイプの追加」 を参照してください。

関連情報

- Netty ネットワーク接続に設定できるその他のパラメーターに関する情報は、付録A *アクセプターおよびコネクター設定パラメーター* を参照してください。

3.2. ネットワーク接続での AMQP の使用

ブローカーは AMQP 1.0 仕様をサポートします。AMQP リンクは、ソースとターゲット間のメッセージ (クライアントとブローカー) の一方向プロトコルです。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以下の例のように、AMQP の値を持つ **protocols** パラメーターを URI の一部として追加または設定することで、**acceptor** を追加または設定し、**AMQP** クライアントを受信します。

```
<acceptors>
  <acceptor name="amqp-acceptor">tcp://localhost:5672?protocols=AMQP</acceptor>
  ...
</acceptors>
```

上記の例では、ブローカーはデフォルトの AMQP ポートであるポート 5672 で AMQP 1.0 クライアントを受け入れます。

AMQP リンクには、送信者と受信側の 2 つのエンドポイントがあります。送信者がメッセージを送信する場合、ブローカーはこれを内部形式に変換するため、ブローカーの宛先に転送できます。受信側はブローカーの宛先に接続し、メッセージを配信前に AMQP に戻します。

AMQP リンクが動的の場合、一時キューが作成され、リモートソースまたはリモートターゲットアドレスのいずれかが一時キューの名前に設定されます。リンクが動的ではない場合、リモートターゲットまたはソースのアドレスがキューに使用されます。リモートターゲットまたはソースが存在しない場合は、例外が発生します。

リンクターゲットは、基礎となるセッションをトランザクションとして処理するために使用される Coordinator でも、ロールバックまたはコミットします。

注記

AMQP ではセッションごとに複数のトランザクション **amqp:multi-txns-per-ssn** を使用できますが、現在のバージョンの AMQ Broker はセッションごとに単一のトランザクションのみをサポートします。

注記

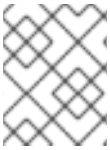
AMQP 内の分散トランザクション (XA) の詳細は、仕様の 1.0 バージョンでは提供されません。お使いの環境で分散トランザクションのサポートが必要な場合は、AMQ Core Protocol JMS を使用することが推奨されます。

プロトコルとその機能の詳細は、AMQP 1.0 仕様を参照してください。

3.2.1. AMQP リンクをトピックとして使用

JMS とは異なり、AMQP プロトコルにはトピックが含まれません。ただし、キューのコンシューマーだけでなく、AMQP コンシューマーまたは受信側をサブスクリプションとして扱うことは可能です。デフォルトでは、接頭辞 **jms.topic.** でアドレスにアタッチする受信リンクがサブスクリプションとして処理され、サブスクリプションキューが作成されます。以下の表でキャプチャーされているように、Terminus Durability の設定方法に応じて、サブスクリプションキューが永続的または揮発性になります。

この種のマルチキャスト専用キューのサブスクリプションを作成します。	Terminus Durability を 下記のようにセットします。
永続性	**UNSETTLED_STATE** または **CONFIGURATION**
Non-durable	**NONE**



注記

永続キューの名前は、コンテナー ID とリンク名 (例: **my-container-id:my-link-name**) で設定されます。

AMQ Broker は qpid-jms クライアントもサポートし、アドレスに使用される接頭辞に関係なくトピックの使用に対応します。

3.2.2. AMQP セキュリティーの設定

ブローカーは AMQP SASL 認証をサポートします。ブローカーで SASL ベースの認証を設定する方法は、Security を参照してください。

3.3. ネットワーク接続での MQTT の使用

ブローカーは MQTT v3.1.1(および古い v3.1 コードメッセージ形式) をサポートします。MQTT は軽量のクライアントからサーバーへ、パブリッシュ/サブスクライブメッセージングプロトコルです。MQTT は、メッセージングのオーバーヘッドおよびネットワークトラフィック、およびクライアントのコードフットプリントを削減します。このような理由から、MQTT は、センサーやアクチュエーターなどのデバイスを制限するのが適しており、この ng(IoT) のインターネット向けの de facto 標準通信プロトコルがすばやく考えられます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. MQTT プロトコルが有効になっているアクセプターを追加します。以下に例を示します。

```
<acceptors>
  <acceptor name="mqtt">tcp://localhost:1883?protocols=MQTT</acceptor>
  ...
</acceptors>
```

MQTT には、以下を含む便利な機能が多数含まれています。

QoS (Quality of Service)

各メッセージは、関連付けられた QoS(Quality of Service) を定義できます。ブローカーは、定義された最大 QoS(Quality of Service) レベルで、サブスクライバーに対してメッセージの配信を試みます。

保持されるメッセージ

特定のアドレスに対してメッセージを保持できます。クライアントの接続前に保持されるメッセージが送信された場合でも、他のメッセージの前に最後に保持されたメッセージを受信する新しいサブスクライバー。

ワイルドカードサブスクリプション

MQTT アドレスは、ファイルシステムの階層と同様に階層です。クライアントは、特定のトピックや、階層のブランチ全体にサブスクライブできます。

メッセージ

クライアントは、接続パケットの一部として will message を設定できます。クライアントが異常に切断されると、ブローカーは指定されたアドレスにメッセージを公開します。他のサブスクライバーはメッセージを受信し、対応できます。

MQTT プロトコルに関する情報の最適なソースは、仕様にあります。MQTT v3.1.1 仕様は、OASIS Web サイト からダウンロードできます。

3.4. ネットワーク接続での OPENWIRE の使用

ブローカーは OpenWire protocol プロトコルをサポートします。これにより、JMS クライアントはブローカーと直接対話できます。このプロトコルを使用して、古いバージョンの AMQ Broker と通信します。

現在、AMQ Broker は標準の JMS API のみを使用する OpenWire クライアントをサポートします。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以下の例にあるように、**acceptor** を追加または変更して、**protocol** パラメーターの一部として **OPENWIRE** が含まれるようにします。

```
<acceptors>
  <acceptor name="openwire-acceptor">tcp://localhost:61616?
protocols=OPENWIRE</acceptor>
  ...
</acceptors>
```

上記の例では、ブローカーは受信 OpenWire コマンドのポート 61616 でリッスンします。

詳細は、**<install_dir>/examples/protocols/openwire** にある例を参照してください。

3.5. ネットワーク接続による STOMP の使用

STOMP は、STOMP クライアントが STOMP Broker と通信できるようにするテキスト指向のワイヤプロトコルです。ブローカーは STOMP 1.0、1.1、および 1.2 をサポートします。STOMP クライアントは複数の言語やプラットフォームで利用できます。これにより、相互運用性の選択肢があります。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 既存の **acceptor** を設定するか、または新しいアクセプターを作成し、以下のように **STOMP** の値を持つ **protocols** パラメーターを追加します。

```
<acceptors>
  <acceptor name="stomp-acceptor">tcp://localhost:61613?protocols=STOMP</acceptor>
  ...
</acceptors>
```

上記の例では、ブローカーはポート **61613** の STOMP 接続を受け入れます。

STOMP を使用したブローカーの設定例については、& **lt;install_dir>/examples/protocols** にある **stomp** の例を参照してください。

3.5.1. STOMP の制限

STOMP を使用する場合、以下の制限が適用されます。

1. 現在、ブローカーは仮想ホストをサポートしません。つまり、**host** フレーム の **CONNECT** ヘッダーは無視されます。

2. メッセージ確認応答はトランザクションではありません。**ACK** フレームはトランザクションの一部にできず、**transaction** ヘッダーが設定されている場合は無視されます。

3.5.2. STOMP メッセージの ID の提供

JMS コンシューマーまたは QueueBrowser を介して STOMP メッセージを受信する場合、メッセージには **JMSMessageID** などの JMS プロパティーは含まれません。ただし、ブローカーパラメーターを使用して、各受信 STOMP メッセージにメッセージ ID を設定できます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

2. 以下の例のように、STOMP 接続に使用される **acceptor** の **stompEnableMessageId** パラメーターを **true** に設定します。

```
<acceptors>
  <acceptor name="stomp-acceptor">tcp://localhost:61613?
protocols=STOMP;stompEnableMessageId=true</acceptor>
  ...
</acceptors>
```

stompEnableMessageId パラメーターを使用することで、このアクセプターを使用して送信される各 stomp メッセージには追加のプロパティーが追加されます。property キーは **amq-message-id** で、以下の例のように、値は 「STOMP」 で始まる内部メッセージ ID の String 表現です。

```
amq-message-id : STOMP12345
```

設定で **stompEnableMessageId** が指定されていない場合、デフォルト値は **false** になります。

3.5.3. 接続時間のライブの設定

STOMP クライアントは、接続を閉じる前に **DISCONNECT** フレームを送信する必要があります。これにより、ブローカーはセッションやコンシューマーなどのサーバー側のリソースを閉じることができます。ただし、STOMP クライアントが DISCONNECT フレームを送信せずに終了する場合、または失敗すると、ブローカーにはクライアントが有効であるかどうかを即座に認識することができません。そのため、STOMP の接続は TTL(Time to Live) が 1 分となるように設定されています。複数の 1 分間の間アイドル状態であった場合、ブローカーは STOMP クライアントへの接続を停止します。

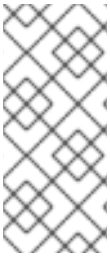
手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

2. 以下の例のように、STOMP 接続に使用される **acceptor** の URI に **connectionTTL** パラメーターを追加します。

```
<acceptors>
  <acceptor name="stomp-acceptor">tcp://localhost:61613?
protocols=STOMP;connectionTTL=20000</acceptor>
  ...
</acceptors>
```

上記の例では、stomp **-acceptor** を使用するすべての stomp 接続では、その TTL を 20 秒に設定します。



注記

STOMP プロトコルのバージョン 1.0 には ハートビートフレーム が含まれていません。そのため、ユーザーは、データが connection-ttl 内に送信されることを確認するか、ブローカーがクライアントが停止されサーバー側のリソースをクリーンアップすることを想定します。バージョン 1.1 では、c he-beats を使用して stomp 接続のライフサイクルを維持することができます。

ブローカーのデフォルト時間の上書き
前述のように、STOMP 接続のデフォルトの TTL は 1 分です。この値は、**connection-ttl-override** 属性をブローカー設定に追加することで上書きできます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

2. **connection-ttl-override** 属性を追加し、新しいデフォルトの値をミリ秒単位で指定します。以下のように、**<core>** スタンザに属します。

```
<configuration ...>
  ...
  <core ...>
    ...
    <connection-ttl-override>30000</connection-ttl-override>
    ...
  </core>
<configuration>
```

上記の例では、STOMP 接続のデフォルトの Time to Live(TTL) は 30 秒 (**30000** ミリ秒) に設定されます。

3.5.4. JMS からの STOMP メッセージの送受信

STOMP は主にテキスト指向のプロトコルです。JMS と相互運用を容易にするため、STOMP 実装は **content-length** ヘッダーの有無を確認し、STOMP メッセージを JMS にマップする方法を決定します。

STOMP のメッセージを…にマッピングしたい場合。	メッセージは下記の通りにしてください。
JMS TextMessage	**content-length** ヘッダーを**含めないでください**。
JMS BytesMessage	**content-length** ヘッダーを**含めます**。

JMS メッセージを STOMP にマップする場合も、同じロジックが適用されます。STOMP クライアントは、**content-length** ヘッダーが存在することを確認して、メッセージボディーのタイプ (文字列またはバイト) を判別できます。

メッセージヘッダーの詳細については、STOMP 仕様を参照してください。

3.5.5. STOMP 宛先の AMQ Broker アドレスおよびキューへのマッピング

メッセージを送信してサブスクライブする場合、STOMP クライアントには通常、**destination** ヘッダーが含まれます。宛先名は文字列の値で、ブローカーの宛先にマッピングされます。AMQ Broker では、これらの宛先は **アドレス** および **キュー** にマッピングされます。宛先フレームの詳細は、STOMP 仕様を参照してください。

たとえば、以下のメッセージ (ヘッダーおよびボディー) を送信する STOMP クライアントの例を考えます。

```
SEND
destination:/my/stomp/queue

hello queue a
^@
```

この場合、ブローカーは **/my/stomp/queue** アドレスに関連付けられたキューへメッセージを転送します。

たとえば、STOMP クライアントが (**SEND** フレームを使用して) メッセージを送信する場合、指定された宛先がアドレスにマッピングされます。

これは、クライアントが **SUBSCRIBE** または **UNSUBSCRIBE** フレームを送信する場合 と同じように機能しますが、この場合は AMQ Broker は **destination** をキューにマッピングします。

```
SUBSCRIBE
destination: /other/stomp/queue
ack: client

^@
```

上記の例では、ブローカーは **destination** を キュー **/other/stomp/queue** にマップします。

STOMP 宛先と JMS 宛先のマッピング
JMS 宛先は、ブローカーアドレスおよびキューにマッピングされます。STOMP を使用してメッセージを JMS 宛先に送信する場合、STOMP 宛先は同じ規則に従う必要があります。

- JMS **Queue** を送受信するには、**jms.queue.** でキュー名を追加します。たとえば、JMS キューの **orders** にメッセージを送信するには、STOMP クライアントはフレームを送信する必要があります。

```
SEND
destination:jms.queue.orders
hello queue orders
^@
```

- **jms.topic.** でトピック名を追加し、JMS **Topic** を送信またはサブスクライブします。たとえば、**stocks** JMS Topic をサブスクライブするには、STOMP クライアントは以下のようなフレームを送信する必要があります。

```
SUBSCRIBE
destination:jms.topic.stocks
^@
```

第4章 アドレスおよびキューの設定

4.1. アドレス、キュー、およびルーティングタイプ

AMQ Broker では、アドレスモデルには、**addresses**、**queues**、および**routing types**の 3 つの主要な概念で設定されています。

アドレス はメッセージングエンドポイントを表します。設定内では、通常のアドレスには一意の名前、1 つ以上のキュー、およびルーティングタイプが指定されます。

キューがアドレスに関連付けられます。アドレスごとに複数のキューが存在する場合があります。受信メッセージがアドレスにマッチすると、設定されたルーティングタイプに応じて、メッセージは 1 つ以上のキューに送信されます。キューは、自動作成および削除ができるように設定できます。また、アドレス (およびその関連付けられたキュー) を **永続** として設定できます。キューのメッセージも永続永続キューにある限り、永続キューのメッセージも永続し、ブローカーのクラッシュや再起動を保ち続けることができます。一方、非永続キューのメッセージは、メッセージ自体が永続的であっても、ブローカーのクラッシュや再起動は維持されません。

ルーティングタイプ は、アドレスに関連付けられたキューへメッセージが送信される方法を決定します。AMQ Broker では、表に示すように、2 つの異なるルーティングタイプでアドレスを設定できます。

メッセージをルーティング先とルーティングする場合	このルーティングタイプを使用する...
ポイントツーポイントのため、一致するアドレス内の単一キュー。	**anycast**
パブリッシュ/サブスクライブ方式で、一致するアドレス内のすべてのキュー。	**multicast**

注記

アドレスには少なくとも 1 つのルーティングタイプが定義されている必要があります。

アドレスごとに複数のルーティングタイプを定義することも**可能です**が、これは推奨されません。

アドレスに 両方の ルーティングタイプが**定義**されていて、クライアントがどちらかを優先していない場合、ブローカーはデフォルトで **multicast** ルーティングタイプに設定されます。

関連情報

- 設定の詳細については、以下を参照してください。
  - **anycast** ルーティングタイプを使用したポイントツーポイントメッセージング。を参照してください。 「ポイントツーポイントメッセージング用のアドレスの設定」
  - **multicast**「パブリッシュサブスクライブメッセージングのアドレスの設定」

4.1.1. アドレスおよびキューの命名要件

アドレスおよびキューを設定する場合は、以下の要件に注意してください。

- クライアントが使用するワイヤプロトコルに関係なく、クライアントがキューに接続できるようにするには、アドレスおよびキュー名には **以下のいずれの文字も含めないでください。 & :: , ? >**
- 数字記号 (**#**) およびアスタリスク (*) 文字はワイルドカード式用に予約されており、アドレスおよびキュー名で使用しないでください。詳細は、「AMQ Broker ワイルドカード構文」 を参照してください。
- アドレスおよびキュー名にはスペースを含めないでください。
- アドレスまたはキュー名で単語を分離するには、設定した区切り文字を使用します。デフォルトの区切り文字はピリオド (.) です。詳細は、「AMQ Broker ワイルドカード構文」 を参照してください。

4.2. アドレスセットへのアドレス設定の適用

AMQ Broker では、ワイルドカード式を使用して一致するアドレス名を表すことで、**address-setting** 要素に指定された設定をアドレス**セット**に適用することができます。

以下のセクションでは、ワイルドカード式の使用方法を説明します。

4.2.1. AMQ Broker ワイルドカード構文

AMQ Broker は、アドレス設定でワイルドカードを表す特定の構文を使用します。ワイルドカードは、セキュリティー設定やコンシューマーの作成時に使用することもできます。

- ワイルドカード式には、ピリオド (.) で区切られた単語が含まれます。
- 数字記号 (**#**) およびアスタリスク (*) 文字には特別な意味があり、以下のように単語の代わりに使用できます。
  - 数字記号は、ゼロ以上の単語のシーケンスの一致を意味します。式の最後に使用します。
  - アスタリスク文字は単一の単語と一致するを意味します。式内のどこかにこの変数を使用します。

マッチングは文字による文字は実行されませんが、各区切り文字境界では文字ごとに一致します。たとえば、名前に **my** を持つキューと一致するよう設定された **address-setting** 要素は、**myqueue** という名前のキューと **一致しません**。

複数の **address-setting** 要素がアドレスと一致する場合、ブローカーオーバーレイ設定は、ベースラインとして最も具体的な一致の設定を使用します。リテラル式はワイルドカードより固有で、アスタリスク (*) は数値記号 (**#**) より具体的なものです。たとえば、**my.destination** と **my.*** の両方がアドレス **my.destination** と一致します。この場合、ワイルドカード式はリテラルよりも具体的なため、ブローカーは最初に **my.*** にある設定を適用します。次に、ブローカーは **my.destination** アドレス設定要素の設定をオーバーレイし、**my.*** と共有される設定を上書きします。たとえば、以下の設定では、my **.destination** に関連付けられたキューは **max-delivery-attempts** を **3** に設定し、**last-value-queue** を **false** に設定します。

```
<address-setting match="my.*">
   <max-delivery-attempts>3</max-delivery-attempts>
   <last-value-queue>true</last-value-queue>
</address-setting>
<address-setting match="my.destination">
   <last-value-queue>false</last-value-queue>
</address-setting>
```

以下の表に示す例は、ワイルドカードを使用してアドレスセットを照合する方法を示しています。

例	説明
#	**broker.xml** で使用されるデフォルトの **address-setting**。すべてのアドレスに一致します。このキャッチオールを適用するか、必要に応じて各アドレスまたはアドレスグループに新しい **address-setting** を追加することができます。
news.europe.#	**news.europe**、**news.europe.sport**、**news.europe.politics.fr** は一致するが、**news.usa** や **europe** は一致しない。
news.*	**news.europe** と **news.usa** は一致するが、**news.europe.sport** は一致しない。
news.*.sport	**news.europe.sport** と **news.usa.sport** は一致するが、**news.europe.fr.sport** は一致しない。

4.2.2. ブローカーのワイルドカード構文の設定

以下の手順では、ワイルドカードアドレスに使用される構文をカスタマイズする方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以下の例のように、**<wildcard-addresses>** セクションを設定に追加します。

```
<configuration>
 <core>
  ...
  <wildcard-addresses> //
   <enabled>true</enabled> //
   <delimiter>,</delimiter> //
   <any-words>@</any-words> //
   <single-word>$</single-word>
  </wildcard-addresses>
  ...
 </core>
</configuration>
```

enabled

true に設定すると、カスタム設定を使用するようにブローカーに指示します。

delimiter

デフォルトの **.** の代わりに **delimiter** として使用するカスタム文字を指定します 。

any-words

any-words の値として提供された文字は、ゼロ以上の単語のシーケンスに一致し、デフォルトの **#** を置き換えます。式の最後にこの文字を使用します。

single-word

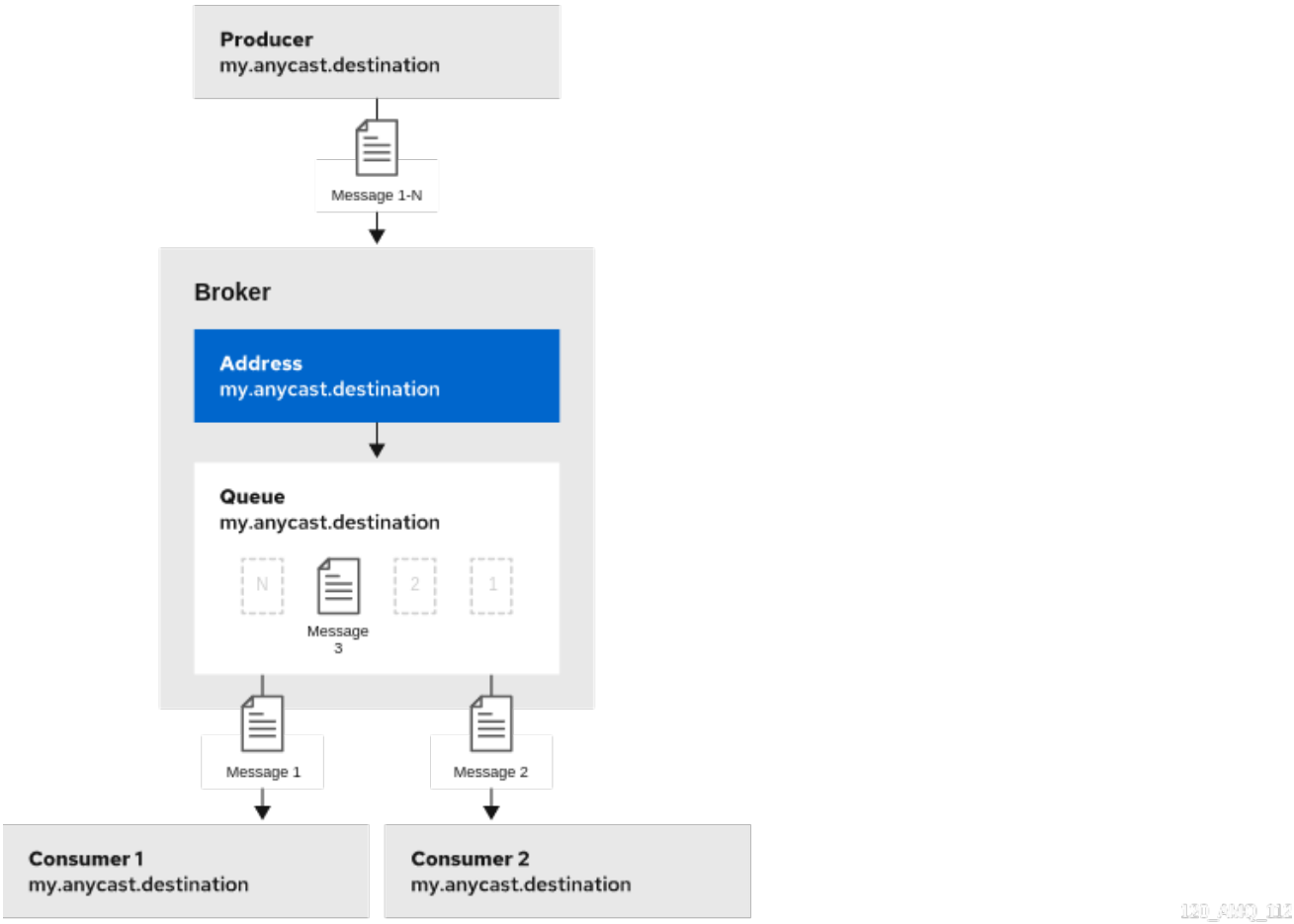
single-word の値として提供された文字は、単一の単語の照合に使用され、デフォルトの * を置き換えます。この文字は式内の任意の場所を使用します。

4.3. ポイントツーポイントメッセージング用のアドレスの設定

ポイントツーポイントメッセージングは、プロデューサーによって送信されたメッセージが 1 つのコンシューマーのみを持つ一般的なシナリオです。AMQP および JMS メッセージプロデューサーおよびコンシューマーは、たとえば、ポイントツーポイントメッセージングキューを使用できます。アドレスに関連付けられたキューがポイントツーポイントでメッセージを受信するようにするには、ブローカー設定で指定の **address** 要素に **anycast** ルーティングタイプを定義します。

anycast を使用してアドレスでメッセージを受信すると、ブローカーはアドレスに関連付けられたキューを見つけ、メッセージへメッセージをルーティングします。その後、コンシューマーはそのキューからメッセージを消費するよう要求される可能性があります。複数のコンシューマーが同じキューに接続する場合、コンシューマーはそれらを同等に処理できる場合、メッセージがコンシューマー間で均等に分散されます。

以下の図は、ポイントツーポイントメッセージングの例を示しています。



4.3.1. 基本的なポイントツーポイントメッセージングの設定

以下の手順は、ポイントツーポイントメッセージングに対して単一のキューを持つアドレスを設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

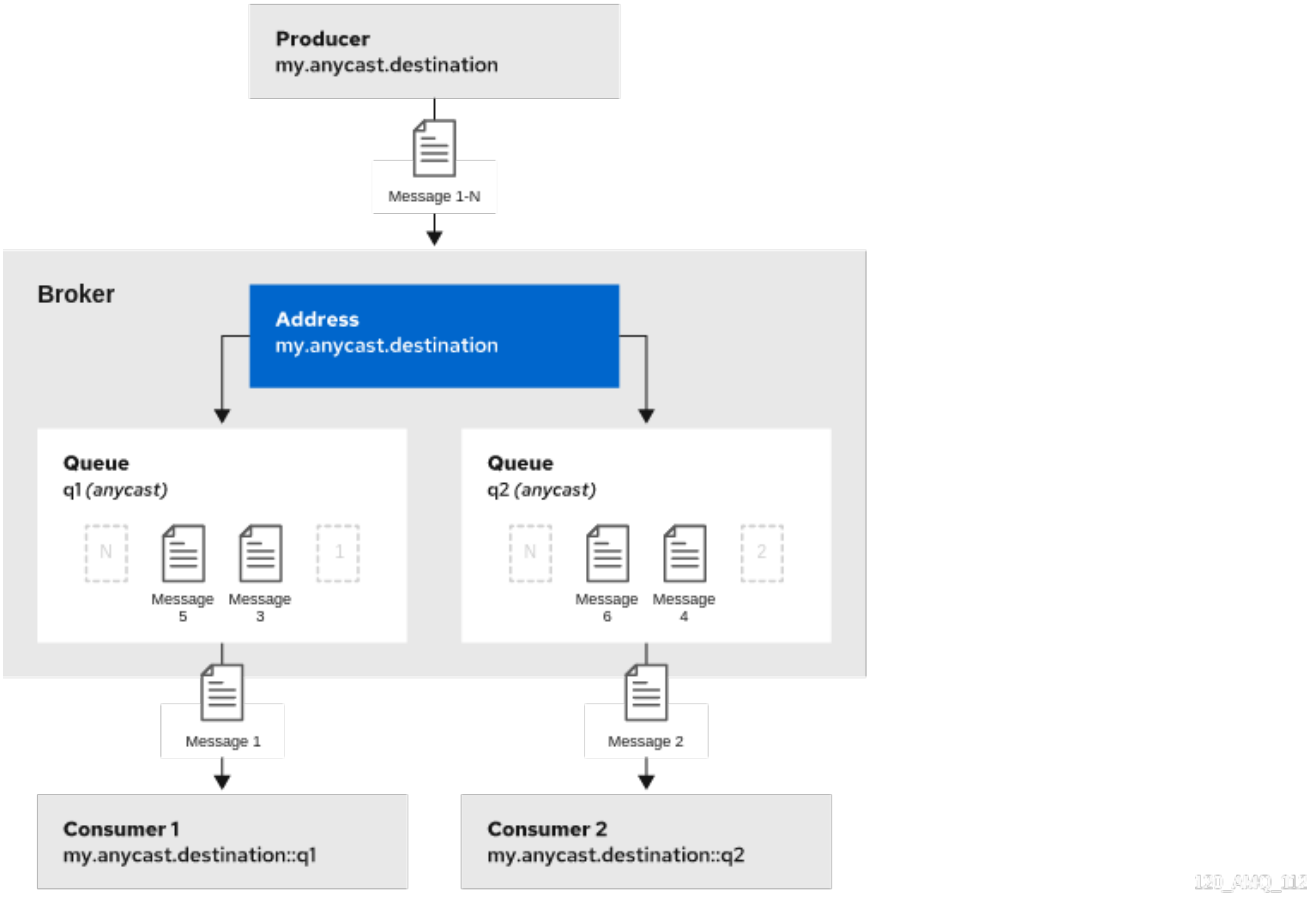
2. **address** の選択された **queue** エレメントの周りに、**anycast** 設定エレメントをラップします。**address** 要素と **queue** 要素の両方の **name** 属性の値が同じであることを確認します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.anycast.destination">
      <anycast>
        <queue name="my.anycast.destination"/>
      </anycast>
    </address>
  </core>
</configuration>
```

4.3.2. 複数のキューのポイントツーポイントメッセージングの設定

anycast ルーティングタイプを使用するアドレスで複数のキューを定義できます。ブローカーは関連するすべてのキューに、**anycast** アドレスに送信されたメッセージを均等に分散します。**Fully Qualified Queue Name**(FQQN) を指定することで、クライアントを特定キューに接続できます。複数のコンシューマーが同じキューに接続する場合、ブローカーはコンシューマー間でメッセージを均等に分散します。

以下の図は、2 つのキューを使用したポイントツーポイントメッセージングの例を示しています。



以下の手順は、複数のキューを持つアドレスにポイントツーポイントメッセージングを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **address** 要素の **queue** 要素で **anycast** 設定要素をラップします。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.anycast.destination">
      <anycast>
        <queue name="q1"/>
        <queue name="q2"/>
      </anycast>
    </address>
  </core>
</configuration>
```

クラスターの複数のブローカーにミラーリングされている設定がある場合、クラスターはプロデューサーおよびコンシューマーへの不透明な方法でポイントツーポイントメッセージングを負荷分散できます。正確な動作は、クラスターに対してメッセージ負荷分散ポリシーの設定方法によって異なります。

関連情報

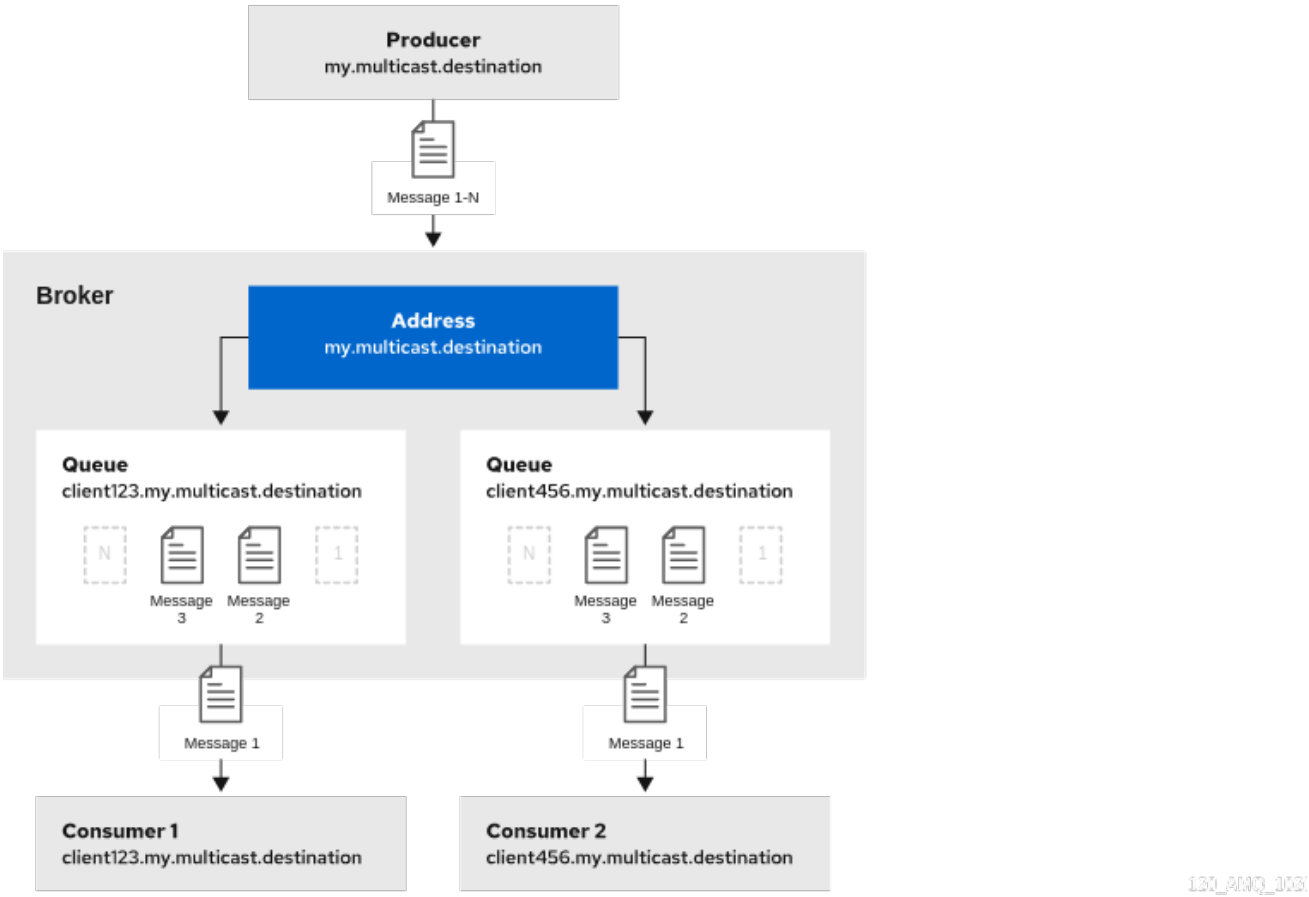
- 詳細情報:
  - 完全修飾キュー名の指定。「完全修飾キュー名の指定」 を参照してください。
  - ブローカークラスターにメッセージの負荷分散を設定する方法は、「ブローカークラスターがメッセージ負荷のバランスを取る方法」 を参照してください。

4.4. パブリッシュサブスクライブメッセージングのアドレスの設定

パブリッシュ/サブスクライブのシナリオでは、メッセージはアドレスにサブスクライブしているすべてのコンシューマーに送信されます。JMS トピックおよび MQTT サブスクリプションは、パブリッシュ/サブスクライブメッセージングの 2 つの例です。アドレスに関連付けられたキューがパブリッシュサブスクライブの方法でメッセージを受信するようにするには、ブローカー設定で指定の **address** 要素に **マルチキャストルーティング** タイプを定義します。

マルチキャスト ルーティング タイプのアドレスでメッセージを受信すると、ブローカーはメッセージのコピーをアドレスに関連付けられた各キューにルーティングします。コピーのオーバーヘッドを減らすために、各キューにはメッセージへの**参照**のみが送信され、完全なコピーは送信されません。

以下の図は、パブリッシュ/サブスクライブメッセージングの例を示しています。



以下の手順は、パブリッシュサブスクライブメッセージングのアドレスを設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 空の **multicast** 設定要素をアドレスに追加します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.multicast.destination">
      <multicast/>
    </address>
  </core>
</configuration>
```

3. (オプション)1 つ以上の **queue** 要素をアドレスに追加し、その中の **multicast** 要素をラップします。ブローカーはクライアントがリクエストする各サブスクリプションのキューを自動的に作成するため、この手順は必要ありません。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.multicast.destination">
      <multicast>
        <queue name="client123.my.multicast.destination"/>
```

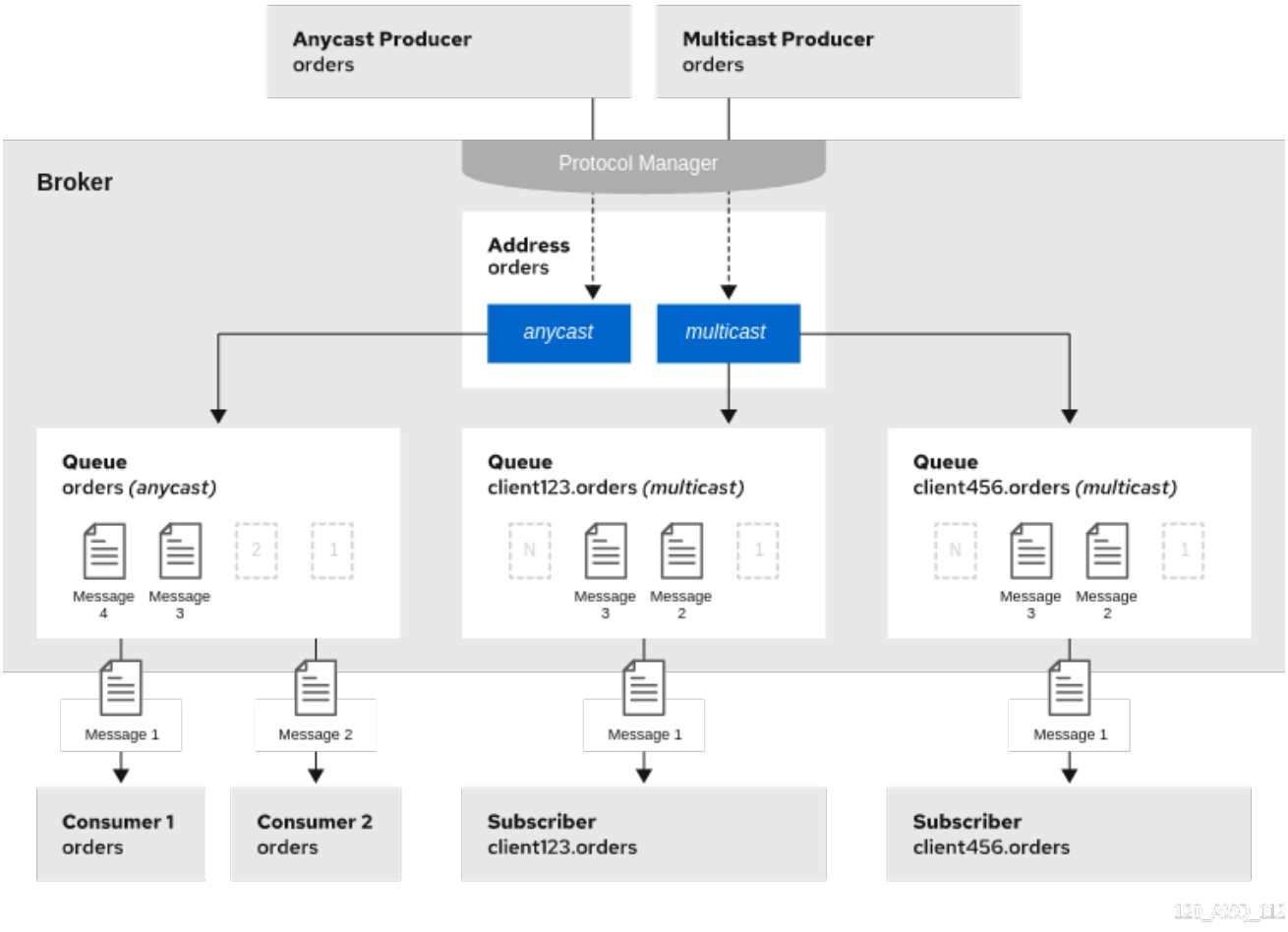
```
        <queue name="client456.my.multicast.destination"/>
      </multicast>
    </address>
  </core>
</configuration>
```

4.5. ポイントツーポイントおよびパブリッシュサブスクライブメッセージング両方のアドレスの設定

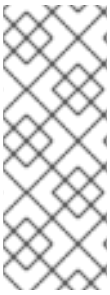
また、ポイントツーポイントとパブリッシュサブスクライブの**両方の**セマンティクスを持つアドレスを設定することもできます。

ポイントツーポイントとパブリッシュ/サブスクライブセマンティクスの両方を使用するアドレスの設定は、通常 **推奨されません**。しかし、例えば、**orders** という名前の JMS キューと、同じく **orders** という名前の JMS トピックが必要な場合には**便利な場合もあります**。異なるルーティングタイプにより、アドレスがクライアント接続で区別されます。このような状況では、JMS キュー・プロデューサーが送信するメッセージは、**anycast** ルーティング・タイプを使用します。JMS トピックプロデューサーによって送信されるメッセージは、**multicast** ルーティング タイプを使用します。JMS トピックコンシューマーがブローカーに接続すると、独自のサブスクリプションキューに割り当てられます。ただし、JMS キューコンシューマーは **anycast** キューに割り当てられます。

以下の図は、ポイントツーポイントおよびパブリッシュサブスクライブメッセージングの例を示しています。



以下の手順は、ポイントツーポイントとパブリッシュ/サブスクライブメッセージングの両方にアドレスを設定する方法を示しています。



注記

このシナリオの動作は、使用されるプロトコルによって異なります。JMS の場合、トピックとキュープロデューサーとコンシューマーの間に明確な区別があり、これによりロジックを簡単に転送できます。AMQP などの他のプロトコルはこの区別を行いません。AMQP 経由で送信されるメッセージは、**anycast** および **multicast** によってルーティングされ、コンシューマーデフォルトは **anycast** です。詳細は、3章ネットワーク接続でのメッセージングプロトコルの設定 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **address** 要素の **queue** 要素で **anycast** 設定要素をラップします。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address name="orders">
      <anycast>
        <queue name="orders"/>
      </anycast>
    </address>
  </core>
</configuration>
```

3. 空の **multicast** 設定要素をアドレスに追加します。

```
<configuration ...>
  <core ...>
    ...
    <address name="orders">
      <anycast>
        <queue name="orders"/>
      </anycast>
      <multicast/>
    </address>
  </core>
</configuration>
```

注記

通常、ブローカーはサブスクリプションキューをオンデマンドで作成します。したがって、**multicast** 要素内に特定のキューを記述する必要はありません。

4.6. アクセプター設定へのルーティングタイプの追加

通常、**anycast** と **multicast** の両方を使用しているアドレスでメッセージを受信した場合、**anycast** のいずれかのキューがメッセージを受信し、**multicast** のすべてのキューが受信します。ただし、クライアントは、アドレスに接続する際に特別な接頭辞を指定して、**anycast** と **multicast** キャストのどちらで接続するかを指定することができます。接頭辞は、ブローカー設定のアクセプターの URL 内の **anycastPrefix** および **multicastPrefix** パラメーターを使用して指定されるカスタム値です。

以下の手順は、特定のアクセプターに接頭辞を設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 特定のアクセプターでは、**anycast** 接頭辞を設定するには、設定済みの URL に **anycastPrefix** を追加します。カスタム値を設定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
      <acceptors>
        <!-- Acceptor for every supported protocol -->
        <acceptor name="artemis">tcp://0.0.0.0:61616?
protocols=AMQP;anycastPrefix=anycast://</acceptor>
      </acceptors>
    ...
  </core>
</configuration>
```

前述の設定により、アクセプタは **anycast** の接頭辞に **anycast://** を使用するように設定されています。クライアントコードは、クライアントが **anycast** キューの 1 つだけにメッセージを送信する必要がある場合は、**anycast://<my.destination>/** を指定できます。

3. 特定のアクセプターでは、**multicast** 接頭辞を設定するには、設定された URL に **multicastPrefix** を追加します。カスタム値を設定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
      <acceptors>
        <!-- Acceptor for every supported protocol -->
        <acceptor name="artemis">tcp://0.0.0.0:61616?
protocols=AMQP;multicastPrefix=multicast://</acceptor>
      </acceptors>
    ...
  </core>
</configuration>
```

前述の設定に基づいて、アクセプターは **multicast** 接頭辞に **multicast://** を使用するよう設定されます。クライアントコードは、クライアントが **multicast** キュー にのみ送信されたメッセージが必要な場合は **multicast://<my.destination>/** を指定できます。

4.7. サブスクリプションキューの設定

ほとんどの場合、サブスクリプションキューを手動で作成する必要はありません。なぜなら、プロトコルマネージャーは、クライアントが最初にアドレスへのサブスクライブを要求したときに、自動的にサブスクリプションキューを作成するからです。詳細は、「プロトコルマネージャーおよびアドレス」 を参照してください。永続サブスクリプションの場合、生成されたキュー名はクライアント ID とアドレスを連結したものです。

以下のセクションでは、必要に応じてサブスクリプションキューを手動で作成する方法を説明します。

4.7.1. 永続サブスクリプションキューの設定

キューが永続サブスクリプションとして設定されると、ブローカーは非アクティブなサブスクライバーのメッセージを格納し、再接続時にサブスクライバーに配信します。そのため、クライアントはサブスクライブ後にキューへ配信される各メッセージを受信することが保証されます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 選択した キューに **永続** 設定要素を追加します。**true** の値を設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.durable.address">
      <multicast>
        <queue name="q1">
          <durable>true</durable>
        </queue>
      </multicast>
    </address>
  </core>
</configuration>
```

注記

キューはデフォルトで永続性があるため、永続性のあるキューを作成するために、**durable** 要素を含めて値を **true** に設定することは、厳密には必要ありません。ただし、要素を明示的に含むと、必要に応じてキューの動作を非永続状態に後で変更できます。

4.7.2. 共有されていない永続的なサブスクリプションキューの設定

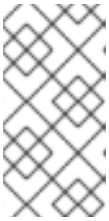
ブローカーは、一度に複数のコンシューマーがキューに接続できないように設定することができます。したがって、この方法で設定したキューのサブスクリプションは、非共有とみなされます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 選択された各キューに **durable** 設定要素を追加します。**true** の値を設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.non.shared.durable.address">
      <multicast>
        <queue name="orders1">
          <durable>true</durable>
        </queue>
        <queue name="orders2">
          <durable>true</durable>
        </queue>
      </multicast>
```

```
    </address>
  </core>
</configuration>
```



注記

キューはデフォルトで永続性があるため、永続性のあるキューを作成するために、**durable** 要素を含めて値を **true** に設定することは、厳密には必要ありません。ただし、要素を明示的に含むと、必要に応じてキューの動作を非永続状態に後で変更できます。

3. 選択した各キューに **max-consumers** 属性を追加します。**1** の値を設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.non.shared.durable.address">
      <multicast>
        <queue name="orders1" max-consumers="1">
          <durable>true</durable>
        </queue>
        <queue name="orders2" max-consumers="1">
          <durable>true</durable>
        </queue>
      </multicast>
    </address>
  </core>
</configuration>
```

4.7.3. 非永続的なサブスクリプションキューの設定

非永続的なサブスクリプションは、通常、一時キューを作成および削除する関連するプロトコルマネージャーによって管理されます。

ただし、非永続サブスクリプションキューのように動作するキューを手動で作成する場合は、キューで **purge-on-no-consumers** 属性を使用できます。**purge-on-no-consumers** が **true** に設定されている場合、コンシューマーが接続されるまでキューはメッセージの受信を開始しません。さらに、最後のコンシューマーがキューから切断されると、キューは **パージ** され ます (つまり、メッセージが削除されます)。キューに新しいコンシューマーがキューに接続するまで、キューはそれ以上のメッセージを受信しません。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 選択した各キューに **purge-on-no-consumers** 属性を追加します。**true** の値を設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.non.durable.address">
      <multicast>
        <queue name="orders1" purge-on-no-consumers="true"/>
      </multicast>
```

```
    </address>
  </core>
</configuration>
```

4.8. アドレスおよびキューの自動作成および削除

アドレスおよびキューを自動的に作成し、使用されなくなったら削除するようにブローカーを設定できます。これにより、クライアントが接続する前に各アドレスを事前に設定する必要がなくなります。

4.8.1. 自動キュー作成および削除用の設定オプション

以下の表は、**address -setting** 要素を設定してキューとアドレス を自動的に作成し、削除する際に利用できる設定要素の一覧です。

address-setting を下記に設定したい場合	この設定を追加してください
クライアントが存在しないアドレスにマッピングされたキューからメッセージを消費するか、または消費しようとするとアドレスを作成します。	**auto-create-addresses**
クライアントがキューからメッセージを消費するか、または消費しようとするとキューを作成します。	**auto-create-queues**
キューがなくなったら、自動的に作成されたアドレスを削除します。	**auto-delete-addresses**
キューのコンシューマー 0 と 0 のメッセージがある場合に、自動作成されたキューを削除します。	**auto-delete-queues**
クライアントが指定しない場合は、特定のルーティングタイプを使用します。	**default-address-routing-type**

4.8.2. アドレスおよびキューの自動作成および削除の設定

以下の手順では、アドレスおよびキューの自動作成および削除を設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 自動作成および削除のための **address-setting** を設定します。以下の例では、前述の表に記載されているすべての設定要素を使用しています。

```
<configuration ...>
 <core ...>
  ...
  <address-settings>
    <address-setting match="activemq.#">
      <auto-create-addresses>true</auto-create-addresses>
      <auto-delete-addresses>true</auto-delete-addresses>
      <auto-create-queues>true</auto-create-queues>
      <auto-delete-queues>true</auto-delete-queues>
      <default-address-routing-type>ANYCAST</default-address-routing-type>
```

```
    </address-setting>
  </address-settings>
  ...
 </core>
</configuration>
```

address-setting

address-setting 要素の設定は、ワイルドカードアドレス **activemq.#** にマッチするすべてのアドレスまたはキューに適用されます。

auto-create-addresses

クライアントが存在しないアドレスへの接続を要求すると、ブローカーはアドレスを作成します。

auto-delete-addresses

自動作成されたアドレスは、キューに関連付けられなくなった時点で削除されます。

auto-create-queues

クライアントが存在しないキューへの接続を要求すると、ブローカーはキューを作成します。

auto-delete-queues

自動作成されたキューは、コンシューマーまたはメッセージがないと削除されます。

default-address-routing-type

クライアントが接続時にルーティングタイプを指定しない場合、ブローカーはアドレスにメッセージを配信する際に **ANYCAST** を使用します。デフォルト値は **MULTICAST** です。

関連情報

- 詳細情報:
  - アドレスの設定時に使用できるワイルドカード構文。「アドレスセットへのアドレス設定の適用」 を参照してください。
  - ルーティングタイプについては、「アドレス、キュー、およびルーティングタイプ」 を参照してください。

4.8.3. プロトコルマネージャーおよびアドレス

protocol manager と呼ばれるコンポーネントは、AMQ Broker アドレスモデル、キューおよびルーティングタイプで使用される概念にプロトコル固有の概念をマッピングします。特定の状況下では、プロトコルマネージャーが自動的にブローカー上にキューを作成することがあります。

例えば、クライアントが **/house/room1/lights** と **/house/room2/lights** のアドレスを持つ MQTT サブスクリプションパケットを送信した場合、MQTT プロトコルマネージャーは、この 2 つのアドレスが **multicast** セマンティクスを必要とすることと理解します。そのため、プロトコルマネージャーはまず、両方のアドレスで **multicast** が有効になっていることを確認します。そうでない場合は、動的に作成を試みます。成功すれば、プロトコル・マネージャーは、クライアントが要求した各サブスクリプションのために特別なサブスクリプションキューを作成します。

各プロトコルの動作は若干異なります。以下の表は、様々なタイプの **queue** へのサブスクライブフレームが要求されたときに、典型的に起こることを説明しています。

キューがこのタイプのものである場合	プロトコルマネージャーの通常のアクションは下記の通りです。
永続性のあるサブスクリプションキュー	適切なアドレスを検索し、**multicast** セマンティクスが有効化されていることを確認します。次に、クライアント ID で特別なサブスクリプションキューとアドレスをその名前として、**multicast** をルーティングタイプとして作成します。 特別な名前を使用すると、プロトコルマネージャーは、必要なクライアントのサブスクリプションキューを迅速に特定し、クライアントの接続を解除し、後で再接続できるようにします。 クライアントがキューのサブスクライブを解除すると、キューが削除されます。
一時サブスクリプションキュー	適切なアドレスを検索し、**multicast** セマンティクスが有効化されていることを確認します。そして、このアドレスの下に、ランダムな (UUID と呼ばれる) 名前のキューを、**multicast** のルーティングタイプで作成します。 クライアントがキューを切断すると、キューが削除されます。
ポイントツーポイントキュー	適切なアドレスを探し、**anycast** ルーティングタイプが有効になっていることを確認します。存在する場合は、アドレスと同じ名前のキューを見つけることを目的としています。存在しない場合は、利用可能な最初のキューを探します。 キューは存在しない場合は自動的に作成されます (これにより、自動作成が有効になっています)。キューコンシューマーはこのキューにバインドされます。 キューが自動作成されると、コンシューマーがなく、メッセージがなければ自動的に削除されます。

4.9. 完全修飾キュー名の指定

内部的には、ブローカーはアドレスのクライアント要求を特定のキューにマッピングします。ブローカーは、メッセージの送信先となるキューまたはメッセージを受信するキューをクライアントに代わって決定します。ただし、より高度なユースケースでは、クライアントが直接キュー名を指定する必要がある場合があります。このような状況では、クライアントは **完全修飾キュー名** (FQQN) を使用できます。FQQN には、**::** で区切られたアドレス名とキュー名の両方が含まれています。

以下の手順では、複数のキューを持つアドレスに接続する際に FQQN を指定する方法を説明します。

前提条件

- 以下の例のように、2 つ以上のキューが設定されているアドレスがあります。

```
<configuration ...>
  <core ...>
    ...
    <addresses>
      <address name="my.address">
        <anycast>
          <queue name="q1" />
          <queue name="q2" />
        </anycast>
      </address>
```

```
    </addresses>
  </core>
</configuration>
```

手順

- クライアントコードで、ブローカーから接続を要求する際に、アドレス名とキュー名の両方を使用します。名前を区切りには、2 つのコロン (**::**) を使用します。以下に例を示します。

```
String FQQN = "my.address::q1";
Queue q1 session.createQueue(FQQN);
MessageConsumer consumer = session.createConsumer(q1);
```

4.10. シャードキューの設定

部分的な順序付けのみが必要とされるキュー全体のメッセージの処理には、**queue sharding**を使用するのが一般的なパターンです。つまり、単一の論理キューとして動作する **anycast** アドレスを定義します。これは、多くの基礎となる物理キューでサポートされます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **address** 要素を追加し、**name** 属性を設定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <addresses>
      <address name="my.sharded.address"></address>
    </addresses>
  </core>
</configuration>
```

3. **anycast** ルーティングタイプを追加し、希望するシャードキューの数を入力します。以下の例では、キュー **q1**、**q2**、**q3** が **エニーキャスト** の宛先として追加されています。

```
<configuration ...>
  <core ...>
    ...
    <addresses>
      <address name="my.sharded.address">
        <anycast>
          <queue name="q1" />
          <queue name="q2" />
          <queue name="q3" />
        </anycast>
      </address>
    </addresses>
  </core>
</configuration>
```

前述の設定に基づき、**my.sharded.address** に送られたメッセージは、**q1**、**q2**、**q3** に均等に配分されます。クライアントは、完全修飾キュー名 (FQQN) の使用時に、特定の物理キューに直接接続して、その特定のキューにのみ送信されたメッセージを受け取ることができます。

特定のメッセージを特定のキューに結びつけるために、クライアントはメッセージごとにメッセージグループを指定できます。ブローカーは、グループ化されたメッセージを同じキューにルーティングし、1 つのコンシューマーはそれをすべて処理します。

関連情報

- 詳細情報:
  - 完全修飾キュー名。「完全修飾キュー名の指定」を参照してください。
  - メッセージのグループ化。AMQ Core Protocol JMS ドキュメントの Using message groups を参照してください。

4.11. 最後の値キューの設定

last value queueとは、同じラストバリューキーの値を持つ新しいメッセージがキューに入ると、キュー内のメッセージを破棄するタイプのキューです。この動作により、最後の値キューは同じキーの最後の値のみを保持します。

最終値キューに対する単純なユースケースは、株式の株価しか監視するためのものです。特定の株式の最新値のみが関心があります。

注記

設定した最後の値キーのないメッセージが最後の値キューに送信される場合、ブローカーはこのメッセージを通常メッセージとして処理します。設定された最後の値キーを持つ新しいメッセージが到達すると、このようなメッセージはキューから消去されません。

最後の値キューを個別に、またはアドレスセットに関連付けられたすべてのキューに設定できます。

以下の手順では、以下の方法で最後の値キューを設定する方法を説明します。

4.11.1. 最後の値キューを個別に設定

以下の手順は、最後の値キューを個別に設定する方法を説明します。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 指定のキューに、**last-value-key** キーを追加し、カスタム値を指定します。以下に例を示します。

```
<address name="my.address">
   <multicast>
      <queue name="prices1" last-value-key="stock_ticker"/>
   </multicast>
</address>
```

3. また、デフォルトのラストバリューキー名 **_AMQ_LVQ_NAME** を使用するラストバリューキューを設定することもできます。これを行うには、与えられたキューに **last-value** のキーを追加します。この値は **true** に設定します。以下に例を示します。

```
<address name="my.address">
   <multicast>
      <queue name="prices1" last-value="true"/>
   </multicast>
</address>
```

4.11.2. アドレスの最後の値キューの設定

次の手順では、アドレスまたは**一連のアドレス**にラストバリューキューを設定します。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **address-setting** 要素に一致するアドレスの場合は、**default-last-value-key** を追加します。カスタム値を指定します。以下に例を示します。

```
<address-setting match="lastValue">
  <default-last-value-key>stock_ticker</default-last-value-key>
</address-setting>
```

   上記の設定に基づいて、**lastValue** アドレスに関連付けられたすべてのキューは、**stock_ticker** の最後の値キーを使用します。デフォルトでは、**default -last-value-key** の値は設定されていません。

3. **一連のアドレス**に対してラストバリューキューを設定するには、アドレスのワイルドカードを指定することができます。以下に例を示します。

```
<address-setting match="lastValue.*">
  <default-last-value-key>stock_ticker</default-last-value-key>
</address-setting>
```

4. または、アドレスに関連付けられたすべてのキューや**一連のアドレス**を設定して、デフォルトの最後の値キー名である **_AMQ_LVQ_NAME** を使用することができます。これを行うには、**default-last-value-key** の代わりに **default-last-value-queue** を追加します。この値は **true** に設定します。以下に例を示します。

```
<address-setting match="lastValue">
  <default-last-value-queue>true</default-last-value-queue>
</address-setting>
```

関連情報

- アドレスの設定時に使用できるワイルドカード構文についての詳細は、「アドレスセットへのアドレス設定の適用」 を参照してください。

4.11.3. 最後の値のキュー動作の例

この例では、最後の値キューの動作を示しています。

broker.xml 設定ファイルで、以下のような設定が追加されているとします。

```
<address name="my.address">
   <multicast>
      <queue name="prices1" last-value-key="stock_ticker"/>
```

```
    </multicast>
  </address>
```

上記の設定では、**prices1** というキューを作成し、最終値のキーを **stock_ticker** としています。

ここで、クライアントが 2 つのメッセージを送信するとします。各メッセージには、プロパティー **stock_ticker** に同じ値 **ATN** があります。各メッセージには **stock_ price** というプロパティーに異なる値があります。各メッセージは、同じキュー **prices1** に送信されます。

```
TextMessage message = session.createTextMessage("First message with last value property set");
message.setStringProperty("stock_ticker", "ATN");
message.setStringProperty("stock_price", "36.83");
producer.send(message);
```

```
TextMessage message = session.createTextMessage("Second message with last value property
set");
message.setStringProperty("stock_ticker", "ATN");
message.setStringProperty("stock_price", "37.02");
producer.send(message);
```

stock_ticker last value キーと同じ値を持つ 2 つのメッセージ (この場合は **ATN**) が **prices1 queue** に到達すると、最新のメッセージのみがキュー内に残り、最初のメッセージがパージされます。コマンドラインで以下の行を入力し、この動作を検証できます。

```
TextMessage messageReceived = (TextMessage)messageConsumer.receive(5000);
System.out.format("Received message: %s\n", messageReceived.getText());
```

この例では、両方のメッセージが最後の値キーに同じ値を使用し、2 番目のメッセージがキューに受信されたため、2 つ目のメッセージが表示されます。

4.11.4. 最後の値キューに対して非破壊的な消費を強制する

コンシューマーがキューに接続すると、通常の動作として、そのコンシューマーに送信されたメッセージがコンシューマーによってのみ取得されます。コンシューマーがメッセージの受信を確認すると、ブローカーはキューからメッセージを削除します。

通常の消費動作の代わりに、**非破壊的な消費を強制するようにキューを設定できます**。この場合、キューがメッセージをコンシューマーに送信すると、他のコンシューマーによってメッセージを受信できます。さらに、コンシューマーが消費した場合でも、メッセージはキューに残ります。このような非破壊的な消費行動を強制する場合、コンシューマーはキュー**ブラウザー**と呼ばれます。

非破壊的な消費を実施すると、キューが特定の最後の値キーに関する最新値を保持するようにするため、最後の値キューでは便利な設定になります。

以下の手順は、最後の値キューに対して非破壊的な消費を強制する方法を示しています。

前提条件

- すでに個別に、あるいは、アドレスや**一連のアドレス**に関連するすべてのキューに対して、最後の値のキューを設定しました。詳細は以下を参照してください。
  - 「最後の値キューを個別に設定」
  - 「アドレスの最後の値キューの設定」

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. キューを最後の値キューとして個別に設定している場合は、**non-destructive** キーを追加します。この値は **true** に設定します。以下に例を示します。

```
<address name="my.address">
  <multicast>
    <queue name="orders1" last-value-key="stock_ticker" non-destructive="true" />
  </multicast>
</address>
```

3. 以前、最後の値キューにアドレスまたは**一連のアドレス** を設定している場合は、**default-non-destructive** キーを追加します。この値は **true** に設定します。以下に例を示します。

```
<address-setting match="lastValue">
  <default-last-value-key>stock_ticker </default-last-value-key>
  <default-non-destructive>true</default-non-destructive>
</address-setting>
```

注記

デフォルトでは、**default-non-destructive** の値は **false** です。

4.12. 期限切れのメッセージを期限切れアドレスに移動する

最後の値キュー以外のキューでは、非破壊的なコンシューマーしかない場合、ブローカーはキューからメッセージを削除できず、キューのサイズが徐々に増加します。キューサイズで制約のない増加を防ぐには、メッセージの有効期限が切れるタイミングを設定し、ブローカーが期限切れのメッセージを移動するアドレスを指定します。

4.12.1. メッセージの有効期限の設定

以下の手順では、メッセージの有効期限を設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素で、**message-expiry-scan-period** を設定して、ブローカーが期限切れのメッセージをスキャンする頻度を指定します。

```
<configuration ...>
  <core ...>
    ...
    <message-expiry-scan-period>1000</message-expiry-scan-period>
    ...
```

前述の設定に基づいて、ブローカーは 1000 ミリ秒ごとに期限切れのメッセージのキューをスキャンします。

3. 一致するアドレスまたは**一連のアドレス**の **address-setting** 要素で、有効期限切れのアドレスを指定します。また、メッセージの有効期限を設定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="stocks">
        ...
        <expiry-address>ExpiryAddress</expiry-address>
        <expiry-delay>10</expiry-delay>
        ...
      </address-setting>
      ...
    <address-settings>
<configuration ...>
```

expiry-address

一致するアドレスや一連のアドレスの有効期限。前述の例では、ブローカーは **stocks** アドレスに対する期限切れメッセージを **ExpiryAddress** と呼ばれる期限切れアドレスに送信します。

expiry-delay

デフォルトの有効期限を使用するメッセージにブローカーが適用される有効期限 (ミリ秒単位)。デフォルトでは、メッセージの有効期限は **0** で、有効期限がないことを意味します。デフォルト以上の有効期限が設定されているメッセージに対しては、**expiry-delay** は効果がありません。
例えば、先ほどの例のように、アドレスの **expiry-delay** を **10** に設定したとします。デフォルトの有効期限が **0** のメッセージがこのアドレスのキューに到着した場合、ブローカーはメッセージの有効期限を **0** から **10** に変更します。しかし、有効期限を **20** に設定している別のメッセージが到着した場合、その有効期限は変更されません。expiry-delay を **-1** に設定した場合、この機能は無効になります。デフォルトでは、**expiry-delay** は **-1** に設定されます。

4. また、**expiry-delay** に値を指定する代わりに、expiry delay の最小値と最大値を指定することもできます。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="stocks">
        ...
        <expiry-address>ExpiryAddress</expiry-address>
        <min-expiry-delay>10</min-expiry-delay>
        <max-expiry-delay>100</max-expiry-delay>
        ...
      </address-setting>
      ...
    <address-settings>
<configuration ...>
```

min-expiry-delay

ブローカーがメッセージに適用される最小有効期限 (ミリ秒単位)。

max-expiry-delay

ブローカーがメッセージに適用される最大有効期限 (ミリ秒単位)。
ブローカーは、以下のように **min-expiry-delay** と **max-expiry-delay** の値を適用します。

- デフォルトの有効期限が **0** のメッセージに対して、ブローカーは有効期限を指定された値の **max-expiry-delay** に設定します。**max-expiry-delay** の値を指定していない場合、ブローカーは指定された **min-expiry-delay** の値に満了時間を設定します。**min-expiry-delay** の値を指定しない場合、ブローカーはメッセージの有効期限を変更しません。
- **max-expiry-delay** の値を上回る有効期限のあるメッセージの場合、ブローカーは有効期限を **max-expiry-delay** の指定値に設定します。
- 有効期限が **min-expiry-delay** の値以下のメッセージに対して、ブローカーは有効期限を指定された **min-expiry-delay** の値に設定します。
- **min-expiry-delay** および **max-expiry-delay** の値の間に有効期限のあるメッセージの場合、ブローカーはメッセージの有効期限を変更しません。
- **expiry-delay** の値 (すなわちデフォルト値の **-1** 以外) を指定すると、**min-expiry-delay** および **max-expiry-delay** に指定する値が上書きされます。
- **min-expiry-delay** と **max-expiry-delay** の両方のデフォルト値は **-1** (つまり無効) です。

5. 設定ファイルの **address** 要素で、以前に **expiry-address** に指定したアドレスを設定します。このアドレスにキューを定義します。以下に例を示します。

```
<addresses>
   ...
   <address name="ExpiryAddress">
      <anycast>
         <queue name="ExpiryQueue"/>
      </anycast>
   </address>
   ...
</addresses>
```

前述の設定例では、期限切れキュー **ExpiryQueue** と期限切れアドレス **ExpiryAddress** を関連付けています。

4.12.2. 期限切れリソースの自動作成

一般的なユースケースとして、期限切れのメッセージを元のアドレスに従って分離することです。例えば、**stocks** というアドレスからの期限切れメッセージを **EXP.stocks** という期限切れキューにルーティングすることを選択したとします。同様に、**orders** というアドレスからの期限切れメッセージを **EXP.orders** という期限切れキューにルーティングする場合もあるでしょう。

このタイプのルーティングパターンにより、期限切れのメッセージを簡単に追跡、検査、および管理できるようになります。ただし、このようなパターンは、主に自動作成されたアドレスおよびキューを使用する環境に実装するのが困難です。このような環境では、管理者は、期限切れのメッセージを保持するためにアドレスおよびキューを手動で作成するために必要な追加の作業を必要としません。

解決策として、特定のアドレスまたは**一連のアドレス** の期限切れのメッセージを処理するように、リソース (すなわちアドレスとキュー) を自動的に作成するようにブローカーを設定できます。以下の手順はその一例です。

前提条件

- 指定したアドレスまたは**一連のアドレス**に対して、すでに有効期限付きのアドレスを設定しています。詳細は、「メッセージの有効期限の設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以前、設定ファイルに追加した **<address-setting>** 要素を探して、一致するアドレスまたは**一連のアドレス**の有効期限を定義します。以下に例を示します。

```
<configuration ...>

  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="stocks">
        ...
        <expiry-address>ExpiryAddress</expiry-address>
        ...
      </address-setting>
      ...
    <address-settings>
<configuration ...>
```

3. **<address-setting>** 要素に、期限切れリソース (すなわちアドレスやキュー) を自動的に作成することや、これらのリソースにどのような名前を付けるかをブローカに指示する設定項目を追加します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="stocks">
        ...
        <expiry-address>ExpiryAddress</expiry-address>
        <auto-create-expiry-resources>true</auto-create-expiry-resources>
        <expiry-queue-prefix>EXP.</expiry-queue-prefix>
        <expiry-queue-suffix></expiry-queue-suffix>
        ...
      </address-setting>
      ...
    <address-settings>
<configuration ...>
```

auto-create-expiry-resources

期限切れのメッセージを受信するため、ブローカーが期限切れアドレスとキューを自動的に作成するかどうかを指定します。デフォルト値は **false** です。
パラメーターの値が **true** に設定されている場合、ブローカーは期限切れアドレスと関連付けられた期限切れキューを定義する **<address>** 要素を自動的に作成します。自動的に作成された **<address>** 要素の名前の値は、**<expiry-address>** に指定された名前の値と一致します。

自動作成された期限切れキューには、**multicast** ルーティングタイプがあります。デフォルトでは、ブローカは失効したメッセージが最初に送信されたアドレス (例えば、**stocks**) と一致するように失効キューに名前を付けています。

ブローカーは、**_AMQ_ORIG_ADDRESS** プロパティーを使用する期限切れキューのフィルターも定義します。このフィルターは、期限切れキューが対応する元のアドレスに送信されるメッセージのみを受け取るようになります。

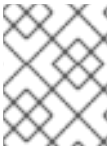
expiry-queue-prefix

ブローカーにより、自動作成された期限切れキューの名前に適用される接頭辞。デフォルト値は **EXP** です。
接頭辞の値を定義した場合、またはデフォルト値を維持した場合、期限切れキューの名前は、接頭辞と元のアドレスを連結したものになります (例: **EXP.stocks**)。

expiry-queue-suffix

ブローカーが自動作成された期限切れキューの名前に適用される接尾辞。デフォルト値は定義されていません (つまり、ブローカーは接尾辞を適用しません)。

キュー名自体を使用して (AMQ Broker Core Protocol JMS クライアントを使用する場合など)、または完全修飾キュー名 (別の JMS クライアントを使用する場合など) を使用して、期限切れキューに直接アクセスできます。



注記

期限切れアドレスとキューは自動的に作成され、自動作成されたアドレスやキューの削除に関連するアドレス設定もこれらの期限切れリソースに適用されます。

関連情報

- 自動作成されたアドレスやキューの自動削除を設定するためのアドレス設定については、「アドレスおよびキューの自動作成および削除の設定」を参照してください。

4.13. 配信されていないメッセージをデッドレターアドレスへ移行

クライアントにメッセージの配信に失敗した場合は、ブローカーがメッセージの配信を継続しようとしない場合があります。無限配信を試行するのを防ぐために、**dead letter address** と 1 つ以上の **dead letter queues**を定義できます。指定の数の配信試行後、ブローカーは元のキューから未配信メッセージを削除し、そのメッセージを設定済みのデッドレターアドレスに送信します。システム管理者は、デッド文字キューから未配信メッセージを後で消費してメッセージを検査できます。

指定のキューにデッドレターアドレスを設定しない場合、ブローカーは指定された数の配信試行後にキューから未配信メッセージを永久に削除します。

デッドレターキューから消費される配信されていないメッセージには、以下のプロパティーがあります。

_AMQ_ORIG_ADDRESS

メッセージの元のアドレスを指定する string プロパティー

_AMQ_ORIG_QUEUE

メッセージの元のキューを指定する string プロパティー

4.13.1. デッドレターアドレスの設定

以下の手順は、デッドレターアドレスと関連するデッドレターキューを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. キュー名と一致する **<address-setting>** 要素で、デッドレターのアドレス名と配信試行回数の最大値を設定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="exampleQueue">
        <dead-letter-address>DLA</dead-letter-address>
        <max-delivery-attempts>3</max-delivery-attempts>
      </address-setting>
    ...
    <address-settings>
<configuration ...>
```

match

ブローカーがこの **address-setting** セクションの設定を適用するアドレス。**<address-setting>** 要素の **match** 属性には、ワイルドカード式を指定できます。ワイルドカード式を使用すると、**<address-setting>** 要素に設定されたデッドレター設定を一致する**一連のアドレス**に関連付ける場合に便利です。

dead-letter-address

デッドレターアドレスの名前。この例では、ブローカーは未配信メッセージをキュー **exampleQueue** から dead letter address(**DLA**) に移動します。

max-delivery-attempts

未配信メッセージを設定済みのデッドレターアドレスに移動するまでの、ブローカーによる配信試行の最大数。この例では、ブローカーは配信に失敗した 3 回失敗した後、未配信メッセージを dead letter address に移動します。デフォルト値は **10** です。ブローカーが再配信の試行を無限にするには、**-1** の値を指定します。

3. **addresses** セクションに、デッドレターアドレス (**DLA**) の **address** 要素を追加します。デッドレターキューをデッドレターアドレスに関連付けるには、**queue** の名前を指定します。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <addresses>
      <address name="DLA">
        <anycast>
          <queue name="DLQ" />
        </anycast>
      </address>
    ...
    </addresses>
  </core>
</configuration>
```

上記の設定では、**DLQ** という名前のデッドレターキューをデッドレターアドレス (**DLA**) に関連付けます。

関連情報

- アドレス設定でワイルドカードを使用する方法は、「アドレスセットへのアドレス設定の適用」 を参照してください。

4.13.2. デッドレターキューの自動作成

一般的なユースケースは、元のアドレスに従って配信されていないメッセージを分離することです。たとえば、**stocks** と呼ばれるアドレスから、**DLQ.stocks** という関連するデッドレターキューを持つ **DLA.stocks** という名前のデッドレターキューに配信されていないメッセージをルーティングすることがあります。同様に、orders と呼ばれるアドレスから **DLA.orders という** デッドレターアドレスに配信されていないメッセージをルーティングする可能性があります。

このタイプのルーティングパターンにより、未配信のメッセージを追跡、検査、および管理が容易になります。ただし、このようなパターンは、主に自動作成されたアドレスおよびキューを使用する環境に実装するのが困難です。このタイプの環境のシステム管理者は、アドレスおよびキューを手動で作成するのに必要な追加の作業を必要としない可能性があります。

解決策として、以下に示すように、未配信メッセージを処理するよう addressees および キューを自動的に作成するようにブローカーを設定できます。

前提条件

- キューまたはキューのセットにデッドレターアドレスがすでに設定されている。詳細は、「デッドレターアドレスの設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一致したキューまたはキューのセットのデッドレターアドレスを定義するために追加した **<address-setting>** 要素を見つけます。以下に例を示します。

```
<configuration ...>
  <core ...>
    ...
    <address-settings>
      ...
      <address-setting match="exampleQueue">
        <dead-letter-address>DLA</dead-letter-address>
        <max-delivery-attempts>3</max-delivery-attempts>
      </address-setting>
    ...
    <address-settings>
<configuration ...>
```

3. **<address-setting>** 要素に、ブローカーに対してデッドレターリソース (アドレスおよびキュー) を自動的に作成し、これらのリソースに名前を付ける設定項目を追加します。以下に例を示します。

```
<configuration ...>
  <core ...>
```

```
      ...
      <address-settings>
        ...
        <address-setting match="exampleQueue">
          <dead-letter-address>DLA</dead-letter-address>
          <max-delivery-attempts>3</max-delivery-attempts>
          <auto-create-dead-letter-resources>true</auto-create-dead-letter-resources>
          <dead-letter-queue-prefix>DLQ.</dead-letter-queue-prefix>
          <dead-letter-queue-suffix></dead-letter-queue-suffix>
        </address-setting>
      ...
      <address-settings>
  <configuration ...>
```

auto-create-dead-letter-resources

ブローカーがデッドレターアドレスおよびキューを自動的に作成し、未配信メッセージを受信するかどうかを指定します。デフォルト値は **false** です。
auto-create-dead-letter-resources が **true** に設定されている場合、ブローカーはデッドレターアドレスと関連するデッドレターキューを定義する **<address>** 要素を自動的に作成します。自動作成された **<address>** 要素の名前は、**<dead-letter-address>** に指定する name の値と一致します。

ブローカーが自動作成された **<address>** 要素で定義するデッドレターキューには、**multicast** ルーティングタイプがあります。デフォルトでは、ブローカーがデッドレターキューに名前を付け、未達のメッセージの元のアドレス (**stocks** など) を照合します。

ブローカーは、**_AMQ_ORIG_ADDRESS** プロパティーを使用するデッドレターキューのフィルターも定義します。このフィルターは、デッドレターキューが対応する元のアドレスに送信されるメッセージのみを受け取るようになります。

dead-letter-queue-prefix

ブローカーにより、自動作成されたデッドレターキューの名前に適用される接頭辞。デフォルト値は **DLQ** です。
接頭辞値を定義するか、デフォルト値を維持する場合、デッドレターキューの名前は接頭辞と元のアドレス (**DLQ.stocks** など) の連結になります。

dead-letter-queue-suffix

ブローカーにより、自動作成されたデッドレターキューに適用される接尾辞。デフォルト値は定義されていません (つまり、ブローカーは接尾辞を適用しません)。

4.14. 期限切れまたは未配信の AMQP メッセージに対するアノテーションおよびプロパティー

ブローカーは、期限切れの AMQP メッセージまたは未配信の AMQP メッセージを、設定した期限切れまたはデッドレターキューに移動する前に、アノテーションおよびプロパティーをメッセージに適用します。クライアントはこれらのプロパティーまたはアノテーションに基づいてフィルターを作成し、期限切れまたはデッドレターキューから消費する特定のメッセージを選択できます。

注記

ブローカーが適用されるプロパティーは **内部** プロパティーです。これらのプロパティーは、通常の使用のためにクライアントに公開されませんが、フィルターのクライアントで指定できます。

以下の表は、ブローカーが期限切れの AMQP メッセージまたは配信されないアノテーションおよび内部プロパティーを表しています。

アノテーション名	内部プロパティー名	説明
x-opt-ORIG-MESSAGE-ID	_AMQ_ORIG_MESSAGE_ID	メッセージが期限切れまたはデッドレターキューに移動される前に、元のメッセージ ID。
x-opt-ACTUAL-EXPIRY	_AMQ_ACTUAL_EXPIRY	最後のエポックの開始からの経過時間 (ミリ秒単位) に指定されたメッセージの有効期限。
x-opt-ORIG-QUEUE	_AMQ_ORIG_QUEUE	期限切れまたは未配信メッセージの元のキュー名。
x-opt-ORIG-ADDRESS	_AMQ_ORIG_ADDRESS	期限切れまたは未配信メッセージの元のアドレス名。

関連情報

- AMQP クライアントがアノテーションに基づいて AMQP メッセージをフィルターするように設定する例は、「アノテーションを基にした AMQP メッセージのフィルター」 を参照してください。

4.15. キューの無効化

ブローカー設定でキューを手動で定義すると、キューはデフォルトで有効になります。

ただし、クライアントがサブスクライブできるようにキューを定義するケースがありますが、メッセージルーティングにキューを使用する準備ができていません。または、キューにメッセージフローを停止しつつも、クライアントをキューにバインドさせる状況もある可能性があります。このような場合は、キューを無効にすることができます。

以下の例は、ブローカー設定で定義したキューを無効にする方法を示しています。

前提条件

- ブローカー設定でアドレスと関連付けられたキューを定義する方法について理解するようにしてください。詳細は、*4章 アドレスおよびキューの設定* を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以前に定義したキューには、**enabled** 属性を追加します。キューを無効にするには、この属性の値を **false** に設定します。以下に例を示します。

```
<addresses>
  <address name="orders">
    <multicast>
      <queue name="orders" enabled="false"/>
```

```
      </multicast>
    </address>
  </addresses>
```

enabled プロパティーのデフォルト値は **true** です。値を **false** に設定すると、メッセージルーティングがキューへ無効になります。

注記

アドレス上のキューを **すべて無効にすると**、そのアドレスに送信されたすべてのメッセージは警告なしで破棄されます。

4.16. キューに接続するコンシューマーの数の制限

max-consumers 属性を使用して、特定のキューに接続するコンシューマーの数を制限します。**max-consumers** フラグを **1** に設定して、排他的コンシューマーを作成します。デフォルト値は **-1** で、無制限のコンシューマーを設定します。

以下の手順では、キューに接続できるコンシューマーの数に制限を設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 指定のキューに、**max-consumers** キーを追加し、値を設定します。

```
<configuration ...>
  <core ...>
    ...
    <addresses>
      <address name="foo">
        <anycast>
          <queue name="q3" max-consumers="20"/>
        </anycast>
      </address>
    </addresses>
  </core>
</configuration>
```

上記の設定に基づいて、同時に 20 のコンシューマーのみが **q3** をキューに接続できます。

3. 排他的コンシューマーを作成するには、**max-consumers** を **1** に設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="foo">
      <anycast>
        <queue name="q3" max-consumers="1"/>
      </anycast>
    </address>
  </core>
</configuration>
```

4. 無制限のコンシューマーを許可するには、**max-consumers** を **-1** に設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="foo">
      <anycast>
        <queue name="q3" max-consumers="-1"/>
      </anycast>
    </address>
  </core>
</configuration>
```

4.17. 排他的キューの設定

排他的キューは、すべてのメッセージを一度に 1 つのコンシューマーにのみルーティングする特別なキューです。この設定は、すべてのメッセージを同じコンシューマーによって順次処理する必要がある場合に便利です。キューに複数のコンシューマーがある場合は、1 つのコンシューマーのみがメッセージを受信します。コンシューマーがキューから切断されると、別のコンシューマーが選択されます。

4.17.1. 排他的キューの個別設定

以下の手順では、特定のキューを個別に排他的に設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 指定されたキューに、**exclusive** キーを追加します。この値は **true** に設定します。

```
<configuration ...>
  <core ...>
    ...
    <address name="my.address">
      <multicast>
        <queue name="orders1" exclusive="true"/>
      </multicast>
    </address>
  </core>
</configuration>
```

4.17.2. アドレスの排他的キューの設定

以下の手順では、関連するすべてのキューが排他的になるようにアドレスまたは**一連のアドレス** を設定する方法を説明します。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一致するアドレスの **address-setting** 要素に **default-exclusive-queue** キーを追加します。この値は **true** に設定します。

```
<address-setting match="myAddress">
    <default-exclusive-queue>true</default-exclusive-queue>
</address-setting>
```

上記の設定に基づいて、**myAddress** に関連付けられたすべてのキューは排他的です。デフォルトでは、**default-exclusive-queue** の値は **false** です。

3. アドレス**セット**に排他的キューを設定するには、アドレスワイルドカードを指定します。以下に例を示します。

```
<address-setting match="myAddress.*">
   <default-exclusive-queue>true</default-exclusive-queue>
</address-setting>
```

関連情報

- アドレスの設定時に使用できるワイルドカード構文についての詳細は、「アドレスセットへのアドレス設定の適用」 を参照してください。

4.18. 一時キューへの特定のアドレス設定の適用

たとえば、JMS を使用する場合、ブローカーはアドレス名とキュー名の両方として汎用一意識別子 (UUID) を割り当て、**一時キュー** を作成します。

デフォルトの **<address-setting match="#">** は、一時的なアドレス設定を含む、設定済みのアドレス設定を **すべてのキューに適用します**。特定のアドレス設定を一時キューのみに適用する場合は、以下で説明されているように **temporary-queue-namespace** をオプションで指定 することができます。次に、namespace に一致するアドレス設定を指定し、ブローカーはそれらの設定をすべての一時キューに適用することができます。

一時キューが作成され、一時キュー namespace が存在する場合、ブローカーは **temporary-queue-namespace** 値と、設定された区切り文字 (デフォルト **.**) をアドレス名に追加します。それを使用して一致するアドレス設定を参照します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **temporary-queue-namespace** 値を追加します。以下は例になります。

```
<temporary-queue-namespace>temp-example</temporary-queue-namespace>
```

3. 一時キューの namespace に対応する **match** 値を使用して **address-setting** 要素を追加します。以下は例になります。

```
<address-settings>
  <address-setting match="temp-example.#">
    <enable-metrics>false</enable-metrics>
  </address-setting>
</address-settings>
```

この例では、ブローカーによって作成されるすべての一時キューのメトリクスを無効にします。

注記

一時的なキュー namespace を指定しても、一時キューには影響を及ぼしません。たとえば、namespace は一時キューの名前を変更しません。名前空間は、一時キューを参照するために使用されます。

関連情報

- アドレス設定でワイルドカードを使用する方法は、「アドレスセットへのアドレス設定の適用」 を参照してください。

4.19. リングキューの設定

通常、AMQ Broker のキューは first-in、first-out(FIFO) セマンティクスを使用します。これは、ブローカーがキューの末尾にメッセージを追加し、それらをヘッドから削除することを意味します。リングキューは、指定された数のメッセージを保持する特別なタイプのキューです。ブローカーは、新規メッセージが到達し、キューがすでに指定された数のメッセージを保持した場合にキューの先頭にメッセージを削除することで、固定キューのサイズを維持します。

たとえば、サイズ **3** で設定されたリングキューと、メッセージ **A**、**B**、**C**、および **D** を順番に送信するプロデューサーについて考えてみます。メッセージ **C** がキューに到達すると、キュー内のメッセージ数が設定済みのリングサイズに達したことになります。この時点で、メッセージ **A** はキューのヘッドにあり、メッセージ **C** はテイールにあります。メッセージ **D** がキューに到達すると、ブローカーはキューの末尾にメッセージを追加します。固定キューサイズを維持するために、ブローカーはキュー (メッセージ **A)** の先頭にメッセージを削除します。メッセージ **B** がキューの先頭にあるようになりました。

4.19.1. リングキューの設定

以下の手順では、リングキューを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 明示的なリングサイズが設定されていない一致するアドレスですべてのキューのデフォルトリングサイズを定義するには、address- **setting** 要素に **default-ring-size** の値を指定します。以下に例を示します。

```
<address-settings>
  <address-setting match="ring.#">
    <default-ring-size>3</default-ring-size>
  </address-setting>
</address-settings>
```

default-ring-size パラメーターは、自動作成されるキューのデフォルトサイズを定義する場合に特に便利です。**default-ring-size** のデフォルト値は **-1**(サイズ制限なし) です。

3. 特定のキューにリングサイズを定義するには、**queue** 要素に **ring-size** キーを追加します。値を指定します。以下に例を示します。

```
<addresses>
  <address name="myRing">
    <anycast>
      <queue name="myRing" ring-size="5" />
```

```
      </anycast>
    </address>
  </addresses>
```

注記

ブローカーの実行中に **ring-size** の値を更新できます。ブローカーは更新を動的に適用します。新しい **ring-size** の値が以前の値よりも小さい場合、ブローカーはキューのヘッドからメッセージをすぐに削除し、新しいサイズを強制しません。キューに送信された新しいメッセージは、古いメッセージの削除を強制的に実行しますが、キューはクライアントによる通常の消費を介して、自然に決まるまで、新しいサイズに到達しません。

4.19.2. リングキューのトラブルシューティング

本セクションでは、リングキューの動作が設定とは異なる状況を説明します。

再配信メッセージおよびロールバック

メッセージがコンシューマーに配信されている場合、メッセージは in-between 状態になります。ここでは、メッセージはキューには技術的には表示されなくなりますが、まだ確認されていません。メッセージは、コンシューマーによって確認されるまで、再配信の状態のままになります。再配信状態のままのメッセージは、リングキューから削除できません。

ブローカーは再配信メッセージを削除できないため、クライアントは許可するリングサイズの設定よりもリングキューにより多くのメッセージを送信できます。たとえば、以下のシナリオについて考えてみましょう。

1. プロデューサーは、**ring-size="3"** で設定したリングキューに 3 つのメッセージを送信します。
2. すべてのメッセージは即座にコンシューマーにディスパッチされます。
   この時点で、**messageCount= 3** および **deliveryCount**= **3** です。
3. プロデューサーは別のメッセージをキューに送信します。その後、メッセージはコンシューマーにディスパッチされます。
   現在、**messageCount** = **4** および **deliveryCount** = **4** です。**4** のメッセージ数は、設定されたリングサイズ **3** を超えています。ただし、ブローカーはキューから再配信メッセージを削除できません。
4. 現在は、メッセージを承認せずにコンシューマーが閉じられているとします。
   この場合、4 つのインポイントで承認されていないメッセージはブローカーにキャンセルされ、消費元の逆順でキューの先頭に追加されます。このアクションにより、設定されたリングサイズにキューが追加されます。リングキューはヘッドでメッセージの末尾にあるメッセージを優先するため、キューは最後のメッセージがキューの先頭に追加されていたため、プロデューサーによって送信された最初のメッセージを破棄します。トランザクションまたはコアセッションのロールバックは同じように処理されます。

コアクライアントを直接使用する場合や、AMQ Core Protocol JMS クライアントを使用する場合は、**consumerWindowSize** パラメーターの値 (デフォルトでは 1024 * 1024 バイト) を減らすことで、配信中のメッセージ数を最小限に抑えることができます。

スケジュールされたメッセージ

スケジュールされたメッセージがキューに送信されると、メッセージは通常のメッセージのようにキューの末尾に即座に追加されません。代わりに、ブローカーはスケジュールされたメッセージを中間バッファーに保持し、メッセージの詳細に従ってキューのヘッドへ配信するようにメッセージをスケ

ジュールします。ただし、スケジュールされたメッセージはキューのメッセージ数に反映されます。再配信メッセージの場合のように、この動作により、ブローカーがリングキューのサイズを強制していないことを確認できます。たとえば、以下のシナリオについて考えてみましょう。

1. 12:00 では、プロデューサーはメッセージ **A** を **ring-size="3"** で設定されたリングキューに送信します。メッセージは 12:05 に対してスケジュールされます。
   この時点で、**messageCount**= **1** および **scheduledCount**= **1** になります。

2. 12:01 では、プロデューサーはメッセージ **B** を同じリングキューに送信します。
   現在、**messageCount**= **2** および **scheduledCount**= **1**。

3. 12:02 では、プロデューサーはメッセージ **C** を同じリングキューに送信します。
   現在、**messageCount**= **3** および **scheduledCount**= **1**。

4. 12:03 時、プロデューサーはメッセージ **D** を同じリングキューに送信します。
   現在、**messageCount**= **4** および **scheduledCount**= **1**。

   キューのメッセージ数は **4** で、設定されたリングサイズから **3 よりも大きい** ようになりました。ただし、スケジュールされたメッセージはキューでは技術的ではありません (つまり、ブローカーにあり、キューに配置するようにスケジュールされています)。スケジュールされた配信時間 12:05 にすると、ブローカーはメッセージをキューのヘッドに配置します。ただし、リングキューが設定サイズをすでに到達しているため、スケジュールされたメッセージ **A** はすぐに削除されます。

ページ化されたメッセージ

スケジュールされたメッセージや配信のメッセージと同様に、ページングされたメッセージは、キューレベルではなく、実際にはアドレスレベルでページングされるため、ブローカーによって実施されるリングキューのサイズにはカウントされません。ページ化されたメッセージはキューでは技術的ではありませんが、キューの **messageCount** 値に反映されます。

リングキューを持つアドレスにはページングを使用しないことが推奨されます。代わりに、アドレス全体をメモリーに収めるようにします。または、 **address-full-policy** パラメーターを **DROP**、**BLOCK** または **FAIL** の値に設定します。

関連情報

- ブローカーは、Retroactive アドレスを設定するときにリングキューの内部インスタンスを作成します。詳細は、「Retroactive アドレスの設定」 を参照してください。

4.20. RETROACTIVE アドレスの設定

アドレスを **retroactive** として設定すると、アドレスに送信されたメッセージを保持することができます。これには、アドレスにキューがバインドされていない場合も含まれます。キューが後に作成され、アドレスにバインドされると、ブローカーはメッセージをこれらのキューにアクティブに配信します。アドレスが **retroactive** として設定されていない場合や、キューがバインドされていない場合、ブローカーはそのアドレスに送信されたメッセージを破棄します。

Retactive アドレスを設定する場合、ブローカーは **ring queue** と呼ばれるタイプのキューの内部インスタンスを作成します。リングキューは、指定された数のメッセージを保持する特別なタイプのキューです。キューが指定されたサイズに達すると、キューに到達する次のメッセージがキューから最も古いメッセージを強制的に強制的に実行します。Retroactive アドレスを設定する場合は、内部リングキューのサイズを間接的に指定します。デフォルトでは、内部キューは **multicast** ルーティングタイプを使用します。

Retactive アドレスによって使用される内部リングキューは、管理 API 経由で公開されます。メトリクスを検査し、キューが空など、その他の一般的な管理操作を実行できます。リングキューは、アドレスの全体的なメモリー使用量にも貢献し、メッセージのページングなどの動作に影響を与えます。

以下の手順では、アドレスを Retroactive として設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **address-setting** 要素で **retroactive-message-count** パラメーターの値を指定します。指定する値は、ブローカーによって保存されるメッセージの数を定義します。以下に例を示します。

```
<configuration>
  <core>
    ...
    <address-settings>
      <address-setting match="orders">
        <retroactive-message-count>100</retroactive-message-count>
      </address-setting>
    </address-settings>
...
  </core>
</configuration>
```

注記

broker.xml 設定ファイルまたは管理 API のいずれかで、ブローカーの実行中に **retroactive-message-count** の値を更新できます。ただし、このパラメーターの値を**減らす** 場合は、Retroactive アドレスがリングキューで実装されるため、追加の手順が必要になります。**ring-size** パラメーターが減少するリングキューは、新しい **ring-size** 値を実現するためにキューからメッセージを自動的に削除しません。この動作は、意図しないメッセージ損失に対する安全なものです。この場合、管理 API を使用してリングキュー内のメッセージ数を手動で減らす必要があります。

関連情報

- リングキューの詳細は、「リングキューの設定」 を参照してください。

4.21. 内部管理のアドレスおよびキューのアドバイザリーメッセージの無効化

デフォルトでは、AMQ Broker は、OpenWire クライアントがブローカーに接続されているときにアドレスおよびキューに関するアドバイザリーメッセージを作成します。アドバイザリーメッセージは、ブローカーによって作成される内部で管理されたアドレスに送信されます。これらのアドレスは、ユーザーがデプロイされたアドレスおよびキューと同じ表示内の AMQ 管理コンソールに表示されます。有用な情報が提供されますが、ブローカーによって多数の宛先を管理する場合に、アドバイザリーメッセージにより不要な結果が生じる可能性があります。たとえば、メッセージはメモリー使用量やステンケーション接続リソースを増やす可能性があります。また、アドバイザリーメッセージを送信するために作成されたすべてのアドレスを表示しようとすると、AMQ 管理コンソールが明確になる可能性があります。このような状況を回避するには、以下のパラメーターを使用して、ブローカーでアドバイザリーメッセージの動作を設定できます。

supportAdvisory

アドバイザリーメッセージの作成を有効にするには、このオプションを **true false** に設定します。デフォルト値は **true** です。

suppressInternalManagementObjects

このオプションを **true** に設定して、アドバイザリーメッセージを JMX レジストリーや AMQ 管理コンソールなどの管理サービスに公開し、**false** に設定して公開しないようにします。デフォルト値は **true** です。

以下の手順では、ブローカーでアドバイザリーメッセージを無効にする方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. OpenWire コネクターの場合は、**supportAdvisory** パラメーターおよび **suppressInternalManagementObjects** パラメーターを設定済みの URL に追加します。本セクションで説明されているように値を設定します。以下に例を示します。

```
<acceptor name="artemis">tcp://127.0.0.1:61616?
protocols=CORE,AMQP,OPENWIRE;supportAdvisory=false;suppressInternalManagementObje
cts=false</acceptor>
```

4.22. アドレスおよびキューのフェデレーション

フェデレーションにより、ブローカーを共通のクラスターに入れることなく、ブローカー間のメッセージの転送が可能になります。ブローカーはスタンドアロンまたは個別のクラスターになります。さらに、ソースおよびターゲットブローカーはさまざまな管理ドメインに配置できます。つまり、ブローカーには異なる設定、ユーザー、およびセキュリティー設定を指定できます。ブローカーは、異なるバージョンの AMQ Broker を使用している場合もあります。

たとえば、フェデレーションは、メッセージをあるクラスターから別のクラスターへ確実に送信するのに適しています。この送信は、大規模なエリアネットワーク (WAN)、クラウドインフラストラクチャーの **リージョン**、またはインターネット上である可能性があります。ソースブローカーからターゲットブローカーへの接続が失われた場合 (ネットワーク障害などの理由により)、ソースブローカーはターゲットブローカーがオンラインに戻るまで接続を再確立しようとします。ターゲットブローカーがオンラインに戻ると、メッセージ送信が再開します。

管理者は、アドレスポリシーおよびキューポリシーを使用してフェデレーションを管理できます。ポリシー設定は特定のアドレスまたはキューに一致させることができます。また、ポリシーには、アドレスまたは **キューのセット**に対して設定に一致するワイルドカード式を含めることができます。そのため、フェデレーションは、一致するセットからキューまたはアドレスが追加されるか、または削除されるため、動的に適用できます。ポリシーには、特定のアドレスやキューを含む、または除外する **複数の式**を含めることができます。さらに、複数のポリシーをブローカーまたはブローカークラスターに適用できます。

AMQ Broker では、2 つの主なフェデレーションオプションは **アドレスフェデレーション** と **キューフェデレーション**です。これらのオプションは、これ以降のセクションで説明します。

注記

ブローカーには、**フェデレーションされたコンポーネントおよびローカルのみのコンポーネント**の設定を含めることができます。つまり、ブローカーでフェデレーションを設定する場合は、そのブローカーですべてをフェデレーションする必要はありません。

4.22.1. アドレスフェデレーションについて

アドレスのフェデレーションは、接続されたブローカー間の完全なマルチキャスト分散パターンと似ています。たとえば、**BrokerA** のアドレスに送信されたすべてのメッセージは、そのブローカーのすべてのキューに送信されます。さらに、各メッセージは **BrokerB** および割り当てられたすべてのキューに配信されます。

アドレスフェデレーションは、ブローカーを動的にリモートブローカーのアドレスにリンクします。たとえば、ローカルブローカーがリモートブローカーのアドレスからメッセージをフェッチする場合は、リモートアドレスにキューが自動的に作成されます。その後、リモートブローカーのメッセージはこのキューによって使用されます。最後に、メッセージは最初にローカルアドレスに直接公開されていましたが、メッセージはローカルブローカーの対応するアドレスにコピーされます。

フェデレーションがアドレスを作成できるように、リモートブローカーを再設定する必要はありません。ただし、ローカルブローカーには リモートアドレスに対するパーミッションを**付与する必要があります**。

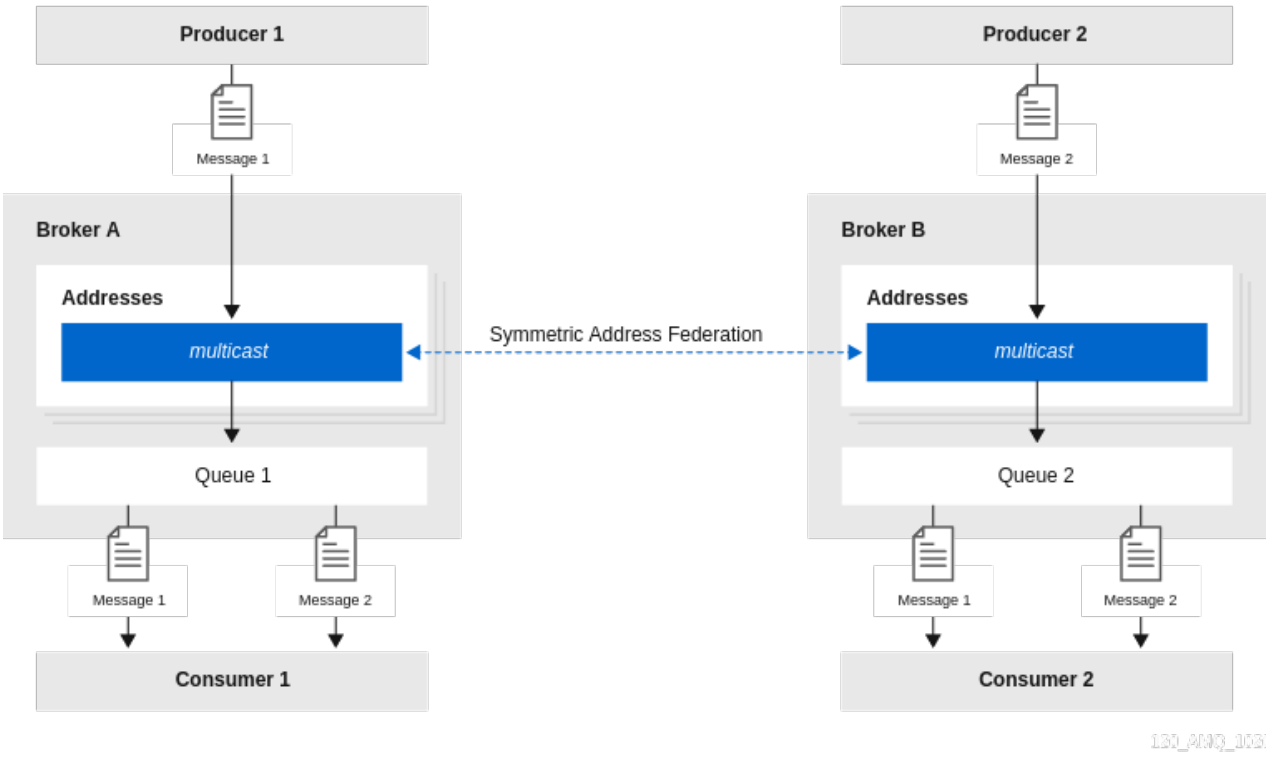
4.22.2. アドレスフェデレーションの一般的なトポロジー

アドレスフェデレーションを使用する一般的なトポロジーの一部を以下に示します。

対称トポロジー

対称トポロジーでは、プロデューサーとコンシューマーは各ブローカーに接続されます。キューとそのコンシューマーは、いずれかのプロデューサーによって公開されるメッセージを受信できます。対称トポロジーの例を以下に示します。

図4.1 対称トポロジーにおけるアドレスフェデレーション

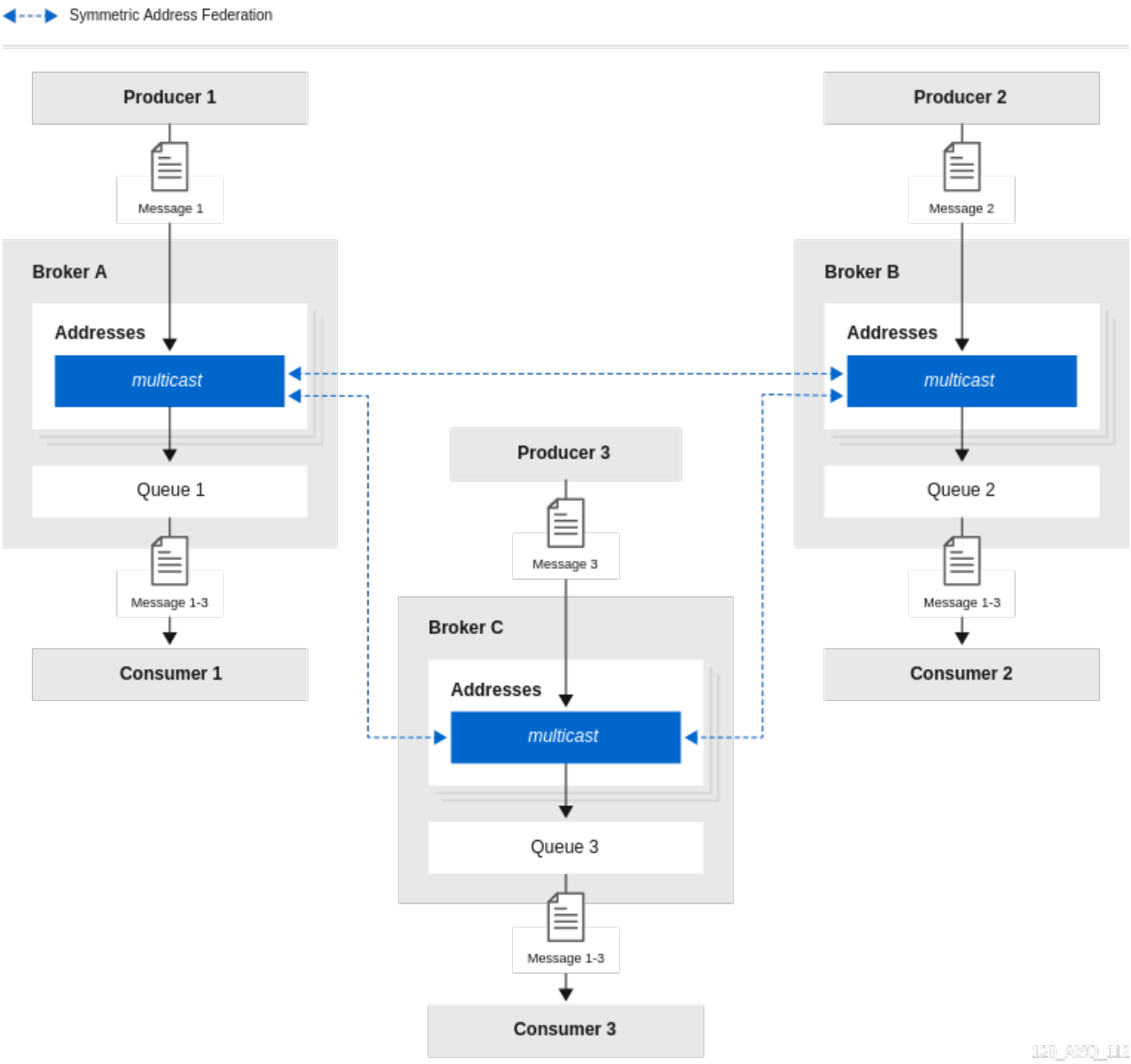


対称トポロジーのアドレスフェデレーションを設定する場合は、アドレスポリシーの **max-hops** プロパティーの値を **1** に設定することが重要です。これにより、メッセージが **1回だけ** コピーされ、cyclic レプリケーションは回避されます。このプロパティーを大きな値に設定すると、コンシューマーは同じメッセージの複数のコピーを受け取ります。

完全なメッシュトポロジー

完全なメッシュトポロジーは対称設定と似ています。3 つ以上のブローカーは相互に対称的に分散し、完全なメッシュを作成します。この設定では、プロデューサーとコンシューマーは各ブローカーに接続されます。キューとそのコンシューマーは任意のプロデューサーによって公開されるメッセージを受信できます。このトポロジーの例を以下に示します。

図4.2 完全なメッシュトポロジーにおけるアドレスフェデレーション

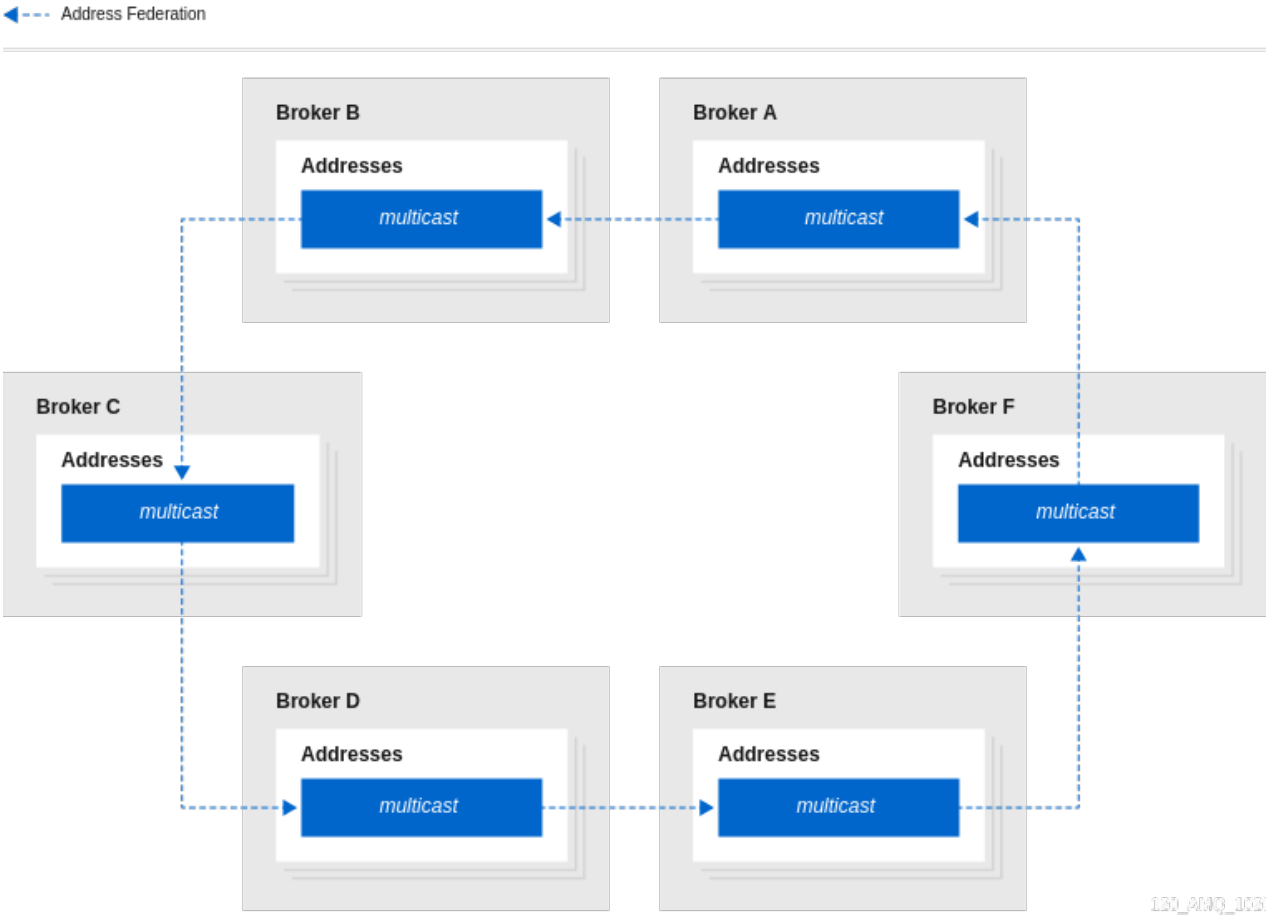


対称設定の場合、完全なメッシュトポロジーのアドレスフェデレーションを設定する場合は、アドレスポリシーの **max-hops** プロパティーの値を **1** に設定することが重要です。これにより、メッセージが **1回だけ** コピーされ、cyclic レプリケーションは回避されます。

リングトポロジー

ブローカーのリングでは、各フェデレーションされたアドレスは、リング内の 1 つだけに対してアップストリームになります。このトポロジーの例を以下に示します。

図4.3 リングトポロジーにおけるアドレスフェデレーション



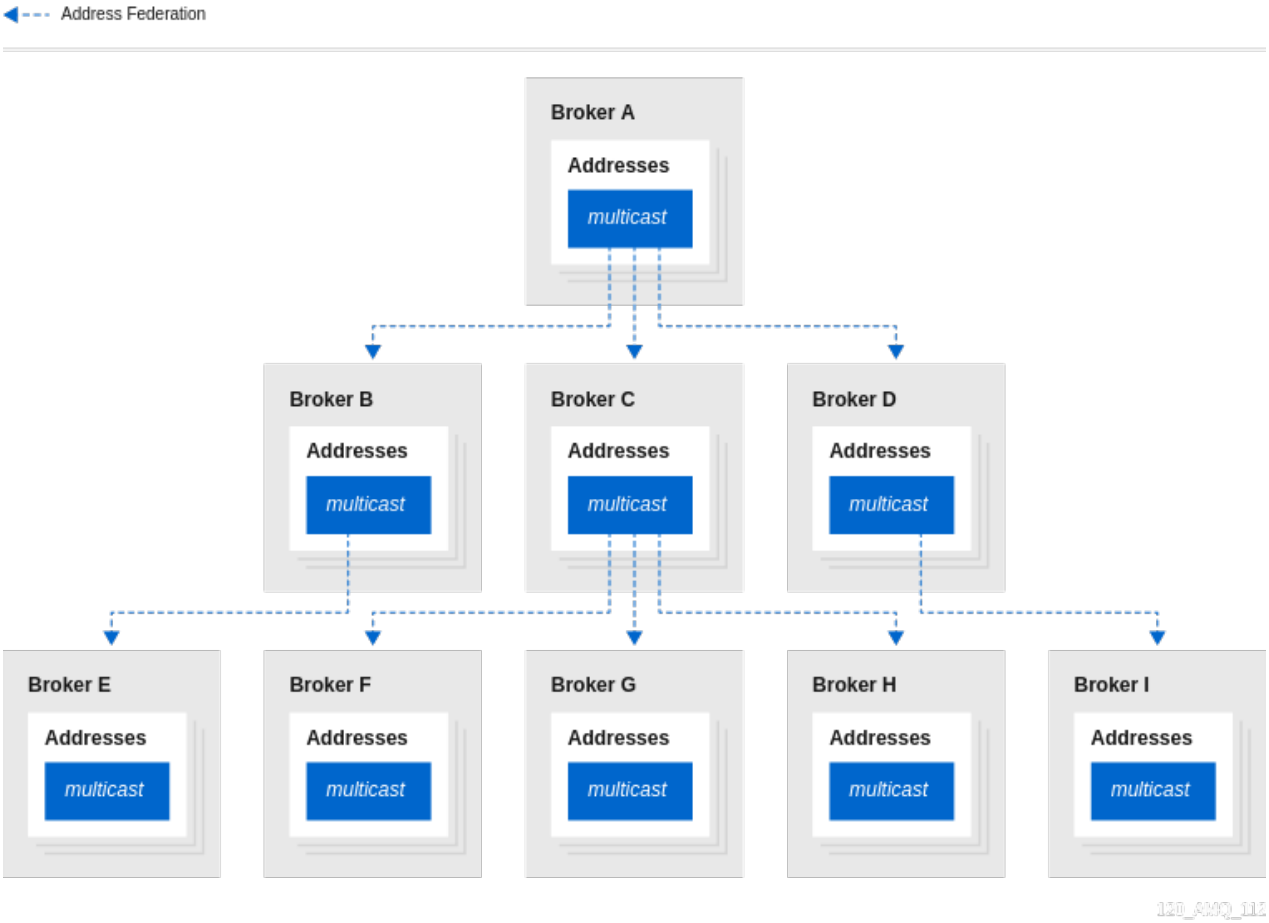
リングトポロジーのフェデレーションを設定する場合は、循環レプリケーションを回避するために、アドレスポリシーの **max-hops** プロパティーを **n-1** の値に設定することが重要です。ここで、nはリング内のノード数になります。たとえば、上記のリングトポロジーでは、**max-hops** の値は **5** に設定されます。これにより、リング内のすべてのアドレスがメッセージが **1度だけ** 見えるようになります。

リングトポロジーの利点は、必要な物理接続の数において、チャイルがセットアップすることです。ただし、このタイプのトポロジーの欠点は、1つのブローカーが失敗した場合にリング全体が失敗することです。

fan-out トポロジー

ファンアウトトポロジーでは、単一のマスターアドレスはフェデレーションされたアドレスのツリーによってリンクされます。マスターアドレスに公開されたすべてのメッセージは、ツリー内の任意のブローカーに接続しているすべてのコンシューマーによって受信できます。ツリーは、深さに設定できます。ツリー内に既存のブローカーを再設定しなくても、ツリーを拡張することもできます。このトポロジーの例を以下に示します。

図4.4 ファンアウトトポロジーでのアドレスフェデレーション



ファンアウトトポロジーのフェデレーションを設定する場合は、アドレスポリシーの **max-hops** プロパティーを **n-1** の値に設定します。ここで、n ツリー内のレベル数になります。たとえば、上記の fan-out トポロジーでは、**max-hops** の値は **2** に設定されます。これにより、ツリー内のすべてのアドレスがメッセージが **1度だけ** 見えるようになります。

4.22.3. アドレスフェデレーション設定での迂回バインディングのサポート

アドレスフェデレーションを設定する際に、アドレスポリシー設定に迂回バインディングのサポートを追加できます。このサポートを追加すると、フェデレーションが迂回バインディングに応答し、リモートブローカーの指定のアドレスのフェデレーションされたコンシューマーを作成できます。

たとえば、**test.federation.source** というアドレスがアドレスポリシーに含まれ、**test.federation.target** という別のアドレスが含まれていない場合は、通常、キューが **test.federation.target** に作成されると、アドレスポリシーの一部ではないため、**フェデレーションされたコンシューマーが作成されません**。ただし、**test.federation.source がソースアドレスで test.federation.target** が転送アドレスに、永続コンシューマーを作成すると、転送アドレスに永続コンシューマーが作成されます。ソースアドレスは引き続き **multicast** ルーティングタイプを使用する必要がありますが、ターゲットアドレスは **multicast** または **anycast** を使用できます。

ユースケースの例は、JMS トピック (**multicast** アドレス) を JMS キュー (**anycast** アドレス) にリダイレクトする迂回です。これにより、JMS 2.0 および共有サブスクリプションをサポートしないレガシーコンシューマーのトピックへのメッセージの負荷分散が可能になります。

4.22.4. ブローカークラスターのフェデレーションの設定

以下のセクションの例では、standaloneローカルブローカーとリモートブローカーとの間でアドレスとキューのフェデレーションを設定する方法について示しています。スタンドアロンブローカー間のフェデレーションの場合、フェデレーション設定の名前、およびアドレスおよびキューポリシー名はローカルブローカーとリモートブローカー間で一意である必要があります。

ただし、clusterでブローカーのフェデレーションを設定する場合は、追加の要件があります。クラスター化されたブローカーでは、フェデレーション設定の名前と、その設定内のアドレスおよびキューポリシーの名前 が、クラスター内の各ブローカーで**同じである必要があります**。

同じクラスターのブローカーが同じフェデレーション設定およびアドレスおよびキューポリシー名を使用するようにし、メッセージの重複を回避します。たとえば、同じクラスター内のブローカーに**異なるフェデレーション設定名がある場合**、複数の方法で名前が異なる転送キューが作成される場合があり、ダウンストリームのコンシューマーでメッセージの重複が生じます。一方、同じクラスターのブローカーが**同じフェデレーション設定名**を使用する場合、基本的にはダウンストリームのコンシューマーに負荷分散される複製された、クラスター転送キューを作成します。これにより、メッセージの重複が回避されます。

4.22.5. アップストリームのアドレスフェデレーションの設定

以下の例は、スタンドアロンブローカー間でアップストリームのアドレスフェデレーションを設定する方法を示しています。この例では、ローカル (つまり**ダウンストリーム**) ブローカーから一部のリモート (つまり**アップストリーム**) ブローカーへのフェデレーションを設定します。

前提条件

- 以下の例は、スタンドアロンブローカー間でアドレスフェデレーションを設定する方法を示しています。ただし、ブローカー **クラスター** のフェデレーションを設定するための要件も理解している必要があります。詳細は、「ブローカークラスターのフェデレーションの設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<federation>** 要素が含まれる新しい **<federations >** 要素を追加します。以下に例を示します。

```
<federations>
  <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">
  </federation>
</federations>
```

name

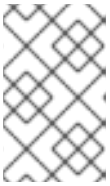
フェデレーション設定の名前。この例では、名前はローカルブローカーの名前に対応します。

user

アップストリームブローカーに接続するための共有ユーザー名。

password

アップストリームブローカーに接続するための共有パスワード。



注記

ユーザーとパスワードの認証情報がリモートブローカーごとに異なる場合は、設定に追加する時にこれらのブローカーの認証情報を個別に指定できます。これは、この手順の後半で説明します。

3. **federation** 要素内に **<address-policy>** 要素を追加します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <address-policy name="news-address-federation" auto-delete="true" auto-delete-
delay="300000" auto-delete-message-count="-1" enable-divert-bindings="false" max-
hops="1" transformer-ref="news-transformer">
      </address-policy>

   </federation>
</federations>
```

name

アドレスポリシーの名前。ブローカーに設定されるアドレスポリシーはすべて一意の名前を指定する必要があります。

auto-delete

アドレスのフェデレーション時に、ローカルブローカーはリモートアドレスに永続キューを動的に作成します。**auto-delete** プロパティーの値は、ローカルブローカーの切断後にリモートキューを削除するかどうかを指定します。また、**auto-delete-delay** および **auto-delete-message-count** プロパティーの値も到達するかどうかを指定します。動的に作成されたキューのクリーンアップを自動化する場合に便利なオプションです。また、ローカルブローカーが長時間切断されている場合に、リモートブローカーでメッセージをビルドできないようにする場合にも便利なオプションです。ただし、接続されていない間にメッセージをローカルブローカーに対して常にキューに入れる必要がある場合、このオプションを **false** に設定します。これにより、ローカルブローカーでメッセージが失われないようにします。

auto-delete-delay

ローカルブローカーが切断されると、このプロパティーの値は、動的に作成されるリモートキューが自動的に削除されるまでの時間 (ミリ秒単位) を指定します。

auto-delete-message-count

ローカルブローカーが切断されると、このプロパティーの値は、キューが自動的に削除される前に動的に作成されたリモートキューにあるメッセージの最大数を指定します。

enable-divert-bindings

このプロパティーを **true** に設定すると、迂回バインディングは必要に応じてリッスンできます。アドレスポリシーに含まれるアドレスに一致するアドレスを持つ迂回バインディングがある場合、迂回の転送アドレスに一致するキューバインディングは要求を作成します。デフォルト値は **false** です。

max-hops

フェデレーション中にメッセージが実行できるホップの最大数。特定のトポロジーでは、このプロパティーに特定の値が必要です。これらの要件の詳細は、「アドレスフェデレーションの一般的なトポロジー」 を参照してください。

transformer-ref

トランスフォーマー設定の名前。フェデレーションされたメッセージ送信時にメッセージを変換したい場合は、トランスフォーマー設定を追加することができます。トランスフォーマー設定は、この手順の後半で説明します。

4. **<address-policy>** 要素内に、アドレスポリシーからアドレスを追加し、アドレスを除外するためのアドレス一致パターンを追加します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <address-policy name="news-address-federation" auto-delete="true" auto-delete-
delay="300000" auto-delete-message-count="-1" enable-divert-bindings="false" max-
hops="1" transformer-ref="news-transformer">

         <include address-match="queue.bbc.new" />
         <include address-match="queue.usatoday" />
         <include address-match="queue.news.#" />

         <exclude address-match="queue.news.sport.#" />
      </address-policy>

   </federation>
</federations>
```

include

この要素の **address-match** プロパティーの値は、アドレスポリシーに含めるアドレスを指定します。**queue.bbc.new** や **queue.usatoday** など、正確なアドレスを指定できます。または、ワイルドカード式を使用して一致するアドレスの **セット** を指定できます。上記の例では、アドレスポリシーには文字列 **queue.news で始まるすべての アドレス名も含まれています**。

exclude

この要素の **address-match** プロパティーの値は、アドレスポリシーから除外するアドレスを指定します。正確なアドレス名を指定するか、ワイルドカード式を使用して一致するアドレスの **セット** を指定できます。上記の例では、アドレスポリシーは文字列 **queue.news.sport** で始まる**すべてのアドレス名**を除外します。

5. (任意)**federation** 要素 では、 **transformer** 要素を追加してカスタムトランスフォーマー実装を参照します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <address-policy name="news-address-federation" auto-delete="true" auto-delete-
delay="300000" auto-delete-message-count="-1" enable-divert-bindings="false" max-
hops="1" transformer-ref="news-transformer">

         <include address-match="queue.bbc.new" />
         <include address-match="queue.usatoday" />
         <include address-match="queue.news.#" />

         <exclude address-match="queue.news.sport.#" />
      </address-policy>
```

```
        <transformer name="news-transformer">
           <class-name>org.foo.NewsTransformer</class-name>
           <property key="key1" value="value1"/>
           <property key="key2" value="value2"/>
        </transformer>

     </federation>
</federations>
```

name

トランスフォーマー設定の名前。この名前は、ローカルブローカーで一意である必要があります。これは、アドレスポリシーの **transformer-ref** プロパティーの値として指定する名前です。

class-name

org.apache.activemq.artemis.core.server.transformer.Transformer インターフェイスを実装するユーザー定義クラスの名前。
トランスフォーマーの **transform()** メソッドは、メッセージが送信される前にメッセージで呼び出されます。これにより、メッセージヘッダーまたはボディーをフェデレーションする前に変換できます。

プロパティー

特定のトランスフォーマー設定のキーと値のペアを保持するために使用されます。

6. **federation** 要素内に、**upstream** 要素を 1 つ以上追加します。各 **upstream** 要素は、リモートブローカーへの接続と、その接続に適用するポリシーを定義します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <upstream name="eu-east-1">
         <static-connectors>
            <connector-ref>eu-east-connector1</connector-ref>
         </static-connectors>
         <policy ref="news-address-federation"/>
      </upstream>

      <upstream name="eu-west-1" >
         <static-connectors>
            <connector-ref>eu-west-connector1</connector-ref>
         </static-connectors>
         <policy ref="news-address-federation"/>
      </upstream>

      <address-policy name="news-address-federation" auto-delete="true" auto-delete-
delay="300000" auto-delete-message-count="-1" enable-divert-bindings="false" max-
hops="1" transformer-ref="news-transformer">

         <include address-match="queue.bbc.new" />
         <include address-match="queue.usatoday" />
         <include address-match="queue.news.#" />

         <exclude address-match="queue.news.sport.#" />
      </address-policy>
```

```
        <transformer name="news-transformer">
            <class-name>org.foo.NewsTransformer</class-name>
            <property key="key1" value="value1"/>
            <property key="key2" value="value2"/>
        </transformer>

    </federation>
</federations>
```

static-connectors

ローカルブローカーの **broker.xml** 設定ファイルの他の場所で定義される **connector** 要素を参照する **connector-ref** 要素の一覧が含まれます。コネクターは、送信接続に使用するトランスポート (TCP、SSL、HTTP など) およびサーバー接続パラメーター (ホスト、ポートなど) を定義します。この手順の次のステップは、**static-connectors** 要素で参照されるコネクターを追加する方法を示しています。

policy-ref

アップストリームブローカーに適用されるダウンストリームブローカーに設定されたアドレスポリシーの名前。

アップストリーム 要素に指定できる追加オプションを以下に示します。

name

アップストリームブローカー設定の名前。この例では、名前は **eu-east-1** と **eu-west-1** というアップストリームブローカーに対応します。

user

アップストリームブローカーへの接続の作成時に使用するユーザー名。指定のない場合は、**federation** 要素の設定に指定された共有ユーザー名が使用されます。

password

アップストリームブローカーへの接続の作成時に使用するパスワード。指定のない場合は、**federation** 要素の設定に指定された共有パスワードが使用されます。

call-failover-timeout

call-timeout と同様ですが、フェイルオーバーの試行中に呼び出しが行われる場合に使用されます。デフォルト値は **-1** で、タイムアウトが無効であることを意味します。

call-timeout

ブロック呼び出しであるパケットを送信すると、フェデレーション接続がリモートブローカーからの応答を待つ時間 (ミリ秒単位)。この時間が経過すると、接続によって例外が発生します。デフォルト値は **30000** です。

check-period

フェデレーション接続の健常性を確認するために、ローカルブローカがリモートブローカに送信する連続した“keep-alive"メッセージ間の期間 (ミリ秒)。フェデレーション接続が正常である場合、リモートブローカーは各キープアライブメッセージに応答します。接続が正常でないと、ダウンストリームブローカーがアップストリームブローカーから応答を受信できない場合に、**サーキットブレーカー** と呼ばれるメカニズムを使用してフェデレーションされたコンシューマーをブロックします。詳細は、**circuit-breaker-timeout** パラメーターの説明を参照してください。**check-period** パラメーターのデフォルト値は **30000** です。

circuit-breaker-timeout

ダウンストリームとアップストリームブローカー間の単一の接続は、多くのフェデレーションされたキューとアドレスコンシューマーによって共有される可能性があります。ブローカー間の接続が失われた場合、フェデレーションされた各コンシューマーは同時に再接続を

試みる可能性があります。これを回避するには、**サーキットブレーカー** と呼ばれるメカニズムはコンシューマーをブロックします。指定したタイムアウト値が経過すると、サーキットブレーカーは接続を再送します。成功すると、コンシューマーはブロックされません。それ以外の場合は、サーキットブレーカーが再度適用されます。

connection-ttl

リモートブローカーからのメッセージを受信しなくなった場合に、フェデレーション接続が存続する時間 (ミリ秒単位)。デフォルト値は **60000** です。

discovery-group-ref

アップストリームブローカーへの接続に静的コネクターを定義する代わりに、この要素を使用して **broker.xml** 設定ファイルの別の場所で設定済みの検出グループを指定できます。具体的には、この要素の **discovery-group-name** プロパティーの値として、既存の検出グループを指定します。検出グループの詳細は、「ブローカー検出メソッド」 を参照してください。

ha

アップストリームブローカーへの接続に対して、高可用性が有効であるかどうかを指定します。このパラメーターの値を **true** に設定すると、ローカルブローカーはアップストリームクラスターで利用可能なブローカーに接続でき、ライブアップストリームブローカーがシャットダウンすると、バックアップブローカーに自動フェイルオーバーされます。デフォルト値は **false** です。

initial-connect-attempts

ダウンストリームブローカーがアップストリームブローカーに接続するようにする初期試行の数。接続を確立せずにこの値に達すると、アップストリームブローカーは永続的にオフラインとみなされます。ダウンストリームブローカーは、メッセージをアップストリームブローカーにルーティングしなくなりました。デフォルト値は **-1 で**、制限なしを意味します。

max-retry-interval

リモートブローカーへの接続に失敗した場合に後続の再接続試行の間隔 (ミリ秒単位)。デフォルト値は **2000** です。

reconnect-attempts

接続が失敗した場合に、ダウンストリームブローカーがアップストリームブローカーへの再接続を試行する回数。接続が再確立されていない状態でこの値に達すると、アップストリームブローカーは永続的にオフラインとみなされます。ダウンストリームブローカーは、メッセージをアップストリームブローカーにルーティングしなくなりました。デフォルト値は **-1 で**、制限なしを意味します。

retry-interval

リモートブローカーへの接続に失敗した場合に、後続の再接続試行の間隔 (ミリ秒単位)。デフォルト値は **500** です。

retry-interval-multiplier

retry-interval パラメーターの値に適用される乗率。デフォルト値は **1** です。

share-connection

同じブローカーにダウンストリーム接続とアップストリーム接続の両方が設定されている場合には、ダウンストリーム設定とアップストリーム設定の両方がこのパラメーターの値を **true** に設定している限り、同じ接続が共有されます。デフォルト値は **false** です。

7. ローカルブローカーで、コネクターをリモートブローカーに追加します。これらは、フェデレーションされたアドレス設定の **static-connectors** 要素で参照されるコネクターです。以下に例を示します。

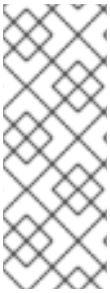
```
<connectors>
  <connector name="eu-west-1-connector">tcp://localhost:61616</connector>
```

```
   <connector name="eu-east-1-connector">tcp://localhost:61617</connector>
</connectors>
```

4.22.6. ダウンストリームアドレスフェデレーションの設定

以下の例は、スタンドアロンブローカーにダウンストリームアドレスフェデレーションを設定する方法を示しています。

ダウンストリームアドレスのフェデレーションにより、1つ以上のリモートブローカーがローカルブローカーに接続するために使用するローカルブローカーに設定を追加できます。このアプローチの利点は、すべてのフェデレーション設定を単一のブローカーに維持できることです。これは、たとえば hub-and-spoke トポロジーに役立ちます。



注記

ダウンストリームアドレスのフェデレーションは、フェデレーション接続の方向対アップストリームアドレス設定の方向を逆にします。したがって、リモートブローカーを設定に追加する際に、**ダウンストリーム** ブローカーとみなされます。ダウンストリームブローカーは、設定の接続情報を使用して、ローカルブローカーに接続し、アップストリームとみなされるようになりました。この例は、この後、リモートブローカーの設定を追加する際に説明します。

前提条件

- アップストリームアドレスフェデレーションの設定を理解している。「アップストリームのアドレスフェデレーションの設定」を参照してください。
- 以下の例は、スタンドアロンブローカー間でアドレスフェデレーションを設定する方法を示しています。ただし、ブローカー **クラスター** のフェデレーションを設定するための要件も理解している必要があります。詳細は、「ブローカークラスターのフェデレーションの設定」 を参照してください。

手順

1. ローカルブローカーで、**<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<federation>** 要素が含まれる **<federations >** 要素を追加します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">
   </federation>
</federations>
```

3. アドレスポリシー設定を追加します。以下に例を示します。

```
<federations>
   ...
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <address-policy name="news-address-federation" max-hops="1" auto-delete="true"
auto-delete-delay="300000" auto-delete-message-count="-1" transformer-ref="news-
transformer">
```

```
            <include address-match="queue.bbc.new" />
            <include address-match="queue.usatoday" />
            <include address-match="queue.news.#" />

            <exclude address-match="queue.news.sport.#" />
        </address-policy>

    </federation>
  ...
</federations>
```

4. 送信前にメッセージを変換する場合は、トランスフォーマー設定を追加します。以下に例を示します。

```
<federations>
    ...
    <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

        <address-policy name="news-address-federation" max-hops="1" auto-delete="true"
auto-delete-delay="300000" auto-delete-message-count="-1" transformer-ref="news-
transformer">

            <include address-match="queue.bbc.new" />
            <include address-match="queue.usatoday" />
            <include address-match="queue.news.#" />

            <exclude address-match="queue.news.sport.#" />
        </address-policy>

        <transformer name="news-transformer">
            <class-name>org.foo.NewsTransformer</class-name>
            <property key="key1" value="value1"/>
            <property key="key2" value="value2"/>
        </transformer>

    </federation>
  ...
</federations>
```

5. 各リモートブローカーに **ダウンストリーム** 要素を追加します。以下に例を示します。

```
<federations>
    ...
    <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

        <downstream name="eu-east-1">
            <static-connectors>
                <connector-ref>eu-east-connector1</connector-ref>
            </static-connectors>
            <transport-connector-ref>netty-connector</transport-connector-ref>
            <policy ref="news-address-federation"/>
        </downstream>
```

```
        <downstream name="eu-west-1" >
            <static-connectors>
               <connector-ref>eu-west-connector1</connector-ref>
            </static-connectors>
            <transport-connector-ref>netty-connector</transport-connector-ref>
            <policy ref="news-address-federation"/>
        </downstream>

        <address-policy name="news-address-federation" max-hops="1" auto-delete="true"
auto-delete-delay="300000" auto-delete-message-count="-1" transformer-ref="news-
transformer">
            <include address-match="queue.bbc.new" />
            <include address-match="queue.usatoday" />
            <include address-match="queue.news.#" />

            <exclude address-match="queue.news.sport.#" />
        </address-policy>

        <transformer name="news-transformer">
            <class-name>org.foo.NewsTransformer</class-name>
            <property key="key1" value="value1"/>
            <property key="key2" value="value2"/>
        </transformer>

    </federation>
  ...
</federations>
```

上記の設定で示されているように、リモートブローカーはローカルブローカーのダウンストリームであると見なされます。ダウンストリームブローカーは、設定の接続情報を使用して、ローカル (**アップストリーム**) ブローカーへ再度接続します。

6. ローカルブローカーで、ローカルブローカーおよびリモートブローカーによって使用されるコネクターとアクセプターを追加して、フェデレーション接続を確立します。以下に例を示します。

```
<connectors>
  <connector name="netty-connector">tcp://localhost:61616</connector>
  <connector name="eu-west-1-connector">tcp://localhost:61616</connector>
  <connector name="eu-east-1-connector">tcp://localhost:61617</connector>
</connectors>

<acceptors>
  <acceptor name="netty-acceptor">tcp://localhost:61616</acceptor>
</acceptors>
```

connector name="netty-connector"

ローカルブローカーがリモートブローカーに送信するコネクター設定。リモートブローカーはこの設定を使用してローカルブローカーに接続し直します。

connector name="eu-west-1-connector", connector name="eu-east-1-connector"

リモートブローカーへのコネクター。ローカルブローカーはこれらのコネクターを使用してリモートブローカーに接続し、リモートブローカーがローカルブローカーに接続するために必要な設定を共有します。

acceptor name="netty-acceptor"

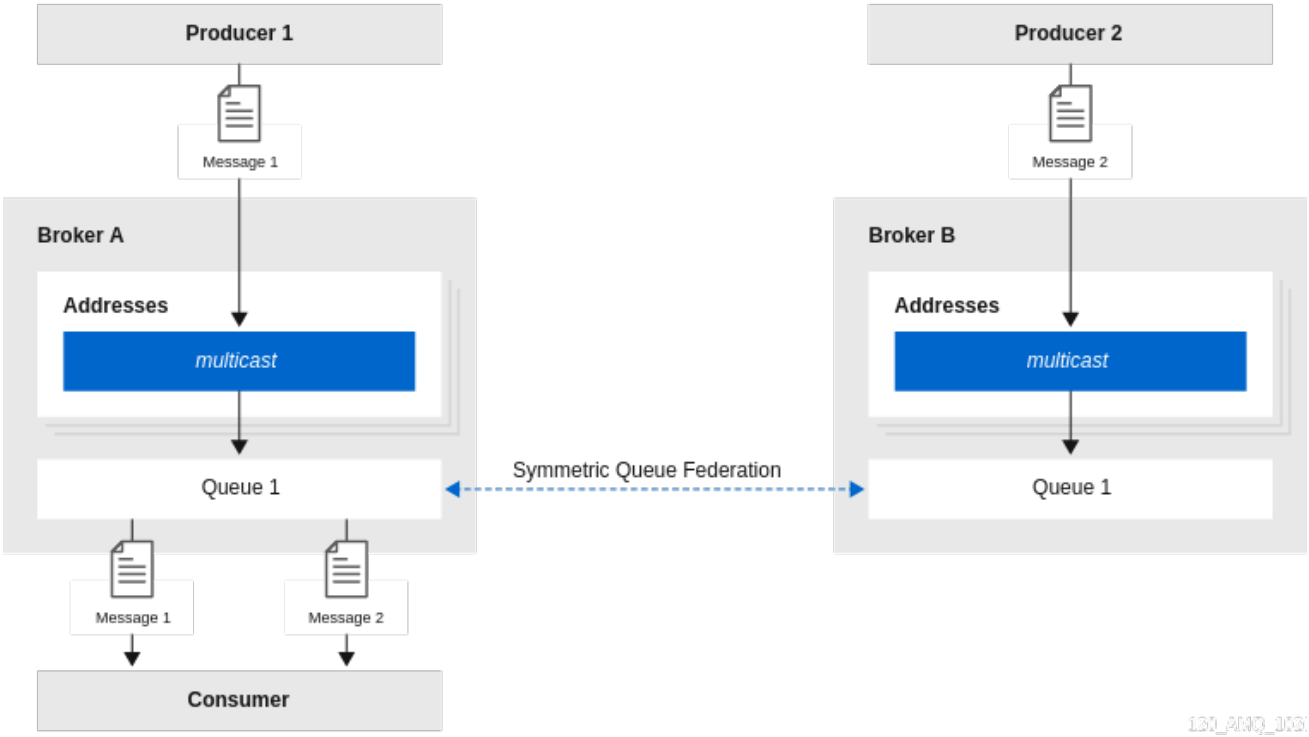
ローカルブローカーに接続するためにリモートブローカーによって使用されるコネクターに対応するローカルブローカーのアクセプター。

4.22.7. キューフェデレーションについて

キューフェデレーションは、他のリモートブローカー全体でローカルブローカーの単一キューの負荷を分散する方法を提供します。

負荷分散を実現するため、ローカルブローカーはローカルコンシューマーからのメッセージの要求を満たすために、リモートキューからメッセージを取得します。以下に例を示します。

図4.5 対称キューフェデレーション



リモートキューを再設定する必要はありません。同じブローカーまたは同じクラスター内に配置する必要はありません。リモートリンクおよびフェデレーションされたキューの作成に必要なすべての設定はローカルブローカーにあります。

4.22.7.1. キューフェデレーションの利点

以下は、キューのフェデレーションの設定を選択する理由です。

容量の増加

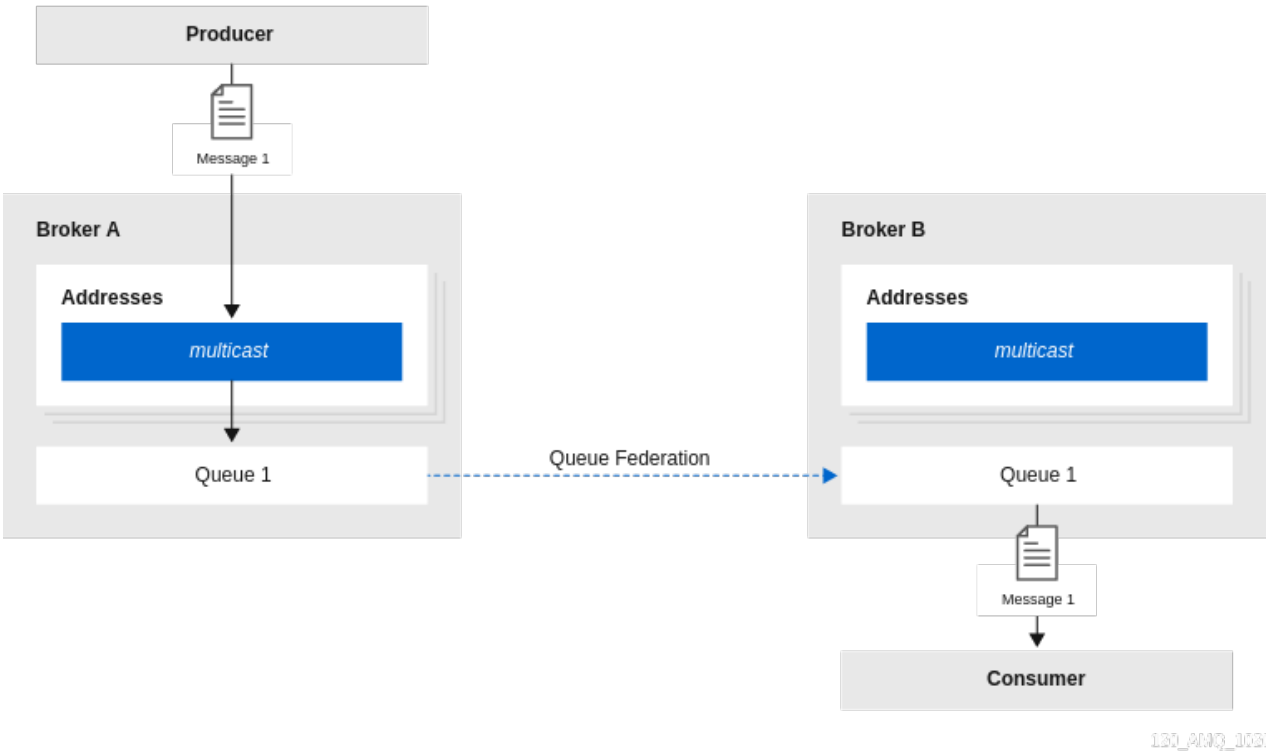
キューフェデレーションは、多くのブローカーに分散される論理キューを作成できます。この論理分散キューは、単一のブローカーにある 1 つのキューよりもはるかに高い容量を持ちます。この設定では、最初に公開されていたブローカーから消費できるメッセージがいくつでも消費されます。システムは、負荷分散が必要な場合にのみ、フェデレーション中のメッセージを移動します。

マルチリージョン設定のデプロイ

マルチリージョン設定では、メッセージプロデューサーが 1 つのリージョンまたは venue にあり、コンシューマーが別のリージョンにある可能性があります。ただし、プロデューサーとコンシューマー接続を指定のリージョンに対してローカルに維持することが理想的です。この場合、プロ

デューサーとコンシューマーが存在する各リージョンにブローカーをデプロイし、キューフェデレーションを使用して、リージョン間での Wide Area Network(WAN) でメッセージを移動できます。以下に例を示します。

図4.6 マルチリージョンキューフェデレーション



安全なエンタープライズ LAN と DMZ 間の通信

ネットワークセキュリティーでは、**demilitarized zone** (DMZ) は物理または論理のサブネットワークで、企業の外部向けサービスを含み、信頼できない外部向けのサービス (通常はインターネットなど、信頼されていない、より大規模なネットワーク) に公開します。その他の企業のローカルエリアネットワーク (LAN) は、ファイアウォールの背後でこの外部ネットワークから分離されます。
セキュアなエンタープライズ LAN の多くのメッセージプロデューサーが DMZ と多数のコンシューマーにある場合、プロデューサーが安全なエンタープライズ LAN のブローカーに接続できないことがあります。この場合、プロデューサーがメッセージを公開できる DMZ にブローカーをデプロイできます。その後、エンタープライズ LAN のブローカーは DMZ のブローカーに接続し、フェデレーションされたキューを使用して DMZ のブローカーからメッセージを受信します。

4.22.8. アップストリームキューフェデレーションの設定

以下の例は、スタンドアロンブローカーにアップストリームのキューフェデレーションを設定する方法を示しています。この例では、ローカル (つまり**ダウンストリーム**) ブローカーから一部のリモート (つまり**アップストリーム**) ブローカーへのフェデレーションを設定します。

前提条件

- 以下の例は、スタンドアロンブローカー間でキューフェデレーションを設定する方法を示しています。ただし、ブローカー **クラスター** のフェデレーションを設定するための要件も理解している必要があります。詳細は、「ブローカークラスターのフェデレーションの設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 新しい **<federations>** 要素に、**<federation>** 要素を追加します。以下に例を示します。

```
<federations>
  <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">
  </federation>
</federations>
```

name

フェデレーション設定の名前。この例では、名前はダウンストリームブローカーの名前に対応します。

user

アップストリームブローカーに接続するための共有ユーザー名。

password

アップストリームブローカーに接続するための共有パスワード。

注記

- ユーザーとパスワードの認証情報がアップストリームブローカーごとに異なる場合は、設定に追加する時にこれらのブローカーの認証情報を個別に指定できます。これは、この手順の後半で説明します。

3. **federation** 要素内に **<queue-policy>** 要素を追加します。**<queue-policy>** 要素のプロパティー値を指定します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <queue-policy name="news-queue-federation" include-federated="true" priority-
adjustment="-5" transformer-ref="news-transformer">
      </queue-policy>

   </federation>
</federations>
```

name

キューポリシーの名前。ブローカーに設定されるキューポリシーはすべて一意の名前である必要があります。

include-federated

このプロパティーの値を **false** に設定すると、設定は、すでにフェデレーションされたコンシューマー (つまりフェデレーションされたキューのコンシューマー) は統合しなおされません。これにより、対称または閉ループトポロジーで、フェデレーションされていないコンシューマーが存在せず、メッセージがシステム内を無限に流れる状況を回避できます。
閉ループトポロジーが **ない** 場合は、このプロパティーの値を **true** に設定できます。たとえば、3 つのブローカー、**BrokerA**、**BrokerB**、および **BrokerC** のチェーンがあり、プロデューサーが **BrokerA** のコンシューマーと **BrokerC** のコンシューマーがあるとします。この場合、**BrokerB が** コンシューマーを **BrokerA** にフェデレーションしなおす必要があります。

priority-adjustment

コンシューマーがキューに接続すると、その優先度は、アップストリーム (**フェデレーションされた**) コンシューマーの作成時に優先順位が使用されます。フェデレーションされたコンシューマーの優先度は、**priority-adjustment** プロパティーの値で調整します。このプロパティーのデフォルト値は **-1** です。これにより、負荷分散時にローカルコンシューマーがフェデレーションされたコンシューマーよりも優先されます。ただし、必要に応じて優先順位の調整の値を変更できます。

transformer-ref

トランスフォーマー設定の名前。フェデレーションされたメッセージ送信時にメッセージを変換したい場合は、トランスフォーマー設定を追加することができます。トランスフォーマー設定は、この手順の後半で説明します。

4. **<queue-policy>** 要素内に、キューポリシーからアドレスを追加し、除外する address-matching パターンを追加します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <queue-policy name="news-queue-federation" include-federated="true" priority-
adjustment="-5" transformer-ref="news-transformer">

         <include queue-match="#" address-match="queue.bbc.new" />
         <include queue-match="#" address-match="queue.usatoday" />
         <include queue-match="#" address-match="queue.news.#" />

         <exclude queue-match="#.local" address-match="#" />

      </queue-policy>

   </federation>
</federations>
```

include

この要素の **address-match** プロパティーの値は、キューポリシーに含めるアドレスを指定します。**queue.bbc.new** や **queue.usatoday** など、正確なアドレスを指定できます。または、ワイルドカード式を使用して一致するアドレスの **セット** を指定できます。上記の例では、アドレスポリシーには文字列 **queue.news** で始まる**すべて**のアドレス名も含まれています。
address-match プロパティーと組み合わせて、**queue-match** プロパティーを使用して、キューポリシーにこれらのアドレスに特定のキューを含めることができます。**address-match** プロパティーと同様に、正確なキュー名を指定するか、ワイルドカード式を使用して**一連の**キューを指定できます。上記の例では、番号記号 (**#**) のワイルドカード文字は、各アドレスまたはアドレスセットにある **すべて** のキューがキューポリシーに含まれることを示しています。

exclude

この要素の **address-match** プロパティーの値は、キューポリシーから除外するアドレスを指定します。正確なアドレスを指定するか、ワイルドカード式を使用して一致するアドレスの **セット** を指定できます。上記の例では、数字記号 (**#**) ワイルドカード文字は、**全** アドレスの **queue-match** プロパティーと一致するキューが**すべて**除外されることを意味します。この場合、**.local** という文字列で終了するキューは除外されます。これは、特定のキューがローカルキューとして保持され、フェデレーションされていないことを示しています。

5. **federation** 要素 では、**transformer** 要素を追加してカスタムトランスフォーマー実装を参照します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <queue-policy name="news-queue-federation" include-federated="true" priority-
adjustment="-5" transformer-ref="news-transformer">

         <include queue-match="#" address-match="queue.bbc.new" />
         <include queue-match="#" address-match="queue.usatoday" />
         <include queue-match="#" address-match="queue.news.#" />

         <exclude queue-match="#.local" address-match="#" />

      </queue-policy>

      <transformer name="news-transformer">
         <class-name>org.foo.NewsTransformer</class-name>
         <property key="key1" value="value1"/>
         <property key="key2" value="value2"/>
      </transformer>

   </federation>
</federations>
```

name

トランスフォーマー設定の名前。この名前は、対象となるブローカーで一意でなければなりません。この名前は、アドレスポリシーの **transformer-ref** プロパティーの値として指定します。

class-name

org.apache.activemq.artemis.core.server.transformer.Transformer インターフェイスを実装するユーザー定義クラスの名前。
トランスフォーマーの **transform()** メソッドは、メッセージが送信される前にメッセージで呼び出されます。これにより、メッセージヘッダーまたはボディーをフェデレーションする前に変換できます。

プロパティー

特定のトランスフォーマー設定のキーと値のペアを保持するために使用されます。

6. **federation** 要素内に、**upstream** 要素を 1 つ以上追加します。各 **upstream** 要素は、アップストリームブローカー接続と、その接続に適用するポリシーを定義します。以下に例を示します。

```
<federations>
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <upstream name="eu-east-1">
         <static-connectors>
            <connector-ref>eu-east-connector1</connector-ref>
         </static-connectors>
         <policy ref="news-queue-federation"/>
      </upstream>
```

```
        <upstream name="eu-west-1" >
            <static-connectors>
                <connector-ref>eu-west-connector1</connector-ref>
            </static-connectors>
            <policy ref="news-queue-federation"/>
        </upstream>

        <queue-policy name="news-queue-federation" include-federated="true" priority-
adjustment="-5" transformer-ref="news-transformer">

            <include queue-match="#" address-match="queue.bbc.new" />
            <include queue-match="#" address-match="queue.usatoday" />
            <include queue-match="#" address-match="queue.news.#" />

            <exclude queue-match="#.local" address-match="#" />

        </queue-policy>

        <transformer name="news-transformer">
            <class-name>org.foo.NewsTransformer</class-name>
            <property key="key1" value="value1"/>
            <property key="key2" value="value2"/>
        </transformer>

    </federation>
</federations>
```

static-connectors

ローカルブローカーの **broker.xml** 設定ファイルの他の場所で定義される **connector** 要素を参照する **connector-ref** 要素の一覧が含まれます。コネクターは、送信接続に使用するトランスポート (TCP、SSL、HTTP など) およびサーバー接続パラメーター (ホスト、ポートなど) を定義します。以下の手順は、フェデレーションされたキュー設定の **static-connectors** 要素で参照されるコネクターを追加する方法を示しています。

policy-ref

アップストリームブローカーに適用されるダウンストリームブローカーに設定されたキューポリシーの名前。

アップストリーム 要素に指定できる追加オプションを以下に示します。

name

アップストリームブローカー設定の名前。この例では、名前は **eu-east-1** と **eu-west-1** というアップストリームブローカーに対応します。

user

アップストリームブローカーへの接続の作成時に使用するユーザー名。指定のない場合は、**federation** 要素の設定に指定された共有ユーザー名が使用されます。

password

アップストリームブローカーへの接続の作成時に使用するパスワード。指定のない場合は、**federation** 要素の設定に指定された共有パスワードが使用されます。

call-failover-timeout

call-timeout と同様ですが、フェイルオーバーの試行中に呼び出しが行われる場合に使用されます。デフォルト値は **-1** で、タイムアウトが無効であることを意味します。

call-timeout

ブロック呼び出しであるパケットを送信すると、フェデレーション接続がリモートブローカーからの応答を待つ時間 (ミリ秒単位)。この時間が経過すると、接続によって例外が発生します。デフォルト値は **30000** です。

check-period

フェデレーション接続の健常性を確認するために、ローカルブローカがリモートブローカに送信する連続した“keep-alive"メッセージ間の期間 (ミリ秒)。フェデレーション接続が正常である場合、リモートブローカーは各キープアライブメッセージに応答します。接続が正常でないと、ダウンストリームブローカーがアップストリームブローカーから応答を受信できない場合に、**サーキットブレーカー** と呼ばれるメカニズムを使用してフェデレーションされたコンシューマーをブロックします。詳細は、**circuit-breaker-timeout** パラメーターの説明を参照してください。**check-period** パラメーターのデフォルト値は **30000** です。

circuit-breaker-timeout

ダウンストリームとアップストリームブローカー間の単一の接続は、多くのフェデレーションされたキューとアドレスコンシューマーによって共有される可能性があります。ブローカー間の接続が失われた場合、フェデレーションされた各コンシューマーは同時に再接続を試みる可能性があります。これを回避するには、**サーキットブレーカー** と呼ばれるメカニズムはコンシューマーをブロックします。指定したタイムアウト値が経過すると、サーキットブレーカーは接続を再送します。成功すると、コンシューマーはブロックされません。それ以外の場合は、サーキットブレーカーが再度適用されます。

connection-ttl

リモートブローカーからのメッセージを受信しなくなった場合に、フェデレーション接続が存続する時間 (ミリ秒単位)。デフォルト値は **60000** です。

discovery-group-ref

アップストリームブローカーへの接続に静的コネクターを定義する代わりに、この要素を使用して **broker.xml** 設定ファイルの別の場所で設定済みの検出グループを指定できます。具体的には、この要素の **discovery-group-name** プロパティーの値として、既存の検出グループを指定します。検出グループの詳細は、「ブローカー検出メソッド」 を参照してください。

ha

アップストリームブローカーへの接続に対して、高可用性が有効であるかどうかを指定します。このパラメーターの値を **true** に設定すると、ローカルブローカーはアップストリームクラスターで利用可能なブローカーに接続でき、ライブアップストリームブローカーがシャットダウンすると、バックアップブローカーに自動フェイルオーバーされます。デフォルト値は **false** です。

initial-connect-attempts

ダウンストリームブローカーがアップストリームブローカーに接続するようにする初期試行の数。接続を確立せずにこの値に達すると、アップストリームブローカーは永続的にオフラインとみなされます。ダウンストリームブローカーは、メッセージをアップストリームブローカーにルーティングしなくなりました。デフォルト値は **-1 で**、制限なしを意味します。

max-retry-interval

リモートブローカーへの接続に失敗した場合に後続の再接続試行の間隔 (ミリ秒単位)。デフォルト値は **2000** です。

reconnect-attempts

接続が失敗した場合に、ダウンストリームブローカーがアップストリームブローカーへの再接続を試行する回数。接続が再確立されていない状態でこの値に達すると、アップストリームブローカーは永続的にオフラインとみなされます。ダウンストリームブローカーは、メッセージをアップストリームブローカーにルーティングしなくなりました。デフォルト値は **-1 で**、制限なしを意味します。

retry-interval

リモートブローカーへの接続に失敗した場合に、後続の再接続試行の間隔 (ミリ秒単位)。デフォルト値は **500** です。

retry-interval-multiplier

retry-interval パラメーターの値に適用される乗率。デフォルト値は **1** です。

share-connection

同じブローカーにダウンストリーム接続とアップストリーム接続の両方が設定されている場合には、ダウンストリーム設定とアップストリーム設定の両方がこのパラメーターの値を **true** に設定している限り、同じ接続が共有されます。デフォルト値は **false** です。

7. ローカルブローカーで、コネクターをリモートブローカーに追加します。これらは、フェデレーションされたアドレス設定の **static-connectors** 要素で参照されるコネクターです。以下に例を示します。

```
<connectors>
  <connector name="eu-west-1-connector">tcp://localhost:61616</connector>
  <connector name="eu-east-1-connector">tcp://localhost:61617</connector>
</connectors>
```

4.22.9. ダウンストリームキューフェデレーションの設定

以下の例は、ダウンストリームキューフェデレーションを設定する方法を示しています。

ダウンストリームキューのフェデレーションにより、1 つ以上のリモートブローカーがローカルブローカーに接続するために使用するローカルブローカーに設定を追加できます。このアプローチの利点は、すべてのフェデレーション設定を単一のブローカーに維持できることです。これは、たとえば hub-and-spoke トポロジーに役立ちます。

注記

ダウンストリームキューのフェデレーションは、フェデレーション接続の方向対アップストリームキュー設定の方向を逆にします。したがって、リモートブローカーを設定に追加する際に、**ダウンストリーム** ブローカーとみなされます。ダウンストリームブローカーは、設定の接続情報を使用して、ローカルブローカーに接続し、アップストリームとみなされるようになりました。この例は、この後、リモートブローカーの設定を追加する際に説明します。

前提条件

- アップストリームキューフェデレーションの設定を理解する必要があります。「アップストリームキューフェデレーションの設定」 を参照してください。
- 以下の例は、スタンドアロンブローカー間でキューフェデレーションを設定する方法を示しています。ただし、ブローカー **クラスター** のフェデレーションを設定するための要件も理解している必要があります。詳細は、「ブローカークラスターのフェデレーションの設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<federation>** 要素が含まれる **<federations >** 要素を追加します。以下に例を示します。

```
<federations>
  <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">
  </federation>
</federations>
```

3. キューポリシー設定を追加します。以下に例を示します。

```
<federations>
    ...
    <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

        <queue-policy name="news-queue-federation" priority-adjustment="-5" include-
federated="true" transformer-ref="new-transformer">

            <include queue-match="#" address-match="queue.bbc.new" />
            <include queue-match="#" address-match="queue.usatoday" />
            <include queue-match="#" address-match="queue.news.#" />

            <exclude queue-match="#.local" address-match="#" />

        </queue-policy>

    </federation>
  ...
</federations>
```

4. 送信前にメッセージを変換する場合は、トランスフォーマー設定を追加します。以下に例を示します。

```
<federations>
    ...
    <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

        <queue-policy name="news-queue-federation" priority-adjustment="-5" include-
federated="true" transformer-ref="news-transformer">

            <include queue-match="#" address-match="queue.bbc.new" />
            <include queue-match="#" address-match="queue.usatoday" />
            <include queue-match="#" address-match="queue.news.#" />

            <exclude queue-match="#.local" address-match="#" />

        </queue-policy>

        <transformer name="news-transformer">
            <class-name>org.foo.NewsTransformer</class-name>
            <property key="key1" value="value1"/>
            <property key="key2" value="value2"/>
        </transformer>
```

```
    </federation>
  ...
</federations>
```

5. 各リモートブローカーに **ダウンストリーム** 要素を追加します。以下に例を示します。

```
<federations>
   ...
   <federation name="eu-north-1" user="federation_username"
password="32a10275cf4ab4e9">

      <downstream name="eu-east-1">
         <static-connectors>
            <connector-ref>eu-east-connector1</connector-ref>
         </static-connectors>
         <transport-connector-ref>netty-connector</transport-connector-ref>
         <policy ref="news-address-federation"/>
      </downstream>

      <downstream name="eu-west-1" >
         <static-connectors>
            <connector-ref>eu-west-connector1</connector-ref>
         </static-connectors>
         <transport-connector-ref>netty-connector</transport-connector-ref>
         <policy ref="news-address-federation"/>
      </downstream>

      <queue-policy name="news-queue-federation" priority-adjustment="-5" include-
federated="true" transformer-ref="new-transformer">

         <include queue-match="#" address-match="queue.bbc.new" />
         <include queue-match="#" address-match="queue.usatoday" />
         <include queue-match="#" address-match="queue.news.#" />

         <exclude queue-match="#.local" address-match="#" />

      </queue-policy>

      <transformer name="news-transformer">
         <class-name>org.foo.NewsTransformer</class-name>
         <property key="key1" value="value1"/>
         <property key="key2" value="value2"/>
      </transformer>

   </federation>
  ...
</federations>
```

上記の設定で示されているように、リモートブローカーはローカルブローカーのダウンストリームであると見なされます。ダウンストリームブローカーは、設定の接続情報を使用して、ローカル (**アップストリーム**) ブローカーへ再度接続します。

6. ローカルブローカーで、ローカルブローカーおよびリモートブローカーによって使用されるコネクターとアクセプターを追加して、フェデレーション接続を確立します。以下に例を示します。

```
<connectors>
  <connector name="netty-connector">tcp://localhost:61616</connector>
  <connector name="eu-west-1-connector">tcp://localhost:61616</connector>
  <connector name="eu-east-1-connector">tcp://localhost:61617</connector>
</connectors>

<acceptors>
  <acceptor name="netty-acceptor">tcp://localhost:61616</acceptor>
</acceptors>
```

connector name="netty-connector"

ローカルブローカーがリモートブローカーに送信するコネクター設定。リモートブローカーはこの設定を使用してローカルブローカーに接続し直します。

connector name="eu-west-1-connector" , connector name="eu-east-1-connector"

リモートブローカーへのコネクター。ローカルブローカーはこれらのコネクターを使用してリモートブローカーに接続し、リモートブローカーがローカルブローカーに接続するために必要な設定を共有します。

acceptor name="netty-acceptor"

ローカルブローカーに接続するためにリモートブローカーによって使用されるコネクターに対応するローカルブローカーのアクセプター。

第5章 ブローカーのセキュリティー保護

5.1. 接続のセキュリティー保護

ブローカーがメッセージングクライアントに接続されている場合や、ブローカーが他のブローカーに接続されている場合は、Transport Layer Security(TLS) を使用してこれらの接続をセキュア化できます。

使用できる TLS 設定は 2 つあります。

- 一方向 TLS。証明書を表示するブローカーのみが表示されます。これが最も一般的な設定です。
- ブローカーとクライアント (または他のブローカー) の両方が証明書を提示する双方向 (または **相互**)TLS。

本セクションの手順では、一方向と双方向 TLS の両方を設定する方法を説明します。

5.1.1. 一方向 TLS の設定

以下の手順は、一方向 TLS に特定のアクセプターを設定する方法を示しています。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 特定のアクセプターでは、**sslEnabled** キーを追加し、値を **true** に設定します。さらに、**keyStorePath** キーおよび **keyStorePassword** キーを追加します。ブローカーキーストアに対応する値を設定します。以下に例を示します。

```
<acceptor name="artemis">tcp://0.0.0.0:61616?
sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!</acceptor>
```

5.1.2. 双方向 TLS の設定

以下の手順では、双方向 TLS を設定する方法を説明します。

前提条件

- 一方向 TLS に対して、指定のアクセプターを設定しておく必要があります。詳細は、「一方向 TLS の設定」 を参照してください。

手順

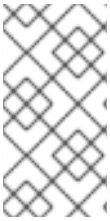
1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一方向 TLS 用に以前に設定したアクセプターの場合は、**needClientAuth** キーを追加します。この値は **true** に設定します。以下に例を示します。

```
<acceptor name="artemis">tcp://0.0.0.0:61616?
sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!;needClientAuth
=true</acceptor>
```

3. 前述の手順の設定は、クライアントの証明書が信頼できるプロバイダーによって署名されていることを前提としています。クライアントの証明書が信頼されるプロバイダー (自己署名の場合など) で署名されて **いない** 場合には、ブローカーはクライアントの証明書をトラストストアに

インポートする必要があります。この場合は、**trustStorePath** キーおよび **trustStorePassword** キーを追加します。ブローカーのトラストストアに対応する値を設定します。以下に例を示します。

```
<acceptor name="artemis">tcp://0.0.0.0:61616?
sslEnabled=true;keyStorePath=../etc/broker.keystore;keyStorePassword=1234!;needClientAuth
=true;trustStorePath=../etc/client.truststore;trustStorePassword=5678!</acceptor>
```



注記

AMQ Broker は複数のプロトコルをサポートし、各プロトコルとプラットフォームには TLS パラメーターを指定する方法が異なります。ただし、コアプロトコル (ブリッジ) を使用するクライアントの場合、TLS パラメーターはブローカーのアクセプターと同様にコネクター URL に設定されます。

5.1.3. TLS 設定オプション

以下の表は、利用可能なすべての TLS 設定オプションを示しています。

オプション	備考
sslEnabled	接続に対して SSL を有効にするかどうかを指定します。TLS を有効にするには **true** に設定する必要があります。デフォルト値は **false** です。
keyStorePath	**アクセプターで使用される場合:** ブローカー証明書を保持するブローカーの TLS キーストアへのパス (自己署名または認証局による署名のいずれか)。 **コネクターで使用される場合:** クライアント証明書を保持するクライアントの TLS キーストアへのパス。これは、双方向の TLS を使用している場合にのみ、コネクターに関係します。この値はブローカーに設定できますが、ダウンロードされ、クライアントによって使用されます。クライアントがブローカーに設定されたものとは異なるパスを使用する必要がある場合は、標準の **javax.net.ssl.keyStore** システムプロパティーまたは AMQ 固有の **org.apache.activemq.ssl.keyStore** システムプロパティーのいずれかを使用してブローカー設定を上書きできます。AMQ 固有のシステムプロパティーは、クライアント上の別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に役立ちます。

オプション	備考
keyStorePassword	**アクセプターで使用される場合:** ブローカーのキーストアのパスワード。 **コネクターで使用される場合:** クライアントのキーストアのパスワード。これは、双方向の TLS を使用している場合にのみ、コネクターに関係します。この値はブローカーに設定できますが、ダウンロードされ、クライアントによって使用されます。クライアントがブローカーに設定されたものとは異なるパスワードを使用する必要がある場合は、標準の **javax.net.ssl.keyStorePassword** システムプロパティーまたは AMQ 固有の **org.apache.activemq.ssl.keyStorePassword** システムプロパティーのいずれかを使用してブローカー設定をオーバーライドできます。AMQ 固有のシステムプロパティーは、クライアント上の別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に役立ちます。
trustStorePath	**アクセプターで使用される場合:** ブローカーが信頼するすべてのクライアントのキーを保持するブローカーの TLS トラストストアへのパス。これは、双方向の TLS を使用している場合にのみ、アクセプターに関係します。 **コネクターで使用される場合:** クライアントが信頼するすべてのブローカーの公開鍵を保持するクライアントの TLS トラストストアへのパス。この値はブローカーに設定できますが、ダウンロードされ、クライアントによって使用されます。クライアントでサーバーの設定と異なるパスを使用する必要がある場合は、標準の **javax.net.ssl.trustStore** システムプロパティーまたは AMQ 固有の **org.apache.activemq.ssl.trustStore** システムプロパティーのいずれかを使用してサーバー側の設定をオーバーライドできます。AMQ 固有のシステムプロパティーは、クライアント上の別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に役立ちます。

オプション	備考
trustStorePassword	**アクセプターで使用される場合:** ブローカーのトラストストアのパスワード。これは、双方向の TLS を使用している場合にのみ、アクセプターに関係します。 **コネクターで使用される場合:** クライアントのトラストストアのパスワード。この値はブローカーに設定できますが、ダウンロードされ、クライアントによって使用されます。クライアントがブローカーに設定されたものとは異なるパスワードを使用する必要がある場合は、標準の **javax.net.ssl.trustStorePassword** システムプロパティーまたは AMQ 固有の **org.apache.activemq.ssl.trustStorePassword** システムプロパティーのいずれかを使用してブローカー設定をオーバーライドできます。AMQ 固有のシステムプロパティーは、クライアント上の別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に役立ちます。
enabledCipherSuites	アクセプターまたはコネクターで使用されるかに関係なく、TLS 通信に使用される暗号スイートのコンマ区切りリストになります。デフォルト値は **null** です (JVM のデフォルト値を使用)。
enabledProtocols	アクセプターまたはコネクターで使用されるかに関係なく、TLS 通信に使用されるプロトコルのコンマ区切りリストになります。デフォルト値は **null** です (JVM のデフォルト値を使用)。
needClientAuth	このプロパティーはアクセプター専用です。これは、双方向 TLS が必要であるアクセプターに接続するクライアントに指示します。有効な値は **true** または **false** です。デフォルト値は **false** です。

5.2. クライアントの認証

5.2.1. クライアント認証方法

ブローカーにクライアント認証を設定するには、以下の方法を使用できます。

ユーザー名とパスワードベースの認証

以下のオプションのいずれかを使用して、ユーザーの認証情報を直接検証します。

- ブローカーにローカルに保存されるプロパティーファイルのセットに対して認証情報を確認します。また、ブローカーへのアクセスを限定して、ログインモジュールを組み合わせてより複雑なユースケースをサポートする **ゲスト** アカウントを設定することもできます。

- 中央の X.500 ディレクトリーサーバーに保存されているユーザーデータに対してクライアントクレデンシャルを確認するように、LDAP (**Lightweight Directory Access Protocol**) ログインモジュールを設定します。

証明書ベースの認証

双方向 **Transport Layer Security**(TLS) を設定して、ブローカーとクライアントの両方が相互認証の証明書を提示するようにします。管理者は、承認されたクライアントユーザーおよびロールを定義するプロパティーファイルも設定する必要があります。これらのプロパティーファイルはブローカーに保存されます。

Kerberos ベースの認証

Simple Authentication and Security Layer(SASL) フレームワークから GSSAPI メカニズムを使用し、クライアントの Kerberos セキュリティー認証情報を認証するようにブローカーを設定します。

次のセクションでは、ユーザーとパスワードと証明書ベースの認証の両方を設定する方法を説明します。

関連情報

- LDAP および Kerberos の完全な認証 **および** 承認ワークフローの詳細は、以下を参照してください。
  - 「認証および承認での LDAP の使用」
  - 「認証および承認での Kerberos の使用」

5.2.2. プロパティーファイルに基づくユーザーおよびパスワード認証の設定

AMQ Broker は、アドレスに基づいてキューにセキュリティーを適用するための柔軟なロールベースのセキュリティーモデルをサポートします。キューは、1 対 1(ポイントツーポイントメッセージングの場合) または多対 1(パブリッシュ/サブスクライブメッセージング用) のいずれかのアドレスにバインドされます。メッセージがアドレスに送信されると、ブローカーはそのアドレスにバインドされたキューのセットを検索し、メッセージをそのキューのセットにルーティングします。

基本的なユーザーとパスワード認証が必要な場合は、**PropertiesLoginModule** を使用して定義します。このログインモジュールは、ブローカーにローカルに保存される以下の設定ファイルに対してユーザーの認証情報をチェックします。

artemis-users.properties

ユーザーおよび対応するパスワードの定義に使用

artemis-roles.properties

ロールを定義し、ユーザーをそれらのロールに割り当てるのに使用します。

login.config

ユーザーおよびパスワード認証、およびゲストアクセス用のログインモジュールの設定に使用

artemis-users.properties ファイルには、セキュリティーを確保するために、ハッシュ化されたパスワードを含めることができます。

以下のセクションでは、設定方法を説明します。

- 基本的なユーザーとパスワード認証
- ゲストアクセスを含むユーザーとパスワード認証

5.2.2.1. 基本的なユーザーとパスワード認証の設定

以下の手順は、基本的なユーザーとパスワード認証を設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/login.config** 設定ファイルを開きます。デフォルトでは、新しい AMQ Broker 7.9 インスタンスのこのファイルには以下の行を追加します。

```
activemq {
  org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule sufficient
    debug=false
    reload=true
    org.apache.activemq.jaas.properties.user="artemis-users.properties"
    org.apache.activemq.jaas.properties.role="artemis-roles.properties";
     };
```

activemq

設定のエイリアス。

org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule

実装クラス。

sufficient

PropertiesLoginModule に必要とされる成功レベルを指定するフラグ。設定可能な値は次のとおりです。

- **必須**: ログインモジュールが正常に実行される必要があります。認証は、成功または失敗に関係なく、指定のエイリアスで設定されたログインモジュールのリストの実行をそのまま継続します。
- **必須**: ログインモジュールが正常に実行される必要があります。失敗により、即座に制御がアプリケーションに返されます。認証は、指定のエイリアス下で設定されたログインモジュールのリストを実行しません。
- **sufficient**: ログインモジュールは正常に実行される必要はありません。成功した場合には、制御がアプリケーションに返り、認証はこれ以上続行しません。認証に失敗すると、認証試行により、指定のエイリアス下で設定されたログインモジュールのリストが続行されます。
- **オプション**: ログインモジュールは正常に実行される必要はありません。認証は、成功または失敗に関係なく、指定のエイリアスで設定されたログインモジュールのリストを継続します。

org.apache.activemq.jaas.properties.user

ログインモジュール実装のユーザーとパスワードのセットを定義するプロパティーファイルを指定します。

org.apache.activemq.jaas.properties.role

ユーザーをログインモジュール実装に定義されたロールにマップするプロパティーファイルを指定します。

2. **<broker_instance_dir>/etc/artemis-users.properties** 設定ファイルを開きます。
3. ユーザーを追加して、ユーザーにパスワードを割り当てます。以下は例になります。

```
user1=secret
user2=access
user3=myPassword
```

4. **<broker_instance_dir>/etc/artemis-roles.properties** 設定ファイルを開きます。

5. **artemis-users.properties** ファイルに追加したユーザーにロール名を割り当てます。以下は例になります。

```
admin=user1,user2
developer=user3
```

6. **<broker_instance_dir>\etc\bootstrap.xml** 設定ファイルを開きます。

7. 必要に応じて、以下のようにセキュリティードメインエイリアス (このインスタンスでは **activemq**) をファイルに追加します。

```
<jaas-security domain="activemq"/>
```

5.2.2.2. ゲストアクセスの設定

ログイン認証情報がないユーザーや、認証情報が認証に失敗するユーザーの場合は、ゲストアカウントを使用してブローカーへの制限されたアクセスを付与できます。

コマンドラインの切り替えを使用して **--allow-anonymous** (**--require-login** の逆)、ゲストアクセスを有効にし、ブローカーインスタンスを作成できます。

以下の手順は、ゲストアクセスを設定する方法を説明します。

前提条件

- この手順では、基本的なユーザーとパスワード認証がすでに設定されていることを前提としています。詳細は、「基本的なユーザーとパスワード認証の設定」 を参照してください。

手順

1. 基本的なユーザーとパスワード認証用に指定した **<broker_instance_dir>/etc/login.config** 設定ファイルを開きます。

2. 以前追加したプロパティーログインモジュール設定の後に、ゲストログインモジュール設定を追加します。以下に例を示します。

```
activemq {
  org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule sufficient
     debug=true
     org.apache.activemq.jaas.properties.user="artemis-users.properties"
     org.apache.activemq.jaas.properties.role="artemis-roles.properties";

  org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule sufficient
     debug=true
     org.apache.activemq.jaas.guest.user="guest"
     org.apache.activemq.jaas.guest.role="restricted";
};
```

org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule

実装クラス。

org.apache.activemq.jaas.guest.user

匿名ユーザーに割り当てられたユーザー名。

org.apache.activemq.jaas.guest.role

匿名ユーザーに割り当てられたロール。

上記の設定に基づいて、ユーザーが認証情報を提供すると、ユーザーとパスワード認証モジュールがアクティブになります。ユーザーが認証情報を提供しない場合や、指定した認証情報が正しくない場合は、ゲスト認証がアクティブになります。

5.2.2.2.1. ゲストアクセスの例

以下の例は、認証情報がないユーザーだけがゲストとしてログインしているユースケースに対するゲストアクセスの設定を示しています。この例では、ログインモジュールの順序が以前の設定手順と照合されていることを確認します。また、プロパティーログインモジュールに割り当てられるフラグは **requisite** に変更されています。

```
activemq {
   org.apache.activemq.artemis.spi.core.security.jaas.GuestLoginModule sufficient
      debug=true
      credentialsInvalidate=true
      org.apache.activemq.jaas.guest.user="guest"
      org.apache.activemq.jaas.guest.role="guests";

   org.apache.activemq.artemis.spi.core.security.jaas.PropertiesLoginModule requisite
      debug=true
      org.apache.activemq.jaas.properties.user="artemis-users.properties"
      org.apache.activemq.jaas.properties.role="artemis-roles.properties";
};
```

前述の設定に基づいて、ログイン認証情報が指定されていない場合は、ゲスト認証モジュールがアクティベートされます。

このユースケースでは、ゲストログインモジュールの設定で **credentialsInvalidate** オプションを **true** に設定する必要があります。

プロパティーログインモジュールは、認証情報が提供されているとアクティベートされます。クレデンシャルが有効である必要があります。

関連情報

- **Java Authentication and Authorization Service**(JAAS) の詳細は、Java ベンダーのドキュメントを参照してください。たとえば、**login.config** の設定に関する Oracle のチュートリアルは、Oracle Java ドキュメントの JAAS Login Configuration File を参照してください。
- クライアントクレデンシャルを検証するように LDAP ログインモジュールを設定する方法は、「クライアント認証用の LDAP の設定」 を参照してください。
- 設定ファイルでパスワードを暗号化する方法は、「設定ファイルでのパスワードの暗号化」 を参照してください。

5.2.3. 証明書ベースの認証の設定

Java Authentication and Authorization Service(JAAS) 証明書ログインモジュールは、Transport Layer Security(TLS) を使用するクライアントの認証および承認を処理します。モジュールを使用するには、双方向の **Transport Layer Security**(TLS) の使用と、独自の証明書でクライアントを設定する必要があります。認証は、JAAS 証明書ログインモジュールから直接ではなく、TLS ハンドシェイク中に実行されます。

証明書ログインモジュールのロールは、以下のとおりです。

- 許可されるユーザーのセットを制限します。関連するプロパティーファイルに明示的に一覧表示されるユーザーの **識別名** (DN) のみが認証の対象となります。
- グループの一覧を受信したユーザー ID に関連付けます。これにより、認証が容易になります。
- 受信クライアント証明書が必要です (デフォルトでは、TLS レイヤーは、クライアント証明書の存在をオプションとして扱うように設定されています)。

証明書ログインモジュールは、フラットテキストファイルのペアに証明書 DN のコレクションを保存します。このファイルは、ユーザー名とグループ ID のリストを各 DN に関連付けます。

証明書ログインモジュールは、**org.apache.activemq.artemis.spi.core.security.jaas.TextFileCertificateLoginModule** クラスで実装されます。

5.2.3.1. 証明書ベースの認証を使用するブローカーの設定

以下の手順では、証明書ベースの認証を使用するようにブローカーを設定する方法を説明します。

前提条件

- 双方向 Transport Layer Security(TLS) を使用するようにブローカーを設定している。詳細は、「双方向 TLS の設定」 を参照してください。

手順

1. 以前ブローカーキーストアにインポートされたユーザー証明書からサブジェクト **識別名** (DN) を取得します。
   a. キーストアファイルから一時ファイルに証明書をエクスポートします。以下に例を示します。

   ```
   keytool -export -file <file_name> -alias broker-localhost -keystore broker.ks -storepass <password>
   ```

   b. エクスポートされた証明書の内容を出力します。

   ```
   keytool -printcert -file <file_name>
   ```

   出力は以下のようになります。

   ```
   Owner: CN=localhost, OU=broker, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
   Issuer: CN=localhost, OU=broker, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
   Serial number: 4537c82e
   Valid from: Thu Oct 19 19:47:10 BST 2006 until: Wed Jan 17 18:47:10 GMT 2007
   ```

```
Certificate fingerprints:
        MD5:  3F:6C:0C:89:A8:80:29:CC:F5:2D:DA:5C:D7:3F:AB:37
        SHA1: F0:79:0D:04:38:5A:46:CE:86:E1:8A:20:1F:7B:AB:3A:46:E4:34:5C
```

Owner エントリーは Subject DN です。Subject DN の入力の使用形式はプラットフォームによって異なります。上記の文字列は、以下のように表現することもできます。

```
Owner: `CN=localhost,\ OU=broker,\ O=Unknown,\ L=Unknown,\ ST=Unknown,\
C=Unknown`
```

2. 証明書ベースの認証を設定します。

a. **<broker_instance_dir>/etc/login.config** 設定ファイルを開きます。証明書ログインモジュールを追加し、ユーザーとロールのプロパティーファイルを参照します。以下に例を示します。

```
activemq {
   org.apache.activemq.artemis.spi.core.security.jaas.TextFileCertificateLoginModule
      debug=true
      org.apache.activemq.jaas.textfiledn.user="artemis-users.properties"
      org.apache.activemq.jaas.textfiledn.role="artemis-roles.properties";
};
```

org.apache.activemq.artemis.spi.core.security.jaas.TextFileCertificateLoginModule

実装クラス。

org.apache.activemq.jaas.textfiledn.user

ログインモジュール実装のユーザーとパスワードのセットを定義するプロパティーファイルを指定します。

org.apache.activemq.jaas.textfiledn.role

ユーザーをログインモジュール実装に定義されたロールにマップするプロパティーファイルを指定します。

b. **<broker_instance_dir>/etc/artemis-users.properties** 設定ファイルを開きます。ユーザーおよび対応する DN はこのファイルで定義されます。以下に例を示します。

```
system=CN=system,O=Progress,C=US
user=CN=humble user,O=Progress,C=US
guest=CN=anon,O=Progress,C=DE
```

前述の設定に基づいて、**system** という名前のユーザーは **CN=system,O=Progress,C=US** Subject DN にマッピングされます。

c. **<broker_instance_dir>/etc/artemis-roles.properties** 設定ファイルを開きます。利用可能なロールと、それらのロールを保持しているユーザーは、このファイルで定義されています。以下に例を示します。

```
admins=system
users=system,user
guests=guest
```

上記の設定では、**users** ロールに対して、複数のユーザーをコンマ区切りリストとして一覧表示します。

d. 以下に示すように、セキュリティードメインエイリアス (このインスタンスでは **activemq**) が **bootstrap.xml** で参照されていることを確認します。

```
<jaas-security domain="activemq"/>
```

5.2.3.2. AMQP クライアントの証明書ベースの認証の設定

Simple Authentication and Security Layer(SASL) EXTERNAL メカニズム設定パラメーターを使用して、ブローカーへの接続時に証明書ベースの認証用に AQMP クライアントを設定します。

ブローカーは、証明書の認証と同じ方法で、AMQP クライアントの **Transport Layer Security** (TLS)/**Secure Sockets Layer**(SSL) 証明書を認証します。

1. ブローカーはクライアントの TLS/SSL 証明書を読み取り、証明書のサブジェクトからアイデンティティーを取得します。
2. 証明書サブジェクトは、証明書ログインモジュールによってブローカー ID にマッピングされます。その後、ブローカーはロールを基にしてユーザーを承認します。

以下の手順では、AMQP クライアントに証明書ベースの認証を設定する方法を説明します。AMQP クライアントが証明書ベースの認証を使用できるようにするには、クライアントがブローカーへの接続に使用する URI に設定パラメーターを追加する必要があります。

前提条件

- 以下を設定している必要があります。
  - 双方向 TLS詳細は、「双方向 TLS の設定」 を参照してください。
  - 証明書ベースの認証を使用するブローカー。詳細は、「証明書ベースの認証を使用するブローカーの設定」 を参照してください。

手順

1. 編集する URI が含まれるリソースを開きます。

```
amqps://localhost:5500
```

2. **sslEnabled=true** パラメーターを追加して、接続の TSL/SSL を有効にします。

```
amqps://localhost:5500?sslEnabled=true
```

3. クライアントトラストストアおよびキーストアに関連するパラメーターを追加して、ブローカーで TSL/SSL 証明書の交換を有効にします。

```
amqps://localhost:5500?
sslEnabled=true&trustStorePath=<trust_store_path>&trustStorePassword=<trust_store_password>&keyStorePath=<key_store_path>&keyStorePassword=<key_store_password>
```

4. パラメーター **saslMechanisms=EXTERNAL** を追加し、TSL/SSL 証明書で見つかったアイデンティティーを使用してブローカーがクライアントを認証するよう要求します。

```
amqps://localhost:5500?
sslEnabled=true&trustStorePath=<trust_store_path>&trustStorePassword=<trust_store_pass
```

```
word>&keyStorePath=<key_store_path>&keyStorePassword=<key_store_password>&saslM
echanisms=EXTERNAL
```

関連情報

- AMQ Broker での証明書ベースの認証に関する詳細は、「証明書ベースの認証を使用するブローカーの設定」 を参照してください。
- AMQP クライアントの設定に関する詳細は、クライアント固有の製品ドキュメントについて Red Hat カスタマーポータル を参照してください。

5.3. クライアントの承認

5.3.1. クライアント承認方法

アドレスおよびキューの作成および削除、およびメッセージの送受信などのブローカーで操作を実行するためのクライアントを承認するには、以下の方法を使用できます。

ユーザーおよびロールベースの承認

認証されたユーザーおよびロールのブローカーセキュリティー設定を設定します。

クライアントを認証するように LDAP を設定

認証と承認の両方を処理するよう **Lightweight Directory Access Protocol** (LDAP) ログインモジュールを設定します。LDAP ログインモジュールは、中央の X.500 ディレクトリーサーバーに保存されているユーザーデータに対して受信認証情報をチェックし、ユーザーロールに基づいてパーミッションを設定します。

クライアントを認証するように Kerberos を設定する

PropertiesLoginModule に認証情報を渡す **Java Authentication and Authorization Service** (JAAS) **Krb5LoginModule** ログインモジュール または AMQ Broker ロールに Keroberos 認証ユーザーをマッピングする **LDAPLoginModule** ログインモジュールを設定します。

5.3.2. ユーザーおよびロールベースの承認の設定

5.3.2.1. パーミッションの設定

パーミッションは、**broker.xml** 設定ファイルの **<security-setting>** 要素でキュー (アドレスに基づく) に対して定義されます。設定ファイルの **<security-settings>** 要素に **<security-setting>** のインスタンスを複数定義できます。アドレス完全一致を指定するか、数字記号 (**#**) およびアスタリスク (*) ワイルドカード文字を使用したワイルドカードの一致を定義できます。

アドレスに一致するキューのセットに異なるパーミッションを指定できます。これらのパーミッションを以下の表に示します。

ユーザーによるアクセス許可	以下のパラメーター...
アドレスの作成	**createAddress**
アドレスの削除	**deleteAddress**
一致するアドレスの永続キューの作成	**createDurableQueue**

ユーザーによるアクセス許可	以下のパラメーター...
一致するアドレスの永続キューの削除	**deleteDurableQueue**
一致するアドレスの非永続キューの作成	**createNonDurableQueue**
一致するアドレスの非永続キューの削除	**deleteNonDurableQueue**
一致するアドレスへのメッセージの送信	**send**
一致するアドレスにバインドされたキューからのメッセージの消費	**consume**
管理アドレスに管理メッセージを送信して管理操作を呼び出します。	**manage**
一致するアドレスにバインドされるキューの参照	**browse**

パーミッションごとに、パーミッションを付与されたロールの一覧を指定します。指定のユーザーにロールがある場合は、そのアドレスセットのパーミッションが付与されます。

次のセクションでは、パーミッションの設定例を示します。

5.3.2.1.1. 単一アドレス向けメッセージ実稼働の設定

以下の手順では、単一のアドレスに対してメッセージの実稼働パーミッションを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<security-settings>** 要素内に単一の **<security-setting>** 要素を追加します。**match** キーには、アドレスを指定します。以下に例を示します。

```
<security-settings>
   <security-setting match="my.destination">
      <permission type="send" roles="producer"/>
   </security-setting>
</security-settings>
```

上記の設定に基づいて、**producer** ロールのメンバーにはアドレス **my.destination** の **送信** パーミッションが割り当てられています。

5.3.2.1.2. 単一アドレスのメッセージ消費の設定

以下の手順では、単一のアドレスに対してメッセージ消費パーミッションを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<security-settings>** 要素内に単一の **<security-setting>** 要素を追加します。**match** キーには、アドレスを指定します。以下に例を示します。

```
<security-settings>
   <security-setting match="my.destination">
      <permission type="consume" roles="consumer"/>
   </security-setting>
</security-settings>
```

上記の設定に基づいて、**consumer** ロールのメンバーには、アドレス **my.destination** の **consume** パーミッションが割り当てられています。

5.3.2.1.3. すべてのアドレスでの完全なアクセスの設定

以下の手順では、すべてのアドレスおよび関連するキューへの完全アクセスを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<security-settings>** 要素内に単一の **<security-setting>** 要素を追加します。**match** キーの場合は、**全** アドレスへのアクセスを設定するには、番号記号 (**#**) ワイルドカード文字を指定します。以下に例を示します。

```
<security-settings>
   <security-setting match="#">
      <permission type="createDurableQueue" roles="guest"/>
      <permission type="deleteDurableQueue" roles="guest"/>
      <permission type="createNonDurableQueue" roles="guest"/>
      <permission type="deleteNonDurableQueue" roles="guest"/>
      <permission type="createAddress" roles="guest"/>
      <permission type="deleteAddress" roles="guest"/>
      <permission type="send" roles="guest"/>
      <permission type="browse" roles="guest"/>
      <permission type="consume" roles="guest"/>
      <permission type="manage" roles="guest"/>
   </security-setting>
</security-settings>
```

上記の設定に基づいて、すべてのキューの **guest** ロールのメンバーに、全パーミッションが付与されます。これは、すべてのユーザーに **guest** ロールを割り当てるように匿名認証を設定する開発のシナリオで役に立ちます。

関連情報

- より複雑なユースケースを設定する方法は、「複数のセキュリティー設定の設定」 を参照してください。

5.3.2.1.4. 複数のセキュリティー設定の設定

以下の手順の例は、一致するアドレスセットに複数のセキュリティー設定を個別に設定する方法を示しています。ここでは、本セクションの上記の例とは対照的で、**すべて** のアドレスに **全** アクセスを付与する方法を説明します。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<security-settings>** 要素内に単一の **<security-setting>** 要素を追加します。**match** キーの場合は、一致するアドレス **セット** に設定を適用する番号記号 (**#**) ワイルドカード文字を含めます。以下に例を示します。

```
<security-setting match="globalqueues.europe.#">
  <permission type="createDurableQueue" roles="admin"/>
  <permission type="deleteDurableQueue" roles="admin"/>
  <permission type="createNonDurableQueue" roles="admin, guest, europe-users"/>
  <permission type="deleteNonDurableQueue" roles="admin, guest, europe-users"/>
  <permission type="send" roles="admin, europe-users"/>
  <permission type="consume" roles="admin, europe-users"/>
</security-setting>
```

match=globalqueues.europe.#

番号記号 (**#**) ワイルドカード文字は、ブローカーによって任意のシーケンスの単語として解釈されます。単語はピリオド (**.**) で区切られています。この例では、セキュリティー設定は、文字列 **globalqueues.europe** で始まるアドレスに適用されます。

permission type="createDurableQueue"

admin ロールが割り当てられたユーザーのみが、文字列 **globalqueues.europe** で始まるアドレスにバインドされた永続キューを作成したり、削除したりできます。

permission type="createNonDurableQueue"

admin ロール、**guest**、または **europe-users** ロールが割り当てられたユーザーは、文字列 **globalqueues.europe** で始まるアドレスにバインドされた一時キューを作成したり、削除したりできます。

permission type="send"

admin ロールまたは **europe-users** ロールが割り当てられたユーザーは、文字列 **globalqueues.europe** で始まるアドレスにバインドされたキューにメッセージを送信できます。

permission type="consume"

admin ロールまたは **europe-users** ロールが割り当てられたユーザーは、文字列 **globalqueues.europe** で始まるアドレスにバインドされたキューからメッセージを消費できます。

3. (オプション) 異なるセキュリティー設定をアドレスのより限定的なセットに適用するには、別の **<security-setting>** 要素を追加します。**match** キーには、より具体的なテキスト文字列を指定します。以下に例を示します。

```
<security-setting match="globalqueues.europe.orders.#">
  <permission type="send" roles="europe-users"/>
  <permission type="consume" roles="europe-users"/>
</security-setting>
```

2 つ目の **security-setting** 要素では、**globalqueues.europe.orders.#** の照合は、最初の **security-setting** 要素で指定した **globalqueues.europe.#** 照合に比べると、具体的です。**globalqueues.europe.orders.#** に一致するアドレスの場合には、**createDurableQueue**、**deleteDurableQueue**、**createNonDurableQueue**、**deleteNonDu**

rableQueue はファイルの最初の **security-setting** 要素から継承され **ません**。たとえば、**globalqueues.europe.orders.plastics** アドレスの場合には、存在するパーミッションは、ロール **europe-users** の **send** と **consume** のみです。

したがって、ある **security-setting** ブロックで指定されたパーミッションは、別のブロックに継承されないため、これらのアクセス許可を指定しないだけで、より詳細な **security-setting** ブロックのパーミッションを効果的に拒否できます。

5.3.2.1.5. ユーザーでのキューの設定

キューが自動的に作成されると、キューには接続クライアントのユーザー名が割り当てられます。このユーザー名は、キューのメタデータとして含まれます。名前は JMX および AMQ Broker 管理コンソールで公開されます。

以下の手順では、ブローカー設定で手動で定義したキューにユーザー名を追加する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 指定のキューに、**ユーザー** キーを追加します。値を割り当てます。以下に例を示します。

```
<address name="ExampleQueue">
   <anycast>
     <queue name="ExampleQueue" user="admin"/>
   </anycast>
</address>
```

上記の設定に基づいて、**admin** ユーザーはキュー **ExampleQueue** に割り当てられます。

注記

- キューでユーザーを設定しても、そのキューのセキュリティーセマンティクスは変更されません。これはそのキューのメタデータにのみ使用されます。
- ユーザー間のマッピングと、ユーザーに割り当てられたロールのマッピングは、**セキュリティーマネージャー** と呼ばれるコンポーネントによって処理されます。セキュリティーマネージャーは、ブローカーに保存されているプロパティーファイルからユーザーの認証情報を読み取ります。デフォルトでは、AMQ Broker は **org.apache.activemq.artemis.spi.core.security.ActiveMQJAASSecurityManager** セキュリティーマネージャーを使用します。このデフォルトのセキュリティーマネージャーは、JAAS および Red Hat JBoss Enterprise Application Platform(JBoss EAP) のセキュリティーとの統合を提供します。
  カスタム セキュリティーマネージャーの使用方法は、「カスタムセキュリティーマネージャーの指定」 を参照してください。

5.3.2.2. ロールベースアクセス制御の設定

ロールベースアクセス制御 (RBAC) は、MBean の属性およびメソッドへのアクセス制限すに使用されます。RBAC を使用すると、管理者はロールに基づいて Web コンソール、管理インターフェイス、コアメッセージなどの全ユーザーに正しいレベルのアクセスを付与できます。

5.3.2.2.1. ロールベースのアクセス設定

以下の手順の例は、ロールを特定の MBean とその属性およびメソッドにマッピングする方法を示しています。

前提条件

- 最初にユーザーとロールを定義する必要があります。詳細は、「基本的なユーザーとパスワード認証の設定」 を参照してください。

手順

1. **<broker_instance_dir>/etc/management.xml** 設定ファイルを開きます。
2. **role-access** 要素を検索し、設定を編集します。以下に例を示します。

```
<role-access>
  <match domain="org.apache.activemq.artemis">
    <access method="list*" roles="view,update,amq"/>
    <access method="get*" roles="view,update,amq"/>
    <access method="is*" roles="view,update,amq"/>
    <access method="set*" roles="update,amq"/>
    <access method="*" roles="amq"/>
  </match>
</role-access>
```

   - この場合、ドメイン名が **org.apache.activemq.apache** の MBean 属性を照合検索します。
   - 一致する MBean 属性に対する **view**、**update**、または **amq** ロールへのアクセスは、ロールを追加する **list***、**get***、**set***、**is***、および * アクセスメソッドによって制御されます。**method = "*"**(ワイルドカード) 構文は、設定にリストされていない他の前メソッドをすべて指定する方法として使用されます。設定の各アクセスメソッドが MBean メソッド呼び出しに変換されます。
   - 呼び出された MBean メソッドは、設定に記載されているメソッドと照合されます。たとえば、ドメインが **org.apache.activemq.artemis** の MBean で **listMessages** というメソッドを呼び出すと、ブローカーは **list** メソッドの設定で定義されたロールと、アクセスの照合を行います。
   - MBean の完全なメソッド名を使用してアクセスを設定することもできます。以下に例を示します。

```
<access method="listMessages" roles="view,update,amq"/>
```

3. ブローカーを起動または再起動します。
   - Linux の場合: **<broker_instance_dir>/bin/artemis run**
   - Windows の場合: **<broker_instance_dir>\bin\artemis-service.exe start**

MBean プロパティーに一致する **key** 属性を追加して、ドメイン内の特定の MBean を照合することもできます。

5.3.2.2.2. ロールベースのアクセスの例

本セクションでは、ロールベースのアクセス制御を適用する以下の例を説明します。

- ロールのドメインのすべてのキューへのマッピング。
- ドメインの特定のキューへのロールのマッピング。
- 指定の接頭辞を含むすべてのキュー名へのロールのマッピング。
- 異なるロールを異なるキューのセットにマッピングする。

以下の例は、**key** 属性を使用して、指定したドメインのすべてのキューにロールをマッピングする方法を示しています。

```
<match domain="org.apache.activemq.artemis" key="subcomponent=queues">
  <access method="list*" roles="view,update,amq"/>
  <access method="get*" roles="view,update,amq"/>
  <access method="is*" roles="view,update,amq"/>
  <access method="set*" roles="update,amq"/>
  <access method="*" roles="amq"/>
</match>
```

以下の例は、**key** 属性を使用して、特定の名前付きキューにロールをマッピングする方法を示しています。この例では、名前付きキューは **exampleQueue** です。

```
<match domain="org.apache.activemq.artemis" key="queue=exampleQueue">
  <access method="list*" roles="view,update,amq"/>
  <access method="get*" roles="view,update,amq"/>
  <access method="is*" roles="view,update,amq"/>
  <access method="set*" roles="update,amq"/>
  <access method="*" roles="amq"/>
</match>
```

以下の例は、指定した接頭辞が含まれるすべてのキューにロールをマップする方法を示しています。この例では、アスタリスク (*) のワイルドカード演算子を使用して、接頭辞 **example** で始まるすべてのキュー名を照合します。

```
<match domain="org.apache.activemq.artemis" key="queue=example*">
  <access method="list*" roles="view,update,amq"/>
  <access method="get*" roles="view,update,amq"/>
  <access method="is*" roles="view,update,amq"/>
  <access method="set*" roles="update,amq"/>
  <access method="*" roles="amq"/>
</match>
```

同じ属性を組み合わせた各種セット (例: さまざまなキューのセット) に対して、異なるロールをマッピングする場合などです。このような場合は、設定ファイルに複数の **match** 要素を含めることができます。ただし、同じドメイン内に複数の一致がある可能性があります。

たとえば、以下のように設定された 2 つ **<match>** 要素について考えてみましょう。

```
<match domain="org.apache.activemq.artemis" key="queue=example*">
```

および

```
<match domain="org.apache.activemq.artemis" key="queue=example.sub*">
```

この設定を基して、**org.apache.activemq.artemis** ドメインの **example.sub.queue** という名前のキューは、両方のワイルドカードキーの式にマッチします。したがって、ブローカーは、最初の **match** 要素で指定されたロール、または 2 番目の **match** 要素で指定されたロールなど、キューにマップするロールのセットを決定するための優先順位付けスキームを必要とします。

同じドメインに複数の一致がある場合、ブローカーはロールのマッピング時に以下の優先順位スキームを使用します。

- 完全一致がワイルドカードの一致よりも優先される
- ワイルドカードのより長い一致が、より短いワイルドカード一致よりも優先されます。

この例では、長いワイルドカード式が **example.sub.queue** のキュー名と一致するため、ブローカーは 2 番目の **<match>** 要素に設定された role-mapping を適用します。

注記

default-access 要素は、**role-access** または **whitelist** 設定で処理されないすべてのメソッド呼び出しをすべて受け入れる要素です。**default-access** 要素および **role-access** 要素には、**match** 要素と同じセマンティクスがあります。

5.3.2.2.3. whitelist 要素の設定

whitelist は、ユーザー認証を必要としない事前承認済みのドメインまたは MBean のセットです。認証を省略する必要のあるドメインの一覧または MBean の一覧、またはその両方を指定できます。たとえば、ホワイトリストを使用して、AMQ Broker 管理コンソールの実行に必要な MBean を指定できます。

以下の手順の例は、**whitelist** 要素を設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/management.xml** 設定ファイルを開きます。
2. **whitelist** 要素を検索し、設定を編集します。

```
<whitelist>
  <entry domain="hawtio"/>
</whitelist>
```

この例では、ドメインが **hawtio** の MBean が、認証なしでアクセスできます。MBean プロパティーに一致させるために **<entry domain="hawtio" key="type=*"/>** 形式のワイルドカードエントリーを使用することもできます。

3. ブローカーを起動または再起動します。
   - Linux の場合: **<broker_instance_dir>/bin/artemis run**
   - Windows の場合: **<broker_instance_dir>\bin\artemis-service.exe start**

5.3.2.3. リソース制限の設定

承認や認証に関連する通常のセキュリティー設定以外に、特定のユーザーが実行できる特定の制限を設定すると便利です。

5.3.2.3.1. 接続およびキュー制限の設定

以下の手順の例は、ユーザーが作成できる接続およびキューの数を制限する方法を示しています。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **resource-limit-settings** 要素を追加します。**max-connections** および **max-queues** の値を指定します。以下に例を示します。

```
<resource-limit-settings>
  <resource-limit-setting match="myUser">
    <max-connections>5</max-connections>
    <max-queues>3</max-queues>
  </resource-limit-setting>
</resource-limit-settings>
```

max-connections

一致したユーザーがブローカーに対して実行できる接続の数を定義します。デフォルトは **-1** で、制限がないことを意味します。

max-queues

一致したユーザーが作成できるキューの数を定義します。デフォルトは **-1** で、制限がないことを意味します。

注記

ブローカー設定の **address-setting** 要素に指定できる **match** 文字列とは異なり、**resource-limit-settings** で指定した **match** 文字列はワイルドカード構文を使用することは **できません**。代わりに、match 文字列は、リソース制限の設定が適用される特定のユーザーを定義します。

5.4. 認証および承認での LDAP の使用

LDAP ログインモジュールは、中央の X.500 ディレクトリーサーバーに保存されているユーザーデータに対して受信認証情報を確認して、認証および承認を有効にします。これは **org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule** で実装されます。

5.4.1. クライアント認証用の LDAP の設定

以下の手順の例は、LDAP を使用してクライアントを認証する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **security-settings** 要素内に **security-setting** 要素を追加してパーミッションを設定します。以下に例を示します。

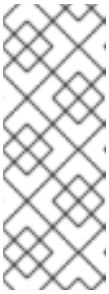
```
<security-settings>
   <security-setting match="#">
      <permission type="createDurableQueue" roles="user"/>
      <permission type="deleteDurableQueue" roles="user"/>
      <permission type="createNonDurableQueue" roles="user"/>
      <permission type="deleteNonDurableQueue" roles="user"/>
      <permission type="send" roles="user"/>
```

```
        <permission type="consume" roles="user"/>
    </security-setting>
</security-settings>
```

上記の設定では、**すべて** のキューに特定のパーミッションを **ユーザー** ロールのメンバーに割り当てます。

3. **<broker_instance_dir>/etc/login.config** ファイルを開きます。
4. 使用しているディレクトリーサービスに基づいて、LDAP ログインモジュールを設定します。
   a. Microsoft Active Directory ディレクトリーサービスを使用している場合は、以下の例のように設定を追加します。

```
activemq {
 org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule required
    debug=true
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="LDAP://localhost:389"

connectionUsername="CN=Administrator,CN=Users,OU=System,DC=example,DC=com"

    connectionPassword=redhat.123
    connectionProtocol=s
    connectionTimeout="5000"
    authentication=simple
    userBase="dc=example,dc=com"
    userSearchMatching="(CN={0})"
    userSearchSubtree=true
    readTimeout="5000"
    roleBase="dc=example,dc=com"
    roleName=cn
    roleSearchMatching="(member={0})"
    roleSearchSubtree=true
    ;
};
```



注記

Microsoft Active Directory を使用し、**connectionUsername** の属性に指定する必要のある値にスペース (例:**OU=System Accounts**) が含まれている場合は、値を二重引用符 (**""**) で囲み、バックスラッシュ (\) を使用してペア内の各二重引用符をエスケープする必要があります。たとえば、**connectionUsername="CN=Administrator,CN=Users,OU=\"System Accounts\",DC=example,DC=com"** などです。

   b. ApacheDS ディレクトリーサービスを使用している場合は、以下の例のような設定を追加します。

```
activemq {
 org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule required
    debug=true
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="ldap://localhost:10389"
    connectionUsername="uid=admin,ou=system"
```

```
    connectionPassword=secret
    connectionProtocol=s
    connectionTimeout=5000
    authentication=simple
    userBase="dc=example,dc=com"
    userSearchMatching="(uid={0})"
    userSearchSubtree=true
    userRoleName=
    readTimeout=5000
    roleBase="dc=example,dc=com"
    roleName=cn
    roleSearchMatching="(member={0})"
    roleSearchSubtree=true
    ;
};
```

debug

デバッグをオン (**true**) またはオフ (**false**) にします。デフォルト値は **false** です。

initialContextFactory

常に **com.sun.jndi.ldap.LdapCtxFactory** に設定する必要があります。

connectionURL

LDAP URL (__<ldap://Host:Port>) を使用するディレクトリーサーバーの場所。オプションでこの URL を修飾するには、スラッシュ / とその後にディレクトリーツリーの特定ノードの DN を追加します。Apache DS のデフォルトポートは **10389** で、Microsoft AD のデフォルト値は **389** です。

connectionUsername

ディレクトリーサーバーへの接続を開くユーザーの識別名 (DN)たとえば、**uid=admin,ou=system** です。ディレクトリーサーバーでは、通常、クライアントが接続を開くためにユーザー名/パスワードの認証情報を提示する必要があります。

connectionPassword

connectionUsername の DN に一致するパスワード。**Directory Information Tree** (DIT) のディレクトリーサーバーでは、パスワードは通常、対応するディレクトリーエントリーに **userPassword** 属性として保存されます。

connectionProtocol

すべての値はサポートされますが、実質的に使用されません。このオプションはデフォルト値がないために明示的に設定する必要があります。

connectionTimeout

ブローカーがディレクトリーサーバーに接続することができる最大時間をミリ秒単位で指定します。ブローカーがこの時間内にディレクトリーに接続できない場合、接続の試行を中止します。このプロパティーにゼロまたはそれよりも小さい値を指定すると、代わりに基盤の TCP プロトコルのタイムアウト値が使用されます。値を指定しない場合、ブローカーは接続を無期限に待機するか、または基盤のネットワークがタイムアウトします。

接続に対して接続プールが要求された場合、このプロパティーは、最大プールサイズにすでに達し、プール内のすべての接続が使用されている場合に、ブローカーが接続を待つ最大時間を指定します。ゼロまたはそれよりも小さい値を指定すると、ブローカーは接続を無期限に利用可能になるまで待機します。それ以外の場合は、ブローカーは最大待機時間に達すると接続の試行を中止します。

authentication

LDAP サーバーにバインドする際に使用する認証方法を指定します。このパラメーターは **simple** (ユーザー名とパスワードが必要) または **none** (匿名アクセスを許可) のいずれかに設定できます。

userBase

ユーザーエントリーを検索する DIT の特定のサブツリーを選択します。サブツリーは、サブツリーのベースノードを指定する DN で指定されます。たとえば、このオプションを **ou=User,ou=ActiveMQ,ou=system** に設定すると、ユーザーエントリーの検索は **ou=User,ou=ActiveMQ,ou=system** ノードの下にあるサブツリーに限定されます。

userSearchMatching

userBase で選択したサブツリーに適用される LDAP 検索フィルターを指定します。詳細は、以下の 「一致するパラメーターの検索」 セクションを参照してください。

userSearchSubtree

userBase で指定されたノードを基準にして、どの程度の深さまでユーザーエントリーの検索を掘り下げるかを指定します。このオプションはブール値です。**false** の値を指定すると、**userBase** ノードの子エントリーのいずれかに一致するものの検索を試行します (**javax.naming.directory.SearchControls.ONELEVEL_SCOPE** にマップ)。**true** の値を指定すると、**userBase** ノードの **サブ** ツリーの配下にあるエントリーに一致するものの検索を試行します (**javax.naming.directory.SearchControls.SUBTREE_SCOPE** にマップ)。

userRoleName

ユーザーのロール名の一覧を含むユーザーエントリーの属性の名前。ロール名は、ブローカーの承認プラグインによってグループ名として解釈されます。このオプションを省略すると、ユーザーエントリーからロール名は抽出されません。

readTimeout

ブローカーがディレクトリーサーバーから LDAP 要求への応答を受信するまで待機する最大時間をミリ秒単位で指定します。この時間内にブローカーがディレクトリーサーバーから応答を受信しない場合、ブローカーは要求を中止します。0 または less の値を指定すると、値を指定しないと、ディレクトリーサーバーから LDAP 要求への応答が無期限に待機します。

roleBase

ロールデータをディレクトリーサーバーに直接保存する場合は、**userRoleName** オプションを指定する代わりに (または指定してその上に)、ロールオプション (**roleBase**、**roleSearchMatching**、**roleSearchSubtree**、および **roleName**) の組み合わせを使用できます。このオプションは、ロール/グループエントリーを検索する DIT の特定のサブツリーを選択します。サブツリーは、サブツリーのベースノードを指定する DN で指定されます。たとえば、このオプションを **ou=Group,ou=ActiveMQ,ou=system** に設定すると、role/group エントリーの検索が **ou=Group,ou=ActiveMQ,ou=system** ノードの下にあるサブツリーに限定されます。

roleName

ロール/グループの名前が含まれるロールエントリーの属性タイプ (C、O、OU など)。このオプションを省略すると、ロール検索機能は事実上無効になっています。

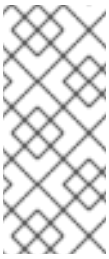
roleSearchMatching

roleBase で選択したサブツリーに適用される LDAP 検索フィルターを指定します。詳細は、以下の 「一致するパラメーターの検索」 セクションを参照してください。

roleSearchSubtree

roleBase で指定されたノードを基準にして、どの程度の深さまでロールエントリーの検索を掘り下げるかを指定します。**false** (デフォルト) に設定すると、**roleBase** ノードの子エントリー (**javax.naming.directory.SearchControls.ONELEVEL_SCOPE** にマッ

プ) のいずれかに一致するものの検索を試行します。**true** の場合、roleBase ノードのサブツリーに属するエントリーに一致するものの検索を試行します (**javax.naming.directory.SearchControls.SUBTREE_SCOPE** にマップ)。



注記

Apache DS は、DN パスの **OID** 部分を使用します。Microsoft Active Directory は **CN** 部分を使用します。たとえば、Apache DS では **oid=testuser,dc=example,dc=com** などの DN パスを使用し、Microsoft Active Directory では **cn=testuser,dc=example,dc=com** などの DN パスを使用できます。

5. ブローカーを起動または再起動します (サービスまたはプロセス)。

5.4.1.1. 一致するパラメーターの検索

userSearchMatching

LDAP 検索操作に渡す前に、この設定パラメーターで指定される文字列の値は **java.text.MessageFormat** クラスで実装される文字列置換の内容により異なります。
つまり、特別な文字列 **{0}** は、受信クライアントの認証情報から抽出されたユーザー名に置き換えられます。置換後、この文字列は LDAP 検索フィルターとして解釈されます (構文は IETF 標準 RFC 2254 で定義されています)。

たとえば、このオプションが **(uid={0})** に設定され、受信したユーザー名が **jdoe** の場合には、文字列置換後の検索フィルターは **(uid=jdoe)** になります。

ユーザーベースが選択したサブツリー (**ou=User,ou=ActiveMQ,ou=system**) に、結果の検索フィルターが適用されると、エントリー **uid=jdoe,ou=User,ou=ActiveMQ,ou=system** にマッチします。

roleSearchMatching

これは、2 つの置換文字列をサポートする点を除き、**userSearchMatching** オプションと同じように機能します。
置換文字列 **{0}** は、一致したユーザーエントリーの DN をすべて置き換えます (つまり、ユーザー検索の結果)。たとえば、ユーザー **jdoe** の場合には、置換された文字列は **uid=jdoe,ou=User,ou=ActiveMQ,ou=system** になります。

置換文字列 **{1}** は、受信したユーザー名を置き換えます。たとえば、**jdoe** です。

このオプションを **(member=uid={1})** に設定し、受信したユーザー名が **jdoe** の場合には、文字列の置換後に検索フィルターは **(member=uid=jdoe)** になります (ApacheDS 検索フィルター構文を想定)。

ロールベース **ou=Group,ou=ActiveMQ,ou=system** で選択したサブツリーに、結果の検索フィルターが適用されると、**uid=jdoe** と同等の **member** 属性を持つすべてのロールエントリーがマッチします (**member** 属性の値は DN です)。

このオプションはデフォルト値がないため、ロールの検索が無効であっても常に設定する必要があります。OpenLDAP を使用すると、検索フィルターの構文は **(member:=uid=jdoe)** になります。

関連情報

- 検索フィルター構文の概要は、Oracle JNDI tutorial を参照してください。

5.4.2. LDAP 認証の設定

LegacyLDAPSecuritySettingPlugin セキュリティー設定プラグインは、**LDAPAuthorizationMap** および **cachedLDAPAuthorizationMap** で過去に AMQ 6 で処理されたセキュリティー情報を読み取り、できるだけ、この情報を対応する AMQ 7 セキュリティー設定に変換します。

AMQ 6 および AMQ 7 のブローカーのセキュリティー実装は、完全に一致しません。そのため、プラグインは、2 つのバージョン間の翻訳を実行し、ほぼ同等の機能を実現します。

以下の例は、プラグインを設定する方法を示しています。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **security-settings** 要素内に **security-setting-plugin** 要素を追加します。以下に例を示します。

```
<security-settings>
   <security-setting-plugin class-
name="org.apache.activemq.artemis.core.server.impl.LegacyLDAPSecuritySettingPlugin">
      <setting name="initialContextFactory" value="com.sun.jndi.ldap.LdapCtxFactory"/>
      <setting name="connectionURL"
value="ldap://localhost:1024"/>`ou=destinations,o=ActiveMQ,ou=system`
      <setting name="connectionUsername" value="uid=admin,ou=system"/>
      <setting name="connectionPassword" value="secret"/>
      <setting name="connectionProtocol" value="s"/>
      <setting name="authentication" value="simple"/>
   </security-setting-plugin>
</security-settings>
```

class-name

この実装は **org.apache.activemq.artemis.core.server.impl.LegacyLDAPSecuritySettingPlugin** です。

initialContextFactory

LDAP への接続に使用される初期コンテキストファクトリー。これは、常に **com.sun.jndi.ldap.LdapCtxFactory** (デフォルト値) に設定する必要があります。

connectionURL

LDAP URL **<ldap://Host:Port>** を使用してディレクトリーサーバーの場所を指定します。オプションでこの URL を修飾するには、スラッシュ / とその後にディレクトリーツリーの特定ノードの識別名 (DN) を追加します。例: **ldap://ldapserver:10389/ou=system**デフォルト値は **ldap://localhost:1024** です。

connectionUsername

ディレクトリーサーバーへの接続を開くユーザーの DN。たとえば、**uid=admin,ou=system** です。ディレクトリーサーバーでは、通常、クライアントが接続を開くためにユーザー名/パスワードの認証情報を提示する必要があります。

connectionPassword

connectionUsername の DN に一致するパスワード。 **Directory Information Tree** (DIT) のディレクトリーサーバーでは、パスワードは通常、対応するディレクトリーエントリーに **userPassword** 属性として保存されます。

connectionProtocol

現在は使用されていません。今後、このオプションを使用すると、ディレクトリーサーバーへの接続に Secure Socket Layer(SSL) を選択できます。このオプションはデフォルト値がないために明示的に設定する必要があります。

authentication

LDAP サーバーにバインドする際に使用する認証方法を指定します。このパラメーターの有効な値は **simple** (ユーザー名とパスワード) または **none** (匿名) です。デフォルト値は **simple** です。

注記

Simple Authentication and Security Layer(SASL) 認証はサポートされ **ません**。

前述の設定例に記載されていない他の設定は次のとおりです。

destinationBase

子がすべての宛先にパーミッションを提供するノードの DN を指定します。この場合、DN はリテラル値です (つまり、プロパティー値の文字列は置き換えられません)。たとえば、このプロパティーの通常の値は **ou=destinations,o=ActiveMQ,ou=system** で、デフォルト値は **ou=destinations,o=ActiveMQ,ou=system** です。

filter

あらゆる種類の宛先のパーミッションを検索するときに使用する LDAP 検索フィルターを指定します。検索フィルターは、キューまたはトピックノードの子孫の 1 つとの照合を試行します。デフォルト値は **(cn=*)** です。

roleAttribute

ロールの DN の値が **filter** に一致するノードの属性を指定します。デフォルト値は **uniqueMember** です。

adminPermissionValue

admin パーミッションに一致する値を指定します。デフォルト値は **admin** です。

readPermissionValue

read パーミッションに一致する値を指定します。デフォルト値は **read** です。

writePermissionValue

write パーミッションに一致する値を指定します。デフォルト値は **write** です。

enableListener

LDAP サーバーでのを自動的に受信し、ブローカーの認証設定をリアルタイムで更新するリスナーを有効にするかどうかを指定します。デフォルト値は **true** です。

mapAdminToManage

レガシー (AMQ 6) の **admin** パーミッションを AMQ 7 の **manage** パーミッションにマップするかどうかを指定します。以下の表のマッピングセマンティクスの詳細を参照してください。デフォルト値は **false** です。
LDAP で定義されたキューまたはトピックの名前は、セキュリティー設定の一致として機能し、パーミッション値は AMQ 6 タイプから AMQ 7 タイプにマッピングされ、ロールはそのままマッピングされます。LDAP で定義されたキューまたはトピックの名前はセキュリティー設定の一致として機能するため、セキュリティー設定は想定どおりに JMS 宛先に適用されない可能性があります。これは、必要に応じて、AMQ 7 は常に JMS 宛先を jms.queue.または jms.topic.で接頭辞を付けるためです。

AMQ 6 には、**read**、**write**、および **admin** の 3 つのパーミッションタイプがあります。これらのパーミッションタイプは、ActiveMQ の Web サイト (Security) に記載されています。

AMQ 7 には以下のパーミッションタイプがあります。

- **createAddress**
- **deleteAddress**
- **createDurableQueue**
- **deleteDurableQueue**
- **createNonDurableQueue**
- **deleteNonDurableQueue**
- **send**
- **consume**
- **manage**
- **browse**
以下の表は、セキュリティー設定プラグインが AMQ 6 パーミッションタイプを AMQ 7 パーミッションタイプにマッピングする方法を示しています。

AMQ 6 パーミッションタイプ	AMQ 7 のパーミッションタイプ
read	consume, browse
write	send
admin	createAddress、deleteAddress、createDurableQueue、deleteDurableQueue、createNonDurableQueue、deleteNonDurableQueue、manage(**mapAdminToManage** が **true** に設定されている場合)

下記のとおり、プラグインが AMQ 6 と AMQ 7 のパーミッションタイプ間の変換を実行するケースがあります。これにより、同等の機能を実現できます。

- AMQ 6 には同様のパーミッションタイプがないため、このマッピングにはデフォルトで、AMQ 7 の **manage** パーミッションタイプが含まれません。ただし、**mapAdminToManage** が **true** に設定されている場合、プラグインは AMQ 6 **admin** パーミッションを AMQ 7 **manage** にマップします。
- AMQ 6 の **admin** パーミッションタイプは、宛先が存在しない場合にブローカーが宛先を自動作成し、ユーザーがその宛先にメッセージを送信するかどうかを決定します。AMQ 7 では、ユーザーが宛先にメッセージを送信するパーミッションがある場合に、自動的に宛先の自動作成を許可します。したがって、プラグインは、デフォルトで、レガシー **admin** パーミッションを上記の AMQ 7 パーミッションにマップします。また、このプラグインは、**mapAdminToManage** が **true** に設定されている場合に、AMQ 6 **admin** パーミッションを AMQ 7 の **manage** パーミッションにマップします。

allowQueueAdminOnRead

createDurableQueue、createNonDurableQueue、および deleteDurableQueue パーミッションにレガシー読み取りパーミッションをマッピングするかどうか。これにより、JMS クライアントが admin パーミッションなしに永続サブスクリプションと非永続サブスクリプションを作成できます。これは AMQ 6 で許可されます。デフォルト値は false です。
以下の表は、**allowQueueAdminOnRead** が **true** の場合に、セキュリティー設定プラグインが AMQ 6 パーミッションタイプを AMQ 7 パーミッションタイプにマッピングする方法を示しています。

AMQ 6 パーミッションタイプ	AMQ 7 のパーミッションタイプ
read	consume, browse, createDurableQueue, createNonDurableQueue, deleteDurableQueue
write	send
admin	createAddress、deleteAddress、deleteNonDurableQueue、manage(**mapAdminToManage** が **true** に設定されている場合)

5.4.3. login.config ファイルでのパスワードの暗号化

組織は LDAP でデータを安全に保存することが多いので、**login.config** ファイルには、ブローカーが組織の LDAP サーバーと通信するために必要な設定を含めることができます。この設定ファイルには、通常、LDAP サーバーにログインするパスワードが含まれるため、このパスワードを暗号化する必要があります。

前提条件

- 「LDAP 認証の設定」 の説明に従って、必要なプロパティーを追加するように **login.config** ファイルを修正している。

手順

以下の手順は、**<broker_instance_dir>/etc/login.config** ファイルにある **connectionPassword** パラメーターの値をマスクする方法を示しています。

1. コマンドプロンプトで、**mask** ユーティリティーを使用してパスワードを暗号化します。

```
$ <broker_instance_dir>/bin/artemis mask <password>
```

```
result: 3a34fd21b82bf2a822fa49a8d8fa115d
```

2. **<broker_instance_dir>/etc/login.config** ファイルを開きます。**connectionPassword** パラメーターを見つけます。

```
connectionPassword = <password>
```

3. プレーンテキストのパスワードは、暗号化された値に置き換えます。

```
connectionPassword = 3a34fd21b82bf2a822fa49a8d8fa115d
```

4. 暗号化された値は、識別子 **"ENC()"** でラップします。

```
connectionPassword = "ENC(3a34fd21b82bf2a822fa49a8d8fa115d)"
```

login.config ファイルにマスクされたパスワードが追加されました。パスワードは **"ENC()"** 識別子でラップされるため、AMQ Broker では使用前にこれを復号化します。

関連情報

- AMQ Broker に含まれる設定ファイルの詳細は、AMQ Broker configuration files and locations を参照してください。

5.4.4. 外部ロールのマッピング

LDAP などの外部認証プロバイダーからのロールを、ブローカーによって内部で使用されるロールにマップできます。

外部ロールをマッピングするには、**broker.xml** 設定ファイルの **security-settings** 要素に role-mapping エントリーを作成します。以下は例になります。

```
<security-settings>
...
   <role-mapping from="cn=admins,ou=Group,ou=ActiveMQ,ou=system" to="my-admin-role"/>
   <role-mapping from="cn=users,ou=Group,ou=ActiveMQ,ou=system" to="my-user-role"/>
</security-settings>
```

注記

- ロールマッピングは加算されます。つまり、ユーザーは元のロールと、新たに割り当てられたロールを保持します。
- ロールマッピングは、キューアクセスを承認するロールにのみ影響し、Web コンソールアクセスを有効にする方法を提供しません。

5.5. 認証および承認での KERBEROS の使用

AMQP プロトコルでメッセージを送受信する場合、クライアントは **Simple Authentication and Security Layer** (SASL) フレームワークの GSSAPI メカニズムを使用して、AMQ Broker が認証する Kerberos セキュリティー認証情報を送信できます。Kerberos 認証情報は、認証されたユーザーを LDAP ディレクトリーまたはテキストベースのプロパティーファイルで設定された割り当てられたロールにマッピングすることで、承認にも使用できます。

Transport Layer Security (TLS) と共に SASL を使用して、メッセージングアプリケーションのセキュリティーを確保できます。SASL はユーザー認証を行い、TLS はデータの整合性を確保します。

重要

- AMQ Broker が Kerberos 認証情報を認証および承認する前に、Kerberos インフラストラクチャーをデプロイし、設定する必要があります。Kerberos のデプロイメントに関する詳細は、オペレーティングシステムのドキュメントを参照してください。
  - RHEL 7 の場合は、System-Level Authentication Guide の Using Kerberos 参照してください。
  - Windows の場合は、Kerberos Authentication Overview を参照してください。
- Oracle または IBM JDK のユーザーは、Java Cryptography Extension(JCE) をインストールする必要があります。詳細は、Oracle version of the JCE または IBM version of the JCE のドキュメントを参照してください。

以下の手順では、認証および承認に Kerberos を設定する方法を説明します。

5.5.1. Kerberos を使用するネットワーク接続の設定

AMQ Broker は、**Simple Authentication and Security Layer**(SASL) フレームワークの GSSAPI メカニズムを使用して、Kerberos セキュリティー認証情報と統合します。AMQ Broker で Kerberos を使用するには、Kerberos 認証情報を使用するクライアントを認証または承認する各アクセプターを GSSAPI メカニズムを使用するように設定する必要があります。

以下の手順では、Kerberos を使用するようにアクセプターを設定する方法を説明します。

前提条件

- AMQ Broker が Kerberos 認証情報を認証および承認する前に、Kerberos インフラストラクチャーをデプロイし、設定する必要があります。

手順

1. ブローカーを停止します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis stop
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe stop
   ```

2. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
3. name-value ペアの **saslMechanisms=GSSAPI** を **acceptor** の URL のクエリー文字列に追加します。

```
<acceptor name="amqp">
  tcp://0.0.0.0:5672?protocols=AMQP;saslMechanisms=GSSAPI
</acceptor>
```

上記の設定は、Kerberos クレデンシャルの認証時に、アクセプターが GSSAPI メカニズムを使用することを意味します。

4. (オプション) **PLAIN** および **ANONYMOUS** SASL メカニズムもサポートされます。複数のメカニズムを指定するには、コンマ区切りリストを使用します。以下に例を示します。

```
<acceptor name="amqp">
  tcp://0.0.0.0:5672?protocols=AMQP;saslMechanisms=GSSAPI,PLAIN
</acceptor>
```

結果は、**GSSAPI** および **PLAIN** SASL メカニズムの両方を使用するアクセプターです。

5. ブローカーを起動します。

a. Linux の場合:

```
<broker_instance_dir>/bin/artemis run
```

b. Windows の場合:

```
<broker_instance_dir>\bin\artemis-service.exe start
```

関連情報

- アクセプターの詳細は、「アクセプターについて」 を参照してください。

5.5.2. Kerberos 認証情報を使用したクライアントの認証

AMQ Broker は、**Simple Authentication and Security Layer**(SASL) フレームワークからの GSSAPI メカニズムを使用する AMQP 接続の Kerberos 認証をサポートします。

ブローカーは、**Java Authentication and Authorization Service**(JAAS) を使用して Kerberos アクセプターの認証情報を取得します。Java インストールに含まれる JAAS ライブラリーは、Kerberos 認証情報を認証するログインモジュール **Krb5LoginModule** でパッケージ化されています。**Krb5LoginModule** の詳細は、Java ベンダーのドキュメントを参照してください。たとえば、Oracle は、Java 8 ドキュメント の一部として、**Krb5LoginModule** ログインモジュールに関する情報を提供します。

前提条件

- Kerberos セキュリティー認証情報を使用して AMQP 接続を承認する前に、アクセプターの GSSAPI メカニズムを有効にする必要があります。詳細は、「Kerberos を使用するネットワーク接続の設定」 を参照してください。

手順

1. ブローカーを停止します。

a. Linux の場合:

```
<broker_instance_dir>/bin/artemis stop
```

b. Windows の場合:

```
<broker_instance_dir>\bin\artemis-service.exe stop
```

2. **<broker_instance_dir>/etc/login.config** 設定ファイルを開きます。
3. **amqp-sasl-gssapi** という名前の設定スコープを追加します。以下の例は、Oracle および OpenJDK バージョンの JDK にある **Krb5LoginModule** の設定を示しています。

```
amqp-sasl-gssapi {
   com.sun.security.auth.module.Krb5LoginModule required
   isInitiator=false
   storeKey=true
   useKeyTab=true
   principal="amqp/my_broker_host@example.com"
   debug=true;
};
```

amqp-sasl-gssapi

デフォルトでは、ブローカーの GSSAPI メカニズム実装は **amqp-sasl-gssapi** という名前の JAAS 設定スコープを使用して Kerberos アクセプター認証情報を取得します。

Krb5LoginModule

このバージョンの **Krb5LoginModule** は、Oracle および OpenJDK バージョンの JDK で提供されます。Java ベンダーのドキュメントを参照して、**Krb5LoginModule** の完全修飾クラス名とその利用可能なオプションを確認します。

useKeyTab

Krb5LoginModule は、プリンシパルの認証時に Kerberos キータブを使用するように設定されます。キータブは、Kerberos 環境からツールを使用して生成されます。Kerberos キータブの生成に関する詳細は、ベンダーのドキュメントを参照してください。

principal

プリンシパルは **amqp/my_broker_host@example.com** に設定されます。この値は、Kerberos 環境で作成されたサービスプリンシパルに対応する必要があります。サービスプリンシパルの作成に関する詳細は、ベンダーのドキュメントを参照してください。

4. ブローカーを起動します。
   a. Linux の場合:

```
<broker_instance_dir>/bin/artemis run
```

   b. Windows の場合:

```
<broker_instance_dir>\bin\artemis-service.exe start
```

5.5.2.1. 代替設定スコープの使用

AMQP アクセプターの URL にパラメーター **saslLoginConfigScope** を追加して、 別の設定スコープを指定できます。以下の設定例では、**saslLoginConfigScope** パラメーターに **alternative-sasl-gssapi** の値が指定されています。結果は、**<broker_instance_dir>/etc/login.config** で宣言される **alternative-sasl-gssapi** という名前の代わりのスコープを使用するアクセプターです。

```
<acceptor name="amqp">
tcp://0.0.0.0:5672?
protocols=AMQP;saslMechanisms=GSSAPI,PLAIN;saslLoginConfigScope=alternative-sasl-gssapi`
```

```
</acceptor>
```

5.5.3. Kerberos 認証情報を使用したクライアントの承認

AMQ Broker には、ロールのマッピング時に他のセキュリティーモジュールで使用される JAAS **Krb5LoginModule** ログインモジュールの実装が含まれています。モジュールは、Kerberos 認証されていないピアプリンシパルを AMQ Broker UserPrincipal として設定された Subject のプリンシパルに追加します。その後、認証情報は **PropertiesLoginModule** または **LDAPLoginModule** モジュールに渡して、Kerberos 認証のピアプリンシパルを AMQ Broker ロールにマップできます。

注記

Kerberos ピアプリンシパルはロールメンバーとしてのみ存在し、ブローカーユーザーとしては存在しません。

前提条件

- Kerberos セキュリティー認証情報を使用して AMQP 接続を承認する前に、アクセプターの GSSAPI メカニズムを有効にする必要があります。

手順

1. ブローカーを停止します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis stop
   ```

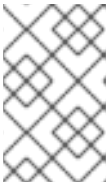
   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe stop
   ```

2. **<broker_instance_dir>/etc/login.config** 設定ファイルを開きます。
3. AMQ Broker **Krb5LoginModule** および **LDAPLoginModule** の設定を追加します。LDAP プロバイダーのドキュメントを参照して、設定オプションを確認します。
   以下は設定例です。

```
org.apache.activemq.artemis.spi.core.security.jaas.Krb5LoginModule required
    ;
org.apache.activemq.artemis.spi.core.security.jaas.LDAPLoginModule optional
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="ldap://localhost:1024"
    authentication=GSSAPI
    saslLoginConfigScope=broker-sasl-gssapi
    connectionProtocol=s
    userBase="ou=users,dc=example,dc=com"
    userSearchMatching="(krb5PrincipalName={0})"
    userSearchSubtree=true
    authenticateUser=false
    roleBase="ou=system"
    roleName=cn
```

```
    roleSearchMatching="(member={0})"
    roleSearchSubtree=false
    ;
```



注記

上記の例で示される **Krb5LoginModule** のバージョンは AMQ Broker で配布され、Kerberos アイデンティティーをロールマッピングに使用できるブローカーアイデンティティーに変換します。

4. ブローカーを起動します。

   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis run
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe start
   ```

関連情報

- AMQ Broker で GSSAPI メカニズムを有効にする方法は、「Kerberos を使用するネットワーク接続の設定」 を参照してください。
- **PropertiesLoginModule** の詳細は、「基本的なユーザーとパスワード認証の設定」 を参照してください。
- **LDAPLoginModule** の詳細は、「クライアント認証用の LDAP の設定」 を参照してください。

5.6. セキュリティーマネージャーの指定

ブローカーは、**セキュリティーマネージャー** と呼ばれるコンポーネントを使用して認証および承認を処理します。

AMQ Broker には 2 つのセキュリティーマネージャーが含まれています。

- **ActiveMQJAASSecurityManager** セキュリティーマネージャー。このセキュリティーマネージャーは、JAAS および Red Hat JBoss Enterprise Application Platform(JBoss EAP) のセキュリティーとの統合を提供します。これは、AMQ Broker によって使用される **デフォルト** のセキュリティーマネージャーです。
- **ActiveMQBasicSecurityManager** セキュリティーマネージャー。この基本セキュリティーマネージャーは JAAS をサポートしません。代わりに、ユーザー名とパスワードの認証情報による認証および承認をサポートします。このセキュリティーマネージャーは、管理 API を使用したユーザーの追加、削除、および更新をサポートします。ユーザーとロールデータはブローカーバインディングジャーナルに保存されます。つまり、ライブブローカーに加えられた変更はバックアップブローカーでも利用できることになります。

含まれるセキュリティーマネージャーの代わりに、システム管理者はブローカーセキュリティーの実装をより詳細に制御することをお勧めします。このような場合には、ブローカー設定で **カスタム** セキュリティーマネージャーを指定することもできます。カスタムセキュリティーマネージャーは、**org.apache.activemq.artemis.spi.core.security.ActiveMQSecurityManager5** インターフェイスを実装するユーザー定義のクラスです。

以下のサブセクションの例では、使用するブローカーを設定する方法を示しています。

- デフォルトの JAAS セキュリティーマネージャーではなく基本セキュリティーマネージャー
- カスタムセキュリティーマネージャー

5.6.1. 基本的なセキュリティーマネージャーの使用

AMQ Broker には、デフォルトの **ActiveMQJAASSecurityManager** セキュリティーマネージャーの他に、**ActiveMQBasicSecurityManager** セキュリティーマネージャーも含まれています。

基本的なセキュリティーマネージャーを使用する場合には、すべてのユーザーおよびロールデータはバインディングジャーナル (または JDBC 永続性を使用している場合は バインディング **テーブル**) に保存されます。したがって、ライブバックアップブローカーグループを設定している場合、ライブブローカーで peform というユーザー管理は、フェイルオーバー時にバックアップブローカーに自動的に反映されます。これにより、LDAP サーバーを個別に管理する必要がなくなりました。これは、この動作を達成する代替方法です。

基本的なセキュリティーマネージャーを設定して使用する前に、以下の点に留意してください。

- 基本的なセキュリティーマネージャーは、デフォルトの JAAS セキュリティーマネージャーのようにプラグ可能でありません。
- 基本的なセキュリティーマネージャーは JAAS をサポートしません。代わりに、ユーザー名とパスワードの認証情報による認証および承認のみをサポートします。
- AMQ 管理コンソールには JAAS が必要です。そのため、基本的なセキュリティーマネージャーを使用し、コンソールを使用する必要がある場合は、ユーザーおよびパスワード認証用の **login.config** 設定ファイルも設定する必要があります。ユーザーおよびパスワード認証の設定に関する詳細は、「基本的なユーザーとパスワード認証の設定」 を参照してください。
- AMQ Broker では、ユーザー管理 はブローカー管理 API によって提供されます。この管理には、ユーザーとロールを追加、一覧表示、更新、および削除する機能が含まれます。これらの機能は、JMX、管理メッセージ、HTTP(Jolokia または AMQ 管理コンソール) および AMQ Broker コマンドラインインターフェイスを使用して実行できます。ブローカーはこのデータを直接格納するため、ユーザーを管理するためにブローカーを実行する必要があります。バインディングデータを手動で変更する方法はありません。
- HTTP(Jolokia または AMQ 管理コンソールを使用するなど) による管理アクセスは、コンソール JAAS ログインモジュールによって処理されます。JConsole またはその他のリモート JMX ツールによる MBean アクセスは、基本的なセキュリティーマネージャーによって処理されます。管理メッセージは、基本的なセキュリティーマネージャーによって処理されます。

5.6.1.1. 基本的なセキュリティーマネージャーの設定

以下の手順は、基本的なセキュリティーマネージャーを使用するようにブローカーを設定する方法を説明します。

手順

1. **<broker-instance-dir>/etc/boostrap.xml** 設定ファイルを編集します。
2. **security-manager** 要素の **class-name** 属性に、**ActiveMQBasicSecurityManager** クラス名をすべて指定します。

```
<broker xmlns="http://activemq.org/schema">
```

```
  ...
  <security-manager class-
name="org.apache.activemq.artemis.spi.core.security.ActiveMQBasicSecurityManager">
  </security-manager>
  ...
</broker>
```

3. ユーザーおよびロールデータを保持するバインディングデータを手動で変更することはできず、ブローカーを実行してユーザーを管理する必要があるため、初回起動時にブローカーのセキュリティーを保護することを推奨します。これを行うには、認証情報を使って他の **ユーザーを追加できるブートストラップ** ユーザーを定義します。
security-manager 要素に **bootstrapUser**、**bootstrapPassword**、および **bootstrapRole** プロパティーを追加し、値を指定します。以下は例になります。

```
<broker xmlns="http://activemq.org/schema">
  ...
  <security-manager class-
name="org.apache.activemq.artemis.spi.core.security.ActiveMQBasicSecurityManager">
      <property key="bootstrapUser" value="myUser"/>
      <property key="bootstrapPassword" value="myPass"/>
      <property key="bootstrapRole" value="myRole"/>
  </security-manager>
  ...
</broker>
```

bootstrapUser

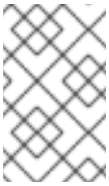
ブートストラップユーザーの名前。

bootstrapPassword

boostrap ユーザーの Passsword。暗号化したパスワードを指定することもできます。

bootstrapRole

boostrap ユーザーのロール。



注記

設定でブートストラップユーザーの前述のプロパティーを定義する場合、ブローカーの実行中に加える変更に関係なく、これらの認証情報はブローカーを起動するたびに設定されます。

4. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

5. **broker.xml** 設定ファイルで、**activemq.management#** アドレス一致に対してデフォルトで定義される **address-setting** 要素を見つけます。これらのデフォルトアドレス設定を以下に示します。

```
<address-setting match="activemq.management#">
   <dead-letter-address>DLQ</dead-letter-address>
   <expiry-address>ExpiryQueue</expiry-address>
   <redelivery-delay>0</redelivery-delay>
   <!--...-->
   <max-size-bytes>-1</max-size-bytes>
   <message-counter-history-day-limit>10</message-counter-history-day-limit>
   <address-full-policy>PAGE</address-full-policy>
```

```
    <auto-create-queues>true</auto-create-queues>
    <auto-create-addresses>true</auto-create-addresses>
    <auto-create-jms-queues>true</auto-create-jms-queues>
    <auto-create-jms-topics>true</auto-create-jms-topics>
</address-setting>
```

6. **activemq.management#** アドレス一致向けのアドレス設定内に、この手順で以前に指定したブートストラップロール名に対して、以下の必要なパーミッションを追加します。

   - **createNonDurableQueue**
   - **createAddress**
   - **consume**
   - **manage**
   - **send**

   以下は例になります。

```
<address-setting match="activemq.management#">
   ...
   <permission type="createNonDurableQueue" roles="myRole"/>
   <permission type="createAddress" roles="myRole"/>
   <permission type="consume" roles="myRole"/>
   <permission type="manage" roles="myRole"/>
   <permission type="send" roles="myRole"/>
</address-setting>
```

関連情報

- **ActiveMQBasicSecurityManager** クラスの詳細は、ActiveMQ Artemis Core API ドキュメントの Class ActiveMQBasicSecurityManager を参照してください。
- 設定ファイルでパスワードを暗号化する方法は、「設定ファイルのパスワードの暗号化」 を参照してください。

5.6.2. カスタムセキュリティーマネージャーの指定

以下の手順では、ブローカー設定でカスタムセキュリティーマネージャーを指定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/boostrap.xml** 設定ファイルを編集します。
2. **security-manager** 要素の **class-name** 属性に、**org.apache.activemq.artemis.spi.core.security.ActiveMQSecurityManager5** インターフェイスのユーザー定義の実装であるクラスを指定します。以下に例を示します。

```
<broker xmlns="http://activemq.org/schema">
  ...
  <security-manager class-name="com.foo.MySecurityManager">
    <property key="myKey1" value="myValue1"/>
```

```
      <property key="myKey2" value="myValue2"/>
   </security-manager>
   ...
</broker>
```

関連情報

- **ActiveMQSecurityManager5** インターフェイスの詳細は、ActiveMQ Artemis Core API ドキュメントの Interface ActiveMQSecurityManager5 を参照してください。

5.6.3. カスタムセキュリティーマネージャーのサンプルプログラムの実行

AMQ Broker には、カスタムセキュリティーマネージャーの実装方法を実証するサンプルプログラムが含まれています。この例では、カスタムセキュリティーマネージャーは認証および承認の詳細をログに記録してから、その詳細を **ActiveMQJAASSecurityManager** (デフォルトのセキュリティーマネージャー) のインスタンスに渡します。

以下の手順は、カスタムセキュリティーマネージャーのサンプルプログラムを実行する方法を示しています。

前提条件

- AMQ Broker サンプルプログラムを実行するようにマシンを設定する必要があります。詳細は、Running the AMQ Broker examples を参照してください。

手順

1. カスタムセキュリティーマネージャーの例が含まれるディレクトリーに移動します。

```
$ cd <install_dir>/examples/features/standard/security-manager
```

2. サンプルを実行します。

```
$ mvn verify
```

注記

サンプルプログラムの実行時にブローカーインスタンスを手動で作成して起動する場合は、前の手順のコマンドを **mvn -PnoServer verify** に置き換えてください。

関連情報

- **ActiveMQJAASSecurityManager** クラスの詳細は、ActiveMQ Artemis Core API ドキュメントの Class ActiveMQJAASSecurityManager を参照してください。

5.7. セキュリティーの無効化

セキュリティーはデフォルトで**有効**になっています。以下の手順では、ブローカーセキュリティーを無効にする方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

2. **core** 要素で、**security-enabled** の値を **false** に設定します。

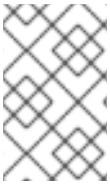
```
<security-enabled>false</security-enabled>
```

3. 必要に応じて、**security-invalidation-interval** の新しい値をミリ秒単位で指定します。このプロパティーの値は、ブローカーが定期的にセキュアなログインを無効にするかどうかを指定します。デフォルト値は **10000** です。

5.8. 検証済みユーザーからのメッセージの追跡

メッセージの発信元の追跡およびロギングを有効にするには (セキュリティー監査の目的など)、**_AMQ_VALIDATED_USER** メッセージキーを使用できます。

broker.xml 設定ファイルで **populate-validated-user** オプションが **true** に設定されている場合には、ブローカーは **_AMQ_VALIDATED_USER** キーを使用して検証済みユーザーの名前をメッセージに追加します。JMS および STOMP クライアントの場合には、このメッセージキーは **JMSXUserID** キーにマッピングされます。



注記

ブローカーは、AMQP JMS クライアントによって生成されたメッセージに、検証されたユーザー名を追加できません。クライアントによって送信された AMQP メッセージのプロパティーを変更すると、AMQP プロトコルの違反があります。

自分の SSL 証明書を基に認証されるユーザーの場合、ブローカーによって設定される検証されたユーザー名は、証明書の識別名 (DN) マップの名前です。

broker.xml 設定ファイルで **security-enabled** が **false** で、**populate-validated-user** が **true** の場合に、ブローカーはクライアントが指定するユーザー名 (ある場合) を指定します。**populate-validated-user** オプションのデフォルトは **false** です。

メッセージの送信時に、クライアントによりユーザー名 (つまり、**JMSXUser ID** キー) がまだ入力されていないメッセージを拒否するようにブローカーを設定できます。ブローカーはこれらのクライアントによって送信されたメッセージについて検証されたユーザー名自体を設定できないため、このオプションが AMQP クライアントに役立ちます。

クライアントによって **JMSXUserID** が設定されていないメッセージを拒否するようにブローカーを設定するには、以下の設定を **broker.xml** 設定ファイルに追加します。

```
<reject-empty-validated-user>true</reject-empty-validated-user>
```

デフォルトでは、**reject-empty-validated-user** は **false** に設定されます。

5.9. 設定ファイルのパスワードの暗号化

デフォルトでは、AMQ Broker はすべてのパスワードをプレーンテキストとして設定ファイルに保存します。承認されていないアクセスを防ぐために、適切なパーミッションですべての設定ファイルのセキュリティーを保護するようにしてください。また、プレーンテキストのパスワードを暗号化するか、**マスク** して、不要なビューアーが読み込まれないようにすることもできます。

5.9.1. 暗号化パスワードについて

暗号化 (**マスクされた**) パスワードは、プレーンテキストのパスワードが暗号化されたバージョンで

す。暗号化バージョンは、AMQ Broker によって提供される **mask** コマンドラインユーティリティーによって生成されます。**mask** ユーティリティーの詳細は、コマンドラインのヘルプドキュメントを参照してください。

```
$ <broker_instance_dir>/bin/artemis help mask
```

パスワードをマスクするには、プレーンテキストの値を暗号化された値に置き換えます。マスクされたパスワードは、実際の値が必要になったときに復号化されるように、識別子 **ENC()** でラップする必要があります。

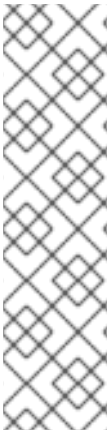
以下の例では、**<broker_instance_dir>/etc/bootstrap.xml** 設定ファイルには、**keyStorePassword** パラメーターおよび **trustStorePassword** パラメーターのマスクされたパスワードが含まれます。

```
<web bind="https://localhost:8443" path="web"
    keyStorePassword="ENC(-342e71445830a32f95220e791dd51e82)"
    trustStorePassword="ENC(32f94e9a68c45d89d962ee7dc68cb9d1)">
   <app url="activemq-branding" war="activemq-branding.war"/>
</web>
```

以下の設定ファイルでは、マスクされたパスワードを使用できます。

- broker.xml
- bootstrap.xml
- management.xml
- artemis-users.properties
- login.config(**LDAPLoginModule** で使用)

設定ファイルは **<broker_instance_dir>/etc** にあります。



注記

artemis-users.properties は、ハッシュ化されたパスワードをマスクする場合のみサポートします。ブローカーの作成時にユーザーが作成されると、**artemis-users.properties** にはデフォルトでハッシュ化されたパスワードが含まれます。デフォルトの **PropertiesLoginModule** は **artemis-users.properties** ファイルのパスワードを復号化しませんが、代わりに入力をハッシュ化してパスワード検証の 2 つのハッシュ値を比較します。ハッシュ化パスワードをマスクされたパスワードに変更しても、AMQ Broker 管理コンソールにはアクセスできません。

broker.xml、**bootstrap.xml**、**management.xml**、および **login.config** はマスクされているが、ハッシュ化されていないパスワードをサポートします。

5.9.2. 設定ファイルでのパスワードの暗号化

以下の例は、**broker.xml** 設定ファイルで **cluster-password** の値をマスクする方法を示しています。

手順

1. コマンドプロンプトで、**mask** ユーティリティーを使用してパスワードを暗号化します。

```
$ <broker_instance_dir>/bin/artemis mask <password>
```

```
result: 3a34fd21b82bf2a822fa49a8d8fa115d
```

2. マスクするプレーンテキストのパスワードが含まれる **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。

```
<cluster-password>
  <password>
</cluster-password>
```

3. プレーンテキストのパスワードは、暗号化された値に置き換えます。

```
<cluster-password>
  3a34fd21b82bf2a822fa49a8d8fa115d
</cluster-password>
```

4. 暗号化された値を識別子 **ENC()** でラップします。

```
<cluster-password>
  ENC(3a34fd21b82bf2a822fa49a8d8fa115d)
</cluster-password>
```

設定ファイルには、暗号化されたパスワードが含まれるようになりました。パスワードは **ENC()** 識別子でラップされるため、AMQ Broker では使用前にこれを復号化します。

関連情報

- AMQ Broker に含まれる設定ファイルの詳細は、「AMQ Broker の設定ファイルおよび場所」を参照してください。

第6章 メッセージデータの永続化

AMQ Broker には、メッセージデータの永続化 (つまり **格納**) の 2 つのオプションがあります。

ジャーナルでのメッセージの永続化

以下はデフォルトのオプションになります。ジャーナルベースの永続性は、ファイルシステムのジャーナルにメッセージを書き込む高パフォーマンスオプションです。

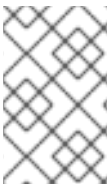
データベースのメッセージの永続化

このオプションは、**Java Database Connectivity** (JDBC) 接続を使用して、選択したデータベースにメッセージを永続化します。

または、ブローカーを設定して、メッセージデータを永続化し **ない** ようにすることもできます。詳細は、「永続性の無効化」 を参照してください。

ブローカーは、メッセージジャーナル以外で大きなメッセージを永続化するために別のソリューションを使用します。詳細は、*8章 大きなメッセージの処理* を参照してください。

ブローカーは、メモリー不足の状況でメッセージをディスクにページングするように設定することもできます。詳細は、「メッセージのページングの設定」 を参照してください。



注記

AMQ Broker でサポートされるデータベースおよびネットワークファイルシステムに関する現在の情報は、Red Hat カスタマーポータルの Red Hat AMQ 7 Supported Configurations を参照してください。

6.1. ジャーナルでのメッセージデータの永続化

ブローカージャーナルは、ディスク上の **append-only** のファイルセットです。各ファイルは固定サイズに事前作成され、最初にパディングが入力されます。メッセージング操作がブローカーで実行されると、レコードがジャーナルの最後に追加されます。レコードを追加すると、ブローカーはディスクヘッドの移動およびランダムアクセス操作を最小限に抑えることができます。これは通常、ディスク上で最も遅い操作です。1 つのジャーナルファイルが満杯になると、ブローカーは新しいジャーナルファイルを作成します。

ジャーナルファイルサイズは設定可能です。各ファイルによって使用されるディスクリプラーの数を最小限に抑えることができます。最新のディスクトポロジーは複雑で、ブローカーはファイルのマッピング先の cylinder を制御することはできません。そのため、ジャーナルファイルのサイジングは正確に制御するのが難しくなります。

ブローカーが使用するその他の永続性関連の機能は、以下のとおりです。

- 特定のジャーナルファイルがまだ使用中かどうかを判断する **ガベージコレクション** アルゴリズム。ジャーナルファイルが使用されなくなった場合、ブローカーはファイルを再利用できるように回収できます。
- ジャーナルからデッドスペースを削除し、データを圧縮する圧縮アルゴリズム。これにより、ジャーナルがディスク上のファイル数より小さくなります。
- ローカルトランザクションのサポート。
- JMS クライアントを使用する場合の Extended Architecture(XA) トランザクションのサポート。

ジャーナルのほとんどは Java で記述されています。ただし、実際のファイルシステムとの対話は抽象化されるため、さまざまなプラグ可能な実装を使用できます。AMQ Broker には以下の実装が含まれます。

NIO

NIO(New I/O) は標準の Java NIO を使用してファイルシステムとインターフェイスします。これにより、非常に優れたパフォーマンスを実現し、Java 6 以降のランタイムを備えたプラットフォーム上で稼働します。Java NIO の詳細は、Java NIO を参照してください。

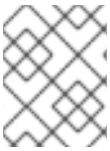
AIO

AIO(Aynshcronous I/O) は、シンネイティブラッパーを使用して、Linux Asynchronous I/O Library(**libaio**) と通信します。AIO では、ブローカーはデータがディスクの作成後に呼び出されるので、同期を明示的に回避できます。デフォルトでは、ブローカーは AIO ジャーナルの使用を試み、AIO が利用できない場合は NIO を使用するようにフォールバックします。
通常 AIO は Java NIO よりもさらにパフォーマンスが優れています。**libaio** のインストール方法は、「Linux 非同期 I/O ライブラリーのインストール」 を参照してください。

以下のサブセクションにある手順は、ジャーナルベースの永続性をブローカーに設定する方法を表しています。

6.1.1. Linux 非同期 I/O ライブラリーのインストール

Red Hat は、永続性のパフォーマンスを向上させるために AIO ジャーナル (NIO ではなく) を使用することを推奨しています。



注記

他のオペレーティングシステムや、それ以前のバージョンの Linux カーネルで AIO ジャーナルを使用することは**できません**。

AIO ジャーナルを使用するには、Linux Asynchronous I/O Library(**libaio**) をインストールする必要があります。**libaio** をインストールするには、以下のように **yum** コマンドを使用します。

```
yum install libaio
```

6.1.2. ジャーナルベースの永続性の設定

以下の手順では、ブローカーがジャーナルベースの永続性に使用するデフォルト設定を確認する方法を説明します。この説明を使用すると、必要に応じて設定を調整できます。

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
デフォルトでは、ブローカーは以下のようにジャーナルベースの永続性を使用するように設定されています。

```
<configuration>
 <core>
  ...
  <persistence-enabled>true</persistence-enabled>
  <journal-type>ASYNCIO</journal-type>
  <bindings-directory>./data/bindings</bindings-directory>
  <journal-directory>./data/journal</journal-directory>
  <journal-datasync>true</journal-datasync>
  <journal-min-files>2</journal-min-files>
```

```
    <journal-pool-files>-1</journal-pool-files>
    <journal-device-block-size>4096</journal-device-block-size>
    <journal-file-size>10M</journal-file-size>
    <journal-buffer-timeout>12000</journal-buffer-timeout>
    <journal-max-io>4096</journal-max-io>
    ...
  </core>
</configuration>
```

persistence-enabled

このパラメーターの値を **true** に設定すると、ブローカーはメッセージ永続性にファイルベースのジャーナルを使用します。

journal-type

使用するジャーナルのタイプ。**ASYNCIO** に設定されている場合には、ブローカーはまず AIO の使用を試行します。AIO が見つからない場合、ブローカーは NIO を使用します。

bindings-directory

バインディングジャーナルのファイルシステムの場所。デフォルト値は、**<broker_instance_dir>** ディレクトリーを起点とした相対パスです。

journal-directory

メッセージジャーナルのファイルシステムの場所。デフォルト値は、**<broker_instance_dir>** ディレクトリーを起点とした相対パスです。

journal-datasync

このパラメーターの値を **true** に設定すると、ブローカーは **fdatasync** 関数を使用してディスク書き込みを確認します。

journal-min-files

ブローカーの起動時に最初に作成するジャーナルファイルの数。

journal-pool-files

未使用のファイルを回収した後に保持するファイルの数。デフォルト値の **-1** は、クリーンアップ中にファイルが削除されないことを意味します。

journal-device-block-size

ストレージデバイスのジャーナルが使用するデータブロックの最大サイズ (バイト単位)。デフォルト値は 4096 バイトです。

journal-file-size

指定したジャーナルディレクトリーの各ジャーナルファイルの最大サイズ (バイト単位)。この制限に達すると、ブローカーは新規ファイルを起動します。このパラメーターは、バイト表記 (K、M、G など)、または同等のバイナリー (Ki、Mi、Gi) もサポートします。このパラメーターが設定で明示的に指定されていない場合、デフォルト値は 10485760 バイト (10MiB) になります。

journal-buffer-timeout

ブローカーがジャーナルバッファーをフラッシュする頻度をナノ秒で指定します。通常、AIO は NIO よりも高いフラッシュレートを使用するため、ブローカーは NIO と AIO の異なるデフォルト値を維持します。このパラメーターが設定で明示的に指定されていない場合、NIO のデフォルト値は 3333333 ナノ秒 (つまり、1 秒あたり 300 回) になります。AIO のデフォルト値は 50000 ナノ秒 (例: 2000 回/秒) です。

journal-max-io

いつでも IO キューに格納できる書き込み要求の最大数。キューが満杯になると、ブローカーは領域が利用可能になるまで追加の書き込みをブロックします。

NIO を使用している場合、この値は常に **1** である必要があります。AIO を使用し、このパラメーターが明示的に設定されていない場合、デフォルト値は **500** になります。

2. 上記の説明に基づいて、ストレージデバイスの必要に応じて永続性設定を調整します。

関連情報

- ジャーナルベースの永続性設定に使用できる **全** パラメーターの詳細は、付録E *メッセージングジャーナル設定要素* を参照してください。

6.1.3. バインディングジャーナルについて

バインディングジャーナルは、ブローカーにデプロイされたキューのセットや属性などのバインディング関連のデータを保存するために使用されます。また、ID シーケンスカウンターなどのデータも格納します。

バインディングジャーナルは常に NIO を使用します。これは通常、メッセージジャーナルと比べるとスループットが低くなるためです。このジャーナルのファイルには **activemq-bindings** という接頭辞が付けられます。各ファイルには拡張子 **.bindings** があり、デフォルトサイズは 1048576 バイトです。

バインディングジャーナルを設定するには、**<broker_instance_dir>/etc/broker.xml** 設定ファイルの **core** 要素に以下のパラメーターを追加します。

bindings-directory

バインディングジャーナルのディレクトリー。デフォルト値は **<broker_instance_dir>/data/bindings** です。

create-bindings-dir

このパラメーターの値を **true** に設定すると、ブローカーは **bindings-directory** で指定された場所 (存在しない場合) にバインディングディレクトリーを自動的に作成します。デフォルト値は **true** です。

6.1.4. JMS ジャーナルについて

JMS ジャーナルは、JMS キュー、トピック、接続ファクトリー、ならびにこれらのリソースの JNDI バインディングを含む JMS 関連のデータをすべて格納します。管理 API で作成された JMS リソースはこのジャーナルに永続化されますが、設定ファイルを介して設定されたリソースは永続化されません。ブローカーは、JMS が使用されている場合に ***のみ*** JMS ジャーナルを作成します。

JMS ジャーナルのファイルには **activemq-jms** という接頭辞が付けられます。各ファイルには拡張子 **.jms** があり、デフォルトサイズは 1048576 バイトです。

JMS ジャーナルはバインディングジャーナルと設定を共有します。

関連情報

- バインディングジャーナルの詳細は、「バインディングジャーナルについて」 を参照してください。

6.1.5. ジャーナルファイルの圧縮

AMQ Broker には、ジャーナルからデッド領域を削除し、データの圧縮解除によりディスク領域が少なくなるようにする圧縮アルゴリズムが含まれています。

以下のサブセクションでは、以下の方法を示しています。

- 特定の基準が満たされたときにジャーナルファイルを自動的に圧縮するようにブローカーを設定する
- コマンドラインインターフェイスからの圧縮プロセスの手動による実行

6.1.5.1. ジャーナルファイル圧縮の設定

ブローカーは以下の基準を使用して、圧縮を開始するタイミングを決定します。

- ジャーナル用に作成されたファイルの数。
- ジャーナルファイルのライブデータの割合。

これらの基準に設定された値に達した後、圧縮プロセスはジャーナルを解析し、デッドレコードをすべて削除します。そのため、ジャーナルにはファイルが少なくなります。

以下の手順は、ジャーナルファイルコンパクション にブローカーを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素内に **journal-compact-min-files** パラメーターおよび **journal-compact-percentage** パラメーターを追加し、値を指定します。以下は例になります。

```
<configuration>
  <core>
    ...
    <journal-compact-min-files>15</journal-compact-min-files>
    <journal-compact-percentage>25</journal-compact-percentage>
    ...
  </core>
</configuration>
```

journal-compact-min-files

圧縮の開始前にブローカーが最小限作成する必要のあるジャーナルファイル数。デフォルト値は **10** です。値を **0** に設定すると、圧縮が無効になります。ジャーナルのサイズが無限に増加する可能性があるため、コンパクションの無効化に注意する必要があります。

journal-compact-percentage

ジャーナルファイルのライブデータの割合。この割合より少ない場合にはライブデータとみなされ、 (**journal-compact-min-files** の設定値に達した場合)、圧縮が開始されます。デフォルト値は **30** です。

6.1.5.2. コマンドラインインターフェイスからの圧縮の実行

以下の手順では、コマンドラインインターフェイス (CLI) を使用してジャーナルファイルを圧縮する方法を説明します。

手順

1. **<broker_instance_dir>** ディレクトリーの所有者として、ブローカーを停止します。以下の例は、ユーザー **amq-broker** を示しています。

```
su - amq-broker
cd <broker_instance_dir>/bin
$ ./artemis stop
```

2. (オプション) 以下の CLI コマンドを実行して、データツールのパラメーターの全一覧を取得します。デフォルトでは、このツールは **<broker_instance_dir>/etc/broker.xml** にある設定を使用します。

```
$ ./artemis help data compact.
```

3. 以下の CLI コマンドを実行して、データを圧縮します。

```
$ ./artemis data compact.
```

4. ツールがデータを正常に圧縮したら、ブローカーを再起動します。

```
$ ./artemis run
```

関連情報

- AMQ Broker には、ジャーナルファイル管理用の CLI コマンドが多数含まれています。詳細は、付録の コマンドラインツール を参照してください。

6.1.6. ディスク書き込みキャッシュの無効化

ほとんどのディスクには、ハードウェア書き込みキャッシュが含まれます。書き込みキャッシュは、後でディスクに遅延書き込みされるため、ディスクの見かけのパフォーマンスを向上させることができます。多くのシステムでは、ディスク書き込みキャッシュがデフォルトで有効になっています。つまり、オペレーティングシステムから同期した後であっても、データが実際にディスクに書き込まれる保証はありません。したがって障害が発生した場合は、重大なデータが失われることがあります。

一部の高価なディスクには、非揮発性、またはバッテリー駆動の書き込みキャッシュがあります。これらを使用した場合は、障害発生時に必ずしもデータが失われるわけではありませんが、テストが必要になります。ディスクにこのような機能がない場合は、書き込みキャッシュを必ず無効にする必要があります。ディスク書き込みキャッシュを無効にすると、パフォーマンスに悪影響を及ぼす可能性があることに注意してください。

以下の手順は、Windows 上の Linux でディスク書き込みキャッシュを無効にする方法を示しています。

手順

1. Linux で、ディスク書き込みキャッシュ設定を管理するには、**hdparm** (IDE ディスクの場合) または **sdparm** または **sginfo** (SDSI/SATA ディスクの場合) ツールを使用します。

2. Windows でディスクライターキャッシュ設定を管理するには、ディスクを右クリックします。**Properties** を選択します。

6.2. データベースのメッセージデータの永続化

メッセージのデータをデータベースで永続化すると、ブローカーは Java Database Connectivity (JDBC) 接続を使用して、メッセージおよびバインディングデータをデータベーステーブルに保存します。テーブルのデータは AMQ Broker ジャーナルエンコーディングを使用してエンコードされます。サ

ポートされるデータベースの詳細は、Red Hat カスタマーポータルの Red Hat AMQ 7 Supported Configurations を参照してください。

重要

管理者は、組織の IT インフラストラクチャーの要件に基づいて、メッセージデータをデータベースに保管できます。ただし、データベースを使用すると、メッセージングシステムのパフォーマンスに悪影響を及ぼす可能性があります。具体的には、JDBC 経由でメッセージングデータをデータベーステーブルに書き込むと、ブローカーのパフォーマンスに大きなオーバーヘッドが発生します。

6.2.1. JDBC 永続性の設定

以下の手順では、メッセージおよびバインディングデータをデータベーステーブルに保存するようにブローカーを設定する方法を説明します。

手順

1. 適切な JDBC クライアントライブラリーをブローカーランタイムに追加します。これを実行するには、関連する **.jar** ファイルを **<broker_instance_dir>/lib** ディレクトリーに追加します。
2. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
3. **core** 要素内に、**database-store** 要素が含まれる **store** 要素を追加します。

```
<configuration>
 <core>
  <store>
   <database-store>
   </database-store>
  </store>
 </core>
</configuration>
```

4. **database-store** 要素内に JDBC 永続化の設定パラメーターを追加し、値を指定します。以下は例になります。

```
<configuration>
 <core>
  <store>
   <database-store>
    <jdbc-connection-url>jdbc:oracle:data/oracle/database-store;create=true</jdbc-connection-url>
    <jdbc-user>ENC(5493dd76567ee5ec269d11823973462f)</jdbc-user>
    <jdbc-password>ENC(56a0db3b71043054269d11823973462f)</jdbc-password>
    <bindings-table-name>BINDINGS_TABLE</bindings-table-name>
    <message-table-name>MESSAGE_TABLE</message-table-name>
    <large-message-table-name>LARGE_MESSAGES_TABLE</large-message-table-name>
    <page-store-table-name>PAGE_STORE_TABLE</page-store-table-name>
    <node-manager-store-table-name>NODE_MANAGER_TABLE</node-manager-store-table-name>
    <jdbc-driver-class-name>oracle.jdbc.driver.OracleDriver</jdbc-driver-class-name>
    <jdbc-network-timeout>10000</jdbc-network-timeout>
    <jdbc-lock-renew-period>2000</jdbc-lock-renew-period>
```

```
        <jdbc-lock-expiration>20000</jdbc-lock-expiration>
        <jdbc-journal-sync-period>5</jdbc-journal-sync-period>
      </database-store>
    </store>
  </core>
</configuration>
```

jdbc-connection-url

データベースサーバーの完全な JDBC 接続 URL。接続 URL には、すべての設定パラメーターとデータベース名が含まれている必要があります。

jdbc-user

データベースサーバー用に暗号化されたユーザー名。設定ファイルで使用するユーザー名とパスワードの暗号化に関する詳細は、「設定ファイルのパスワードの暗号化」 を参照してください。

jdbc-password

データベースサーバー用に暗号化されたパスワード。設定ファイルで使用するユーザー名とパスワードの暗号化に関する詳細は、「設定ファイルのパスワードの暗号化」 を参照してください。

bindings-table-name

データのバインディングが保存されるテーブルの名前。このテーブル名を指定すると、干渉なしに複数のサーバー間で単一のデータベースを共有できます。

message-table-name

メッセージデータが保存されるテーブルの名前。このテーブル名を指定すると、干渉なしに複数のサーバー間で単一のデータベースを共有できます。

large-message-table-name

サイズの大きいメッセージと関連データが永続化されるテーブルの名前。さらに、クライアントがサイズの大きいメッセージをチャンクでストリーミングする場合に、チャンクはこのテーブルに保存されます。このテーブル名を指定すると、干渉なしに複数のサーバー間で単一のデータベースを共有できます。

page-store-table-name

ページストアディレクトリー情報が格納されるテーブルの名前。このテーブル名を指定すると、干渉なしに複数のサーバー間で単一のデータベースを共有できます。

node-manager-store-table-name

共有ストア高可用性 (HA) がライブおよびバックアップブローカー向けにロックされ、他の HA 関連のデータがブローカーサーバーに保存されているテーブルの名前。このテーブル名を指定すると、干渉なしに複数のサーバー間で単一のデータベースを共有できます。共有ストア HA を使用する各ライブ/バックアップペアは、同じテーブル名を使用する必要があります。複数の (および関連性のない) ライブ/バックアップペア間で同じテーブルを共有できません。

jdbc-driver-class-name

JDBC データベースドライバーの完全修飾クラス名。サポートされるデータベースの詳細は、Red Hat カスタマーポータルの Red Hat AMQ 7 Supported Configurations を参照してください。

jdbc-network-timeout

JDBC ネットワーク接続のタイムアウト (ミリ秒単位)。デフォルト値は 20000 ミリ秒です。共有ストア HA に JDBC を使用する場合は、**jdbc-lock-expiration** 未満の値にタイムアウトを設定することが推奨されます。

jdbc-lock-renew-period

現在の JDBC ロックの更新期間の長さ (ミリ秒単位)。この時間が経過すると、ブローカーは

ロックを更新できます。**jdbc-lock-expiration** の値の数分の 1 の値を設定することをお勧めします。これにより、ブローカーはリースを延長するのに十分な時間を確保でき、接続に問題が発生した場合にブローカーがロックの更新を試みる時間を確保できます。デフォルト値は 2000 ミリ秒です。

jdbc-lock-expiration

jdbc-lock-renew-period の値が経過した場合でも、現在の JDBC ロックが所有 (取得または更新) されているとみなされる時間 (ミリ秒単位)。
ブローカーは、**jdbc-lock-renew-period** の値に従って、所有するロックの定期更新を試みます。ブローカーがロックの更新に **失敗** した場合 (接続の問題などにより)、ブローカーはロックが最後に正常に取得または更新されてから **jdbc-lock-expiration** の値が経過するまでロックの更新を試み続けます。

上記の更新動作の例外は、別のブローカーがロックを取得する場合です。これは、Database Management System (DBMS) とブローカー間の時間の不整合が発生した場合や、ガベージコレクションの一時停止期間が長い場合に発生する可能性があります。この場合、最初にロックを所有していたブローカーは、ロックが失われたと判断し、更新を試行しません。

有効期限の経過後、現在 JDBC ロックを所有しているブローカーによって JDBC ロックが更新されない場合、別のブローカーが JDBC ロックを確立できます。

jdbc-lock-expiration のデフォルト値は 20000 ミリ秒です。

jdbc-journal-sync-period

ブローカージャーナルが JDBC と同期する期間 (ミリ秒単位)。デフォルト値は 5 ミリ秒です。

6.2.2. JDBC 接続プールの設定

JDBC 永続化のブローカーを設定した場合、ブローカーは JDBC 接続を使用してメッセージおよびバインディングデータをデータベーステーブルに保存します。

JDBC 接続が失敗した場合に、失敗時にアクティブな接続アクティビティー (データベースの読み取りや書き込みなど) がないことを確認した場合、ブローカーは実行中のままとなり、データベース接続の再確立を試みます。そのために、AMQ Broker は JDBC **接続プール** を使用します。

通常、**接続プール** は、複数のアプリケーション間で共有できる指定のデータベースにオープン接続のセットを提供します。ブローカーの場合、ブローカーとデータベース間の接続に失敗すると、ブローカーはプールからの異なる接続を使用してデータベースへの再接続を試みます。プールは、ブローカーが受信する前に新しい接続をテストします。

以下の例は、JDBC 接続プールを設定する方法を示しています。

重要

明示的に JDBC 接続プールを設定しない場合、ブローカーはデフォルト設定で接続プールを使用します。デフォルト設定では、既存の JDBC 設定の値が使用されます。詳細は、Default connection pooling configuration を参照してください。

前提条件

- この例は JDBC 永続性を設定する例をもとにしています。「JDBC 永続性の設定」 を参照してください。

- 接続プールを有効にするには、AMQ Broker は Apache Commons DBCP パッケージを使用します。ブローカーの JDBC 接続プールを設定する前に、このパッケージが提供する内容を理解する必要があります。詳細は以下を参照してください。
  - Apache Commons DBCP の概要
  - Apache Commons DBCP 設定パラメーター

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 以前に JDBC 設定に追加した **database-store** 要素内で、**jdbc-driver-class-name**、**jdbc-connection-url**、**jdbc-user**、jdbc-**password パラメーター** を削除します。この手順の後半で、これらの設定は、対応する DBCP 設定パラメーターに置き換えます。

注記

上記のパラメーターを明示的に削除しない場合には、この手順の後半で追加する対象の DBCP パラメーターが優先されます。

3. **database-store** 要素内に **data-source-properties** 要素を追加します。以下は例になります。

```
<store>
   <database-store>
      <data-source-properties>
      </data-source-properties>
      <bindings-table-name>BINDINGS</bindings-table-name>
      <message-table-name>MESSAGES</message-table-name>
      <large-message-table-name>LARGE_MESSAGES</large-message-table-name>
      <page-store-table-name>PAGE_STORE</page-store-table-name>
      <node-manager-store-table-name>NODE_MANAGER_STORE</node-manager-store-
table-name>
      <jdbc-network-timeout>10000</jdbc-network-timeout>
      <jdbc-lock-renew-period>2000</jdbc-lock-renew-period>
      <jdbc-lock-expiration>20000</jdbc-lock-expiration>
      <jdbc-journal-sync-period>5</jdbc-journal-sync-period>
   </database-store>
</store>
```

4. 新しい **data-source-properties** 要素内で、接続プールに DBCP データソースプロパティーを追加します。キーと値のペアを指定します。以下は例になります。

```
<store>
   <database-store>
      <data-source-properties>
         <data-source-property key="driverClassName" value="com.mysql.jdbc.Driver" />
         <data-source-property key="url" value="jdbc:mysql://localhost:3306/artemis" />
         <data-source-property key="username"
value="ENC(5493dd76567ee5ec269d1182397346f)"/>
         <data-source-property key="password"
value="ENC(56a0db3b71043054269d1182397346f)"/>
         <data-source-property key="poolPreparedStatements" value="true" />
         <data-source-property key="maxTotal" value="-1" />
      </data-source-properties>
```

```
        <bindings-table-name>BINDINGS</bindings-table-name>
        <message-table-name>MESSAGES</message-table-name>
        <large-message-table-name>LARGE_MESSAGES</large-message-table-name>
        <page-store-table-name>PAGE_STORE</page-store-table-name>
        <node-manager-store-table-name>NODE_MANAGER_STORE</node-manager-store-
table-name>
        <jdbc-network-timeout>10000</jdbc-network-timeout>
        <jdbc-lock-renew-period>2000</jdbc-lock-renew-period>
        <jdbc-lock-expiration>20000</jdbc-lock-expiration>
        <jdbc-journal-sync-period>5</jdbc-journal-sync-period>
      </database-store>
</store>
```

driverClassName

JDBC データベースドライバーの完全修飾クラス名。

url

データベースサーバーの完全な JDBC 接続 URL。

username

データベースサーバー用に暗号化されたユーザー名。この値は、暗号化されていないプレーンテキストとして指定することもできます。設定ファイルで使用するユーザー名とパスワードの暗号化に関する詳細は、「設定ファイルのパスワードの暗号化」 を参照してください。

password

データベースサーバー用に暗号化されたパスワード。この値は、暗号化されていないプレーンテキストとして指定することもできます。設定ファイルで使用するユーザー名とパスワードの暗号化に関する詳細は、「設定ファイルのパスワードの暗号化」 を参照してください。

poolPreparedStatements

このパラメーターの値を **true** に設定すると、プールには、無制限の準備済みキャッシュステートメントを追加できます。これにより、初期化コストが削減されます。

maxTotal

プールの最大接続数。このパラメーターの値を **-1** に設定すると、制限はありません。

明示的に JDBC 接続プールを設定しない場合、ブローカーはデフォルト設定で接続プールを使用します。デフォルト設定は、表で説明されています。

表6.1 デフォルトの接続プール設定

DBCP 設定パラメーター	デフォルト値
driverClassName	既存の **jdbc-driver-class-name** パラメーターの値
url	既存の **jdbc-connection-url** パラメーターの値
username	既存の **jdbc-user** パラメーターの値
password	既存の **jdbc-password** パラメーターの値
poolPreparedStatements	**true**

DBCP 設定パラメーター	デフォルト値
maxTotal	**-1**

注記

再接続は、クライアントがブローカーにメッセージを送信していない場合に **のみ** 機能します。再接続時にデータベーステーブルへの書き込みを試みると、ブローカーは失敗し、シャットダウンします。

関連情報

- AMQ Broker でサポートされるデータベースの詳細は、Red Hat カスタマーポータルの Red Hat AMQ 7 Supported Configurations を参照してください。
- Apache Commons DBCP パッケージで利用可能なすべての設定オプションについては、Apache Commons DBCP Configuration Parameters を参照してください。

6.3. 永続性の無効化

場合によっては、メッセージングシステムがデータを保存し **ない** という要件がある可能性があります。このような状況では、ブローカーで永続性を無効にすることができます。

以下の手順では、永続性を無効にする方法を示します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素内で、**persistence-enabled** パラメーターの値を **false** に設定します。

```
<configuration>
  <core>
    ...
    <persistence-enabled>false</persistence-enabled>
    ...
  </core>
</configuration>
```

メッセージデータ、バインディングデータ、大きなメッセージデータ、重複 ID キャッシュ、またはページングデータは永続化されません。

第7章 アドレスの最大メモリー使用量の設定

AMQ Broker は、ブローカーをホストするマシンが制限されたメモリーで実行されている場合でも、数百万のメッセージが含まれる膨大なキューを透過的にサポートします。

このような状況では、すべてのキューを 1 度にメモリーに保存できない可能性があります。超過したメモリー消費から保護するため、ブローカーの各アドレスに許可される最大メモリー使用量を設定できます。さらに、指定のアドレスにおいてこの制限に到達した際にブローカーが実行するアクションを指定できます。

特に、アドレスのメモリー使用量が設定済みの制限に達すると、ブローカーが以下のアクションのいずれかを実行するように設定できます。

- メッセージをページ化
- メッセージを通知せずに破棄
- メッセージを破棄および送信クライアントへ通知
- クライアントのメッセージ送信をブロック

以下のセクションでは、アドレスの最大メモリー使用量と、アドレスの制限に達したときにブローカーが取る、対応するアクションの設定方法を説明します。

重要

トランザクションを使用すると、ブローカーはトランザクションの一貫性を確保するために追加のメモリーを割り当てる可能性があります。この場合、ブローカーによって報告されるメモリー使用量は、メモリーで使用される合計バイト数を反映しない可能性があります。そのため、指定された最大メモリー使用量に基づいてメッセージをページ化、破棄、またはブロックするようにブローカーを設定する場合、トランザクションも使用しないでください。

7.1. メッセージのページングの設定

最大メモリー使用量制限が指定されたアドレスに対して、使用量制限に達した際にブローカーが実行するアクションを指定することもできます。設定可能なオプションの 1 つが **ページング** です。

ページングオプションを設定する場合は、アドレスの最大サイズに達すると、ブローカーは、ディスク上のそのアドレスのメッセージを、**ページファイル** と呼ばれるファイルに保存します。各ページファイルには設定可能な最大サイズがあります。この方法で設定する各アドレスには、ページ化されたメッセージを格納するためにファイルシステム内に専用のフォルダーがあります。

キューのメッセージを検査する際に、キューブラウザーとコンシューマーの両方がページファイルに移動できます。ただし、非常に特殊なフィルターを使用しているコンシューマーは、キュー内の既存のメッセージが最初に消費されるまで、ページファイルに保存されているメッセージを消費できない可能性があります。たとえば、コンシューマーフィルターに **"color='red'"** などの文字列式が含まれているとします。この条件を満たすメッセージがプロパティー **"color='blue'"** の 100 万メッセージに従う場合、コンシューマーは **"color='blue'"** のメッセージが最初に消費されるまで、メッセージを消費できません。

ブローカーは、クライアントが消費する準備ができたときに、ディスクからメモリーにメッセージを転送 (**非ページ化**) します。ファイルのすべてのメッセージが確認されると、ブローカーはディスクからページファイルを削除します。

以下の手順は、メッセージのページングを設定する方法を示しています。

7.1.1. ページングディレクトリーの指定

以下の手順では、ページングディレクトリーの場所を指定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素内に **paging-directory** 要素を追加します。ファイルシステムのページングディレクトリーの場所を指定します。

```
<configuration ...>
  <core ...>
    ...
    <paging-directory>/path/to/paging-directory</paging-directory>
    ...
  </core>
</configuration>
```

その後ページング用に設定するアドレスごとに、ブローカーは指定したページングディレクトリーに専用のディレクトリーを追加します。

7.1.2. ページングのアドレスの設定

以下の手順では、ページング用のアドレスを設定する方法を説明します。

前提条件

- アドレスおよびアドレス設定の設定方法を理解している。詳細は、*4章 アドレスおよびキューの設定* を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一致するアドレスまたはアドレス **セット** 用に設定した **address-setting** 要素の場合は、設定要素を追加して最大メモリー使用量を指定し、ページング動作を定義します。以下は例になります。

```
<address-settings>
   <address-setting match="my.paged.address">
      ...
      <max-size-bytes>104857600</max-size-bytes>
      <page-size-bytes>10485760</page-size-bytes>
      <address-full-policy>PAGE</address-full-policy>
      ...
   </address-setting>
</address-settings>
```

max-size-bytes

ブローカーが **address-full-policy** に指定されたポリシーを実行する前に、アドレスに許可されるメモリーの最大サイズ (バイト単位)。デフォルト値は **-1 で**、制限なしを意味します。指定する値は、K、MB、GB などのバイト表記もサポートします。

page-size-bytes

ページングシステムで使用される各ページファイルのサイズ (バイト単位)。デフォルト値は **10485760** (つまり 10 MiB) です。指定する値は、K、MB、GB などのバイト表記もサポートします。

address-full-policy

アドレスの最大サイズに達したときにブローカーが取るアクション。デフォルト値は **PAGE** です。有効な値は以下のとおりです。

PAGE

ブローカーは、追加のメッセージをディスクにページングします。

DROP

ブローカーは追加のメッセージを通知せずに破棄します。

FAIL

ブローカーは、クライアントメッセージプロデューサーに対して追加のメッセージおよび例外をドロップします。

BLOCK

追加のメッセージを送信しようとすると、クライアントメッセージプロデューサーがブロックされます。

前述の例に示されて **いない** 追加のページング設定要素は以下のとおりです。

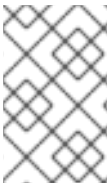
page-max-cache-size

ページングナビゲーション中に IO を最適化するためにブローカーがメモリーに保持するページファイルの数。デフォルト値は **5** です。

page-sync-timeout

定期的なページ同期の間隔 (ナノ秒単位)。非同期 IO ジャーナルを使用している場合 (つまり、**journal-type** が **broker.xml** 設定ファイルで **ASYNCIO** に設定されている場合)、デフォルト値は **3333333** です。標準の Java NIO ジャーナルを使用している場合 (**journal-type** が **NIO** に設定されている場合)、デフォルト値は **journal-buffer-timeout** パラメーターの設定済みの値です。

前述の例では、**my.paged.address** アドレスに送信されたメッセージがメモリーの 104857600 バイトを超えると、ブローカーはページングを開始します。



注記

address-setting 要素で **max-size-bytes** を指定すると、一致する **各** アドレスに値が適用されます。この値を指定すると、一致するすべてのアドレスの **合計** サイズが **max-size-bytes** の値に制限されるわけでは **ありません**。

7.1.3. グローバルページングサイズの設定

たとえば、ブローカーで使用パターンが異なるアドレスを多数管理する場合など、**アドレスごと** のメモリー制限の設定は実用的ではない場合があります。このような状況では、グローバルメモリー制限を指定できます。グローバル制限は、ブローカーがすべてのアドレスに使用できるメモリーの **合計** 量です。このメモリー制限に達すると、ブローカーは新しい受信メッセージに関連付けられたアドレスの **address-full-policy** に指定されたポリシーを実行します。

以下の手順では、グローバルページングサイズを設定する方法を説明します。

前提条件

- ページングのアドレスの設定方法を理解している必要があります。詳細は、「ページングのアドレスの設定」 を参照してください。

手順

1. ブローカーを停止します。

   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis stop
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe stop
   ```

2. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

3. **core** 要素内に **global-max-size** 要素を追加し、値を指定します。以下は例になります。

   ```
   <configuration>
    <core>
     ...
     <global-max-size>1GB</global-max-size>
     ...
    </core>
   </configuration>
   ```

   global-max-size

   ブローカーがすべてのアドレスに使用できるメモリーの合計量 (バイト単位)。この制限に達すると、受信メッセージに関連付けられたアドレスに対して、ブローカーは **address-full-policy** の値として指定されたポリシーを実行します。**global-max-size** のデフォルト値は、ブローカーをホストする Java 仮想マシン (JVM) で利用可能な最大メモリーの半分です。
   global-max-size の値はバイト単位ですが、バイト表記にも対応します (例 : "K"、"Mb"、"GB")。

   上記の例では、ブローカーはメッセージの処理時に利用可能な最大 1 ギガバイトのメモリーを使用するように設定されています。

4. ブローカーを起動します。

   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis run
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe start
   ```

7.1.4. ページング時のディスク使用量の制限

ブローカーが受信メッセージをページングせずにブロックする前に、ブローカーが使用可能な物理ディスク領域の量を制限できます。

以下の手順では、ページング中にディスク使用量の制限を設定する方法を説明します。

手順

1. ブローカーを停止します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis stop
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe stop
   ```

2. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
3. **core** 要素内に **max-disk-usage** 設定要素を追加し、値を指定します。以下は例になります。

   ```
   <configuration>
    <core>
     ...
     <max-disk-usage>50</max-disk-usage>
     ...
    </core>
   </configuration>
   ```

   max-disk-usage

   メッセージのページング時にブローカーが使用できる利用可能なディスク領域の最大パーセンテージ。この制限に達すると、ブローカーはページングではなく受信メッセージをブロックします。デフォルト値は **90** です。
   上記の例では、ブローカーはメッセージをページングする際にディスク領域の fifty パーセントの使用に制限されます。

4. ブローカーを起動します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis run
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe start
   ```

7.2. メッセージドロップの設定

「ページングのアドレスの設定」 では、ページングのアドレスの設定方法を示します。この手順の一環として、 **address-full-policy** の値を **PAGE** に設定します。

アドレスが指定された最大サイズに達した際に (ページングではなく) メッセージを **ドロップ** するには、**address-full-policy** の値を以下のいずれかに設定します。

DROP

指定のアドレスの最大サイズに達すると、ブローカーは追加のメッセージを通知せずにドロップします。

FAIL

特定のアドレスの最大サイズに達すると、ブローカーは追加のメッセージを削除し、プロデューサーに例外を発行します。

7.3. メッセージブロックの設定

以下の手順では、指定のアドレスが指定した最大サイズ制限に達した際に、メッセージブロックを設定する方法を説明します。

注記

メッセージブロックは、Core、OpenWire、および AMQP プロトコルに対して **のみ** 設定できます。

7.3.1. Core および OpenWire プロデューサーのブロック

以下の手順は、指定のアドレスが指定した最大サイズ制限に達した際の、Core および OpenWire メッセージプロデューサーのメッセージブロックを設定する方法を示しています。

前提条件

- アドレスおよびアドレス設定の設定方法を理解している。詳細は、*4章 アドレスおよびキューの設定* を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一致するアドレスまたはアドレス **セット** 用に設定した **address-setting** 要素の場合は、メッセージブロック動作を定義する設定要素を追加します。以下は例になります。

```
<address-settings>
   <address-setting match="my.blocking.address">
      ...
      <max-size-bytes>300000</max-size-bytes>
      <address-full-policy>BLOCK</address-full-policy>
      ...
   </address-setting>
</address-settings>
```

max-size-bytes

ブローカーが **address-full-policy** に指定されたポリシーを実行する前に、アドレスに許可されるメモリーの最大サイズ (バイト単位)。指定する値は、K、MB、GB などのバイト表記もサポートします。

注記

address-setting 要素で **max-size-bytes** を指定すると、一致する **各** アドレスに値が適用されます。この値を指定すると、一致するすべてのアドレスの **合計** サイズが **max-size-bytes** の値に制限されるわけでは **ありません**。

address-full-policy

アドレスの最大サイズに達したときにブローカーが取るアクション。

上記の例では、アドレス **my.blocking.address** に送信されたメッセージがメモリーの 300000 バイトを超えると、ブローカーは Core または OpenWire メッセージプロデューサーからの追加のメッセージをブロックします。

7.3.2. AMQP プロデューサーのブロック

Core や OpenWire などのプロトコルは、ウィンドウサイズのフロー制御システムを使用します。このシステムでは、クレジットはバイトを表し、プロデューサーに割り当てられます。プロデューサーがメッセージを送信する場合、プロデューサーはメッセージのサイズに対して十分なクレジットがあるまで待機する必要があります。

対照的に、AMQP フロー制御のクレジットはバイトを表します。代わりに、AMQP クレジットは、メッセージサイズに関係なく、プロデューサーが送信できるメッセージの数を表します。そのため、AMQP プロデューサーがアドレスの **max-size-bytes** の値を大幅に超過することがあります。

そのため、AMQP プロデューサーをブロックするには、別の設定要素 **max-size-bytes-reject-threshold** を使用する必要があります。一致するアドレスまたはアドレスセットの場合、この要素はメモリーのすべての AMQP メッセージの最大サイズをバイト単位で指定します。メモリーのすべてのメッセージの合計サイズが指定の制限に達すると、ブローカーは AMQP プロデューサーが追加のメッセージを送信しなくなります。

以下の手順では、AMQP メッセージプロデューサーのメッセージブロックを設定する方法を説明します。

前提条件

- アドレスおよびアドレス設定の設定方法を理解している。詳細は、*4章 アドレスおよびキューの設定* を参照してください。

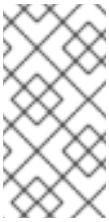
手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. 一致するアドレスまたはアドレス **セット** に設定した **address-setting** 要素の場合は、メモリーのすべての AMQP メッセージの最大サイズを指定します。以下は例になります。

```
<address-settings>
   <address-setting match="my.amqp.blocking.address">
      ...
      <max-size-bytes-reject-threshold>300000</max-size-bytes-reject-threshold>
      ...
   </address-setting>
</address-settings>
```

max-size-bytes-reject-threshold

ブローカーが AMQP メッセージをさらにブロックする前に、アドレスに許可されるメモリーの最大サイズ (バイト単位)。指定する値は、K、MB、GB などのバイト表記もサポートします。デフォルトでは、**max-size-bytes-reject-threshold** は **-1** に設定されます。これは、最大サイズがないことを意味します。



注記

address-setting 要素で **max-size-bytes-reject-threshold** を指定する場合、値は一致する **各** アドレスに適用されます。この値を指定すると、一致するすべてのアドレスの **合計** サイズが **max-size-bytes-reject-threshold** の値に制限されるわけでは **ありません**。

上記の例では、**my.amqp.blocking.address** アドレスに送信されたメッセージがメモリーの 300000 バイトを超えると、ブローカーは AMQP プロデューサーからの追加のメッセージをブロックし始めます。

7.4. マルチキャストアドレスでのメモリー使用量について

マルチキャストのキューがバインドされているアドレスへメッセージが転送されると、メッセージのコピーはメモリー内に 1 つだけ存在します。各キューにはメッセージへの **参照** のみがあります。このため、関連付けられたメモリーは、メッセージを参照する **すべて** のキューがメッセージを配信した後にのみ解放されます。

このような状況では、コンシューマーの速度が遅いと、アドレス全体がパフォーマンスに悪影響を及ぼす可能性があります。

たとえば、以下のシナリオについて考えてみましょう。

- アドレスには、マルチキャストルーティングタイプを使用する 10 個のキューがあります。
- 低速なコンシューマーにより、キューの 1 つがメッセージを配信しません。他の 9 つのキューは引き続きメッセージの配信を継続し、空になっています。
- メッセージはアドレスに到達し続けます。低速なコンシューマーを持つキューはメッセージへの参照を蓄積し続け、ブローカーはメッセージをメモリーに保持します。
- アドレスの最大サイズに達すると、ブローカーはメッセージのページングを開始します。

このシナリオでは、低速なコンシューマーが 1 つあるため、**すべて** のキューのコンシューマーはページシステムからメッセージを消費することが強制され、追加の IO が必要になります。

関連情報

- ブローカーとプロデューサーとコンシューマー間のデータのフローを調整するようにフロー制御を設定する方法は、AMQ Core Protocol JMS ドキュメントの Flow control を参照してください。

第8章 大きなメッセージの処理

クライアントは、ブローカーの内部バッファーのサイズを超える大きなメッセージを送信する可能性があり、予期せぬエラーが発生する可能性があります。この状態を回避するには、メッセージが指定の最小値よりも大きい場合にメッセージをファイルとして保存するようにブローカーを設定できます。このように大きなメッセージを処理すると、ブローカーはメモリー内にメッセージを保持しません。代わりに、ディスクまたはブローカーが大きなメッセージファイルを保存するデータベーステーブルのディレクトリーを指定します。

ブローカーがメッセージを大きなメッセージとして保存すると、キューは大きなメッセージディレクトリーまたはデータベーステーブルのファイルへの参照を保持します。

大規模なメッセージ処理は、Core Protocol、AMQP、OpenWire、および STOMP プロトコルで利用できます。

Core Protocol および OpenWire プロトコルの場合、クライアントは接続設定でメッセージの最小サイズを指定します。AMQP および STOMP プロトコルの場合は、ブローカー設定のプロトコルごとに定義されたアクセプターに大きなメッセージの最小サイズを指定します。

注記

大きなメッセージを生成および消費するのに、異なるプロトコルを使用 **しない** ことが推奨されます。これには、ブローカーはメッセージの複数の変換を実行する必要がある場合があります。たとえば、AMQP プロトコルを使用してメッセージを送信し、OpenWire を使用して受信したいとします。この場合、ブローカーは最初に大きなメッセージのボディー全体を読み取り、Core プロトコルを使用するように変換する必要があります。次に、ブローカーは別の変換を実行し、今回は OpenWire プロトコルへ変換する必要があります。このようなメッセージ変換により、ブローカーに大きな処理のオーバーヘッドが発生します。

前述のプロトコルに指定した最小大きなメッセージサイズは、利用可能なディスク領域やメッセージのサイズなどのシステムリソースの影響を受けます。適切なサイズを決定するために、いくつかの値を使用してパフォーマンステストを実行することが推奨されます。

本セクションの手順では以下の方法を説明します。

- 大きなメッセージを格納するようにブローカーを設定します。
- 大きなメッセージ処理のための AMQP および STOMP プロトコルのアクセプター設定

このセクションでは、大きなメッセージと連携する AMQ Core Protocol および AMQ OpenWire JMS クライアントの設定に関する追加リソースへのリンクも提供します。

8.1. 大きなメッセージ処理のためのブローカーの設定

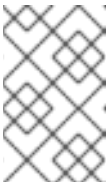
以下の手順では、ブローカーが大きなメッセージファイルを保存するディスクまたはデータベーステーブルにディレクトリーを指定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. ブローカーが大きなメッセージファイルを保存する場所を指定します。

a. ディスクに大きなメッセージを保存する場合は、**core** 要素に **large-messages-directory** パラメーターを追加し、ファイルシステムの場所を指定します。以下は例になります。

```
<configuration>
  <core>
    ...
    <large-messages-directory>/path/to/my-large-messages-directory</large-messages-directory>
    ...
  </core>
</configuration>
```

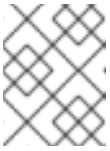


注記

large-messages-directory の値を明示的に指定しない場合、ブローカーは **<broker_instance_dir> /data/largemessages** のデフォルト値を使用します。

b. 大きなメッセージをデータベーステーブルに保存する場合は、**database-store** 要素に **large-message-table** パラメーターを追加して値を指定します。以下に例を示します。

```
<store>
  <database-store>
    ...
    <large-message-table>MY_TABLE</large-message-table>
    ...
  </database-store>
</store>
```



注記

large-message-table の値を明示的に指定しない場合、ブローカーは **LARGE_MESSAGE_TABLE** のデフォルト値を使用します。

関連情報

- データベースストアの設定に関する詳細は、「データベースのメッセージデータの永続化」 を参照してください。

8.2. 大規模なメッセージ処理のための AMQP アクセプターの設定

以下の手順は、指定したサイズよりも大きい AMQP メッセージを大規模メッセージとして処理するように AMQP アクセプターを設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
ブローカー設定ファイルのデフォルトの AMQP アクセプターは以下のようになります。

```
<acceptors>
    ...
    <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;a
```

```
mqpCredits=1000;amqpLowCredits=300</acceptor>
   ...
</acceptors>
```

2. デフォルトの AMQP アクセプター (または設定した別の AMQP アクセプター) で、**amqpMinLargeMessageSize** プロパティーを追加し、値を指定します。以下に例を示します。

```
<acceptors>
   ...
   <acceptor name="amqp">tcp://0.0.0.0:5672?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=AMQP;useEpoll=true;a
mqpCredits=1000;amqpLowCredits=300;amqpMinLargeMessageSize=204800</acceptor>
   ...
</acceptors>
```

上記の例では、ブローカーはポート 5672 で AMQP メッセージを受け入れるように設定されます。**amqpMinLargeMessageSize** の値に基づいて、アクセプターが 204800 バイトよりも大きい AMQP メッセージ (200 キロバイト以上) を受信する場合、ブローカーはメッセージを大きなメッセージとして格納します。このプロパティーの値を明示的に指定しない場合、 ブローカーは 102400 (100 キロバイト) のデフォルト値を使用します。

注記

- **amqpMinLargeMessageSize** を -1 に設定すると、AMQP メッセージに対するサイズの大きいメッセージ処理が無効になります。
- ブローカーが **amqpMinLargeMessageSize** の値を超えない永続的な AMQP メッセージを受信する場合で、これがメッセージングジャーナルバッファーのサイズ (**journal-buffer-size** 設定パラメーターを使用して指定) を **超える** 場合、ブローカーはメッセージをジャーナルに保存する前に大きな Core Protocol メッセージに変換します。

8.3. サイズの大きいメッセージ処理向けの STOMP アクセプターの設定

以下の手順は、指定したサイズよりも大きい STOMP メッセージをサイズの大きいメッセージとして処理するように STOMP アクセプターを設定する方法を説明します。

手順

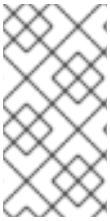
1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
ブローカー設定ファイルのデフォルトの AMQP アクセプターは以下のようになります。

```
<acceptors>
   ...
   <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true
</acceptor>
   ...
</acceptors>
```

2. デフォルトの STOMP アクセプター (または設定した別の STOMP アクセプター) で、**stompMinLargeMessageSize** プロパティーを追加し、値を指定します。以下に例を示します。

```
<acceptors>
   ...
   <acceptor name="stomp">tcp://0.0.0.0:61613?
tcpSendBufferSize=1048576;tcpReceiveBufferSize=1048576;protocols=STOMP;useEpoll=true;
stompMinLargeMessageSize=204800</acceptor>
   ...
</acceptors>
```

前の例では、ブローカーはポート 61613 で STOMP メッセージを受け入れるように設定されています。**stompMinLargeMessageSize** の値に基づいて、アクセプターが 204800 バイトよりも大きい STOMP メッセージ (200 キロバイト以上) を受信する場合、ブローカーはメッセージを大きなメッセージとして格納します。このプロパティーの値を明示的に指定しない場合、 ブローカーは 102400 (100 キロバイト) のデフォルト値を使用します。



注記

大きなメッセージを STOMP コンシューマーに配信するために、ブローカーは自動的にメッセージを大きなメッセージから通常のメッセージに変換してからクライアントに送信します。大きなメッセージが圧縮されている場合、ブローカーはこれを STOMP クライアントに送信する前に圧縮します。

8.4. 大きなメッセージと JAVA クライアント

大きなメッセージを使用するクライアントを作成している Java 開発者には、2 つのオプションがあります。

1 つのオプションとして、**InputStream** および **OutputStream** のインスタンスを使用することができます。たとえば、**FileInputStream** を使用して、物理ディスク上の大きなファイルから作成されたメッセージを送信します。その後、受信者が **FileOutputStream** を使用して、メッセージをローカルファイルシステムの場所にストリーミングできます。

別のオプションとして、JMS **BytesMessage** または **StreamMessage** を直接ストリーミングする方法もあります。以下に例を示します。

```
BytesMessage rm = (BytesMessage)cons.receive(10000);
byte data[] = new byte[1024];
for (int i = 0; i < rm.getBodyLength(); i += 1024)
{
   int numberOfBytes = rm.readBytes(data);
   // Do whatever you want with the data
}
```

関連情報

- AMQ Core Protocol JMS クライアントでの大きなメッセージの使用方法は、以下を参照してください。
  - 大型メッセージのオプション
  - ストリーミングされた大きなメッセージへの書き込み
  - ストリームされた大きなメッセージからの読み取り

- AMQ OpenWire JMS クライアントでの大きなメッセージの使用方法は、以下を参照してください。
  - 大型メッセージのオプション
  - ストリーミングされた大きなメッセージへの書き込み
  - ストリームされた大きなメッセージからの読み取り
- 大きなメッセージの例については、AMQ Broker インストールの **<install_dir>/examples/features/standard/** ディレクトリーの **large-message** の例を参照してください。サンプルプログラムの実行に関する詳細は、Running an AMQ Broker example program を参照してください。

第9章 デッド接続の検出

クライアントが予期せずに停止し、それらのリソースをクリーンアップする機会がないことがあります。これが発生すると、リソースが faulty 状態のままになり、ブローカーがメモリー不足または他のシステムリソースで実行されている可能性があります。ブローカーは、ガベージコレクション時にクライアントの接続が適切にシャットダウンされなかったことを検出します。その後、コネクションは閉じられ、以下のようなメッセージがログに書き込まれます。ログは、クライアントセッションがインスタンス化されたコードの正確な行を取得します。これにより、エラーを特定し、これを修正できます。

```
[Finalizer] 20:14:43,244 WARNING [org.apache.activemq.artemis.core.client.impl.DelegatingSession]
I'm closing a JMS Conection you left open. Please make sure you close all connections explicitly
before let
ting them go out of scope!
[Finalizer] 20:14:43,244 WARNING [org.apache.activemq.artemis.core.client.impl.DelegatingSession]
The session you didn't close was created here:
java.lang.Exception
   at org.apache.activemq.artemis.core.client.impl.DelegatingSession.<init>
(DelegatingSession.java:83)
   at org.acme.yourproject.YourClass (YourClass.java:666) (1)
```

(1) 接続がインスタンス化されたクライアントコードの行。

9.1. 接続 TIME-TO-LIVE

クライアントとサーバー間のネットワーク接続に失敗してオンラインに戻る可能性があるため、AMQ Broker は非アクティブなサーバー側のリソースをクリーンアップします。この待機時間は Time-to-live (TTL) と呼ばれます。ネットワークベースの接続のデフォルトの TTL は **60000** ミリ秒 (1 分) です。in-VM 接続のデフォルトの TTL は **-1** です。つまり、ブローカーはブローカー側で接続をタイムアウトしません。

ブローカーでの Time-To-Live の設定

クライアントが独自の接続 TTL を指定しないようにするには、ブローカー側でグローバル値を設定します。これは、ブローカー設定で **connection-ttl-override** 要素を指定して実行できます。

connection-ttl-check-interval 要素によって決定されるように、TTL 違反の接続をチェックするロジックはブローカーで定期的に実行されます。

手順

- 以下の例のように、**connection-ttl-override** 設定要素を追加し、time-to-live の値を指定して **<broker_instance_dir> /etc/broker.xml** を編集します。

```
<configuration>
 <core>
  ...
  <connection-ttl-override>30000</connection-ttl-override> (1)
  <connection-ttl-check-interval>1000</connection-ttl-check-interval> (2)
  ...
 </core>
</configuration>
```

(1) すべての接続のグローバル TTL は 30000 ミリ秒に設定されます。デフォルト値は **-1** で、クライアントが独自の TTL を設定できるようにします。

2 デッド接続をチェックする間隔は 1000 ミリ秒に設定されます。デフォルトでは、チェックは 2000 ミリ秒ごとに行われます。

9.2. 非同期接続実行の無効化

サーバー側で受信されたパケットの多くは、**リモート** スレッドで実行されます。これらのパケットは短時間実行される操作を表し、パフォーマンス上の理由から常に **リモーティング** スレッドで実行されます。ただし、一部のパケットタイプは **リモーティング** スレッドではなくスレッドプールを使用して実行され、ネットワークのレイテンシーが少し追加されます。

スレッドプールを使用するパケットタイプは、以下に示す Java クラス内に実装されます。クラスはすべて **org.apache.actiinvemq.artemis.core.protocol.core.impl.wireformat** パッケージにあります。

- RollbackMessage
- SessionCloseMessage
- SessionCommitMessage
- SessionXACommitMessage
- SessionXAPrepareMessage
- SessionXARollbackMessage

手順

- 非同期接続実行を無効にするには、以下の例のように **async-connection-execution-enabled** 設定要素を **<broker_instance_dir> /etc/broker.xml** に追加し、**false** に設定します。デフォルト値は **true** です。

```
<configuration>
 <core>
  ...
  <async-connection-execution-enabled>false</async-connection-execution-enabled>
  ...
 </core>
</configuration>
```

関連情報

- デッド接続を検出する AMQ Core Protocol JMS クライアントを設定する方法は、AMQ Core Protocol JMS ドキュメントの Detecting dead connections を参照してください。
- AMQ Core Protocol JMS クライアントで接続の存続時間を設定する方法については、AMQ Core Protocol JMS ドキュメントの Configuring time-to-live を参照してください。

第10章 重複メッセージの検出

複製メッセージを自動的に検出し、フィルターリングするようにブローカーを設定できます。つまり、独自の重複検出ロジックを実装する必要はありません。

重複検出がないと、予期しない接続障害が発生した場合、クライアントはブローカーに送信されたメッセージが受信されたかどうかを判断できません。この場合、クライアントはブローカーがメッセージを受信しなかったことを仮定し、再送信します。これにより、メッセージが複製されます。

たとえば、クライアントがブローカーにメッセージを送信するとします。ブローカーまたは接続がブローカーによって受信および処理される **前** に失敗すると、メッセージはそのアドレスに到達しません。失敗により、クライアントはブローカーから応答を受信しません。ブローカーによってメッセージが受信および処理された **後** にブローカーまたは接続が失敗すると、メッセージは正しくルーティングされますが、クライアントは応答を受信しません。

また、トランザクションを使用して成功を判断することは、必ずしも役立つとは限りません。トランザクションコミットの処理中にブローカーまたは接続が失敗する場合、クライアントはメッセージに正常に送信されたかどうかを判断できません。

このような状況では、クライアントが直近のメッセージを再送信して、想定された障害を修正します。その結果、システムに悪影響を及ぼす重複メッセージが表示される可能性があります。たとえば、注文可能なシステムでブローカーを使用している場合、重複メッセージは、発注書が 2 回処理されることを意味します。

以下の手順では、このような状況から保護するように重複メッセージ検出を設定する方法を説明します。

10.1. 重複 ID キャッシュの設定

ブローカーが重複メッセージを検出できるようにするには、プロデューサーは各メッセージの送信時にメッセージプロパティー **_AMQ_DUPL_ID** に一意の値を提供する必要があります。ブローカーは、**_AMQ_DUPL_ID** プロパティーの受信値のキャッシュを維持します。ブローカーがアドレスで新しいメッセージを受信すると、そのアドレスのキャッシュをチェックし、このプロパティーに同じ値でメッセージが処理されていないことを確認します。

各アドレスには独自のキャッシュがあります。各キャッシュのサイズは円形で固定されます。つまり、新しいエントリーはキャッシュ領域の要求に合わせて最も古いエントリーを置き換えます。

以下の手順では、ブローカーの各アドレスによって使用される ID キャッシュをグローバルに設定する方法を説明します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素内に **id-cache-size** プロパティーおよび **persist-id-cache** プロパティーを追加し、値を指定します。以下は例になります。

```
<configuration>
  <core>
    ...
    <id-cache-size>5000</id-cache-size>
    <persist-id-cache>false</persist-id-cache>
  </core>
</configuration>
```

id-cache-size

キャッシュ内の個別のエントリー数として指定される ID キャッシュの最大サイズ。デフォルト値は 20,000 エントリーです。この例では、キャッシュサイズは 5,000 エントリーに設定されます。

注記

キャッシュの最大サイズに達すると、ブローカーが重複メッセージの処理を開始できます。たとえば、キャッシュのサイズを **3000** に設定するとします。以前のメッセージが、**_AMQ_DUPL_ID** が同じ値を持つ新しいメッセージの到着前に 3,000 を **超える** メッセージを受信すると、ブローカーは重複を検出できません。これにより、両方のメッセージがブローカーによって処理されます。

persist-id-cache

このプロパティーの値を **true** に設定すると、ブローカーは ID の受信時にディスクに永続化します。デフォルト値は **true** です。上記の例では、値を **false** に設定して永続性を無効にします。

関連情報

- AMQ Core Protocol JMS クライアントを使用して重複 ID メッセージプロパティーを設定する方法は、AMQ Core Protocol JMS クライアントドキュメントの Using duplicate message detection を参照してください。

10.2. クラスター接続の複製検出の設定

クラスター接続を設定して、クラスター全体で移動するメッセージごとに重複 ID ヘッダーを挿入できます。

前提条件

- ブローカークラスターがすでに設定されている必要があります。詳細は、「ブローカークラスターの作成」 を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **core** 要素内に、指定のクラスター接続に **use-duplicate-detection** プロパティーを追加し、値を指定します。以下は例になります。

```
<configuration>
  <core>
    ...
    <cluster-connections>
      <cluster-connection name="my-cluster">
        <use-duplicate-detection>true</use-duplicate-detection>
        ...
      </cluster-connection>
        ...
```

```
    </cluster-connections>
  </core>
</configuration>
```

use-duplicate-detection

このプロパティーの値を **true** に設定すると、クラスターコネクションは、処理するメッセージごとに重複する ID ヘッダーを挿入します。

第11章 メッセージの傍受

AMQ Broker では、ブローカーに出入りするパケットを傍受して、パケットの監査やメッセージのフィルターを実行できます。インターセプターはインターセプトするパケットを変更できます。これにより、強力になりますが、潜在的に危険性があります。

ビジネス要件を満たすためのインターセプターを開発できます。インターセプターはプロトコル固有であるため、適切なインターフェイスを実装する必要があります。

インターセプターは、ブール値を返す **intercept()** メソッドを実装する必要があります。値が **true** の場合、メッセージパケットは続行されます。**false** の場合、プロセスは中止され、他のインターセプターは呼び出されず、メッセージパケットはこれ以上処理されません。

11.1. インターセプターの作成

独自の受信インターセプターおよび発信インターセプターを作成できます。すべてのインターセプターはプロトコル固有で、サーバーに出入りするパケットに対して呼び出されます。これにより、監査パケットなどのビジネス要件を満たすインターセプターを作成できます。インターセプターは、傍受するパケットを変更できます。これにより、危険が伴います。そのため、注意して使用してください。

インターセプターとその依存関係は、ブローカーの Java クラスに配置する必要があります。**<broker_instance_dir>/lib** ディレクトリーは、デフォルトでクラスパスに含まれているため、使用することができます。

手順

以下の例は、渡された各パケットのサイズをチェックするインターセプターを作成する方法を示しています。この例では、プロトコルごとに特定のインターフェイスを実装します。

- 適切なインターフェイスを実装し、その **intercept()** メソッドをオーバーライドします。
  - AMQP プロトコルを使用している場合は、**org.apache.activemq.artemis.protocol.amqp.broker.AmqpInterceptor** インターフェイスを実装してください。

```
package com.example;

import org.apache.activemq.artemis.protocol.amqp.broker.AMQPMessage;
import org.apache.activemq.artemis.protocol.amqp.broker.AmqpInterceptor;
import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements AmqpInterceptor
{
  private final int ACCEPTABLE_SIZE = 1024;

  @Override
  public boolean intercept(final AMQPMessage message, RemotingConnection
connection)
  {
    int size = message.getEncodeSize();
    if (size <= ACCEPTABLE_SIZE) {
      System.out.println("This AMQPMessage has an acceptable size.");
      return true;
    }
```

```
    return false;
  }
 }
```

- Core Protocol を使用している場合、インターセプターは、**org.apache.artemis.activemq.api.core.Interceptor** インターフェイスを実装する必要があります。

```
package com.example;

import org.apache.artemis.activemq.api.core.Interceptor;
import org.apache.activemq.artemis.core.protocol.core.Packet;
import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor
{
  private final int ACCEPTABLE_SIZE = 1024;

  @Override
  boolean intercept(Packet packet, RemotingConnection connection)
  throws ActiveMQException
  {
    int size = packet.getPacketSize();
    if (size <= ACCEPTABLE_SIZE) {
      System.out.println("This Packet has an acceptable size.");
      return true;
    }
    return false;
  }
}
```

- MQTT プロトコルを使用している場合は、**org.apache.activemq.artemis.core.protocol.mqtt.MQTTInterceptor** インターフェイスを実装してください。

```
package com.example;

import org.apache.activemq.artemis.core.protocol.mqtt.MQTTInterceptor;
import io.netty.handler.codec.mqtt.MqttMessage;
import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor
{
  private final int ACCEPTABLE_SIZE = 1024;

  @Override
  boolean intercept(MqttMessage mqttMessage, RemotingConnection connection)
  throws ActiveMQException
  {
    byte[] msg = (mqttMessage.toString()).getBytes();
    int size = msg.length;
    if (size <= ACCEPTABLE_SIZE) {
      System.out.println("This MqttMessage has an acceptable size.");
      return true;
    }
```

```
    return false;
  }
}
```

- STOMP プロトコルを使用している場合は、**org.apache.activemq.artemis.core.protocol.stomp.StompFrameInterceptor** インターフェイスを実装してください。

```
package com.example;

import org.apache.activemq.artemis.core.protocol.stomp.StompFrameInterceptor;
import org.apache.activemq.artemis.core.protocol.stomp.StompFrame;
import org.apache.activemq.artemis.spi.core.protocol.RemotingConnection;

public class MyInterceptor implements Interceptor
{
  private final int ACCEPTABLE_SIZE = 1024;

  @Override
  boolean intercept(StompFrame stompFrame, RemotingConnection connection)
  throws ActiveMQException
  {
    int size = stompFrame.getEncodedSize();
    if (size <= ACCEPTABLE_SIZE) {
      System.out.println("This StompFrame has an acceptable size.");
      return true;
    }
    return false;
  }
}
```

11.2. インターセプターを使用するためのブローカーの設定

インターセプターを作成したら、それを使用するようにブローカーを設定する必要があります。

前提条件

ブローカーで使用するために、インターセプタークラスを作成し、ブローカーの Java クラスパス (およびその依存関係) に追加する必要があります。**<broker_instance_dir>/lib** ディレクトリーは、デフォルトでクラスパスに含まれているため、使用することができます。

手順

- ブローカーがインターセプターを使用するように設定するには、**<broker_instance_dir>/etc/broker.xml** に設定を追加します。
  - インターセプターが着信メッセージを対象としている場合は、その **class-name** を **remoting-incoming-interceptors** のリストに追加します。

```
<configuration>
  <core>
    ...
    <remoting-incoming-interceptors>
      <class-name>org.example.MyIncomingInterceptor</class-name>
    </remoting-incoming-interceptors>
```

```
    ...
  </core>
</configuration>
```

- インターセプターが発信メッセージを対象としている場合は、その **class-name** を **remoting-outgoing-interceptors** のリストに追加します。

```
<configuration>
  <core>
    ...
    <remoting-outgoing-interceptors>
      <class-name>org.example.MyOutgoingInterceptor</class-name>
    </remoting-outgoing-interceptors>
  </core>
</configuration>
```

関連情報

- AMQ Core Protocol JMS クライアントでインターセプターを設定する方法は、AMQ Core Protocol JMS ドキュメントの Using message interceptors を参照してください。

第12章 メッセージの迂回およびメッセージフローの分割

AMQ Broker では、**迂回** と呼ばれるオブジェクトを設定できます。これにより、クライアントアプリケーションロジックを変更せずにメッセージをあるアドレスから別のアドレスに透過的に迂回できます。迂回を設定してメッセージの **コピー** を指定された転送アドレスに転送し、メッセージフローを効果的に分割することもできます。

12.1. メッセージの迂回の仕組み

迂回により、クライアントアプリケーションロジックを変更せずに、あるアドレスにルーティングされたメッセージを他のアドレスに透過的に迂回できます。ブローカーサーバーの迂回のセットをメッセージのルーティングテーブルの種類と見なすことができます。

迂回は **排他的** にすることができます。つまり、メッセージは元のアドレスに入りずに指定されたフォワードアドレスに迂回されます。

迂回は **排他的** ではない場合もあります。つまり、ブローカーはメッセージのコピーを指定された転送アドレスに送信する一方で、メッセージを元のアドレスに引き続き送信します。そのため、メッセージフローを分割するのに排他的でない迂回を使用できます。たとえば、注文キューに送信された全順序を個別に監視する場合は、メッセージフローを分割できます。

アドレスに排他的な迂回と非排他的な迂回の両方が設定されている場合、ブローカーは特別な迂回を最初に処理します。特定のメッセージがすでに特別な迂回によって迂回されている場合、ブローカーはそのメッセージの特別でない迂回を処理しません。この場合、メッセージは元のアドレスには決して送信されません。

ブローカーがメッセージを迂回すると、ブローカーは新しいメッセージ ID を割り当て、メッセージアドレスを新しい転送アドレスに設定します。元のメッセージ ID およびアドレスの値は、**_AMQ_ORIG_ADDRESS** (文字列タイプ) および **_AMQ_ORIG_MESSAGE_ID** (long タイプ) メッセージプロパティーから取得できます。コア API を使用している場合は、**Message.HDR_ORIGINAL_ADDRESS** プロパティーおよび **Message.HDR_ORIG_MESSAGE_ID** プロパティーを使用します。

注記

同じブローカーサーバーのアドレスにのみメッセージを迂回できます。別のサーバーのアドレスに迂回したい場合は、最初にメッセージをローカルストアアンドフォワードキューに迂回する一般的な解決策があります。次に、そのキューから消費し、メッセージを別のブローカーのアドレスに転送するブリッジを設定します。迂回とブリッジを組み合わせると、地理的に分散したブローカーサーバー間のルーティング接続の分散ネットワークを作成できます。これにより、グローバルメッセージングメッシュを作成できます。

12.2. メッセージ迂回の設定

ブローカーインスタンスで迂回を設定するには、**broker.xml** 設定ファイルの **core** 要素に **divert** 要素を追加します。

```
<core>
...
  <divert name= >
      <address> </address>
      <forwarding-address> </forwarding-address>
      <filter string= >
```

```
        <routing-type> </routing-type>
        <exclusive> </exclusive>
    </divert>
...
</core>
```

divert

迂回の名前付きインスタンス。各迂回に一意の名前がある限り、複数の **divert** 要素を **broker.xml** 設定ファイルに追加できます。

address

メッセージを迂回するアドレス

forwarding-address

メッセージを転送する アドレス

filter

オプションのメッセージフィルター。フィルターを設定すると、フィルター文字列に一致するメッセージのみが迂回されます。フィルターを指定しない場合、すべてのメッセージは迂回と一致すると見なされます。

routing-type

迂回されたメッセージのルーティングタイプ。迂回は以下に設定できます。

- **anycast** または **マルチキャスト** ルーティングのタイプのメッセージへの適用
- 既存のルーティングタイプを **削除** します。
- 既存のルーティングタイプを **通過** します (つまり保持されます)。

ルーティングタイプの制御は、メッセージにルーティングタイプがすでに設定されているものの、別のルーティングタイプを使用するアドレスにメッセージを迂回する必要がある場合に役立ちます。たとえば、ブローカーは、迂回の **routing-type** パラメーターを **MULTICAST** に設定しない限り、**anycast** ルーティングタイプのメッセージを **マルチキャスト** を使用するキューにルーティングできません。迂回の **routing-type** パラメーターの有効な値は **ANYCAST**、**MULTICAST**、**PASS**、および **STRIP** です。デフォルト値は **STRIP** です。

exclusive

迂回が排他的であるか (プロパティーを **true** に設定) または非排他的であるかを指定します (プロパティーを **false** に設定)。

以下のサブセクションは、排他的な迂回および排他的でない迂回の設定例を示しています。

12.2.1. 排他的な迂回の例

以下は、排他的な迂回の設定例です。排他的な迂回により、一致するメッセージはすべて最初に設定されたアドレスから新しいアドレスに迂回されます。一致するメッセージは元のアドレスにルーティングされません。

```
<divert name="prices-divert">
   <address>priceUpdates</address>
   <forwarding-address>priceForwarding</forwarding-address>
   <filter string="office='New York'"/>
   <exclusive>true</exclusive>
</divert>
```

上記の例では、**prices-divert** と呼ばれる迂回を定義します。これは、アドレス **priceUpdates** に送信されたメッセージを別のローカルアドレスである **priceForwarding** に迂回します。メッセージフィルター文字列も指定します。メッセージプロパティー **office** と値 **New York** を持つメッセージのみが迂回されます。その他のメッセージはすべて元のアドレスにルーティングされます。最後に、迂回が排他的であることを指定します。

12.2.2. 排他的でない迂回の例

以下は、排他的でない迂回の設定例です。排他的でない迂回では、メッセージは元のアドレスに送信されますが、ブローカーはメッセージのコピーを指定された転送アドレスにも送信します。したがって、排他的でない迂回は、メッセージフローを分割する方法です。

```
<divert name="order-divert">
  <address>orders</address>
  <forwarding-address>spyTopic</forwarding-address>
  <exclusive>false</exclusive>
</divert>
```

上記の例では、**order-divert** という迂回を定義し、アドレスの **順序** に送信されたすべてのメッセージのコピーを取り、**spyTopic** と呼ばれるローカルアドレスに送信します。また、迂回が排他的ではないように指定します。

関連情報

排他的な迂回と非排他的な迂回の両方を使用する詳細な例は、Divert Example (外部) を参照してください。

第13章 メッセージのフィルターリング

AMQ Broker は、SQL 92 式構文のサブセットに基づいて強力なフィルター言語を提供します。フィルター言語は JMS セレクターに使用されるものと同じ構文を使用しますが、事前定義された識別子は異なります。以下の表は、AMQ Broker メッセージに適用される識別子を示しています。

識別子	属性
AMQPriority	メッセージの優先度。メッセージの優先度は、**0** から **9** 間の有効な値の整数を指定します。**0** の優先度が最も低く、**9** が最も高くなります。
AMQExpiration	メッセージの有効期限。値は長い整数です。
AMQDurable	メッセージが永続化されているかどうか。値は文字列です。有効な値は **Durable** または **NonDurable** です。
AMQTimestamp	メッセージが作成された時点のタイムスタンプです。値は長い整数です。
AMQSize	メッセージの **encodeSize** プロパティーの値。**encodeSize** の値は、メッセージがジャーナルで起動するスペース (バイト単位) です。ブローカーは二重バイト文字セットを使用してメッセージをエンコードするので、メッセージの実際のサイズは **encodeSize** の半分になります。

コアフィルター式で使用される他の識別子はメッセージのプロパティーであると考えられます。JMS メッセージのセレクター構文に関するドキュメントは、Java EE API を参照してください。

13.1. フィルターを使用するようにキューを設定する

<broker_instance_dir> /etc/broker.xml で設定するキューにフィルターを追加できます。フィルター式に一致するメッセージのみがキューに格納されます。

手順

- **filter** 要素を希望の **キュー** に追加し、要素の値として適用するフィルターを追加します。以下の例では、フィルター **NEWS='technology'** がキュー **technologyQueue** に追加されます。

```
<configuration>
 <core>
  ...
  <addresses>
    <address name="myQueue">
      <anycast>
        <queue name="myQueue">
          <filter string="NEWS='technology'"/>
        </queue>
      </anycast>
    </address>
  </addresses>
 </core>
</configuration>
```

13.2. JMS メッセージプロパティーのフィルターリング

JMS 仕様は、セレクターで使用されると String プロパティーを数値型に変換してはならないことを示しています。たとえば、メッセージの **age** プロパティーが String 値 **21** に設定されていると、セレクターの **age > 18** は一致できません。この制限により、STOMP クライアントは String プロパティーでメッセージを送信できるため制限されます。

文字列を数値に変換するフィルターの設定
String プロパティーを数値型に変換するには、接頭辞 **convert_string_expressions:** を **filter** の値に追加します。

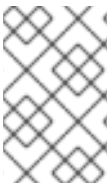
手順

- 接頭辞 **convert_string_expressions:** を必要な **フィルター** に適用して、**<broker_instance_dir> /etc/broker.xml** を編集します。以下の例では、**age > 18** から **convert_string_expressions:age > 18** に **フィルター** 値を編集します。

```
<configuration>
 <core>
  ...
  <addresses>
    <address name="myQueue">
      <anycast>
        <queue name="myQueue">
          <filter string="convert_string_expressions='age > 18'"/>
        </queue>
      </anycast>
    </address>
  </addresses>
 </core>
</configuration>
```

13.3. アノテーションを基にした AMQP メッセージのフィルター

ブローカーは、期限切れの AMQP メッセージまたは未配信の AMQP メッセージを、設定した期限切れまたはデッドレターキューに移動する前に、アノテーションおよびプロパティーをメッセージに適用します。クライアントはこれらのプロパティーまたはアノテーションに基づいてフィルターを作成し、期限切れまたはデッドレターキューから消費する特定のメッセージを選択できます。



注記

ブローカーが適用されるプロパティーは **内部** プロパティーです。これらのプロパティーは、通常の使用のためにクライアントに公開されませんが、フィルターのクライアントで指定**できます**。

以下は、メッセージプロパティーとアノテーションに基づくフィルターの例です。このアプローチではブローカーによる処理が少なくなるため、プロパティーに基づくフィルターリングは可能な場合に推奨される方法です。

メッセージプロパティーを基にしたフィルター

```
ConnectionFactory factory = new JmsConnectionFactory("amqp://localhost:5672");
Connection connection = factory.createConnection();
Session session = connection.createSession(false, Session.AUTO_ACKNOWLEDGE);
```

```
connection.start();
javax.jms.Queue queue = session.createQueue("my_DLQ");
MessageConsumer consumer = session.createConsumer(queue,
"_AMQ_ORIG_ADDRESS='original_address_name'");
Message message = consumer.receive();
```

メッセージのアノテーションに基づくフィルター

```
ConnectionFactory factory = new JmsConnectionFactory("amqp://localhost:5672");
Connection connection = factory.createConnection();
Session session = connection.createSession(false, Session.AUTO_ACKNOWLEDGE);
connection.start();
javax.jms.Queue queue = session.createQueue("my_DLQ");
MessageConsumer consumer = session.createConsumer(queue, "\"m.x-opt-ORIG-
ADDRESS\"='original_address_name'");
Message message = consumer.receive();
```

注記

アノテーションに基づいて AMQP メッセージを消費する場合、クライアントには前述の例に示されるように **m.** 接頭辞をメッセージアノテーションに追加する必要があります。

関連情報

- ブローカーが期限切れの AMQP メッセージまたは未配信の AMQP メッセージに適用するアノテーションおよびプロパティーに関する詳細は、「期限切れまたは未配信の AMQP メッセージに対するアノテーションおよびプロパティー」 を参照してください。

13.4. XML メッセージのフィルターリング

AMQ Broker では、XPath を使用して XML ボディーが含まれるテキストメッセージをフィルターできます。XPath (XML Path Language) は、XML ドキュメントからノードを選択するためのクエリー言語です。

注記

テキストベースのメッセージのみがサポートされます。大きなメッセージのフィルターリングはサポートされていません。

テキストベースのメッセージをフィルターするには、**XPATH '<xpath-expression>** の形式のメッセージセレクターを作成する必要があります。

メッセージボディーの例

```
<root>
   <a key='first' num='1'/>
   <b key='second' num='2'>b</b>
</root>
```

XPath クエリーに基づくフィルター

```
PATH 'root/a'
```

警告

XPath はメッセージのボディーに適用され、XML の解析を必要とするため、フィルターリングは通常のフィルターよりも大幅に遅くなります。

XPath フィルターは、以下のプロトコルを使用するプロデューサーとコンシューマー間でサポートされます。

- OpenWire JMS
- Core (および Core JMS)
- STOMP
- AMQP

XML Parser の設定

デフォルトでは、Broker によって使用される XML Parser は JDK によって使用されるプラットフォームのデフォルト DocumentBuilderFactory インスタンスです。

XPath デフォルト設定に使用される XML パーサーには、以下の設定が含まれます。

- **http://xml.org/sax/features/external-general-entities**: **false**
- **http://xml.org/sax/features/external-parameter-entities**: **false**
- **http://apache.org/xml/features/disallow-doctype-decl**: **true**

ただし、実装固有の問題に対応するために、機能をカスタマイズするには、**artemis.profile** 設定ファイルでシステムプロパティーを設定します。

org.apache.activemq.documentBuilderFactory.feature:prefix

機能設定の例

```
-Dorg.apache.activemq.documentBuilderFactory.feature:http://xml.org/sax/features/external-general-entities=true
```

第14章 ブローカークラスターの設定

クラスターは、グループ化された複数のブローカーインスタンスで設定されます。ブローカークラスターは、メッセージ処理の負荷を複数のブローカーに分散してパフォーマンスを向上します。さらに、ブローカークラスターは、高可用性によりダウンタイムを最小限に抑えることができます。

多くの異なるクラストポロジーでブローカーを接続できます。クラスター内では、アクティブな各ブローカーは独自のメッセージを管理し、独自の接続を処理します。

また、クラスター全体でクライアント接続を分散し、メッセージの再分配を行うことで、ブローカーの不足を避けることもできます。

14.1. ブローカークラスターについて

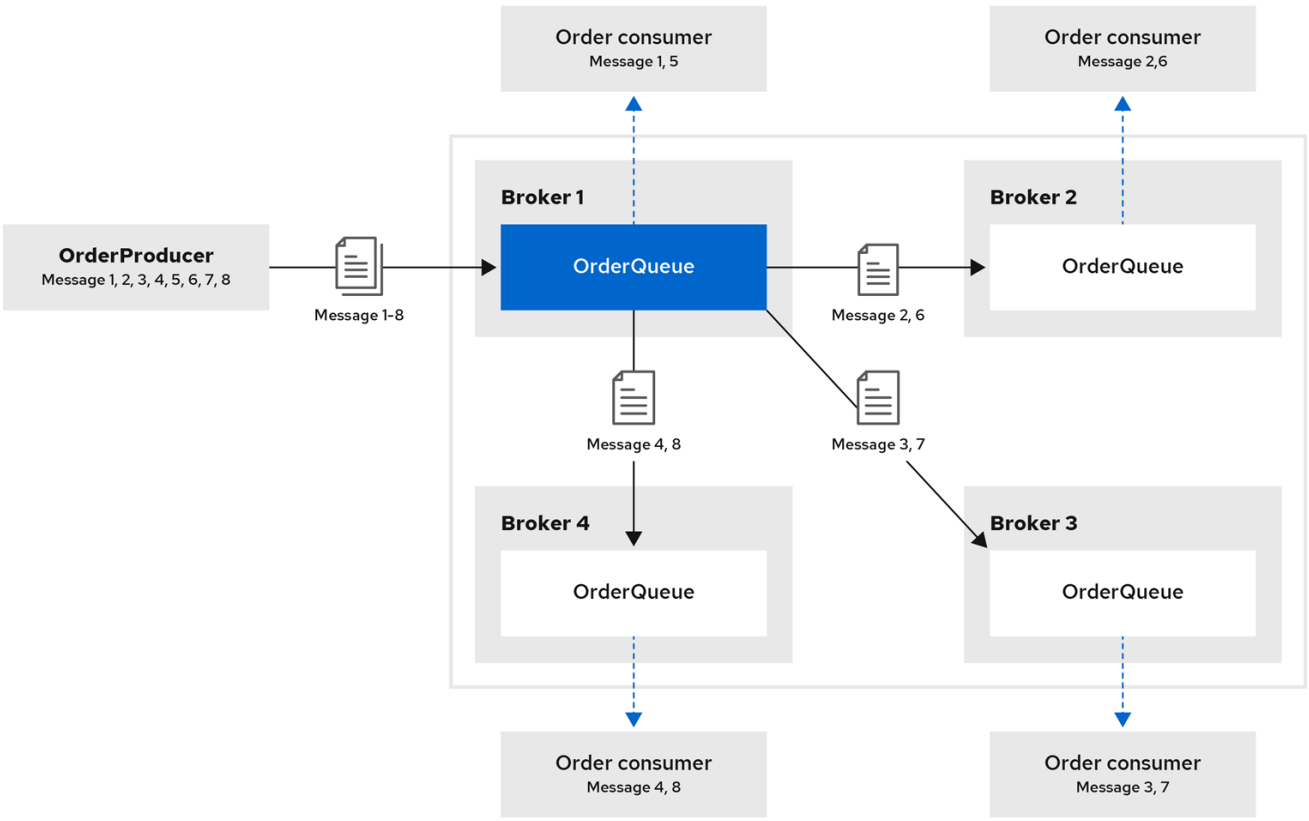
ブローカークラスターを作成する前に、いくつかの重要なクラスターリングの概念を理解する必要があります。

14.1.1. ブローカークラスターがメッセージ負荷のバランスを取る方法

ブローカーがクラスターを形成するとき、AMQ Broker はブローカー間でメッセージの負荷を自動的に分散します。これにより、クラスターが高メッセージスループットを維持できるようになります。

4 つのブローカーの対称クラスターについて考えてみましょう。各ブローカーは **OrderQueue** という名前のキューで設定されます。**OrderProducer** クライアントは **Broker1** に接続し、メッセージを **OrderQueue** に送信します。**Broker1** は、ラウンドロビン方式でメッセージを他のブローカーに転送します。各ブローカーに接続されている **OrderConsumer** クライアントはメッセージを消費します。正確な順序は、ブローカーが起動した順序によって異なります。

図14.1 メッセージの負荷分散



メッセージの負荷分散がない場合、**Broker1** に送信されたメッセージは **Broker1** に残り、**OrderConsumer1** のみがそれらを消費できます。

AMQ Broker はデフォルトでメッセージを自動的に負荷分散しますが、以下を設定できます。

- 一致するキューを持つブローカーへのメッセージの負荷分散を行うクラスター。
- 一致するキューとアクティブなコンシューマーを持つブローカーへのメッセージの負荷分散を行うクラスター。
- 負荷分散は行わないが、コンシューマーを持つキューへコンシューマーを持たないキューからのメッセージの再分配を実行するクラスター。
- コンシューマーのないキューからコンシューマーを持つキューへのメッセージを自動的に再分散するアドレス。

関連情報

- メッセージの負荷分散ポリシーは、各ブローカーのクラスター接続の **message-load-balancing** プロパティーで設定されます。詳細は、付録C *クラスター接続設定要素* を参照してください。
- メッセージ再分配に関する詳細は、「メッセージ再分配の設定」 を参照してください。

14.1.2. ブローカークラスターが信頼性を向上させる方法

ブローカークラスターは高可用性とフェイルオーバーを可能にします。これにより、スタンドアロンブローカーよりも信頼性が高くなります。高可用性を設定すると、ブローカーが障害イベントに遭遇しても、クライアントアプリケーションがメッセージを送受信できます。

高可用性により、クラスターのブローカーはライブバックアップグループにグループ化されます。ライブバックアップグループは、クライアントのリクエストに対応するライブブローカーと、パッシブに待機してライブブローカーを置き換える 1 つ以上のバックアップブローカーで設定されます。障害が発生した場合、バックアップブローカーはライブバックアップグループのライブブローカーを置き換え、クライアントが再接続して作業を続行します。

14.1.3. ノード ID について

ブローカー **ノード ID** は、ブローカーインスタンスのジャーナルの初回作成および初期化時にプログラムで生成されるグローバルー意識別子 (GUID) です。ノード ID は **server.lock** ファイルに保存されます。ノード ID は、ブローカーがスタンドアロンインスタンスか、またはクラスターの一部であるかに関わらず、ブローカーインスタンスを一意に識別するために使用されます。ライブバックアップブローカーペアは、同じジャーナルを共有するため、同じノード ID を共有します。

ブローカークラスターでは、ブローカーインスタンス (ノード) は相互に接続し、ブリッジおよび内部のストアアンドフォワードキューを作成します。これらの内部キューの名前は、他のブローカーインスタンスのノード ID に基づいています。ブローカーインスタンスは、独自のノード ID のクラスターブロードキャストも監視します。ブローカーは、重複 ID を特定する場合にログに警告メッセージを生成します。

レプリケーション高可用性 (HA) ポリシーを使用している場合、起動するマスターブローカーと、**check-for-live-server** が **true** に設定されたマスターブローカーは、ノード ID を使用するブローカーを検索します。マスターブローカーが同じノード ID を使用して別のブローカーを見つける場合、それは起動しないか、または HA 設定に基づいてフェイルバックを開始します。

ノード ID は **永続性** があるため、ブローカーの再起動後も維持されます。ただし、(ジャーナルを含む) ブローカーインスタンスを削除すると、ノード ID も永続的に削除されます。

関連情報

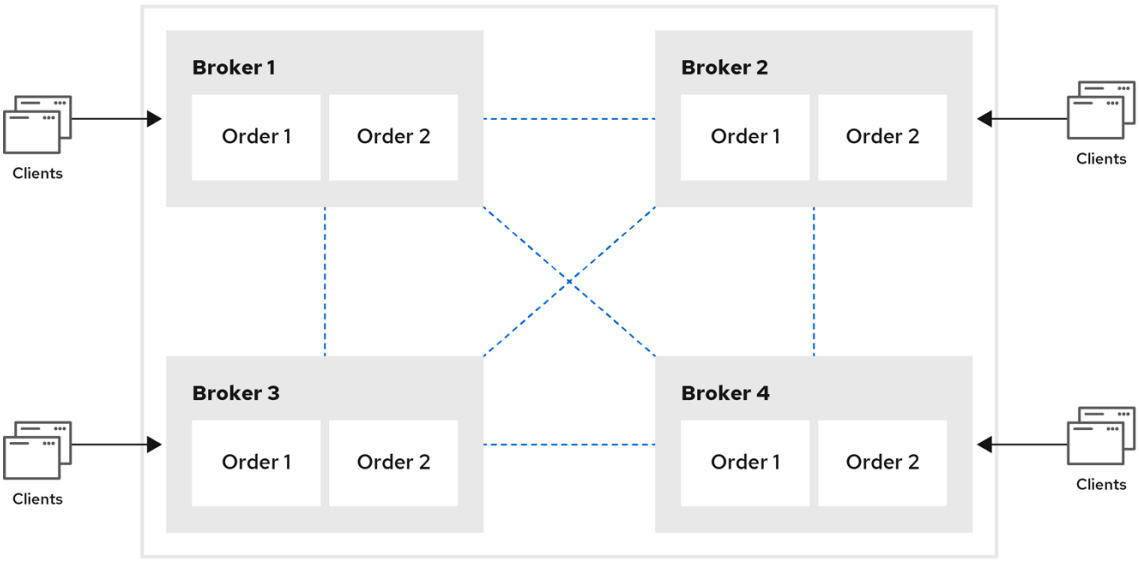
- レプリケーション HA ポリシーの設定に関する詳細は、Configuring replication high availability を参照してください。

14.1.4. 一般的なブローカークラストポロジー

ブローカーに接続し、**対称** または **チェーン** クラストポロジーのいずれかを形成できます。実装するトポロジーは、環境およびメッセージングの要件によって異なります。

対称クラスター
対称クラスターでは、すべてのブローカーが他のすべてのブローカーに接続されます。つまり、すべてのブローカーは他のすべてのブローカーから複数のホップを削除できません。

図14.2 対称クラスター



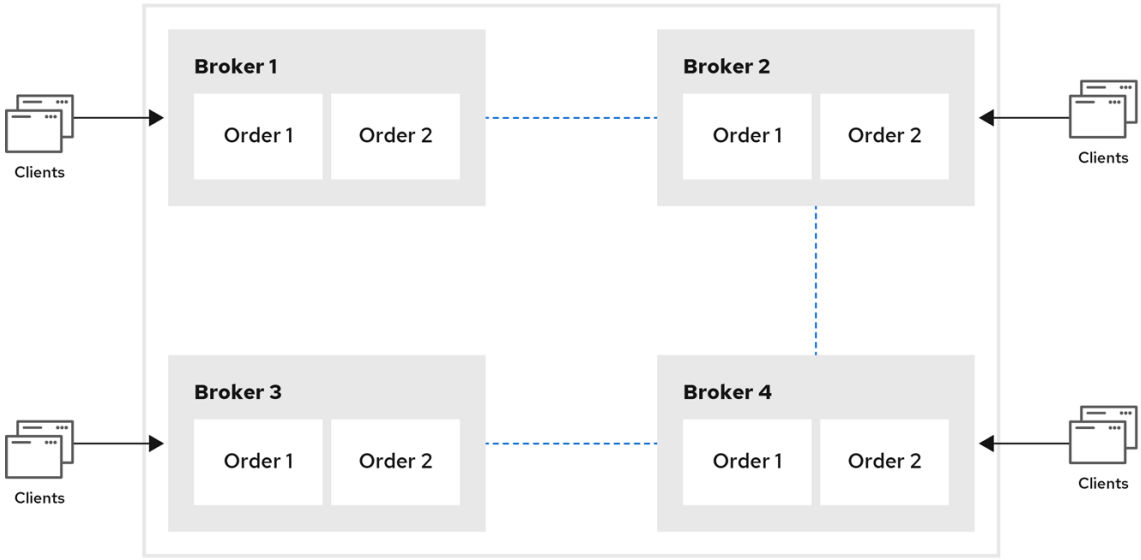
120_AMQ_1120

対称クラスターの各ブローカーは、クラスター内の他のすべてのブローカーに存在するすべてのキューと、これらのキューでリッスンしているコンシューマーを認識します。そのため、対称クラスターは、メッセージをチェーンクラスターよりも最適に負荷分散および再分散できます。

対称クラスターはチェーンクラスターよりも設定が簡単ですが、ネットワーク制限が原因でブローカーが直接接続されないようにする環境では使用が困難になる可能性があります。

チェーンクラスター
チェーンクラスターでは、クラスターの各ブローカーはクラスター内のすべてのブローカーに直接接続されません。代わりに、ブローカーはチェーンの最後ごとにブローカーと、チェーンの前のブローカーおよび次のブローカーに接続するすべてのブローカーでチェーンを形成します。

図14.3 チェーンクラスター



チェーンクラスターは対称クラスターよりも設定が難しくなりますが、ブローカーが別個のネットワーク上にあり、直接接続できない場合に役立ちます。チェーンクラスターを使用すると、中間ブローカーは 2 つのブローカーを間接的に接続し、2 つのブローカーが直接接続されていない場合でも、メッセージ間のフローが可能になります。

14.1.5. ブローカー検出メソッド

検出は、クラスターのブローカーが接続の詳細を相互に伝播するメカニズムです。AMQ Broker は、**動的検出** と **静的検出** の両方をサポートします。

動的検出
クラスターの各ブローカーは、UDP マルチキャストまたは JGroups のいずれかを使用して接続設定を他のメンバーにブロードキャストします。この方法では、各ブローカーは以下を使用します。

- クラスター接続に関する情報をクラスターの他の潜在的なメンバーにプッシュする **ブロードキャストグループ**。
- クラスターの他のブローカーに関するクラスター接続情報を受信し、保存する **ディスカバリーグループ**。

静的検出
ネットワークで UDP または JGroups を使用できない場合や、クラスターの各メンバーを手動で指定する場合は、静的検出を使用できます。この方法では、2 番目のブローカーに接続し、その接続の詳細を送信することで、ブローカーを結合します。次に、2 番目のブローカーはそれらの詳細をクラスターの他のブローカーに伝播します。

14.1.6. クラスターのサイジングに関する考慮事項

ブローカークラスターを作成する前に、メッセージングのスループット、トポロジー、および高可用性の要件を考慮してください。これらの要因は、クラスターに追加するブローカーの数に影響します。

注記

クラスターの作成後に、ブローカーを追加および削除してサイズを調整できます。メッセージを失うことなく、ブローカーを追加および削除できます。

メッセージングスループット
クラスターには、必要なメッセージングスループットを提供するのに十分なブローカーが含まれる必要があります。クラスターの他のブローカーにより、スループットが高くなります。ただし、大規模なクラスターは管理が複雑になる可能性があります。

トポロジー
対称クラスターまたはチェーンクラスターのいずれかを作成できます。選択したトポロジーのタイプは、必要なブローカーの数に影響します。

詳細は、「一般的なブローカークラスタートポロジー」 を参照してください。

高可用性
高可用性 (HA) が必要な場合は、クラスターを作成する前に HA ポリシーを選択することを検討してください。各マスターブローカーは少なくとも 1 つのスレーブブローカーを持つ必要があるため、HA ポリシーはクラスターのサイズに影響します。

詳細は、「高可用性の実装」 を参照してください。

14.2. ブローカークラスターの作成

クラスターに参加する各ブローカーにクラスター接続を設定して、ブローカークラスターを作成します。クラスター接続は、ブローカーが他のブローカーに接続する方法を定義します。

静的検出または動的検出を使用するブローカークラスターを作成できます (UDP マルチキャストまたは JGroups のいずれか)。

前提条件

- ブローカークラスターのサイズを決定する必要があります。
  詳細は、「クラスターのサイジングに関する考慮事項」 を参照してください。

14.2.1. 静的検出を使用したブローカークラスターの作成

ブローカーの静的リストを指定して、ブローカークラスターを作成できます。ネットワーク上で UDP マルチキャストまたは JGroups を使用できない場合は、この静的検出メソッドを使用します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<core>** 要素内に以下のコネクターを追加します。
   - 他のブローカーがこのブローカーに接続する方法を定義するコネクター。
   - このブローカーがクラスター内の他のブローカーに接続する方法を定義する 1 つ以上のコネクター。

```
<configuration>
  <core>
    ...
```

```
      <connectors>
         <connector name="netty-connector">tcp://localhost:61617</connector> (1)
         <connector name="broker2">tcp://localhost:61618</connector> (2)
         <connector name="broker3">tcp://localhost:61619</connector>
      </connectors>
      ...
   </core>
</configuration>
```

(1) このコネクターは、他のブローカーがこの接続に使用できる接続情報を定義します。この情報は、検出中にクラスター内の他のブローカーに送信されます。

(2) **broker2** および **broker3** コネクターは、このブローカーがクラスター内の 2 つの他のブローカーに接続する方法を定義します。クラスターに他のブローカーがある場合、それらは最初の接続が確立されたときにこれらのコネクターのいずれかによって検出されます。

コネクターの詳細は、「コネクター」 を参照してください。

3. クラスター接続を追加し、静的検出を使用するように設定します。
デフォルトでは、クラスター接続は対称トポロジーのすべてのアドレスに対してメッセージの負荷分散を行います。

```
<configuration>
   <core>
      ...
      <cluster-connections>
         <cluster-connection name="my-cluster">
            <connector-ref>netty-connector</connector-ref>
            <static-connectors>
               <connector-ref>broker2-connector</connector-ref>
               <connector-ref>broker3-connector</connector-ref>
            </static-connectors>
         </cluster-connection>
      </cluster-connections>
      ...
   </core>
</configuration>
```

cluster-connection

name 属性を使用してクラスター接続の名前を指定します。

connector-ref

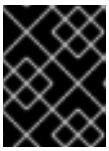
他のブローカーがこのブローカーに接続する方法を定義するコネクター。

static-connectors

このブローカーがクラスター内の別のブローカーへの最初の接続を確立するために使用できる 1 つ以上のコネクター。この最初の接続を行った後、ブローカーはクラスター内の他のブローカーを検出します。クラスターが静的検出を使用する場合のみ、このプロパティーを設定する必要があります。

4. クラスター接続の追加プロパティーを設定します。
これらの追加のクラスター接続プロパティーには、最も一般的なユースケースに適したデフォルト値があります。そのため、デフォルト動作が必要ない場合のみこのプロパティーを設定する必要があります。詳細は、付録C *クラスター接続設定要素* を参照してください。

5. クラスターユーザーおよびパスワードを作成します。
AMQ Broker にはデフォルトのクラスター認証情報が同梱されていますが、承認されていないリモートクライアントがこれらのデフォルト認証情報を使用してブローカーに接続するのを防ぐため、これらの変更を行う必要があります。



重要

クラスターのパスワードは、クラスター内のすべてのブローカーで同じである必要があります。

```
<configuration>
  <core>
    ...
    <cluster-user>cluster_user</cluster-user>
    <cluster-password>cluster_user_password</cluster-password>
    ...
  </core>
</configuration>
```

6. 追加のブローカーごとにこの手順を繰り返します。
クラスター設定を各追加ブローカーにコピーできます。ただし、他の AMQ Broker データファイルはコピーしないでください (バインディング、ジャーナル、大きなメッセージディレクトリーなど)。これらのファイルは、クラスター内のノード間で一意である必要があり、クラスターが適切に形成されません。

関連情報

- 静的検出を使用するブローカークラスターの例は、**clustered-static-discovery** AMQ Broker example program を参照してください。

14.2.2. UDP ベースの動的検出を使用したブローカークラスターの作成

ブローカーが UDP マルチキャストを使用して動的に相互を検出するブローカークラスターを作成できます。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

2. **<core>** 要素内にコネクターを追加します。
このコネクターは、他のブローカーがこの接続に使用できる接続情報を定義します。この情報は、検出中にクラスター内の他のブローカーに送信されます。

```
<configuration>
  <core>
    ...
    <connectors>
      <connector name="netty-connector">tcp://localhost:61617</connector>
    </connectors>
    ...
  </core>
</configuration>
```

3. UDP ブロードキャストグループを追加します。
ブロードキャストグループにより、ブローカーはクラスター接続に関する情報をクラスター内の他のブローカーにプッシュできます。このブロードキャストグループは UDP を使用して接続設定をブロードキャストします。

```
<configuration>
  <core>
    ...
    <broadcast-groups>
      <broadcast-group name="my-broadcast-group">
        <local-bind-address>172.16.9.3</local-bind-address>
        <local-bind-port>-1</local-bind-port>
        <group-address>231.7.7.7</group-address>
        <group-port>9876</group-port>
        <broadcast-period>2000</broadcast-period>
        <connector-ref>netty-connector</connector-ref>
      </broadcast-group>
    </broadcast-groups>
    ...
  </core>
</configuration>
```

特に指示がない限り、以下のパラメーターが必要です。

broadcast-group

name 属性を使用してブロードキャストグループの一意の名前を指定します。

local-bind-address

UDP ソケットがバインドされるアドレス。ブローカーに複数のネットワークインターフェイスがある場合は、ブロードキャストに使用するインターフェイスを指定する必要があります。このプロパティーが指定されていない場合、ソケットはオペレーティングシステムによって選択される IP アドレスにバインドされます。これは UDP 固有の属性です。

local-bind-port

データグラムソケットがバインドされるポート。ほとんどの場合、匿名ポートを指定するデフォルト値の **-1** を使用します。このパラメーターは、**local-bind-address** との接続で使用されます。これは UDP 固有の属性です。

group-address

データがブロードキャストされるマルチキャストアドレス。これは、**224.0.0.0** - **239.255.255.255** の範囲のクラス D IP アドレスです。アドレス **224.0.0.0** は予約されており、使用することはできません。これは UDP 固有の属性です。

group-port

ブロードキャストに使用される UDP ポート番号。これは UDP 固有の属性です。

broadcast-period (オプション)

連続するブロードキャストの間隔 (ミリ秒単位)。デフォルト値は 2000 ミリ秒です。

connector-ref

ブロードキャストされる必要がある以前に設定されたクラスターコネクター。

4. UDP 検出グループを追加します。
検出グループは、このブローカーが他のブローカーからコネクター情報を受け取る方法を定義します。ブローカーはコネクターのリストを維持します (各ブローカーに 1 エントリー)。ブローカーからブロードキャストを受信すると、そのエントリーが更新されます。期間のブローカーからブロードキャストを受信しない場合は、エントリーを削除します。

この検出グループは UDP を使用してクラスター内のブローカーを検出します。

```
<configuration>
   <core>
      ...
      <discovery-groups>
         <discovery-group name="my-discovery-group">
            <local-bind-address>172.16.9.7</local-bind-address>
            <group-address>231.7.7.7</group-address>
            <group-port>9876</group-port>
            <refresh-timeout>10000</refresh-timeout>
         </discovery-group>
      <discovery-groups>
      ...
   </core>
</configuration>
```

特に指示がない限り、以下のパラメーターが必要です。

discovery-group

name 属性を使用して検出グループの一意の名前を指定します。

local-bind-address (オプション)

ブローカーが稼働しているマシンが複数のネットワークインターフェイスを使用する場合は、ディスカバリーグループがリッスンするネットワークインターフェイスを指定できます。これは UDP 固有の属性です。

group-address

リッスンするグループのマルチキャストアドレス。リッスンするブロードキャストグループの **group-address** と一致する必要があります。これは UDP 固有の属性です。

group-port

マルチキャストグループの UDP ポート番号。リッスンするブロードキャストグループの **group-port** と一致する必要があります。これは UDP 固有の属性です。

refresh-timeout (オプション)

特定のブローカーから最後のブロードキャストを受信した後、そのブローカーのコネクターペアエントリーをリストから削除するまで、ディスカバリーグループが待機する時間 (ミリ秒単位)。デフォルトは 10000 ミリ秒 (10 秒) です。
この値は、ブロードキャストグループの **broadcast-period** よりも大きな値に設定します。そうしないと、(タイミングで若干の違いを及ぼすため) ブロードキャスト中であってもブローカーが一覧から定期的に消える可能性があります。

5. クラスター接続を作成し、動的検出を使用するように設定します。
デフォルトでは、クラスター接続は対称トポロジーのすべてのアドレスに対してメッセージの負荷分散を行います。

```
<configuration>
   <core>
      ...
      <cluster-connections>
         <cluster-connection name="my-cluster">
            <connector-ref>netty-connector</connector-ref>
            <discovery-group-ref discovery-group-name="my-discovery-group"/>
         </cluster-connection>
```

```
        </cluster-connections>
        ...
    </core>
</configuration>
```

cluster-connection

name 属性を使用してクラスター接続の名前を指定します。

connector-ref

他のブローカーがこのブローカーに接続する方法を定義するコネクター。

discovery-group-ref

このブローカーがクラスターの他のメンバーを見つけるために使用する検出グループ。クラスターが動的検出を使用する場合のみ、このプロパティーを設定する必要があります。

6. クラスター接続の追加プロパティーを設定します。
これらの追加のクラスター接続プロパティーには、最も一般的なユースケースに適したデフォルト値があります。そのため、デフォルト動作が必要ない場合のみこのプロパティーを設定する必要があります。詳細は、付録C *クラスター接続設定要素* を参照してください。

7. クラスターユーザーおよびパスワードを作成します。
AMQ Broker にはデフォルトのクラスター認証情報が同梱されていますが、承認されていないリモートクライアントがこれらのデフォルト認証情報を使用してブローカーに接続するのを防ぐため、これらの変更を行う必要があります。

重要

クラスターのパスワードは、クラスター内のすべてのブローカーで同じである必要があります。

```
<configuration>
    <core>
        ...
        <cluster-user>cluster_user</cluster-user>
        <cluster-password>cluster_user_password</cluster-password>
        ...
    </core>
</configuration>
```

8. 追加のブローカーごとにこの手順を繰り返します。
クラスター設定を各追加ブローカーにコピーできます。ただし、他の AMQ Broker データファイルはコピーしないでください (バインディング、ジャーナル、大きなメッセージディレクトリーなど)。これらのファイルは、クラスター内のノード間で一意である必要があり、クラスターが適切に形成されません。

関連情報

- UDP で動的検出を使用するブローカークラスター設定の例は、 **clustered-queue** AMQ Broker example program を参照してください。

14.2.3. JGroups ベースの動的検出を使用したブローカークラスターの作成

すでに JGroups をお使いの環境で使用している場合は、これを使用して、ブローカーが相互に動的に検出するブローカークラスターを作成できます。

前提条件

- JGroups がインストールされ、設定されている必要があります。
  JGroups 設定ファイルの例は、 **clustered-jgroups** AMQ Broker example program を参照してください。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<core>** 要素内にコネクターを追加します。
   このコネクターは、他のブローカーがこの接続に使用できる接続情報を定義します。この情報は、検出中にクラスター内の他のブローカーに送信されます。

```
<configuration>
   <core>
      ...
      <connectors>
         <connector name="netty-connector">tcp://localhost:61617</connector>
      </connectors>
      ...
   </core>
</configuration>
```

3. **<core>** 要素内に JGroups ブロードキャストグループを追加します。
   ブロードキャストグループにより、ブローカーはクラスター接続に関する情報をクラスター内の他のブローカーにプッシュできます。このブロードキャストグループは JGroups を使用して接続設定をブロードキャストします。

```
<configuration>
   <core>
      ...
      <broadcast-groups>
         <broadcast-group name="my-broadcast-group">
            <jgroups-file>test-jgroups-file_ping.xml</jgroups-file>
            <jgroups-channel>activemq_broadcast_channel</jgroups-channel>
            <broadcast-period>2000</broadcast-period>
            <connector-ref>netty-connector</connector-ref>
         </broadcast-group>
      </broadcast-groups>
      ...
   </core>
</configuration>
```

   特に指示がない限り、以下のパラメーターが必要です。

   broadcast-group

   name 属性を使用してブロードキャストグループの一意の名前を指定します。

   jgroups-file

   JGroups チャネルを初期化する JGroups 設定ファイルの名前。ブローカーが読み込めるように、このファイルは Java リソースパスにある必要があります。

   jgroups-channel

   ブロードキャストするために接続する JGroups チャネルの名前。

broadcast-period (オプション)

連続するブロードキャストの間隔 (ミリ秒単位)。デフォルト値は 2000 ミリ秒です。

connector-ref

ブロードキャストされる必要がある以前に設定されたクラスターコネクター。

4. JGroups 検出グループを追加します。
検出グループは、コネクター情報を受け取る方法を定義します。ブローカーはコネクターのリストを維持します (各ブローカーに 1 エントリー)。ブローカーからブロードキャストを受信すると、そのエントリーが更新されます。期間のブローカーからブロードキャストを受信しない場合は、エントリーを削除します。

この検出グループは JGroups を使用してクラスター内のブローカーを検出します。

```
<configuration>
   <core>
      ...
      <discovery-groups>
         <discovery-group name="my-discovery-group">
            <jgroups-file>test-jgroups-file_ping.xml</jgroups-file>
            <jgroups-channel>activemq_broadcast_channel</jgroups-channel>
            <refresh-timeout>10000</refresh-timeout>
         </discovery-group>
      <discovery-groups>
      ...
   </core>
</configuration>
```

特に指示がない限り、以下のパラメーターが必要です。

discovery-group

name 属性を使用して検出グループの一意の名前を指定します。

jgroups-file

JGroups チャネルを初期化する JGroups 設定ファイルの名前。ブローカーが読み込めるように、このファイルは Java リソースパスにある必要があります。

jgroups-channel

ブロードキャストを受信するために接続する JGroups チャネルの名前。

refresh-timeout (オプション)

特定のブローカーから最後のブロードキャストを受信した後、そのブローカーのコネクターペアエントリーをリストから削除するまで、ディスカバリーグループが待機する時間 (ミリ秒単位)。デフォルトは 10000 ミリ秒 (10 秒) です。
この値は、ブロードキャストグループの **broadcast-period** よりも大きな値に設定します。そうしないと、(タイミングで若干の違いを及ぼすため) ブロードキャスト中であってもブローカーが一覧から定期的に消える可能性があります。

5. クラスター接続を作成し、動的検出を使用するように設定します。
デフォルトでは、クラスター接続は対称トポロジーのすべてのアドレスに対してメッセージの負荷分散を行います。

```
<configuration>
   <core>
      ...
```

```
      <cluster-connections>
         <cluster-connection name="my-cluster">
            <connector-ref>netty-connector</connector-ref>
            <discovery-group-ref discovery-group-name="my-discovery-group"/>
         </cluster-connection>
      </cluster-connections>
      ...
   </core>
</configuration>
```

cluster-connection

name 属性を使用してクラスター接続の名前を指定します。

connector-ref

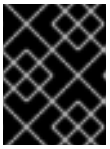
他のブローカーがこのブローカーに接続する方法を定義するコネクター。

discovery-group-ref

このブローカーがクラスターの他のメンバーを見つけるために使用する検出グループ。クラスターが動的検出を使用する場合のみ、このプロパティーを設定する必要があります。

6. クラスター接続の追加プロパティーを設定します。
これらの追加のクラスター接続プロパティーには、最も一般的なユースケースに適したデフォルト値があります。そのため、デフォルト動作が必要ない場合のみこのプロパティーを設定する必要があります。詳細は、付録C *クラスター接続設定要素* を参照してください。

7. クラスターユーザーおよびパスワードを作成します。
AMQ Broker にはデフォルトのクラスター認証情報が同梱されていますが、承認されていないリモートクライアントがこれらのデフォルト認証情報を使用してブローカーに接続するのを防ぐため、これらの変更を行う必要があります。



重要

クラスターのパスワードは、クラスター内のすべてのブローカーで同じである必要があります。

```
<configuration>
   <core>
      ...
      <cluster-user>cluster_user</cluster-user>
      <cluster-password>cluster_user_password</cluster-password>
      ...
   </core>
</configuration>
```

8. 追加のブローカーごとにこの手順を繰り返します。
クラスター設定を各追加ブローカーにコピーできます。ただし、他の AMQ Broker データファイルはコピーしないでください (バインディング、ジャーナル、大きなメッセージディレクトリーなど)。これらのファイルは、クラスター内のノード間で一意である必要があり、クラスターが適切に形成されません。

関連情報

- JGroups で動的検出を使用するブローカークラスターの例は、**clustered-jgroups** AMQ Broker example program を参照してください。

14.3. 高可用性の実装

高可用性 (HA) を実装することでその信頼性を強化し、ブローカークラスターは 1 つ以上のブローカーがオフラインになっても機能し続けます。

HA の実装には、複数のステップが関係します。

1. 「ブローカークラスターの作成」 の説明に従って、HA 実装のブローカークラスターを設定します。
2. ライブバックアップグループの概要を理解し、要件に最も適した HA ポリシーを選択する必要があります。Understanding how HA works in AMQ Broker を参照してください。
3. 適切な HA ポリシーを選択したら、クラスター内の各ブローカーに HA ポリシーを設定します。以下を参照してください。
   - Configuring shared store high availability
   - Configuring replication high availability
   - Configuring limited high availability with live-only
   - Configuring high availability with colocated backups
4. フェイルオーバーを使用するようにクライアントアプリケーションを設定します。

注記

高可用性用に設定されたブローカークラスターをトラブルシューティングする必要がある場合は、クラスターでブローカーを実行している各 Java Virtual Machine (JVM) インスタンスにガベージコレクション (GC) ロギングを有効にすることが推奨されます。JVM で GC ログを有効にする方法については、JVM で使用される Java Development Kit (JDK) バージョンの公式ドキュメントを参照してください。AMQ Broker がサポートする JVM バージョンの詳細は、Red Hat AMQ 7 Supported Configurations を参照してください。

14.3.1. High Availability Deployment and Usage

AMQ Broker では、クラスターでブローカーを **ライブバックアップグループ** にグループ化して、高可用性 (HA) を実装します。ライブバックアップグループでは、ライブブローカーはバックアップブローカーにリンクされ、失敗した場合はライブブローカーを引き継ぐことができます。AMQ Broker は、ライブバックアップグループ内のフェイルオーバー (**HA ポリシー** と呼ばれる) にいくつかの異なるストラテジーも提供します。

14.3.1.1. ライブバックアップグループがどのように高可用性を提供するか

AMQ Broker では、クラスターにブローカーをリンクして高可用性 (HA) を実装し、**ライブバックアップグループ** を形成します。ライブバックアップグループは **フェイルオーバー** を提供します。つまり、1 つのブローカーが失敗すると、別のブローカーがメッセージ処理を引き継ぐことができます。

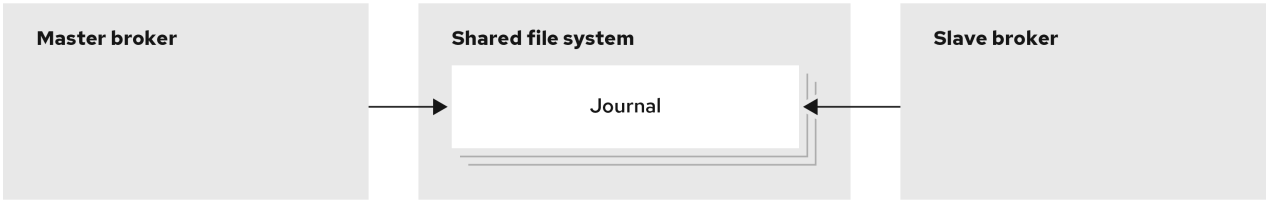
ライブバックアップグループは、1 つ以上のバックアップブローカー (**スレーブ** ブローカーとも呼ばれる) にリンクされた 1 つのライブブローカー (**マスター** ブローカーとも呼ばれる) で設定されます。ライブブローカーはクライアント要求に対応し、バックアップブローカーはパッシブモードで待機します。ライブブローカーが失敗すると、バックアップブローカーはライブブローカーに置き換わり、クライアントが再接続し、作業を続行します。

14.3.1.2. 高可用性ポリシー

高可用性 (HA) ポリシーは、ライブバックアップグループでのフェイルオーバーの発生方法を定義します。AMQ Broker では、複数の HA ポリシーが提供されます。

共有ストア (推奨)

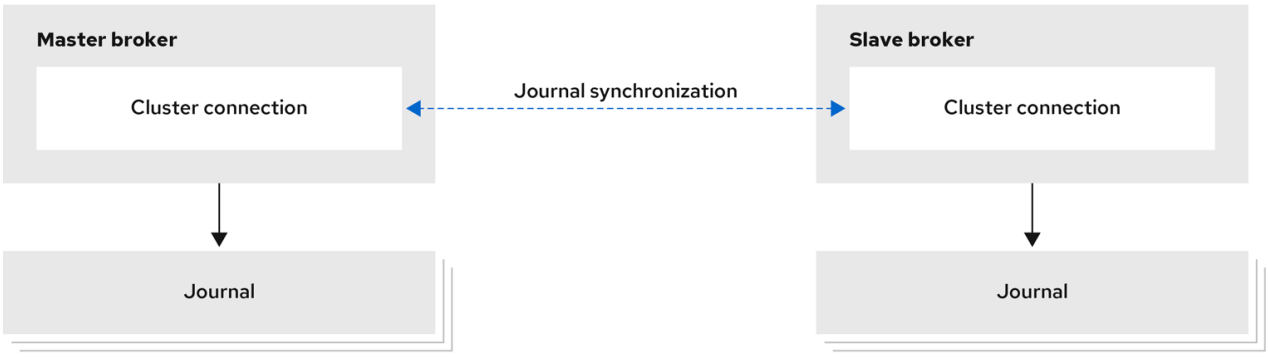
ライブおよびバックアップブローカーは、メッセージングデータを共有ファイルシステム上の共通ディレクトリー (通常は Storage Area Network (SAN) または Network File System (NFS) サーバー) に保存します。また、JDBC ベースの永続を設定している場合は、ブローカーデータを指定されたデータベースに保存することもできます。共有ストアでは、ライブブローカーが失敗すると、バックアップブローカーは共有ストアからメッセージデータを読み込み、失敗したライブブローカーに対して引き継ぎします。
ほとんどの場合、レプリケーションの代わりに共有ストアを使用する必要があります。共有ストアはネットワーク経由でデータを複製しないため、通常はレプリケーションよりもパフォーマンスが向上します。共有ストアは、ライブブローカーとそのバックアップが同時に行われるという問題である、ネットワーク分離 (スプリットブレインとも呼ばれる) を回避します。



レプリケーション

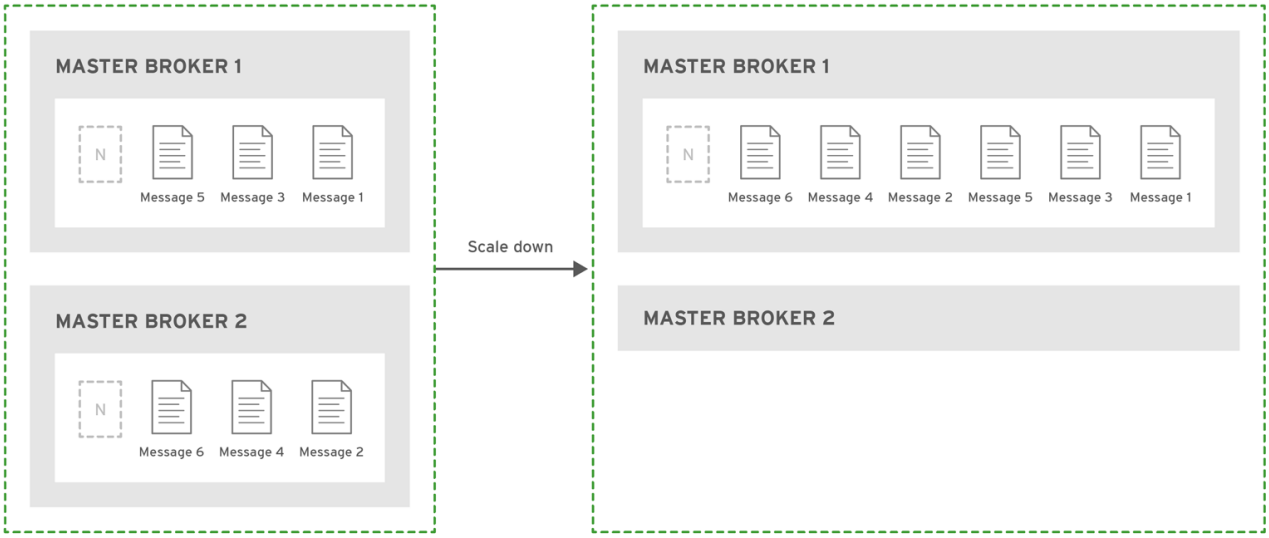
ライブおよびバックアップブローカーは、そのメッセージングデータをネットワーク経由で継続的に同期します。ライブブローカーが失敗すると、バックアップブローカーは同期データを読み込み、失敗したライブブローカーに対して引き継ぎます。
ライブブローカーとバックアップブローカー間のデータ同期により、ライブブローカーが失敗してもメッセージングデータが失われないようにします。ライブブローカーおよびバックアップブローカーが最初に結合すると、ライブブローカーはネットワーク経由ですべての既存データをバックアップブローカーに複製します。この最初のフェーズが完了すると、ライブブローカーは永続データを、ライブブローカーが受信時にバックアップブローカーに複製します。つまり、ライブブローカーがネットワークから切断されると、バックアップブローカーには、ライブブローカーが受信したすべての永続データが含まれます。

レプリケーションはネットワーク経由でデータを同期するため、ネットワーク障害により、ライブブローカーとそのバックアップが同時に存続するネットワーク分離が発生する可能性があります。



ライブのみ (限定 HA)

ライブブローカーが正常に停止されると、メッセージとトランザクションの状態を別のライブブローカーにコピーし、シャットダウンします。その後、クライアントは他のブローカーに再接続し、メッセージの送受信を続行します。



関連情報

- ライブバックアップグループのブローカー間で共有される永続メッセージデータの詳細は、「ジャーナルでのメッセージデータの永続化」 を参照してください。

14.3.1.3. レプリケーションポリシーの制限

ネットワーク分離 (スプリットブレインと呼ばれることもあります) は、レプリケーションの高可用性 (HA) ポリシーの制限です。その発生方法、およびその回避方法を理解している必要があります。

ライブブローカーとそのバックアップが接続を失うと、ネットワーク分離が発生する可能性があります。この場合、ライブブローカーとそのバックアップの両方を同時にアクティブにすることができます。具体的には、バックアップブローカーがクラスター内のライブブローカーの半分以上に接続できる場合は、アクティブになります。この状況では、ブローカー間でメッセージレプリケーションがないため、各ブローカーはクライアントとプロセスメッセージに、他のメッセージを認識せずに提供します。この場合、各ブローカーは完全に異なるジャーナルを持ちます。この状況からの復元は非常に困難であり、場合によっては不可能です。

ネットワーク分離を回避するには、以下の点を考慮してください。

- ネットワーク分離の可能性を **なくす** には、**共有ストア** HA ポリシーを使用します。
- レプリケーション HA ポリシーを使用する場合は、**少なくとも 3 つのライブ / バックアップのペア** を使用することで、ネットワーク分離が発生する可能性を軽減 (ただし除外しない) できます。
  少なくとも 3 つのライブ / バックアップのペアを使用することで、ライブ / バックアップブローカーのペアでレプリケーションが中断された場合に発生する **クォーラム票** で過半数の結果を得ることができます。

レプリケーション HA ポリシーを使用する場合の追加に関する考慮事項は以下のとおりです。

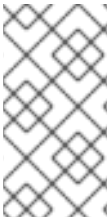
- ライブブローカーが失敗し、バックアップがライブに移行すると、新しいバックアップブローカーがライブに割り当てられるまで、または元のライブブローカーへのフェイルバックが発生するまでレプリケーションは行われません。
- ライブバックアップグループでバックアップブローカーが失敗すると、ライブブローカーはメッセージを提供します。ただし、メッセージは別のブローカーがバックアップとして追加されるか、または元のバックアップブローカーが再起動されるまで複製されません。この間、メッセージはライブブローカーにのみ永続化されます。
- ライブバックアップペアの両方のブローカーが以前にシャットダウンしたが、再起動できるようになったとします。この場合、メッセージが失われないようにするには、最初にアクティブなブローカーを再起動する必要があります。最近アクティブなブローカーがバックアップブローカーであった場合は、このブローカーをマスターブローカーとして手動で再設定し、最初に再起動できるようにする必要があります。

14.3.2. Configuring shared store high availability

共有ストア高可用性 (HA) ポリシーを使用して HA をブローカークラスターに実装できます。共有ストアでは、ライブおよびバックアップブローカーの両方が、共有ファイルシステム上の共通ディレクトリー (通常は Storage Area Network (SAN) または Network File System (NFS) サーバー) にアクセスします。また、JDBC ベースの永続を設定している場合は、ブローカーデータを指定されたデータベースに保存することもできます。共有ストアでは、ライブブローカーが失敗すると、バックアップブローカーは共有ストアからメッセージデータを読み込み、失敗したライブブローカーに対して引き継ぎします。

通常、SAN は NFS サーバーよりもパフォーマンスが向上する (速度など)、推奨されるオプションになります (利用可能な場合)。NFS サーバーを使用する必要がある場合は、AMQ Broker がサポートするネットワークファイルシステムに関する詳細は、Red Hat AMQ 7 Supported Configurations を参照してください。

ほとんどの場合、レプリケーションの代わりに共有ストア HA を使用する必要があります。共有ストアはネットワーク経由でデータを複製しないため、通常はレプリケーションよりもパフォーマンスが向上します。共有ストアは、ライブブローカーとそのバックアップが同時に行われるという問題である、ネットワーク分離 (スプリットブレインとも呼ばれる) を回避します。



注記

共有ストアを使用する場合、バックアップブローカーの起動時間はメッセージジャーナルのサイズによって異なります。バックアップブローカーが失敗したライブブローカーに対して引き継がると、共有ストアからジャーナルが読み込まれます。ジャーナルに多くのデータが含まれる場合、このプロセスには時間がかかることがあります。

14.3.2.1. NFS 共有ストアの設定

共有ストアの高可用性を使用する場合、ライブおよびバックアップブローカーの両方を、共有ファイルシステムの共通ディレクトリーを使用するように設定する必要があります。通常、Storage Area Network (SAN) またはネットワークファイルシステム (NFS) サーバーを使用します。

以下は、各ブローカーインスタンスの NFS サーバーからエクスポートされたディレクトリーをマウントする際に推奨される設定オプションです。

sync

すべての変更が即時にディスクにフラッシュされることを指定します。

intr

サーバーがダウンした場合やサーバーにアクセスできない場合に、NFS 要求の割り込みを許可します。

noac

属性キャッシュを無効にします。この動作は、複数のクライアント間で属性キャッシュの一貫性を実現するために必要です。

軽度

NFS サーバーが利用できない場合、サーバーがオンラインに戻るのを待つのではなく、エラーを報告する必要があることを指定します。

lookupcache=none

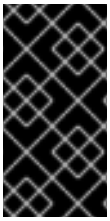
ルックアップキャッシングを無効にします。

timeo=n

NFS クライアント (ブローカー) が NFS サーバーからの応答を待機する時間 (デシ秒 (10 秒)) は、要求を再試行するまで NFS サーバーからの応答を待つ時間です。TCP 経由の NFS の場合、デフォルトの **timeo** 値は **600** (60 秒) です。UDP 経由の NFS では、クライアントは適応アルゴリズムを使用して、読み取り要求や書き込み要求など、頻繁に使用される要求のタイプに適切なタイムアウト値を予測します。

retrans=n

さらなるリカバリーアクションを試行する前に、NFS クライアントが要求を再試行する回数。**retrans** オプションが指定されていない場合、NFS クライアントは各リクエストを 3 回試行します。



重要

timeo オプションおよび **retrans** オプションを設定する場合、適切な値を使用することが重要です。デフォルト **timeo** の 600 デシ秒 (60 秒) と **retrans** 値の 5 を組み合わせると、ActiveMQ Artemis が NFS 接続の切断を検出するのを 5 分間待機する可能性があります。

関連情報

- NFS サーバーからエクスポートしたディレクトリーをマウントする方法は、Red Hat Enterprise Linux ドキュメントの Mounting an NFS share with mount を参照してください。
- AMQ Broker でサポートされるネットワークファイルシステムに関する詳細は、Red Hat AMQ 7 Supported Configurations を参照してください。

14.3.2.2. Configuring shared store high availability

この手順では、ブローカークラスターの共有ストアの高可用性を設定する方法を説明します。

前提条件

- 共有ストレージシステムは、ライブブローカーおよびバックアップブローカーからアクセスできる必要があります。
  - 通常、Storage Area Network (SAN) またはネットワークファイルシステム (NFS) サーバーを使用して共有ストアを提供します。サポートされるネットワークファイルシステムの詳細は、Red Hat AMQ 7 Supported Configurations を参照してください。
  - JDBC ベースの永続性を設定している場合は、指定したデータベースを使用して共有ストアを提供できます。JDBC 永続性の設定方法は、「データベースのメッセージデータの永続化」 を参照してください。

手順

1. クラスターのブローカーをライブバックアップグループにグループ化します。
ほとんどの場合、ライブバックアップグループは、ライブブローカーとバックアップブローカーという 2 つのブローカーで設定される必要があります。クラスターに 6 つのブローカーがある場合は、3 つのライブバックアップグループが必要になります。

2. 1 つのライブブローカーと 1 つのバックアップブローカーで設定される最初のライブバックアップグループを作成します。

   a. ライブブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。

   b. 以下を使用している場合:

      i. 共有ストアを提供するネットワークファイルシステム。ライブブローカーのページング、バインディング、ジャーナル、および大きなメッセージディレクトリーが、バックアップブローカーがアクセスできる共有場所をポイントすることを確認します。

```
<configuration>
   <core>
      ...
      <paging-directory>../sharedstore/data/paging</paging-directory>
      <bindings-directory>../sharedstore/data/bindings</bindings-directory>
      <journal-directory>../sharedstore/data/journal</journal-directory>
      <large-messages-directory>../sharedstore/data/large-messages</large-
messages-directory>
      ...
   </core>
</configuration>
```

      ii. 共有ストアを提供するデータベース。マスターとバックアップブローカーの両方が同じデータベースに接続でき、同じ設定を **broker.xml** 設定ファイルの **database-store** 要素に指定できるようにします。以下は設定例です。

```
<configuration>
  <core>
    <store>
      <database-store>
        <jdbc-connection-url>jdbc:oracle:data/oracle/database-store;create=true</jdbc-
connection-url>
        <jdbc-user>ENC(5493dd76567ee5ec269d11823973462f)</jdbc-user>
        <jdbc-password>ENC(56a0db3b71043054269d11823973462f)</jdbc-
password>
        <bindings-table-name>BINDINGS_TABLE</bindings-table-name>
        <message-table-name>MESSAGE_TABLE</message-table-name>
        <large-message-table-name>LARGE_MESSAGES_TABLE</large-message-
table-name>
        <page-store-table-name>PAGE_STORE_TABLE</page-store-table-name>
        <node-manager-store-table-name>NODE_MANAGER_TABLE<node-
manager-store-table-name>
        <jdbc-driver-class-name>oracle.jdbc.driver.OracleDriver</jdbc-driver-class-
name>
        <jdbc-network-timeout>10000</jdbc-network-timeout>
        <jdbc-lock-renew-period>2000</jdbc-lock-renew-period>
        <jdbc-lock-expiration>15000</jdbc-lock-expiration>
        <jdbc-journal-sync-period>5</jdbc-journal-sync-period>
```

```
        </database-store>
      </store>
    </core>
  </configuration>
```

c. HA ポリシーの共有ストアを使用するようにライブブローカーを設定します。

```
<configuration>
  <core>
    ...
    <ha-policy>
      <shared-store>
        <master>
          <failover-on-shutdown>true</failover-on-shutdown>
        </master>
      </shared-store>
    </ha-policy>
    ...
  </core>
</configuration>
```

failover-on-shutdown

このブローカーが正常に停止された場合、このプロパティーはバックアップブローカーが稼働して引き継ぐかどうかを制御します。

d. バックアップブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。

e. 以下を使用している場合:

i. 共有ストアを提供するネットワークファイルシステム。バックアップブローカーのページング、バインディング、ジャーナル、および大きなメッセージディレクトリーがライブブローカーと同じ共有場所をポイントすることを確認します。

```
<configuration>
  <core>
    ...
    <paging-directory>../sharedstore/data/paging</paging-directory>
    <bindings-directory>../sharedstore/data/bindings</bindings-directory>
    <journal-directory>../sharedstore/data/journal</journal-directory>
    <large-messages-directory>../sharedstore/data/large-messages</large-
messages-directory>
    ...
  </core>
</configuration>
```

ii. 共有ストアを提供するデータベース。マスターとバックアップブローカーの両方が同じデータベースに接続でき、**broker.xml** 設定ファイルの **database-store** 要素に同じ設定が指定されるようにします。

f. HA ポリシーの共有ストアを使用するようにバックアップブローカーを設定します。

```
<configuration>
  <core>
    ...
```

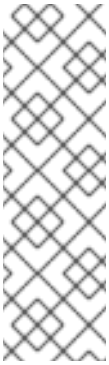
```
        <ha-policy>
           <shared-store>
              <slave>
                 <failover-on-shutdown>true</failover-on-shutdown>
                 <allow-failback>true</allow-failback>
                 <restart-backup>true</restart-backup>
              </slave>
           </shared-store>
        </ha-policy>
        ...
     </core>
  </configuration>
```

failover-on-shutdown

このブローカーが稼働状態になり、通常は停止された場合、このプロパティーはバックアップブローカー (元のライブブローカー) が有効になり、引き継ぐかどうかを制御します。

allow-failback

フェイルオーバーが発生し、バックアップブローカがライブブローカを引き継いだ場合、このプロパティーは、バックアップブローカが再起動してクラスターに再接続したときに、元のライブブローカにフェイルバックするかどうかを制御します。



注記

フェイルバックは、ライブバックアップのペア (単一のバックアップブローカーとペアの 1 つのライブブローカー) を対象としています。ライブブローカーが複数のバックアップで設定されている場合、フェイルバックは発生しません。代わりに、フェイルオーバーイベントが発生すると、バックアップブローカーはライブになり、次のバックアップがバックアップになります。元のライブブローカーがオンラインに戻ると、現在のブローカーにバックアップがすでにあるため、フェイルバックを開始できなくなります。

restart-backup

このプロパティーは、ライブブローカーにフェイルバックした後にバックアップブローカーを自動的に再起動するかどうかを制御します。このプロパティーのデフォルト値は **true** です。

3. クラスター内の残りのライブバックアップグループごとに、ステップ 2 を繰り返します。

14.3.3. Configuring replication high availability

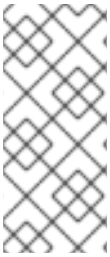
レプリケーション高可用性 (HA) ポリシーを使用して HA をブローカークラスターに実装できます。レプリケーションでは、永続データはライブブローカーとバックアップブローカー間で同期されます。ライブブローカーが障害に遭遇すると、メッセージデータはバックアップブローカーに同期され、失敗したライブブローカーに対して引き継ぎされます。

共有ファイルシステムがない場合は、共有ストアの代わりにレプリケーションを使用する必要があります。ただし、レプリケーションにより、ライブブローカーとそのバックアップが同時に存続するネットワークの分離が発生する可能性があります。

レプリケーションでは、ネットワークの分離のリスクを低くするために (ただし、除外しない)、**少なくとも 3 つのライブバックアップペア** が必要です。3 つ以上のライブバックアップブローカーのペアを

使用すると、クラスターは **クォーラムの投票** を使用して 2 つのライブブローカーを持つことができます。

以下のセクションでは、クォーラムの投票の仕組みと、少なくとも 3 つのライブバックアップのペアを使用してブローカークラスターにレプリケーション HA を設定する方法を説明します。



注記

ライブおよびバックアップブローカーは、ネットワーク経由でメッセージングデータを同期する必要があるため、レプリケーションによりパフォーマンスのオーバーヘッドが追加されます。この同期プロセスでは、ジャーナル操作がブロックされますが、クライアントはブロックされません。データの同期のためにジャーナル操作がブロックできる最大時間を設定できます。

14.3.3.1. クォーラムの投票

ライブブローカーとそのバックアップでレプリケーション接続が中断された場合、**クォーラム投票** と呼ばれるプロセスを設定して、ネットワーク分離 (スプリットブレイン) の問題を軽減することができます。ネットワーク分離中、ライブブローカーとそのバックアップを同時にアクティブにすることができます。

以下の表は、AMQ Broker が使用する 2 種類のクォーラム投票を示しています。

投票タイプ	説明	イニシエーター	必要な設定	参加者	投票の結果に基づくアクション
バックアップ投票	バックアップブローカーがライブブローカーへのレプリケーション接続を失うと、バックアップブローカーはこの投票の結果に基づいて開始するかどうかを決定します。	バックアップブローカー	なし。バックアップブローカーがレプリケーションパートナーへの接続を失った際に、バックアップ評価が自動的に行われます。 ただし、これらのパラメーターにカスタムの値を指定すると、バックアップ評価のプロパティーを制御できます。 ● **quorum-vote-wait** ● **vote-retries** ● **vote-retry-wait**	クラスターの他のライブブローカー	バックアップブローカーは、クラスター内の他のライブブローカーから過半数 (**クォーラム**) 票を受信すると開始します。これは、レプリケーションパートナーが利用可能でなくなったことを示しています。

投票タイプ	説明	イニシエーター	必要な設定	参加者	投票の結果に基づくアクション
ライブ評価	ライブブローカーがレプリケーションパートナーへの接続を失った場合、ライブブローカーはこの投票に基づいて実行を継続するかどうかを決定します。	ライブブローカー	ライブ評価は、ライブブローカーがレプリケーションパートナーへの接続を失い、**vote-on-replication-failure** が **true** に設定されている場合に発生します。アクティブになったバックアップブローカーはライブブローカーと見なされ、ライブ評価を開始できます。	クラスターの他のライブブローカー	ライブブローカーは、クラスターの他のライブブローカーから過半数を受け取ら **ない** 場合はシャットダウンします。これは、クラスター接続がまだアクティブであることを示します。

重要

以下は、ブローカークラスターの設定がクォーラム投票の動作にどのように影響するかについて留意すべき重要な事項になります。

- クォーラム評価を成功させるには、クラスターのサイズで、過半数の結果が得られる必要があります。そのため、レプリケーション HA ポリシーを使用する場合、クラスターには**少なくとも 3 つの**ライブバックアップブローカーのペアが必要です。
- クラスターに追加するその他のライブバックアップブローカーのペア。クラスターのフォールトトレランス全体を増やすことができます。たとえば、ライブ / バックアップのペアが 3 つあるとします。完全なライブバックアップペアがなくなると、残りの 2 つのライブ / バックアップペアが、後続のクォーラムの投票で最大数に達することができません。この状況では、クラスターでさらにレプリケーションが中断されると、ライブブローカーがシャットダウンし、バックアップブローカーが起動しない可能性があります。例えば 5 組のブローカペアでクラスターを設定することで、クラスターでは少なくとも 2 つの障害が発生することができますが、それでもクォーラム投票で過半数の結果を得ることができます。
- クラスター内のライブバックアップブローカーのペアの数を意図的に **減らす** と、過半数に以前に設定されたしきい値は自動的に減らされません。この間、失われたレプリケーション接続によってトリガーされるクォーラム評価は成功せず、クラスターがネットワーク分離に対してより脆弱になります。クラスターがクォーラム票の過半数を再計算するには、まずクラスターから削除するライブバックアップのペアをシャットダウンします。次に、クラスター内の残りのライブバックアップペアを再起動します。残りのブローカーがすべて再起動すると、クラスターはクォーラム評価しきい値を再計算します。

14.3.3.2. レプリケーションの高可用性のためのブローカークラスターの設定

以下の手順では、6 つのブローカークラスターにレプリケーションの高可用性 (HA) を設定する方法を説明します。このトポロジーでは、6 つのブローカーはライブバックアップのペアにグループ化されます。3 つのライブブローカーは、専用のバックアップブローカーとペアになります。

レプリケーションでは、ネットワークの分離のリスクを低くするために (ただし、除外しない)、少なくとも 3 つのライブバックアップペアが必要です。

前提条件

- 6 つ以上のブローカーを持つブローカークラスターが必要です。
  6 つのブローカーは 3 つのライブバックアップペアに設定されます。ブローカーのクラスターへの追加に関する詳細は、14章 *ブローカークラスターの設定* を参照してください。

手順

1. クラスターのブローカーをライブバックアップグループにグループ化します。
   ほとんどの場合、ライブバックアップグループは、ライブブローカーとバックアップブローカーという 2 つのブローカーで設定される必要があります。クラスターに 6 つのブローカーがある場合は、3 つのライブバックアップグループが必要です。

2. 1 つのライブブローカーと 1 つのバックアップブローカーで設定される最初のライブバックアップグループを作成します。

   a. ライブブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。

   b. HA ポリシーのレプリケーションを使用するようにライブブローカーを設定します。

```
<configuration>
  <core>
    ...
    <ha-policy>
      <replication>
        <master>
          <check-for-live-server>true</check-for-live-server>
          <group-name>my-group-1</group-name>
          <vote-on-replication-failure>true</vote-on-replication-failure>
          ...
        </master>
      </replication>
    </ha-policy>
    ...
  </core>
</configuration>
```

check-for-live-server

ライブブローカーが失敗すると、このプロパティーは、再起動時にクライアントがフェイルバックするかどうかを制御します。
このプロパティーを **true** に設定すると、以前のフェイルオーバー後にライブブローカーが再起動すると、同じノード ID を持つクラスター内の別のブローカーを検索します。ライブブローカーが同じノード ID を持つ別のブローカーを見つけると、ライブブローカーの失敗時にバックアップブローカーが正常に起動することを示しています。この場合、ライブブローカーはデータをバックアップブローカーと同期します。その後、ライブブローカーはバックアップブローカーにシャットダウンするよう要求します。以下に示すように、バックアップブローカーがフェイルバック用に設定されている場合、シャットダウンします。その後、ライブブローカーはアクティブなロールを再開します。そして、クライアントはこれに再接続します。

警告

ライブブローカーで **check-for-live-server** を **true** に設定しない場合、以前のフェイルオーバー後にライブブローカーを再起動すると、重複したメッセージング処理が発生する可能性があります。具体的には、このプロパティーを **false** に設定してライブブローカーを再起動すると、ライブブローカーはバックアップブローカーとデータを同期しません。この場合、ライブブローカーはバックアップブローカーがすでに処理された同じメッセージを処理し、重複が発生する可能性があります。

group-name

この live-backup グループの名前。ライブバックアップグループを形成するには、ライブおよびバックアップブローカーを同じグループ名で設定する必要があります。

vote-on-replication-failure

このプロパティーは、レプリケーション接続が中断された場合に、ライブブローカーが**ライブ評価** と呼ばれるクォーラム評価を開始するかどうかを制御します。
ライブ評価は、ライブブローカーで、それまたはパートナーが中断されたレプリケーション接続の原因であるかどうかを判断する方法です。評価の結果に基づいて、ライブブローカーは稼働またはシャットダウンします。

重要

クォーラム評価を成功させるには、クラスターのサイズで、過半数の結果が得られる必要があります。そのため、レプリケーション HA ポリシーを使用する場合、クラスターには**少なくとも 3 つの**ライブバックアップブローカーのペアが必要です。

クラスターに設定するブローカーのペアが多いほど、クラスターの全体的なフォールトトレランスが向上します。たとえば、3 つのライブバックアップブローカーのペアがあるとします。完全なライブバックアップペアへの接続を失った場合、残りの 2 つのライブ / バックアップペアが、クォーラムの投票で過半数に達しなくなります。この状況では、後続のレプリケーションが中断されると、ライブブローカーがシャットダウンし、バックアップブローカーが起動しない可能性があります。例えば 5 組のブローカペアでクラスターを設定することで、クラスターでは少なくとも 2 つの障害が発生することができますが、それでもクォーラム投票で過半数の結果を得ることができます。

c. ライブブローカーの追加の HA プロパティーを設定します。
これらの追加の HA プロパティーには、最も一般的なユースケースに適したデフォルト値があります。そのため、デフォルト動作が必要ない場合のみこのプロパティーを設定する必要があります。詳細は、付録F *レプリケーション高可用性設定要素* を参照してください。

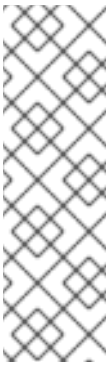
d. バックアップブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。

e. HA ポリシーのレプリケーションを使用するようにバックアップ (スレーブ) ブローカーを設定します。

```
<configuration>
  <core>
    ...
    <ha-policy>
      <replication>
        <slave>
          <allow-failback>true</allow-failback>
          <restart-backup>true</restart-backup>
          <group-name>my-group-1</group-name>
          <vote-on-replication-failure>true</vote-on-replication-failure>
          ...
        </slave>
      </replication>
    </ha-policy>
    ...
  </core>
</configuration>
```

allow-failback

フェイルオーバーが発生し、バックアップブローカがライブブローカを引き継いだ場合、このプロパティーは、バックアップブローカが再起動してクラスターに再接続したときに、元のライブブローカにフェイルバックするかどうかを制御します。



注記

フェイルバックは、ライブバックアップのペア (単一のバックアップブローカーとペアの 1 つのライブブローカー) を対象としています。ライブブローカーが複数のバックアップで設定されている場合、フェイルバックは発生しません。代わりに、フェイルオーバーイベントが発生すると、バックアップブローカーはライブになり、次のバックアップがバックアップになります。元のライブブローカーがオンラインに戻ると、現在のブローカーにバックアップがすでにあるため、フェイルバックを開始できなくなります。

restart-backup

このプロパティーは、ライブブローカーにフェイルバックした後にバックアップブローカーを自動的に再起動するかどうかを制御します。このプロパティーのデフォルト値は **true** です。

group-name

このバックアップが接続するライブブローカーのグループ名。バックアップブローカーは、同じグループ名を共有するライブブローカーにのみ接続します。

vote-on-replication-failure

このプロパティーは、レプリケーション接続が中断された場合に、ライブブローカーが **ライブ評価** と呼ばれるクォーラム評価を開始するかどうかを制御します。アクティブになったバックアップブローカーはライブブローカーと見なされ、ライブ評価を開始できます。
ライブ評価は、ライブブローカーで、それまたはパートナーが中断されたレプリケーション接続の原因であるかどうかを判断する方法です。評価の結果に基づいて、ライブブローカーは稼働またはシャットダウンします。

f. (任意設定) バックアップブローカーが開始するクォーラム票のプロパティーを設定します。

```
<configuration>
  <core>
    ...
    <ha-policy>
      <replication>
        <slave>
        ...
          <vote-retries>12</vote-retries>
          <vote-retry-wait>5000</vote-retry-wait>
        ...
        </slave>
      </replication>
    </ha-policy>
    ...
  </core>
</configuration>
```

vote-retries

このプロパティーは、バックアップブローカーの起動を可能にする大部分の結果を受信するために、バックアップブローカーがクォーラム評価を再試行する回数を制御します。

vote-retry-wait

このプロパティーは、バックアップブローカーがクォーラム評価の再試行ごとに待機する期間 (ミリ秒単位) を制御します。

g. バックアップブローカーの追加の HA プロパティーを設定します。
これらの追加の HA プロパティーには、最も一般的なユースケースに適したデフォルト値があります。そのため、デフォルト動作が必要ない場合のみこのプロパティーを設定する必要があります。詳細は、付録F *レプリケーション高可用性設定要素* を参照してください。

3. クラスター内の追加のライブバックアップグループごとに、手順 2 を繰り返します。
クラスターに 6 つのブローカーがある場合は、この手順を 2 回ずつ繰り返し、残りのライブバックアップグループごとに 1 回ずつ繰り返します。

関連情報

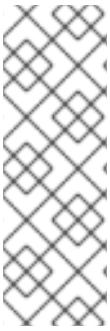
- HA のレプリケーションを使用するブローカークラスターの例については、HA サンプルプログラム を参照してください。
- ノード ID の詳細は、Understanding node IDs を参照してください。

14.3.4. Configuring limited high availability with live-only

ライブのみの HA ポリシーを使用すると、メッセージを失わずにクラスターのブローカーをシャットダウンすることができます。ライブのみでは、ライブブローカーが正常に停止されると、メッセージとトランザクションの状態を別のライブブローカーにコピーし、シャットダウンします。その後、クライアントは他のブローカーに再接続し、メッセージの送受信を続行します。

ライブのみの HA ポリシーは、ブローカーが正常に停止された場合にのみケースを処理します。予期しないブローカーの失敗を処理しません。

ライブのみの HA はメッセージの損失を防ぎますが、メッセージの順序は保持されない可能性があります。ライブのみの HA で設定されたブローカーが停止すると、そのメッセージは別のブローカーのキューの最後に追加されます。



注記

ブローカーがスケールダウンする準備時に、接続が切断される前に、新しいブローカーがメッセージを処理する準備ができていることを通知する前に、メッセージをクライアントに送信します。ただし、クライアントは、初期ブローカーがスケールダウンされた後にのみ新しいブローカーに再接続する必要があります。これにより、キューやトランザクションなどの状態が、クライアントが再接続する際に他のブローカーで利用可能になります。通常の再接続設定はクライアントが再接続する際に適用されるため、スケールダウンに必要な時間を処理するのに十分な時間を設定する必要があります。

この手順では、クラスター内の各ブローカーをスケールダウンするように設定する方法を説明します。この手順を完了すると、ブローカーが正常に停止されるたびに、メッセージとトランザクションの状態がクラスター内の別のブローカーにコピーされます。

手順

1. 最初のブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。
2. ライブのみの HA ポリシーを使用するようにブローカーを設定します。

```
<configuration>
   <core>
      ...
      <ha-policy>
         <live-only>
         </live-only>
      </ha-policy>
      ...
   </core>
</configuration>
```

3. ブローカークラスターをスケールダウンする方法を設定します。
このブローカーがスケールダウンするブローカーのブローカーまたはグループを指定します。

スケールダウン	以下を行います

クラスター内の特定のブローカー	スケールダウンするブローカーのコネクターを指定します。
	`<live-only>`
	`  <scale-down>`
	`  <connectors>`
	`  <connector-ref>broker1-connector</connector-ref>`
	`  </connectors>`
	`  </scale-down>`
	`</live-only>`

スケールダウン	以下を行います

クラスター内のすべてのブローカー	ブローカークラスターの検出グループを指定します。
	
	`<live-only>`
	`  <scale-down>`
	`  <discovery-group-ref discovery-group-name="my-discovery-group"/>`
	`  </scale-down>`
	`</live-only>`

特定のブローカーグループのブローカー	ブローカーグループを指定します。
	
	`<live-only>`
	`  <scale-down>`
	`  <group-name>my-group-name</group-name>`
	`  </scale-down>`
	`</live-only>`

4. クラスター内の残りのブローカーごとに、この手順を繰り返します。

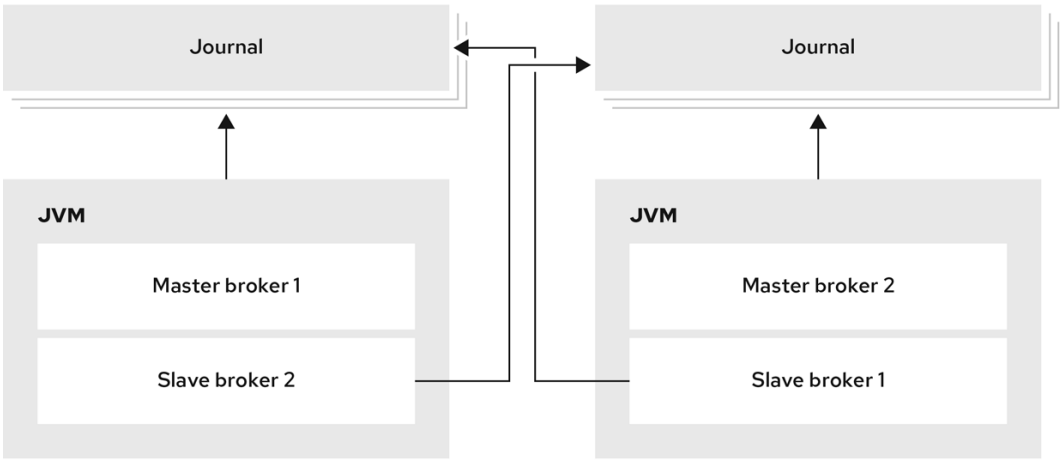
関連情報

- クラスターをスケールダウンするためにライブのみを使用するブローカークラスターの例については、scale-down example programs を参照してください。

14.3.5. Configuring high availability with colocated backups

ライブバックアップグループを設定するのではなく、バックアップブローカーを別のライブブローカーと同じ JVM にコロケートできます。この設定では、各ライブブローカーは別のライブブローカーを要求し、その JVM でバックアップブローカーを作成し、開始します。

図14.4 コロケートされたライブブローカーおよびバックアップブローカー



コロケーションは、共有ストアまたはレプリケーションのいずれかを高可用性 (HA) ポリシーとして使用できます。新しいバックアップブローカーは、これを作成するライブブローカーからその設定を継承します。バックアップの名前は、**colocated_backup_n** に設定されます。**n** は、ライブブローカーが作成したバックアップの数です。

さらに、バックアップブローカーは、コネクターと、これを作成するライブブローカーからアクセプターの設定を継承します。デフォルトでは、ポートオフセット 100 がそれぞれに適用されます。たとえば、ライブブローカーにポート 61616 のアクセプターがある場合、作成される最初のバックアップブローカーはポート 61716 を使用し、2 番目のバックアップは 61816 を使用します。

ジャーナル、大きなメッセージ、ページングのディレクトリーは、選択した HA ポリシーに従って設定されます。共有ストアを選択する場合、要求ブローカーはターゲットブローカーに対し、使用するディレクトリーについて通知します。レプリケーションが選択されている場合、ディレクトリーは作成ブローカーから継承され、新しいバックアップの名前が追加されます。

この手順では、共有のストア HA を使用するようにクラスター内の各ブローカーを設定し、バックアップを作成してクラスター内の別のブローカーと共存させるよう要求します。

手順

1. 最初のブローカーの **<broker_instance_dir> /etc/broker.xml** 設定ファイルを開きます。
2. HA ポリシーとコロケーションを使用するようにブローカーを設定します。
   この例では、ブローカーは共有ストア HA およびコロケーションで設定されます。

```
<configuration>
  <core>
    ...
    <ha-policy>
      <shared-store>
        <colocated>
          <request-backup>true</request-backup>
          <max-backups>1</max-backups>
          <backup-request-retries>-1</backup-request-retries>
          <backup-request-retry-interval>5000</backup-request-retry-interval/>
          <backup-port-offset>150</backup-port-offset>
          <excludes>
            <connector-ref>remote-connector</connector-ref>
          </excludes>
          <master>
            <failover-on-shutdown>true</failover-on-shutdown>
          </master>
          <slave>
            <failover-on-shutdown>true</failover-on-shutdown>
            <allow-failback>true</allow-failback>
            <restart-backup>true</restart-backup>
          </slave>
        </colocated>
      </shared-store>
    </ha-policy>
    ...
  </core>
</configuration>
```

request-backup

このプロパティーを **true** に設定すると、このブローカーはクラスター内の別のライブブローカーによって作成されるバックアップブローカーを要求します。

max-backups

このブローカーが作成できるバックアップブローカーの数。このプロパティーを **0** に設定すると、このブローカーはクラスターの他のブローカーからのバックアップ要求を受け入れません。

backup-request-retries

このブローカーがバックアップブローカーの作成を要求する回数。デフォルトは、無制限を意味する **-1** です。

backup-request-retry-interval

バックアップブローカーを作成する要求を再試行する前にブローカーが待機する時間 (ミリ秒単位)。デフォルトは **5000** (5 秒) です。

backup-port-offset

新しいバックアップブローカーにアクセプターおよびコネクターに使用するポートオフセット。このブローカーがクラスター内の別のブローカーのバックアップを作成する要求を受信すると、この量によってポートオフセットでバックアップブローカーが作成されます。デフォルトは **100** です。

excludes (オプション)

バックアップポートのオフセットからコネクターを除外します。バックアップポートのオフセットから除外する必要のある外部ブローカーのコネクターを設定している場合は、コネクターごとに **<connector-ref>** を追加します。

master

このブローカーの共有ストアまたはレプリケーションフェイルオーバーの設定。

slave

このブローカーのバックアップの共有ストアまたはレプリケーションのフェイルオーバー設定。

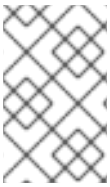
3. クラスター内の残りのブローカーごとに、この手順を繰り返します。

関連情報

- コロケートバックアップを使用するブローカークラスターの例については、HA example programs を参照してください。

14.3.6. フェイルオーバーするクライアントの設定

ブローカークラスターで高可用性を設定したら、クライアントがフェイルオーバーするように設定します。クライアントのフェイルオーバーにより、ブローカーが失敗すると、接続したクライアントは最小限のダウンタイムでクラスター内の別のブローカーに再接続できます。



注記

一時的なネットワークの問題が発生すると、AMQ Broker は同じブローカーへの接続を自動的に再割り当てします。これは、クライアントが同じブローカーに再接続する以外は failover と似ています。

2 種類のクライアントフェイルオーバーを設定できます。

自動クライアントフェイルオーバー

クライアントは、初回接続時にブローカークラスターに関する情報を受け取ります。接続先のブ

ローカーが失敗すると、クライアントはブローカーのバックアップに自動的に再接続し、バックアップブローカーはフェイルオーバーの前に各接続に存在するセッションおよびコンシューマーを再作成します。

アプリケーションレベルのクライアントフェイルオーバー

自動クライアントのフェイルオーバーの代わりに、障害ハンドラーで独自のカスタム再接続ロジックを使用してクライアントアプリケーションをコーディングすることもできます。

手順

- AMQ Core Protocol JMS を使用して、自動またはアプリケーションレベルのフェイルオーバーでクライアントアプリケーションを設定します。
  詳細は、Using the AMQ Core Protocol JMS Client を参照してください。

14.4. メッセージ再分配の有効化

ブローカークラスターに **message-load-balancing** が **ON_DEMAND** または **OFF_WITH_REDISTRIBUTION** に設定されている場合、コンシューマーにメッセージを消費するコンシューマーがないキューでメッセージが stuck にならないように **メッセージ再分配** を設定できます。

本セクションでは、以下の情報を提供します。

- メッセージディストリビューションについて
- メッセージ再分配の設定

14.4.1. メッセージ再分配について

ブローカークラスターは負荷分散を使用して、メッセージの負荷をクラスター全体に分散します。クラスター接続で負荷分散を設定する場合は、以下の **message-load-balancing** 設定を使用して再分配を有効にできます。

- **ON_DEMAND** - 負荷分散を有効にし、再分配を許可します。
- **OFF_WITH_REDISTRIBUTION** - 負荷分散を無効にしますが、再分配を許可します。

いずれの場合も、ブローカーは一致するコンシューマーを持つ他のブローカーにのみメッセージを転送します。この動作により、メッセージがメッセージを消費するコンシューマーを持たないキューに移動されないようにします。ただし、メッセージがブローカーに転送された後にキューにアタッチされたコンシューマーがブローカーに転送されると、これらのメッセージはキュー内でストックになり、消費されません。この問題は、**不足**と呼ばれることもあります。

メッセージ再分配は、一致するコンシューマーを持つクラスター内のコンシューマーのないキューからメッセージを自動的に再分配することで、不足を防ぎます。

OFF_WITH_REDISTRIBUTION を使用すると、ブローカーは、アクティブなローカルコンシューマーがない場合に、一致するコンシューマーを持つ他のブローカーにのみメッセージを転送するため、コンシューマーが利用できない場合にブローカーの優先順位付けを実行できます。

メッセージ再分配は、フィルター (**セレクター** とも呼ばれる) の使用をサポートします。つまり、利用可能なローカルコンシューマーのセレクターと一致しない場合、メッセージは再分配されます。

関連情報

- クラスターの負荷分散に関する詳細は、「ブローカークラスターがメッセージ負荷のバランスを取る方法」 を参照してください。

14.4.2. メッセージ再分配の設定

この手順では、負荷分散を使用してメッセージ再分配を設定する方法を説明します。負荷分散なしでメッセージ再分配を行う場合は、**<message-load-balancing>** を **OFF_WITH_REDISTRIBUTION** に設定します。

手順

1. **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。
2. **<cluster-connection>** 要素で、**<message-load-balancing>** が **ON_DEMAND** に設定されていることを確認します。

```
<configuration>
  <core>
    ...
    <cluster-connections>
      <cluster-connection name="my-cluster">
        ...
        <message-load-balancing>ON_DEMAND</message-load-balancing>
        ...
      </cluster-connection>
    </cluster-connections>
  </core>
</configuration>
```

3. **<address-settings>** 要素内で、キューまたはキューのセットの再分配遅延を設定します。この例では、**my.queue** へのメッセージの負荷分散は、最後のコンシューマーが閉じられてから 5000 ミリ秒に再分散されます。

```
<configuration>
  <core>
    ...
    <address-settings>
      <address-setting match="my.queue">
        <redistribution-delay>5000</redistribution-delay>
      </address-setting>
    </address-settings>
    ...
  </core>
</configuration>
```

address-setting

match 属性を、メッセージを再分配するキューの名前に設定します。ブローカーのワイルドカード構文を使用してキューの範囲を指定できます。詳細は、「アドレスセットへのアドレス設定の適用」 を参照してください。

redistribution-delay

このキューの最後のコンシューマーが閉じられてからクラスターの他のブローカーにメッセージを再分配するまでブローカーが待機する時間 (ミリ秒単位)。これを **0** に設定すると、メッセージは即座に再分配されます。ただし、通常は、再分配する前に遅延を設定する必要があります。コンシューマーを閉じるのは一般的ですが、同じキューに別のキューを迅速に作成する必要があります。

4. クラスター内の追加のブローカーごとにこの手順を繰り返します。

関連情報

- メッセージを再分散するブローカークラスター設定の例は、**queue-message-redistribution** AMQ Broker のサンプルプログラム を参照してください。

14.5. クラスター化されたメッセージのグループ化の設定

メッセージのグループ化により、クライアントは特定のタイプのメッセージのグループを、同じコンシューマーによって順次処理できます。クラスターの各ブローカーにグルーピングハンドラーを追加すると、クライアントはグループ化されたメッセージをクラスター内のブローカーに送信し、それらのメッセージを同じコンシューマーによって正しい順序で消費できるようにします。

注記

クラスターリングは並列処理を提供し、水平方向にスケーリングできます。一方、グループ化方法は、特定のコンシューマーにグループ化されたメッセージを直接送信します。

Red Hat では、クラスターリングまたはグループ化の **いずれか** を使用し、クラスターリングとグループ化の使用を避けることを推奨します。

グルーピングハンドラーには、**ローカルハンドラー**と**リモートハンドラー**の 2 つのタイプがあります。ブローカークラスターは、特定のグループのすべてのメッセージを適切なキューにルーティングし、目的のコンシューマーが正しい順序でそれらを使用できるようにします。

前提条件

- クラスターの各ブローカーに少なくとも 1 つのコンシューマーが必要です。
  メッセージがキュー上のコンシューマーに固定されると、同じグループ ID を持つすべてのメッセージがそのキューにルーティングされます。コンシューマーが削除されると、キューはコンシューマーがない場合でもメッセージを受信し続けます。

手順

1. クラスター内の 1 つのブローカーにローカルハンドラーを設定します。
   高可用性を使用している場合、これはマスターブローカーである必要があります。

   a. ブローカーの **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

   b. **<core>** 要素内にローカルハンドラーを追加します。
      ローカルハンドラーはリモートハンドラーの Arbiter として機能します。ルート情報を保存し、これを他のブローカーと通信します。

```
<configuration>
  <core>
    ...
    <grouping-handler name="my-grouping-handler">
      <type>LOCAL</type>
      <timeout>10000</timeout>
    </grouping-handler>
    ...
  </core>
</configuration>
```

grouping-handler

name 属性を使用してグルーピングハンドラーに一意の名前を指定します。

type

これを **LOCAL** に設定します。

timeout

メッセージをルーティングする場所について決定する待機時間 (ミリ秒単位)。デフォルトは 5000 ミリ秒です。ルーティングを決定する前にタイムアウトに達すると、例外が発生します。これにより、厳格なメッセージの順序が確保されます。
ブローカーがグループ ID を持つメッセージを受信すると、コンシューマーが割り当てられるキューへのルートを提案します。ルートがクラスターの他のブローカーのグルーピングハンドラーによって許可される場合、ルートが確立されます。クラスター内のすべてのブローカーは、このグループ ID を持つメッセージをそのキューに転送します。
ブローカーのルートプロポーザルが拒否されると、別のルートを提案し、ルートが受け入れられるまでプロセスを繰り返します。

2. 高可用性を使用している場合、ローカルハンドラー設定をマスターブローカーのスレーブブローカーにコピーします。
ローカルハンドラー設定をスレーブブローカーにコピーしても、ローカルハンドラーに対する単一障害点を防ぐことができます。

3. クラスターの残りの各ブローカーで、リモートハンドラーを設定します。

   a. ブローカーの **<broker_instance_dir>/etc/broker.xml** 設定ファイルを開きます。

   b. **<core>** 要素内にリモートハンドラーを追加します。

```
<configuration>
  <core>
    ...
    <grouping-handler name="my-grouping-handler">
      <type>REMOTE</type>
      <timeout>5000</timeout>
    </grouping-handler>
    ...
  </core>
</configuration>
```

grouping-handler

name 属性を使用してグルーピングハンドラーに一意の名前を指定します。

type

これは **REMOTE** に設定します。

timeout

メッセージをルーティングする場所について決定する待機時間 (ミリ秒単位)。デフォルトは 5000 ミリ秒です。この値をローカルハンドラーの半分以上に設定します。

関連情報

- メッセージのグループ化に設定されたブローカークラスターの例は、 **clustered-grouping** AMQ Broker example program を参照してください。

14.6. クライアントのブローカークラスターへの接続

AMQ JMS クライアントを使用してクラスターに接続できます。JMS を使用すると、メッセージングクライアントを設定して、ブローカーのリストを動的または静的に検出できます。クライアント側の負荷分散を設定して、クラスター全体で接続から作成されたクライアントセッションを分散することもできます。

手順

- AMQ Core Protocol JMS を使用して、ブローカークラスターに接続するクライアントアプリケーションを設定します。
  詳細は、Using the AMQ Core Protocol JMS Client を参照してください。

第15章 CEPH を使用したマルチサイトの耐障害性のあるメッセージングシステムの設定

大規模なエンタープライズメッセージングシステムには、通常、地理的に分散したデータセンターに個別のブローカークラスターがあります。データセンターが停止した場合に、システム管理者は既存のメッセージングデータを保持し、クライアントアプリケーションがメッセージを生成および消費できるようにする必要がある場合があります。特定のブローカートポロジーおよび Red Hat Ceph Storage (ソフトウェア定義ストレージプラットフォーム) を使用して、データセンターの停止時にメッセージングシステムの継続性を確保できます。このタイプのソリューションは、**マルチサイトのフォールトトレランスアーキテクチャー**と呼ばれます。

注記

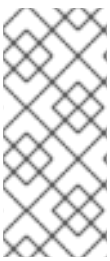
AMQP プロトコルサポートのみが必要な場合は、*16章 ブローカー接続を使用したマルチサイトのフォールトトレランスメッセージングシステムの設定* を検討してください。

以下のセクションでは、Red Hat Ceph Storage を使用して、メッセージングシステムをデータセンターの停止から保護する方法を説明します。

- Red Hat Ceph Storage クラスターの仕組み
- Red Hat Ceph Storage クラスターのインストールおよび設定
- データセンターが停止した場合に、ライブブローカーからバックアップブローカーを引き継ぐためのバックアップブローカーの追加
- Ceph クライアントロールを使用したブローカーサーバーの設定
- 共有ストア高可用性 (HA) ポリシーを使用するように各ブローカーを設定し、各ブローカーでメッセージングデータを保存する場所を指定する
- データセンターが停止した場合に新しいブローカーに接続するためのクライアントアプリケーションの設定
- 停止後のデータセンターの再起動

注記

マルチサイトのフォールトトレランスは、データセンター**内**の高可用性 (HA) ブローカーの冗長性の代わりではありません。ライブバックアップグループに基づくブローカーの冗長性は、単一クラスター内の単一ブローカー障害に対する自動保護を提供します。これとは対照的に、マルチサイトのフォールトトレランスは、大規模なデータセンターの停止から保護します。



注記

Red Hat Ceph Storage を使用してメッセージングシステムの継続を確保するには、共有ストアの高可用性 (HA) ポリシーを使用するようにブローカーを設定する必要があります。レプリケーション HA ポリシーを使用するようにブローカーを設定することはできません。これらのポリシーについての詳細は、Implementing High Availability を参照してください。

15.1. RED HAT CEPH STORAGE クラスターの仕組み

Red Hat Ceph Storage は、クラスター化されたオブジェクトストレージシステムです。Red Hat Ceph Storage は、オブジェクトおよびポリシーベースのレプリケーションのデータシャーディングを使用して、データの整合性とシステムの可用性を保証します。

Red Hat Ceph Storage は CRUSH (Controlled Replication Under Scalable Hashing) と呼ばれるアルゴリズムを使用して、データストレージの場所を自動的に計算してデータを保存および取得する方法を決定します。**CRUSH マップ** と呼ばれる Ceph アイテムを設定します。これは、クラスターのトポロジーの詳細と、ストレージクラスター全体でデータの複製方法を指定します。

CRUSH マップには、オブジェクトストレージデバイス (OSD) の一覧、デバイスを障害ドメイン階層に集約するためのバケットの一覧、および CRUSH に Ceph クラスターのプールでデータを複製する方法を指示するルールが含まれます。

インストールの基礎となる物理組織を反映することで、CRUSH マップはモデル化し、物理近接性、共有電源ソース、共有ネットワークなどの関連するデバイス障害の潜在的なソースとなります。この情報をクラスターマップにエンコードすることで、CRUSH は異なる障害ドメイン (データセンターなど) 間でオブジェクトレプリカを分離しつつ、ストレージクラスター全体でデータの擬似分散を維持できます。これは、データ損失を回避し、クラスターが動作が低下した状態で動作できるようにします。

Red Hat Ceph Storage クラスターでは、動作に多数のノード (物理または仮想) が必要です。クラスターには以下のタイプのノードが含まれている必要があります。

ノードの監視

各モニターノード (MON) は、クラスターマップのマスターコピーを維持する monitor デーモン (**ceph-mon**) を実行します。クラスターマップにはクラスタートポロジーが含まれます。Ceph クラスターに接続するクライアントは、モニターからクラスターマップの現在のコピーを取得します。これにより、クライアントがクラスターへのデータの読み取りおよび書き込みが可能になります。

重要

Red Hat Ceph Storage クラスターは 1 つの Monitor ノードで実行できますが、実稼働クラスターで高可用性を確保するために、Red Hat は 3 つ以上の Monitor ノードを持つデプロイメントのみをサポートします。少なくとも 3 つのモニターノードは、1 つのモニターに障害が発生したり、1 つのモニターが利用できなくなると、クラスター内の残りの Monitor ノードが新しいリーダーを選択するためにクォーラムが存在することを意味します。

Manager ノード

各 Manager (MGR) ノードは Ceph Manager デーモン (**ceph-mgr**) を実行します。これは、ストレージ使用率、現在のパフォーマンスメトリック、システム負荷など、ランタイムメトリクスと Ceph クラスターの現在の状態を追跡します。通常、Manager ノードは (つまり、同じホストマシンにある) モニター ノードの同じ場所に配置されます。

オブジェクトストレージデバイスノード

各 Object Storage Device (OSD) ノードは Ceph OSD デーモン (**ceph-osd**) を実行し、ノードに割り当てられている論理ディスクと相互作用します。Ceph は OSD ノードにデータを保存します。Ceph は、非常に少数の OSD ノード (デフォルトは 3) で実行できますが、実稼働クラスターでは、ストレージクラスターで中程度のスケール (たとえば OSD が 50 個) のパフォーマンスが実現されます。ストレージクラスターに複数の OSD を持つと、システム管理者は CRUSH マップ内に分離された障害ドメインを定義できます。

メタデータサーバーノード

各 Metadata Server (MDS) ノードは、Ceph ファイルシステム (CephFS) に保存されているファイルに関連する MDS デーモン (**ceph-mds**) を実行します。MDS デーモンは、共有クラスターへのアクセスも調整します。

関連情報

Red Hat Ceph Storage の詳細は、What is Red Hat Ceph Storage? を参照してください。

15.2. RED HAT CEPH STORAGE のインストール

AMQ Broker のマルチサイトのフォールトトレランスアーキテクチャーは、Red Hat Ceph Storage 3 を使用します。データセンター間でデータを複製することで、Red Hat Ceph Storage クラスターは、別のデータセンターのブローカーで利用可能な共有ストアを効果的に作成します。共有ストア高可用性 (HA) ポリシーを使用し、メッセージングデータを Red Hat Ceph Storage クラスターに保存するようにブローカーを設定します。

実稼働環境で使用する Red Hat Ceph Storage クラスターには、少なくとも以下の項目が必要です。

- 3 つのモニター (MON) ノード
- 3 台のマネージャー (MGR) ノード
- 複数の OSD デーモンが含まれる 3 つのオブジェクトストレージデバイス (OSD) ノード
- 3 台のメタデータサーバー (MDS) ノード

重要

OSD、MON、MGR、および MDS ノードは、同じまたは別個の物理または仮想マシンで実行できます。ただし、Red Hat Ceph Storage クラスター内でフォールトトレランスを確保するには、これらのタイプのノードを異なるデータセンターに分散することが推奨されます。特に、1 つのデータセンターが停止した場合に、ストレージクラスターに少なくとも 2 つの MON ノードが含まれるようにする必要があります。そのため、クラスターに 3 つの MON ノードがある場合、それらの各ノードは別々のデータセンターにある別のホストマシンで実行する必要があります。このデータセンターに障害が発生しても残りの MON ノードが 1 つしかないままであるため、単一のデータセンターでは 2 つの MON ノードを実行しないでください。この場合、ストレージクラスターは機能しなくなります。

本セクションのリンク先の手順では、MON、MGR、OSD、および MDS ノードが含まれる Red Hat Ceph Storage 3 クラスターをインストールする方法について説明します。

前提条件

- Red Hat Ceph Storage インストールの準備に関する情報は、以下を参照してください。
  - 前提条件
  - Red Hat Ceph Storage のインストール要件チェックリスト

手順

- MON、MGR、OSD、および MDS ノードを含む Red Hat Ceph 3 ストレージクラスターのインストール方法を示す手順については、以下を参照してください。
  - Red Hat Ceph Storage クラスターのインストール

- メタデータサーバーのインストール

15.3. RED HAT CEPH STORAGE CLUSTER の設定

以下の手順では、フォールトトレランスを確保するために Red Hat Ceph Storage クラスターを設定する方法を説明します。CRUSH バケットを作成し、Object Storage Device (OSD) ノードを実際の物理インストールを反映したデータセンターに集約します。さらに、CRUSH に対してストレージプールでデータを複製する方法を指示するルールを作成します。以下の手順は、Ceph インストールで作成されたデフォルトの CRUSH マップを更新します。

前提条件

- Red Hat Ceph Storage クラスターがすでにインストールされている。詳細は、Installing Red Hat Ceph Storage を参照してください。
- Red Hat Ceph Storage が配置グループ (PG) を使用してプール内に多数のデータオブジェクトを整理する方法、およびプールで使用する PG の数を計算する方法を理解する必要があります。詳細は、Placement Groups (PGs) を参照してください。
- プール内のオブジェクトレプリカ数の設定方法を理解している。詳細は、Set the Number of Object Replicas を参照してください。

手順

1. CRUSH バケットを作成し、OSD ノードを整理します。バケットは、データセンターなどの物理的な場所に基づく OSD の一覧です。Ceph では、これらの物理的な場所は **障害ドメイン** と呼ばれます。

```
ceph osd crush add-bucket dc1 datacenter
ceph osd crush add-bucket dc2 datacenter
```

2. OSD ノードのホストマシンを、作成したデータセンター CRUSH バケットに移動します。ホスト名 **host1** - **host4** は、ホスト マシン名に置き換えます。

```
ceph osd crush move host1 datacenter=dc1
ceph osd crush move host2 datacenter=dc1
ceph osd crush move host3 datacenter=dc2
ceph osd crush move host4 datacenter=dc2
```

3. 作成した CRUSH バケットが **デフォルト** の CRUSH ツリーに含まれていることを確認します。

```
ceph osd crush move dc1 root=default
ceph osd crush move dc2 root=default
```

4. データセンター全体でストレージオブジェクトレプリカをマッピングするルールを作成します。これにより、データ損失を回避でき、1 つのデータセンターが停止した場合にクラスターが稼働を継続できるようになります。
ルールを作成するコマンドは、**ceph osd crush rule create-replicated <rule-name> <root> <failure-domain> <class>** 構文を使用します。以下に例を示します。

```
ceph osd crush rule create-replicated multi-dc default datacenter hdd
```

注記

上記のコマンドでは、ストレージクラスターがソリッドステートドライブ (SSD) を使用する場合は、**hdd** (ハードディスクドライブ) の代わりに **ssd** を指定します。

5. 作成したルールを使用するように、Ceph データおよびメタデータプールを設定します。最初は、これにより、CRUSH アルゴリズムによって決定されるストレージの宛先にデータがバックフィルされる可能性があります。

```
ceph osd pool set cephfs_data crush_rule multi-dc
ceph osd pool set cephfs_metadata crush_rule multi-dc
```

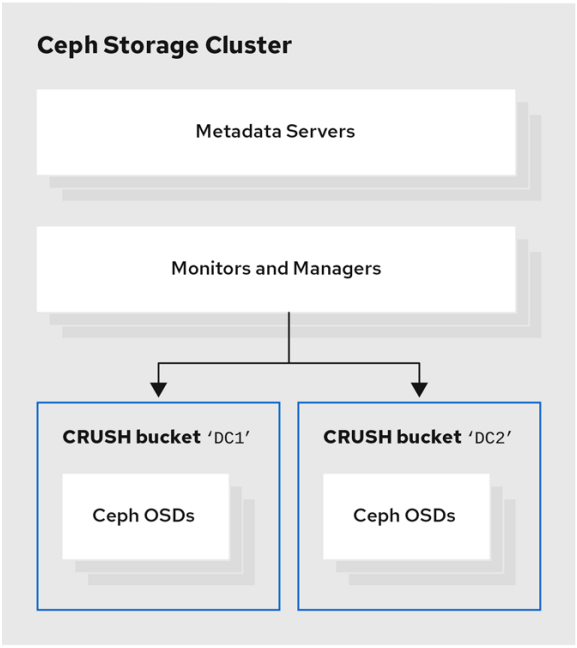
6. メタデータおよびデータプールの配置グループ (PG) および配置グループ (PGP) の数を指定します。PGP の値は PG の値と同じである必要があります。

```
ceph osd pool set cephfs_metadata pg_num 128
ceph osd pool set cephfs_metadata pgp_num 128

ceph osd pool set cephfs_data pg_num 128
ceph osd pool set cephfs_data pgp_num 128
```

7. データおよびメタデータプールによって使用されるレプリカの数を指定します。

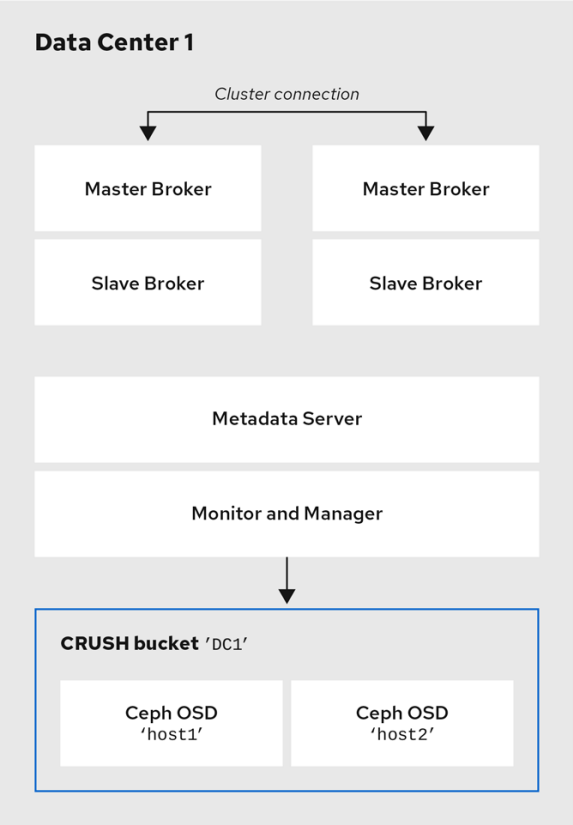
```
ceph osd pool set cephfs_data min_size 1
ceph osd pool set cephfs_metadata min_size 1

ceph osd pool set cephfs_data size 2
ceph osd pool set cephfs_metadata size 2
```

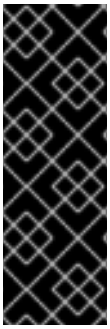
以下の図は、前述の例で作成した Red Hat Ceph Storage クラスターを示しています。ストレージクラスターには、データセンターに対応する CRUSH バケットに OSD が編成されています。



以下の図は、ブローカーサーバーを含む最初のデータセンターのレイアウトを示しています。特に、データセンターホスト。

- 2 つのライブバックアップブローカーペアのサーバー
- 前の手順で最初のデータセンターに割り当てられた OSD ノード
- 単一の Metadata Server、Monitor、および Manager ノード。Monitor ノードおよび Manager ノードは通常、同じマシンに共存します。

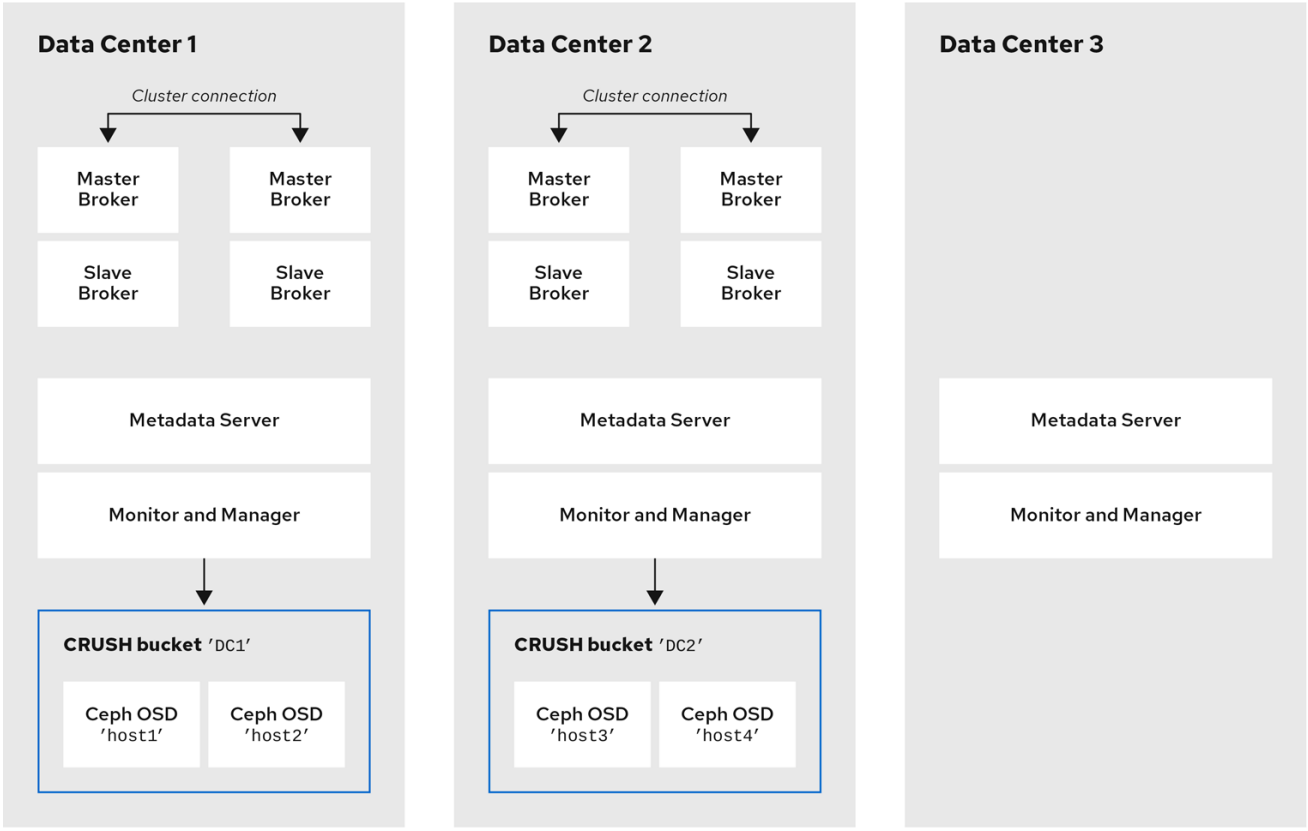


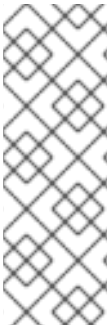


重要

OSD、MON、MGR、および MDS ノードは、同じまたは別個の物理または仮想マシンで実行できます。ただし、Red Hat Ceph Storage クラスター内でフォールトトレランスを確保するには、これらのタイプのノードを異なるデータセンターに分散することが推奨されます。特に、1 つのデータセンターが停止した場合に、ストレージクラスターに少なくとも 2 つの MON ノードが含まれるようにする必要があります。そのため、クラスターに 3 つの MON ノードがある場合、それらの各ノードは別々のデータセンターにある別のホストマシンで実行する必要があります。

以下の図は、トポロジーの完全な例を示しています。ストレージクラスターでのフォールトトレランスを確保するために、MON、MGR、および MDS ノードは 3 つの異なるデータセンターに分散されます。

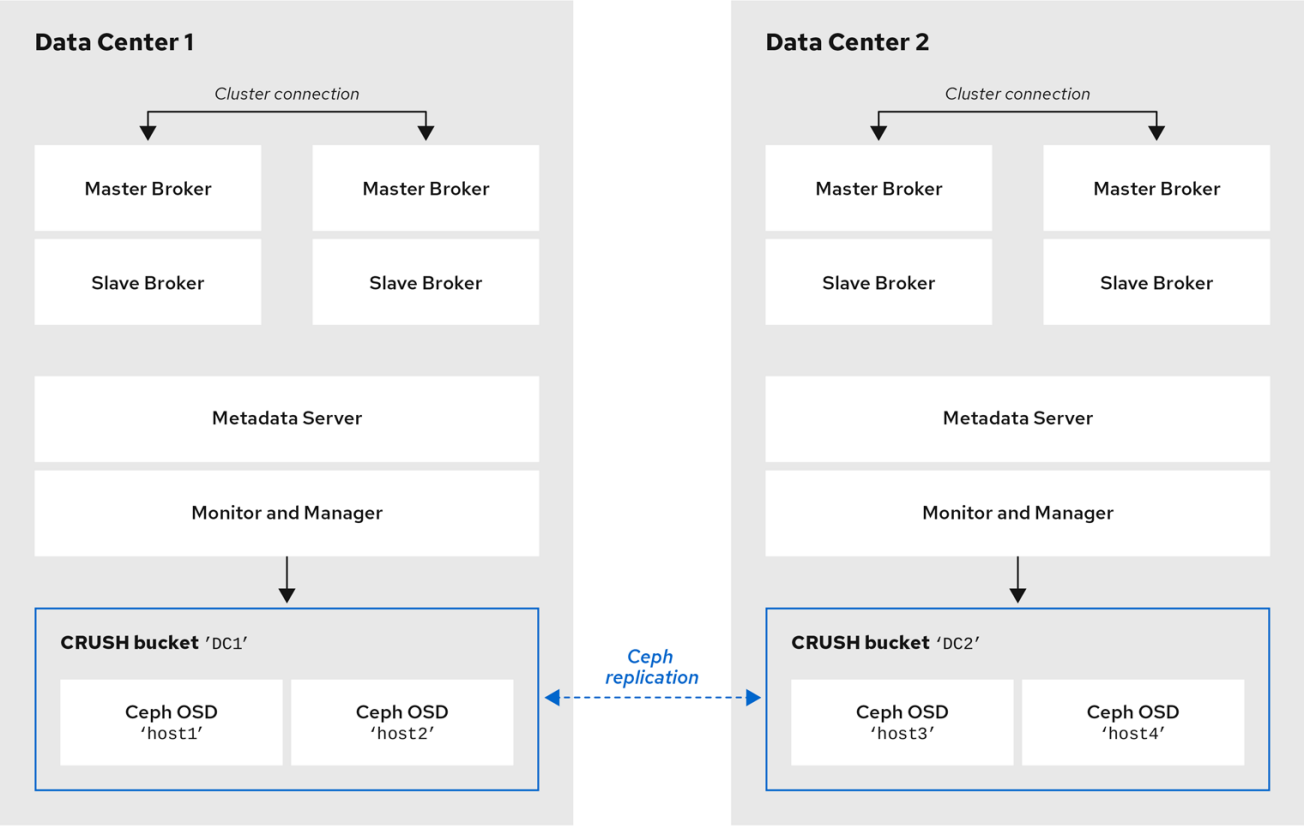




注記

ブローカーサーバーと同じデータセンターに特定の OSD ノードのホストマシンを見つけると、メッセージングデータを特定の OSD ノードに保存するわけではありません。メッセージングデータを Ceph File System の指定されたディレクトリーに保存するようにブローカーを設定します。クラスター内の Metadata Server ノードは、保存したデータをデータセンターで利用可能なすべての OSD に配信し、データセンター全体でこのデータの複製を処理する方法を決定します。以下のセクションでは、ブローカーを設定して Ceph File System にメッセージングデータを保存する方法を紹介します。

以下の図は、ブローカーサーバーを持つ 2 つのデータセンター間のデータレプリケーションを示しています。



関連情報

詳細情報:

- Red Hat Ceph Storage クラスターの CRUSH の管理については、CRUSH Administration を参照してください。
- ストレージプールに設定できる属性の完全なセットについては、Pool Values を参照してください。

15.4. ブローカーサーバーへの CEPH FILE SYSTEM のマウント

メッセージングデータを Red Hat Ceph Storage クラスターに保管するようにメッセージングシステムにブローカーを設定する前に、まず Ceph File System (CephFS) をマウントする必要があります。

本セクションのリンク先の手順では、CephFS をブローカーサーバーにマウントする方法を説明します。

前提条件

- 以下を行いました。
  - Red Hat Ceph Storage クラスターをインストールおよび設定していること。詳細は、Installing Red Hat Ceph Storage および Configuring a Red Hat Ceph Storage cluster を参照してください。
  - 3 つ以上の Ceph Metadata Server デーモンをインストールし、設定します (**ceph-mds**)。詳細は、Installing Metadata Servers および Configuring Metadata Server Daemons を参照してください。

- Monitor ノードから Ceph File System を作成します。詳細は、Creating the Ceph File System を参照してください。
- ブローカーサーバーが承認されたアクセスに使用できるキーで Ceph File System クライアントユーザーを作成しました。詳細は、Creating Ceph File System Client Users を参照してください。

手順

ブローカーサーバーに Ceph File System をマウントする方法は、Mounting the Ceph File System as a kernel client を参照してください。

15.5. マルチサイトの耐障害性のあるメッセージングシステムでのブローカーの設定

マルチサイトの耐障害性のあるメッセージングシステムの一部としてブローカーを設定するには、以下を行う必要があります。

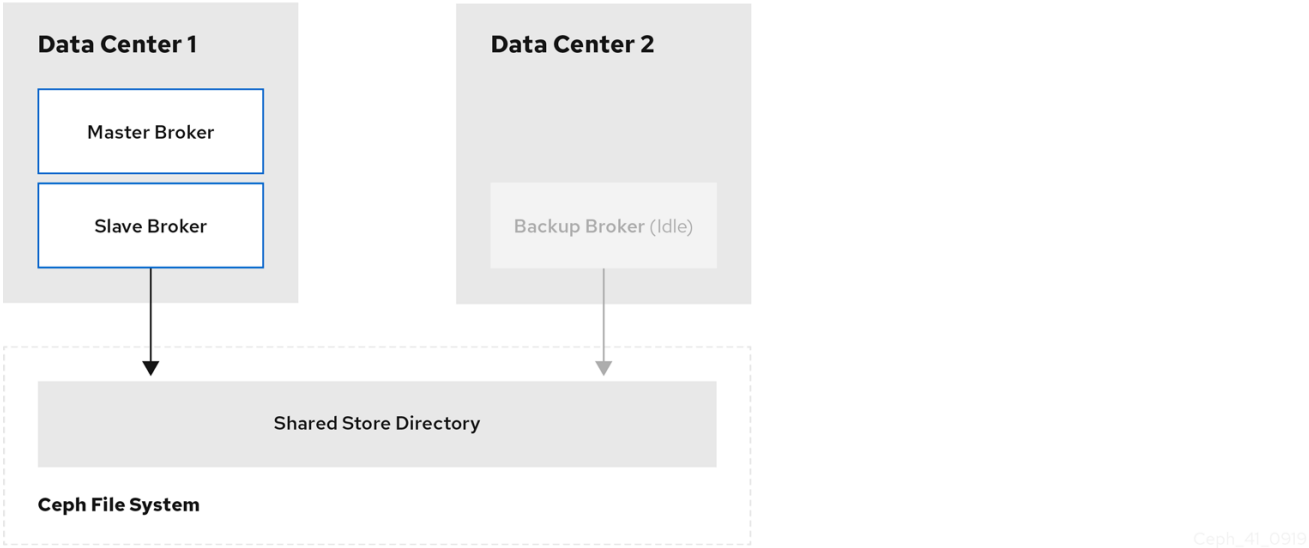
- データセンターに障害が発生した場合のライブブローカーから取得するアイドルバックアップブローカーを追加する
- Ceph クライアントロールですべてのブローカーサーバーの設定
- 共有ストア高可用性 (HA) ポリシーを使用するように各ブローカーを設定します。これは、ブローカーがメッセージングデータを保存する Ceph File System の場所を指定する

15.5.1. バックアップブローカーの追加

各データセンター内で、データセンターが停止した場合にシャットダウンするライブの master-slave ブローカーグループから引き継ぐアイドルバックアップブローカーを追加する必要があります。アイドルバックアップブローカーでライブマスターブローカーの設定を複製する必要があります。また、既存のブローカーと同じ方法でクライアント接続を受け入れるようにバックアップブローカーを設定する必要もあります。

後の手順で、既存の master-slave ブローカーグループに参加するようにアイドルバックアップブローカーを設定する方法を説明します。ライブの master-slave ブローカーグループのデータセンターとは別のデータセンターでアイドル状態のバックアップブローカーを見つける必要があります。また、データセンターに障害が発生した場合のみ、アイドルバックアップブローカーを手動で起動することが推奨されます。

以下の図はトポロジーの例を示しています。



関連情報

- 追加のブローカーインスタンスの作成方法は、Creating a standalone broker を参照してください。
- ブローカーネットワーク接続の設定に関する詳細は、*2章 ネットワーク接続でのアクセプターおよびコネクターの設定* を参照してください。

15.5.2. Ceph クライアントとしてのブローカーの設定

耐障害性の高いシステムに必要なバックアップブローカーを追加したら、すべてのブローカーサーバーを Ceph クライアントロールで設定する必要があります。クライアントロールにより、ブローカーは Red Hat Ceph Storage クラスターにデータを保存できます。

Ceph クライアントを設定する方法は、Installing the Ceph Client Role を参照してください。

15.5.3. Configuring shared store high availability

Red Hat Ceph Storage クラスターは、異なるデータセンターのブローカーで利用可能な共有ストアを効果的に作成します。失敗時にメッセージがブローカークライアントが利用可能なままになるように、ライブバックアップグループの各ブローカーが以下を使用するように設定します。

- 共有ストア高可用性 (HA) ポリシー
- Ceph ファイルシステム内の同じジャーナル、ページング、および大きなメッセージディレクトリー。

以下の手順では、ライブバックアップグループのマスター、スレーブ、およびアイドルバックアップブローカーに共有ストア HA ポリシーを設定する方法を説明します。

手順

1. ライブバックアップグループの各ブローカーの **broker.xml** 設定ファイルを編集します。Ceph File System で、同じページング、バインディング、ジャーナル、および大きなメッセージディレクトリーを使用するように各ブローカーを設定します。

```
# Master Broker - DC1
```

```
<paging-directory>mnt/cephfs/broker1/paging</paging-directory>
<bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
<journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
<large-messages-directory>mnt/cephfs/data/broker1/large-messages</large-messages-
directory>

# Slave Broker - DC1
<paging-directory>mnt/cephfs/broker1/paging</paging-directory>
<bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
<journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
<large-messages-directory>mnt/cephfs/data/broker1/large-messages</large-messages-
directory>

# Backup Broker (Idle) - DC2
<paging-directory>mnt/cephfs/broker1/paging</paging-directory>
<bindings-directory>/mnt/cephfs/data/broker1/bindings</bindings-directory>
<journal-directory>/mnt/cephfs/data/broker1/journal</journal-directory>
<large-messages-directory>mnt/cephfs/data/broker1/large-messages</large-messages-
directory>
```

2. 以下に示すように、バックアップブローカーを HA ポリシー内のマスターとして設定します。この設定により、手動で起動すると、バックアップブローカーがマスターにすぐにになります。ブローカーはアイドル状態のバックアップであるため、アクティブなマスターブローカーに指定できる **failover-on-shutdown** パラメーターは適用されません。

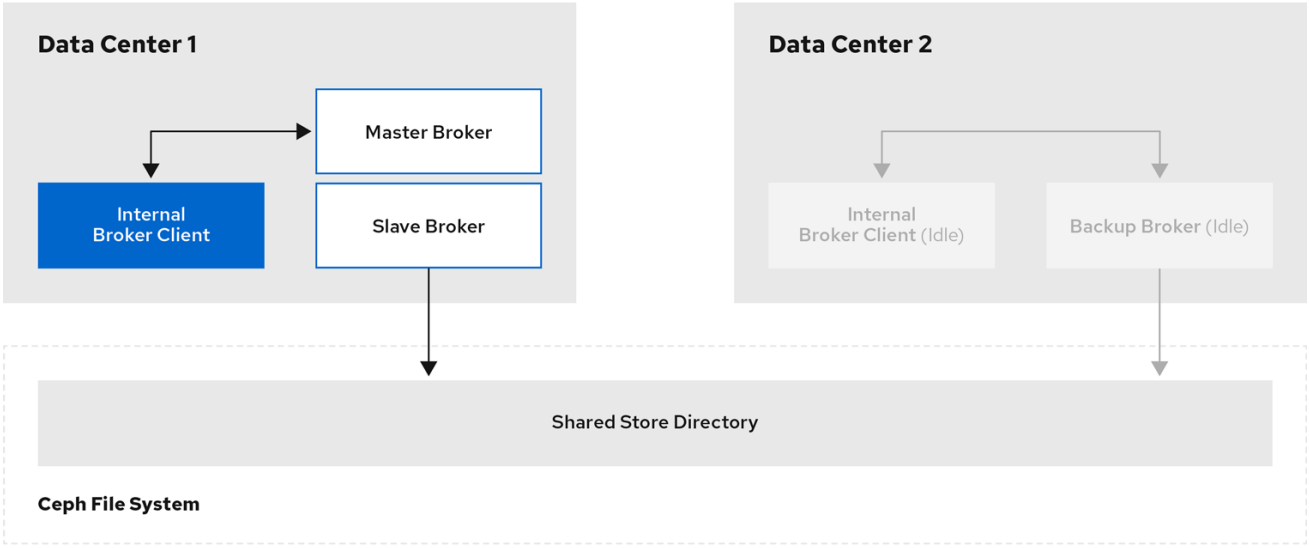
```
<configuration>
  <core>
    ...
    <ha-policy>
      <shared-store>
        <master>
        </master>
      </shared-store>
    </ha-policy>
    ...
  </core>
</configuration>
```

関連情報

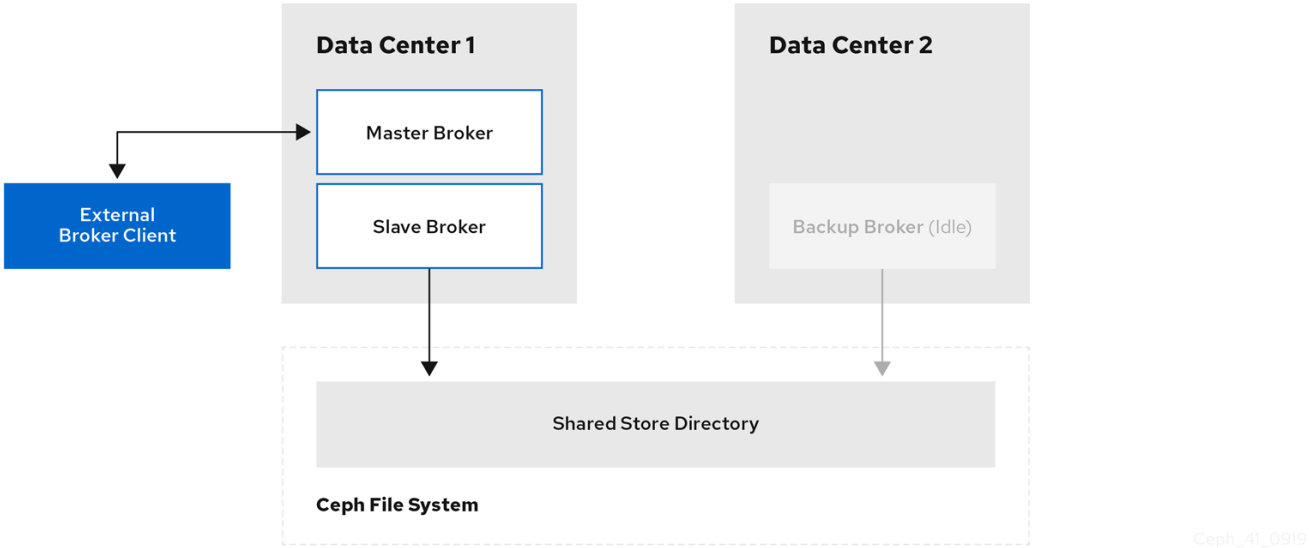
- ライブバックアップブローカーグループに共有ストアの高可用性ポリシーの設定に関する詳細は、Configuring shared store high availability を参照してください。

15.6. マルチサイトの耐障害性のあるメッセージングシステムでのクライアントの設定

内部クライアントアプリケーションは、ブローカーサーバーと同じデータセンターにあるマシンで実行されているアプリケーションです。以下の図はこのトポロジーを示しています。



外部クライアントアプリケーションは、ブローカーデータセンター外のマシンで実行されているものです。以下の図はこのトポロジーを示しています。



以下のサブセクションでは、データセンターが停止した場合に別のデータセンターのバックアップブローカーに接続するように内部および外部クライアントアプリケーションを設定する例を示します。

15.6.1. 内部クライアントの設定

データセンターが停止した場合に、内部クライアントアプリケーションがブローカーと共にシャットダウンします。この状況を軽減するには、別のデータセンターで利用可能なクライアントアプリケーションの別のインスタンスが必要です。データセンターが停止した場合に、バックアップクライアントを手動で起動し、手動で開始したバックアップブローカーに接続します。

バックアップクライアントがバックアップブローカーに接続できるようにするには、プライマリーデータセンターのクライアントと同じクライアント接続を設定する必要があります。

例

以下は、マスター / スレーブブローカーグループへの AMQ Core Protocol JMS クライアントの基本的な接続設定です。この例では、**host1** および **host2** はマスターおよびスレーブブローカーのホストサーバーです。

```
<ConnectionFactory connectionFactory = new
ActiveMQConnectionFactory("(tcp://host1:port,tcp://host2:port)?
ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
```

データセンターが停止した場合にバックアップブローカーに接続するようにバックアップクライアントを設定するには、同様の接続設定を使用しますが、バックアップブローカーサーバーのホスト名のみを指定します。この例では、バックアップブローカーサーバーは **host3** です。

```
<ConnectionFactory connectionFactory = new ActiveMQConnectionFactory("(tcp://host3:port)?
ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
```

関連情報

- ブローカーネットワーク接続の設定に関する詳細は、*2章 ネットワーク接続でのアクセプターおよびコネクターの設定* を参照してください。

15.6.2. 外部クライアントの設定

外部ブローカークライアントがデータセンターが停止した場合にメッセージングデータの生成または消費を継続できるようにするには、別のデータセンターのブローカーにフェイルオーバーするようにクライアントを設定する必要があります。マルチサイトのフォールトトレランスシステムの場合、障害が発生したときに手動で起動するバックアップブローカーにクライアントがフェイルオーバーするように設定します。

例

以下は、プライマリーマスターとスレーブグループが利用できない場合に、AMQ Core Protocol JMS および AMQ JMS クライアントがバックアップブローカーにフェイルオーバーするように設定する例です。この例では、**host1** および **host2** はプライマリーマスターおよびスレーブブローカーのホストサーバーですが、**host3** は、データセンターが停止した場合に手動で起動するバックアップブローカーのホストサーバーです。

- AMQ Core Protocol JMS クライアントを設定するには、クライアントが接続しようとするブローカーの順序付けされたリストにバックアップブローカーを含めます。

  ```
  <ConnectionFactory connectionFactory = new
  ActiveMQConnectionFactory("(tcp://host1:port,tcp://host2:port,tcp://host3:port)?
  ha=true&retryInterval=100&retryIntervalMultiplier=1.0&reconnectAttempts=-1");
  ```

- AMQ JMS クライアントを設定するには、クライアントに設定するフェイルオーバー URI にバックアップブローカーを含めます。

  ```
  failover:(amqp://host1:port,amqp://host2:port,amqp://host3:port)?
  jms.clientID=foo&failover.maxReconnectAttempts=20
  ```

関連情報

- フェイルオーバーの設定に関する詳細は、以下を行います。

- AMQ Core Protocol JMS クライアントについては、Reconnect and failover を参照してください。
- AMQ JMS クライアントについては、Failover options を参照してください。
- サポートされるその他のクライアントについては、Red Hat AMQ 7.9 の製品ドキュメントの AMQ Clients セクションのクライアント固有のドキュメントを参照してください。

15.7. データセンターの停止時のストレージクラスターの正常性の確認

フォールトトレランスのために Red Hat Ceph Storage クラスターを設定すると、データセンターのいずれかに障害が発生しても、クラスターはデータを損失せずに動作が低下します。

この手順では、動作が低下した状態でクラスターのステータスを検証する方法を説明します。

手順

1. Ceph Storage クラスターのステータスを確認するには、**health** または **status** コマンドを使用します。

```
# ceph health
# ceph status
```

2. コマンドラインでクラスターの続行中のイベントを監視するには、新しいターミナルを開きます。次に、以下を入力します。

```
# ceph -w
```

上記のコマンドを実行すると、ストレージクラスターが実行中であるものの、動作が低下したことを示す出力が表示されます。具体的には、以下のような警告が表示されます。

```
health: HEALTH_WARN
        2 osds down
        Degraded data redundancy: 42/84 objects degraded (50.0%), 16 pgs unclean, 16 pgs degraded
```

関連情報

- Red Hat Ceph Storage クラスターの正常性のモニターリングについての詳細は、Monitoring を参照してください。

15.8. データセンターの停止時のメッセージングの持続性の維持

以下の手順は、データセンターの停止時にブローカーおよび関連するメッセージングデータをクライアントが利用できる状態にする方法を説明します。特に、データセンターに障害が発生した場合に、以下を行う必要があります。

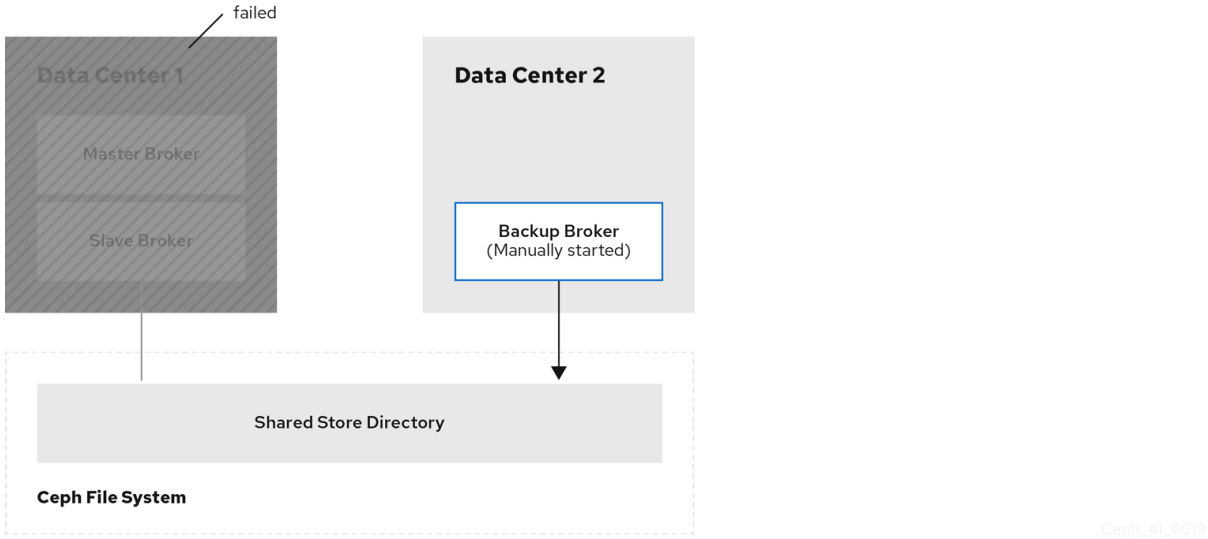
- 失敗したデータセンターのブローカーを引き継ぐために作成したアイドルバックアップブローカーを手動で開始します。
- 内部クライアントまたは外部クライアントを新しいアクティブなブローカーに接続します。

前提条件

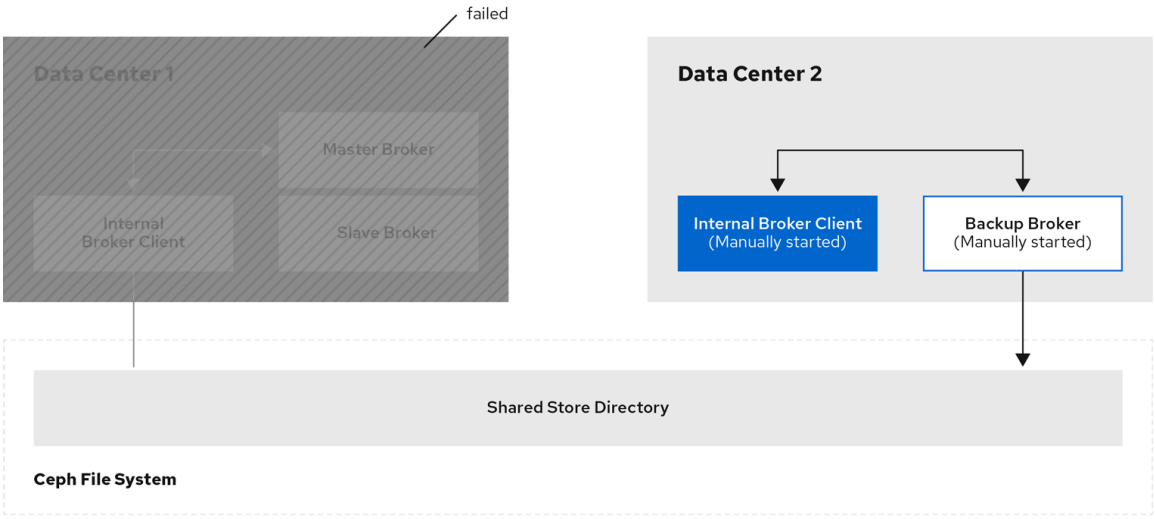
- 以下が必要になります。
  - Red Hat Ceph Storage クラスターをインストールおよび設定していること。詳細は、Installing Red Hat Ceph Storage および Configuring a Red Hat Ceph Storage cluster を参照してください。
  - Ceph File System をマウントしました。詳細は、Mounting the Ceph File System on your broker servers を参照してください。
  - データセンターに障害が発生した場合のライブブローカーから取得するためにアイドルバックアップブローカーを追加。詳細は、Adding backup brokers を参照してください。
  - Ceph クライアントロールを使用したブローカーサーバーを設定。詳細は、Configuring brokers as Ceph clients を参照してください。
  - 共有ストア高可用性 (HA) ポリシーを使用するように各ブローカーを設定し、各ブローカーでメッセージングデータを保存する場所を指定。詳細は、Configuring shared store high availability を参照してください。
  - データセンターが停止した場合にバックアップブローカーに接続するようにクライアントを設定する。詳細は、Configuring clients in a multi-site, fault-tolerant messaging system を参照してください。

手順

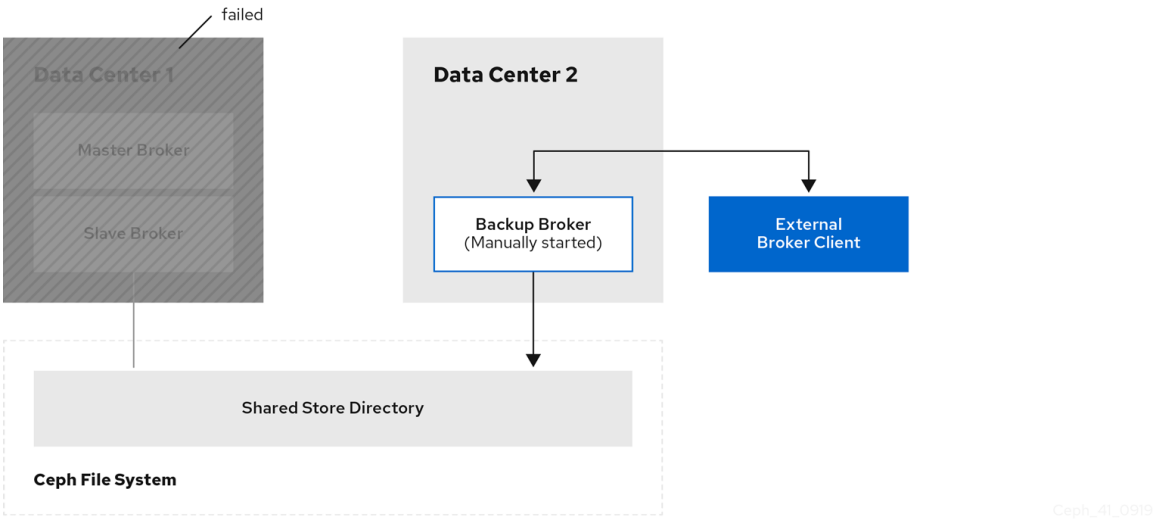
1. 失敗したデータセンターの各 master-slave ブローカーペアに対して、追加したアイドルバックアップブローカーを手動で起動します。



2. クライアント接続を再確立します。
   a. 障害の発生したデータセンターで内部クライアントを使用している場合は、作成したバックアップクライアントを手動で起動します。Configuring clients in a multi-site, fault-tolerant messaging system で説明されているように、手動で開始したバックアップブローカーに接続するようにクライアントを設定する必要があります。
   以下の図は、新しいトポロジーを示しています。



b. 外部クライアントがある場合、外部クライアントを手動で新しいアクティブなブローカーに接続するか、設定に基づいて、クライアントが新しいアクティブなブローカーに自動的にフェイルオーバーすることを確認します。詳細は、Configuring external clients を参照してください。
以下の図は、新しいトポロジーを示しています。



15.9. 以前に失敗したデータセンターの再起動

以前失敗したデータセンターがオンラインに戻る場合は、以下の手順に従ってメッセージングシステムの元の状態を復元します。

- Red Hat Ceph Storage クラスターのノードをホストするサーバーを再起動します。
- メッセージングシステムでブローカーを再起動します。
- クライアントアプリケーションから復元されたブローカーへの接続を再確立します。

以下のサブセクションでは、これらのステップを実行する方法を示します。

15.9.1. ストレージクラスターサーバーの再起動

以前障害の発生したデータセンターで Monitor、metadata Server、Manager、および Object Storage Device (OSD) ノードを再起動する際に、Red Hat Ceph Storage クラスターの自己修復を行い、データの冗長性を完全に復元します。このプロセス中に、Red Hat Ceph Storage は必要に応じて復元された OSD ノードにデータを自動的にバックフィルします。

ストレージクラスターが自動的に自己修復され、データ冗長性を完全に復元していることを確認するには、上記の Verifying storage cluster health during a data center outage に記載のコマンドを使用します。これらのコマンドを再実行すると、以前の **HEALTH_WARN** メッセージによるパフォーマンスの低下により、100% に戻るまで改善が開始することが分かります。

15.9.2. ブローカーサーバーの再起動

以下の手順では、ストレージクラスターが degraded 状態で機能しなくなったときにブローカーサーバーを再起動する方法を説明します。

手順

1. データセンターが停止したときに手動で開始したバックアップブローカーに接続されているクライアントアプリケーションを停止します。
2. 手動で起動したバックアップブローカーを停止します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis stop
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe stop
   ```

3. 以前はデータセンターに障害が発生し、元のマスターおよびスレーブブローカーを再起動します。
   a. Linux の場合:

   ```
   <broker_instance_dir>/bin/artemis run
   ```

   b. Windows の場合:

   ```
   <broker_instance_dir>\bin\artemis-service.exe start
   ```

元のマスターブローカーは、再起動時にそのロールを master として自動的に再開します。

15.9.3. クライアント接続の再設定

ブローカーサーバーを再起動したら、クライアントアプリケーションをこれらのブローカーに再接続します。以下のサブセクションでは、内部と外部の両方のクライアントアプリケーションを再接続する方法を説明します。

15.9.3.1. 内部クライアントの再接続

内部クライアントは、復元されたブローカーと同じデータセンターで実行されているクライアントです。内部クライアントを再接続するには、そのクライアントを再起動します。各クライアントアプリケーションは、接続設定に指定された復元されたマスターブローカーに再接続します。

ブローカーネットワーク接続の設定に関する詳細は、*2章 ネットワーク接続でのアクセプターおよびコネクターの設定* を参照してください。

15.9.3.2. 外部クライアントの再接続

外部クライアントは、以前に失敗したデータセンター外で実行されているものです。クライアントの種類と、外部ブローカークライアントの設定 に関する情報に基づいて、クライアントをバックアップブローカーに自動的にフェイルオーバーするように設定するか、この接続を手動で確立します。以前に失敗したデータセンターを復元する際に、以下で説明されているように、クライアントから復元されたマスターブローカーへの接続を再確立します。

- 外部クライアントをバックアップブローカーに自動的にフェイルオーバーするように設定した場合、バックアップブローカーをシャットダウンして元のマスターブローカーを再起動すると、クライアントは元のマスターブローカーに自動的に失敗します。
- データセンターが停止したときに外部クライアントをバックアップブローカーに手動で接続した場合、再起動する元のマスターブローカーに手動でクライアントを再接続する必要があります。

第16章 ブローカー接続を使用したマルチサイトのフォールトトレランスメッセージングシステムの設定

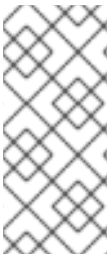
大規模なエンタープライズメッセージングシステムには、通常、地理的に分散したデータセンターに個別のブローカークラスターがあります。データセンターが停止した場合に、システム管理者は既存のメッセージングデータを保持し、クライアントアプリケーションがメッセージを生成および消費できるようにする必要がある場合があります。データセンターが停止した場合に、ブローカー接続を使用して、メッセージングシステムの継続的な停止を確保できます。このタイプのソリューションは、**マルチサイトのフォールトトレランスアーキテクチャー**と呼ばれます。

注記

ブローカー接続のブローカー間の通信では、AMQP プロトコルのみがサポートされます。クライアントは、サポートされる任意のプロトコルを使用できます。現時点で、メッセージはミラーリングプロセスで AMQP に変換されます。

以下のセクションでは、ブローカー接続を使用して、メッセージングシステムをデータセンターの停止から保護する方法を説明します。

- 「ブローカー接続について」
- 「ブローカー接続の設定」



注記

マルチサイトのフォールトトレランスは、データセンター**内**の高可用性 (HA) ブローカーの冗長性の代わりではありません。ライブバックアップグループに基づくブローカーの冗長性は、単一クラスター内の単一ブローカー障害に対する自動保護を提供します。これとは対照的に、マルチサイトのフォールトトレランスは、大規模なデータセンターの停止から保護します。

16.1. ブローカー接続について

ブローカー接続を使用すると、ブローカーは別のブローカーへの接続を確立し、そのブローカーとの間でメッセージをミラーリングできます。

AMQP サーバー接続

ブローカーは、ブローカー接続を使用して AMQP プロトコルを使用して他のエンドポイントへの接続を開始できます。たとえば、ブローカーは他の AMQP サーバーに接続し、それらの接続で要素を作成できます。

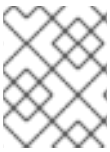
以下のタイプの操作は AMQP サーバー接続でサポートされます。

- mirrors: ブローカーは AMQP 接続を使用して別のブローカーに複製し、メッセージを重複して、ネットワーク上で確認応答を送信します。
- 送信側: 特定のキューで受信されたメッセージは、別のブローカーに転送されます。
- 受信者: ブローカーは別のブローカーからメッセージをプルします。
- ピア: ブローカーは、AMQ Interconnect エンドポイントで送信側と受信側の両方を作成します。

本章では、ブローカー接続を使用してフォールトトレランスシステムを作成する方法を説明します。送信者、受信側、およびピアオプションに関する詳細は、17章 *ブローカーのブリッジ* を参照してください。

以下のイベントはミラーリング経由で送信されます。

- メッセージ送信:1 つのブローカーに送信されたメッセージは、ターゲットブローカーに複製されます。
- メッセージ確認応答:1 つのブローカーでメッセージを削除する確認はターゲットブローカーに送信されます。
- キューとアドレスの作成。
- キューおよびアドレスの削除。



注記

メッセージがターゲットミラーのコンシューマーに保留中の場合、確認は成功せず、メッセージが両方のブローカーによって配信される可能性があります。

ミラーリングは操作をブロックせず、ブローカーのパフォーマンスには影響しません。

ブローカーは、ミラーが設定された時点から送信されるメッセージのみを反映します。以前のバージョンでは、既存のメッセージは他のブローカーに転送されません。

16.2. ブローカー接続の設定

以下の手順では、ブローカー間でメッセージをミラーリングするようにブローカー接続を設定する方法を説明します。いずれかのブローカーのみがアクティブになり、すべてのメッセージが他のブローカーにミラーリングされます。

前提条件

- 2 つの稼働中のブローカーがある。

手順

1. 最初のブローカーの **broker.xml** ファイルに **broker-connections** 要素を作成します。以下に例を示します。

```
<broker-connections>
  <amqp-connection uri="tcp://<hostname>:<port>" name="DC1">
    <mirror/>
  </amqp-connection>
</broker-connections>
```

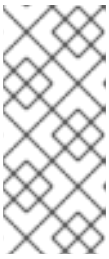
<hostname>
他のブローカーインスタンスのホスト名。

<port>
他のホストでブローカーによって使用されるポート。

最初のブローカーのメッセージはすべて 2 番目のブローカーにミラーリングされますが、ミラーの作成前に存在していたメッセージはミラーリングされません。

以下の追加機能を設定することもできます。

- **queue-removal** : queue- または address-removal イベントを送信するかどうかを指定します。デフォルト値は **true** です。
- **message-acknowledgements** : メッセージ確認応答を送信するかどうかを指定します。デフォルト値は **true** です。
- **queue-creation** : queue- または address-creation イベントを送信するかどうかを指定します。デフォルト値は **true** です。



注記

この例のブローカー接続名である **DC1** は、**$ACTIVEMQ_ARTEMIS_MIRROR_mirror** という名前のキューを作成するために使用されます。キューがそのブローカーで表示されない場合でも、対応するブローカーがこれらのメッセージを受け入れるように設定されていることを確認します。

2. 2 番目のブローカーの **broker.xml** ファイルに **broker-connections** 要素を作成します。以下に例を示します。

```
<broker-connections>
  <amqp-connection uri="tcp://<hostname>:<port>" name="DC2">
    <mirror/>
  </amqp-connection>
</broker-connections>
```

注記

Red Hat は、コンシューマーが両方ではなく、ブローカーのいずれかからのメッセージを受け入れるように設定することを推奨します。

3. 「マルチサイトの耐障害性のあるメッセージングシステムでのクライアントの設定」 に記載されている説明を使用してクライアントを設定します。これはブローカー接続でなく、共有ストレージはありません。

第17章 ブローカーのブリッジ

ブリッジは、2 つのブローカーを接続する方法を提供し、メッセージを 1 つから別のブローカーに転送します。

以下のブリッジが利用可能です。

コア

1 つのブローカーにデプロイされたコアブリッジを示す例が提供されます。これは、ローカルキューからメッセージを消費し、2 番目のブローカーのアドレスに転送します。ブローカーインストールの **<install_dir> /examples/features/standard/** ディレクトリーにある **core-bridge** の例を参照してください。

ミラーリング

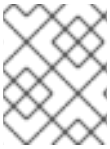
16章 *ブローカー接続を使用したマルチサイトのフォールトトレランスメッセージングシステムの設定* を参照してください。

送信側および受信側

「ブローカー接続の送信者およびレシーバー設定」 を参照してください。

ピア

「ブローカー接続のピア設定」 を参照してください。



注記

コアブリッジの **broker.xml** 要素は **ブリッジ** です。他のブリッジ技術は **<broker-connection>** 要素を使用します。

17.1. ブローカー接続の送信者およびレシーバー設定

broker.xml の **<broker-connections>** セクションに送信側または受信側ブローカーの接続要素を作成して、ブローカーを別のブローカーに接続できます。

送信側 の場合、ブローカーは別のブローカーにメッセージを送信するキューにメッセージコンシューマーを作成します。

受信側 の場合、ブローカーは別のブローカーからメッセージを受信するアドレスにメッセージプロデューサーを作成します。

どちらの要素もメッセージブリッジとして機能します。ただし、メッセージを処理するために必要な追加のオーバーヘッドはありません。送信側および受信側は、ブローカーの他のコンシューマーまたはプロデューサーと同様に動作します。

特定のキューは、送信側または受信側で設定できます。ワイルドカード式は、送信側および受信側を特定のアドレスまたはアドレス **セット** に一致させるために使用できます。送信側またはレシーバーを設定する場合は、以下のプロパティーを設定できます。

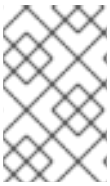
- **address-match** : ワイルドカード式を使用して、送信側または受信側を特定のアドレスまたはアドレス **セット** に一致させます。
- **queue-name** : 特定のキューの送信側または受信側を設定します。
- アドレス式の使用。

```
<broker-connections>
  <amqp-connection uri="tcp://HOST:PORT" name="other-server">
```

```
    <sender address-match="queues.#"/>
    <!-- notice the local queues for remotequeues.# need to be created on this broker -->
    <receiver address-match="remotequeues.#"/>
  </amqp-connection>
</broker-connections>

<addresses>
  <address name="remotequeues.A">
    <anycast>
      <queue name="remoteQueueA"/>
    </anycast>
  </address>
  <address name="queues.B">
    <anycast>
      <queue name="localQueueB"/>
    </anycast>
  </address>
</addresses>
```

- キュー名の使用。

```
<broker-connections>
  <amqp-connection uri="tcp://HOST:PORT" name="other-server">
    <receiver queue-name="remoteQueueA"/>
    <sender queue-name="localQueueB"/>
  </amqp-connection>
</broker-connections>

<addresses>
  <address name="remotequeues.A">
    <anycast>
      <queue name="remoteQueueA"/>
    </anycast>
  </address>
  <address name="queues.B">
    <anycast>
      <queue name="localQueueB"/>
    </anycast>
  </address>
</addresses>
```



注記

受信側は、すでに存在するローカルキューにのみ一致できます。そのため、受信側が使用されている場合は、キューがローカルに事前作成されることを確認します。そうしないと、ブローカーはリモートキューおよびアドレスに一致できません。

注記

送信側と受信側は同じ宛先で作成しないでください。送受信の無限ループが発生するためです。

17.2. ブローカー接続のピア設定

ブローカーは、AMQ Interconnect インスタンスに接続するピアとして設定し、ブローカーがそのルーターに設定された指定の AMQP ウェイポイントアドレスのストアアンド転送キューとして機能するように指示します。このシナリオでは、クライアントはルーターに接続してウェイポイントアドレスを使用してメッセージを送受信し、ルーターはこれらのメッセージをブローカーのキューへ / からルーティングします。

このピア設定は、ブローカーのブローカー接続設定に一致する各宛先の送信者と受信側のペアを作成します。これらのペアには、ルーターがブローカーと連携できるようにする設定が含まれます。この機能により、ルーターが接続を開始し、自動リンクを作成する必要がありません。

ルーター設定の詳細は、Using the AMQ Interconnect router を参照してください。

ピア設定では、送信側と受信側がある場合と同じプロパティーが存在します。たとえば、名前が **queue**. で始まるキューを持つキューがある設定は、一致するルーターのウェイポイントアドレスのストレージとして機能します。

```
<broker-connections>
  <amqp-connection uri="tcp://HOST:PORT" name="router">
    <peer address-match="queues.#"/>
  </amqp-connection>
</broker-connections>

<addresses>
   <address name="queues.A">
     <anycast>
       <queue name="queues.A"/>
     </anycast>
   </address>
   <address name="queues.B">
     <anycast>
       <queue name="queues.B"/>
     </anycast>
   </address>
</addresses>
```

ルーターには一致するアドレスウェイポイント設定が必要です。これは、ブローカーがウェイポイントにアタッチする特定のルーターに対処するよう指示します。たとえば、以下の接頭辞ベースのルーターアドレス設定を参照してください。

```
address {
    prefix: queue
    waypoint: yes
}
```

このオプションについての詳細は、Using the AMQ Interconnect router を参照してください。

注記

peer オプションを使用して、別のブローカーに直接接続しないでください。このオプションを使用して別のブローカーに接続すると、すべてのメッセージが即座に消費できる状態になり、送信および受信が無限のエコーが作成されます。

第18章 ロギング

AMQ Broker は JBoss Logging フレームワークを使用してロギングを実行し、**<broker_instance_dir>/etc/logging.properties** 設定ファイルで設定できます。この設定ファイルはキーと値のペアの一覧です。

以下に示すように、**logging.properties** 設定ファイルの **ロガー** キーに追加して、ブローカー設定でロガーを指定します。

```
loggers=org.eclipse.jetty,org.jboss.logging,org.apache.activemq.artemis.core.server,org.apache.activem
q.artemis.utils,org.apache.activemq.artemis.journal,org.apache.activemq.artemis.jms.server,org.apache
activemq.artemis.integration.bootstrap,org.apache.activemq.audit.base,org.apache.activemq.audit.mess
age,org.apache.activemq.audit.resource
```

AMQ Broker で利用可能なロガーを以下の表に示します。

ロガー	説明
org.jboss.logging	ルートロガー。他のブローカーロガーによって処理されない呼び出しをログに記録します。
org.apache.activemq.artemis.core.server	ブローカーコアをログに記録します。
org.apache.activemq.artemis.utils	ユーティリティー呼び出しのログ
org.apache.activemq.artemis.journal	Journal 呼び出しのログ
org.apache.activemq.artemis.jms	JMS 呼び出しをログに記録します。
org.apache.activemq.artemis.integration.bootstrap	ブートストラップ呼び出しのログ
org.apache.activemq.audit.base	すべての JMX オブジェクトメソッドへのアクセスをログに記録します。
org.apache.activemq.audit.message	実稼働、消費消費、メッセージのブラウジングなどのメッセージ操作をロギングします。
org.apache.activemq.audit.resource	JMX または AMQ Broker 管理コンソールからの認証イベント、作成または削除、および管理コンソールでのメッセージの参照をログに記録します。

また、以下のように **logger.handlers** キーに設定されたデフォルトのロギングハンドラーが 2 つあります。

```
logger.handlers=FILE,CONSOLE
```

logger.handlers=FILE

ロガーはログエントリーをファイルに出力します。

logger.handlers=CONSOLE

ロガーはログエントリーを AMQ Broker 管理コンソールに出力します。

18.1. ログレベルを変更する

すべてのロガーのデフォルトのロギングレベルは **INFO** で、以下のようにルートロガーで設定されます。

```
logger.level=INFO
```

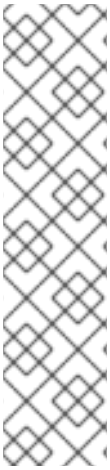
以下に示すように、他のすべてのロガーのログレベルを個別に設定できます。

```
logger.org.apache.activemq.artemis.core.server.level=INFO
logger.org.apache.activemq.artemis.journal.level=INFO
logger.org.apache.activemq.artemis.utils.level=INFO
logger.org.apache.activemq.artemis.jms.level=INFO
logger.org.apache.activemq.artemis.integration.bootstrap.level=INFO
logger.org.apache.activemq.audit.base.level=INFO
logger.org.apache.activemq.audit.message.level=INFO
logger.org.apache.activemq.audit.resource.level=INFO
```

利用可能なロギングレベルは、以下の表で説明されています。ロギングレベルは、最低詳細から順に昇順に一覧表示されます。

レベル	説明
FATAL	重要なサービス障害を示すイベントには、FATAL ロギングレベルを使用します。サービスが FATAL エラーを発行すると、あらゆる種類の要求を実行できません。
ERROR	リクエストが中断されたことを示すイベントまたはリクエストを処理する機能を示す ERROR ロギングレベルを使用します。このエラーの発生時に要求の処理を続行するには、サービスの **ある程度の** 容量が必要です。
WARN	重要でないサービスエラーを示す可能性のあるイベントの WARN ロギングレベルを使用します。再開可能なエラー、またはリクエスト内のマイナーな違反がこの説明を満たすことが期待されます。WARN と ERROR の違いは、アプリケーション開発者にとっての 1 つです。これを区別するための簡単な条件として、エラーがテクニカルサポートをシークする必要が生じるかどうかが挙げられます。エラーがテクニカルサポートを必要とする場合は、ロギングレベルを ERROR に設定します。それ以外の場合は、レベルを WARN に設定します。

レベル	説明
INFO	サービスのライフサイクルイベントおよびその他の重要な関連情報には INFO ロギングレベルを使用します。特定のサービスカテゴリーの INFO レベルメッセージは、サービスの状態を明確に示す必要があります。
DEBUG	ライフサイクルイベントに関する追加情報を伝えるログメッセージには DEBUG ロギングレベルを使用します。開発者向けの情報や技術サポートに必要な詳細情報については、このログレベルを使用します。DEBUG ロギングレベルを有効にすると、サーバー要求の数と比例して JBoss サーバーのログが増加 **しないはず** です。所定のサービスカテゴリーの DEBUG および INFO レベルのメッセージは、サービスがどの状態にあるか、ポート、インターフェイス、ログファイルなど、どのブローカーリソースを使用しているかを明確に示する必要があります。
TRACE	リクエストアクティビティーに直接関連するログメッセージに TRACE ロギングレベルを使用します。このようなメッセージは、ロガーカテゴリーの優先度のしきい値でメッセージがレンダリングされることを示す場合を除き、ロガーに送信しないでください。**Logger.isTraceEnabled()** メソッドを使用して、カテゴリーの優先度のしきい値が有効かどうかを判断します。TRACE レベルのロギングは、必要に応じてブローカーの動作のディーププローティングを有効にします。TRACE ロギングレベルが有効な場合、JBoss ログのメッセージ数は少なくとも **a** * **N** まで増えます。ここで、**N** はブローカーによって受信されるリクエストの数で、**a** は何らかの定数になります。トレースされるリクエスト処理層によっては、サーバーログが **N** のべき乗に増加する可能性があります。



注記

- **INFO** は、**logger.org.apache.activemq.audit.base**、**logger.org.apache.activemq.audit.message**、および **logger.org.apache.activemq.audit.resource** 監査ロガーの唯一の利用可能なロギングレベルです。
- ルートロガーに指定されたロギングレベルは、他のロガーにより詳細なログレベルが指定されている場合でも、**すべて** のロガーに対して最も詳細なログレベルを決定します。たとえば、**org.apache.activemq.artemis.utils** に **DEBUG** の指定されたロギングがあり、ルートロガーの **org.jboss.logging** のロギングレベルが **WARN** であるとします。この場合、両方のロガーはログレベル **WARN** を使用します。

18.2. 監査ロギングの有効化

有効化には 3 つの監査ロガーを使用できます。これは、ベース監査ロガー、メッセージ監査ロガー、およびリソース監査ロガーです。

ベース監査ロガー (org.apache.activemq.audit.base)

アドレスやキューの作成や削除など、すべての JMX オブジェクトメソッドへの **アクセス** をログに記録します。ログには、これらの操作が成功したか失敗したかは表示 **されません**。

メッセージ監査ロガー (org.apache.activemq.audit.message)

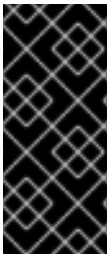
実稼働、消費、メッセージの参照などのメッセージ関連のブローカー操作をログに記録します。

リソース監査ロガー (org.apache.activemq.audit.resource)

クライアント、ルート、および AMQ Broker 管理コンソールから認証の成功または失敗をログに記録します。また、JMX または管理コンソールからキューの作成、更新、または削除をログに記録し、管理コンソールでメッセージを閲覧します。

各監査ロガーは、互いに独立して有効にできます。デフォルトでは、各監査ロガーは無効になっています (つまり、ロギングレベルは **ERROR** に設定され、監査ロガーの有効なログレベルではありません)。監査ロガーの 1 つを有効にするには、ロギングレベルを **INFO** に設定します。以下に例を示します。

```
logger.org.apache.activemq.audit.base.level=INFO
```



重要

メッセージ監査ロガーは、ブローカーのパフォーマンス集約型パスで実行されます。ロガーを有効にすると、特にブローカーがメッセージング負荷の高い状態で実行されている場合は、ブローカーのパフォーマンスに悪影響を与える可能性があります。高スループットが必要なメッセージングシステムでは、メッセージ監査ロガーの使用は推奨されません。

18.3. コンソールロギングの設定

以下のキーを使用してコンソールロギングを設定できます。

```
handler.CONSOLE=org.jboss.logmanager.handlers.ConsoleHandler
handler.CONSOLE.properties=autoFlush
handler.CONSOLE.level=DEBUG
handler.CONSOLE.autoFlush=true
handler.CONSOLE.formatter=PATTERN
```

注記

handler.CONSOLE は **logger.handlers** キーで指定された名前を参照します。

コンソールのロギング設定オプションは、以下の表で説明されています。

プロパティー	説明
name	ハンドラー名
encoding	ハンドラーによって使用される文字エンコーディング

プロパティー	説明
level	メッセージレベルを記録したログレベル。この値よりも小さいメッセージレベルは破棄されます。
formatter	フォーマッターを定義します。「ロギング形式の設定」 を参照してください。
autoflush	書き込みのたびにログを自動的にフラッシュするかどうかを設定します。
target	コンソールハンドラーのターゲット。値は SYSTEM_OUT または SYSTEM_ERR のいずれかになります。

18.4. ファイルロギングの設定

以下のキーを使用して、ファイルロギングを設定できます。

```
handler.FILE=org.jboss.logmanager.handlers.PeriodicRotatingFileHandler
handler.FILE.level=DEBUG
handler.FILE.properties=suffix,append,autoFlush,fileName
handler.FILE.suffix=.yyyy-MM-dd
handler.FILE.append=true
handler.FILE.autoFlush=true
handler.FILE.fileName=${artemis.instance}/log/artemis.log
handler.FILE.formatter=PATTERN
```

注記

handler.FILE は **logger.handlers** キーで指定された名前を参照します。

ファイルのロギング設定オプションについては、以下の表で説明されています。

プロパティー	説明
name	ハンドラー名
encoding	ハンドラーによって使用される文字エンコーディング
level	メッセージレベルを記録したログレベル。この値よりも小さいメッセージレベルは破棄されます。
formatter	フォーマッターを定義します。「ロギング形式の設定」 を参照してください。

プロパティー	説明
autoflush	書き込みのたびにログを自動的にフラッシュするかどうかを設定します。
append	ターゲットファイルに追加するかどうかを指定します。
file	パスと任意の相対パスで設定されるファイルの説明。

18.5. ロギング形式の設定

フォーマッターはログメッセージの表示方法を記述します。デフォルト設定は次のとおりです。

```
formatter.PATTERN=org.jboss.logmanager.formatters.PatternFormatter
formatter.PATTERN.properties=pattern
formatter.PATTERN.pattern=%d{HH:mm:ss,SSS} %-5p [%c] %s%E%n
```

上記の設定では、**%s** がメッセージで、**%E** が存在する場合は例外となります。

形式は Log4J 形式と同じです。詳細は、こちら を参照してください。

18.6. クライアントまたは埋め込みサーバーのロギング

クライアントでロギングを有効にする場合は、クライアントのクラスパスに JBoss ロギング JAR を含める必要があります。Maven を使用している場合は、以下の依存関係を追加します。

```
<dependency>
  <groupId>org.jboss.logmanager</groupId>
  <artifactId>jboss-logmanager</artifactId>
  <version>1.5.3.Final</version>
</dependency>
<dependency>
  <groupId>org.apache.activemq</groupId>
  <artifactId>artemis-core-client</artifactId>
  <version>1.0.0.Final</version>
</dependency>
```

Java プログラムの開始時に設定する必要があるプロパティーは 2 つあります。1 つ目は、Log Manager が JBoss Log Manager を使用するように設定することです。これは、'-Djava.util.logging.manager' プロパティーを設定して行います。以下に例を示します。

```
-Djava.util.logging.manager=org.jboss.logmanager.LogManager
```

2 つ目は、使用する **logging.properties** ファイルの場所を設定します。これは、**-Dlogging.configuration** プロパティーに有効な URL を設定して行います。以下に例を示します。

```
-Dlogging.configuration=file:///home/user/projects/myProject/logging.properties
```

以下は、クライアントの典型的な **logging.properties** ファイルです。

```
# Root logger option
loggers=org.jboss.logging,org.apache.activemq.artemis.core.server,org.apache.activemq.artemis.utils,o
g.apache.activemq.artemis.journal,org.apache.activemq.artemis.jms,org.apache.activemq.artemis.ra

# Root logger level
logger.level=INFO
# ActiveMQ Artemis logger levels
logger.org.apache.activemq.artemis.core.server.level=INFO
logger.org.apache.activemq.artemis.utils.level=INFO
logger.org.apache.activemq.artemis.jms.level=DEBUG

# Root logger handlers
logger.handlers=FILE,CONSOLE

# Console handler configuration
handler.CONSOLE=org.jboss.logmanager.handlers.ConsoleHandler
handler.CONSOLE.properties=autoFlush
handler.CONSOLE.level=FINE
handler.CONSOLE.autoFlush=true
handler.CONSOLE.formatter=PATTERN

# File handler configuration
handler.FILE=org.jboss.logmanager.handlers.FileHandler
handler.FILE.level=FINE
handler.FILE.properties=autoFlush,fileName
handler.FILE.autoFlush=true
handler.FILE.fileName=activemq.log
handler.FILE.formatter=PATTERN

# Formatter pattern configuration
formatter.PATTERN=org.jboss.logmanager.formatters.PatternFormatter
formatter.PATTERN.properties=pattern
formatter.PATTERN.pattern=%d{HH:mm:ss,SSS} %-5p [%c] %s%E%n
```

18.7. AMQ BROKER プラグインのサポート

AMQ はカスタムプラグインをサポートします。このプラグインを使用して、デバッグログでのみ使用できる各種のさまざまな種類のイベントに関する情報をログに記録できます。複数のプラグインは、登録、関連付け、および実行が可能です。プラグインは登録順序に基づいて実行されます。つまり、最初に登録されたプラグインは常に最初に実行されます。

カスタムプラグインを作成して、**ActiveMQServerPlugin** インターフェイスを使用して実装できます。このインターフェイスにより、プラグインがクラスパスに置かれ、ブローカーに登録されます。すべてのインターフェイスメソッドはデフォルトで実装されるため、実装する必要がある動作のみを追加する必要があります。

18.7.1. プラグインのクラスパスへの追加

関連する **.jar** ファイルを **<broker_instance_dir> /lib** ディレクトリーに追加して、カスタム作成したブローカープラグインをブローカーランタイムに追加します。

埋め込みシステムを使用している場合は、**.jar** ファイルを埋め込みアプリケーションの通常のクラスパス下に置きます。

18.7.2. プラグインの登録

broker.xml 設定ファイルに **broker-plugins** 要素を追加してプラグインを登録する必要があります。**property** 子要素を使用して、プラグイン設定値を指定できます。これらのプロパティーは、プラグインがインスタンス化された後にプラグインの init (Map<String, String>) 操作を読み取り、渡されます。

```
<broker-plugins>
  <broker-plugin class-name="some.plugin.UserPlugin">
    <property key="property1" value="val_1" />
    <property key="property2" value="val_2" />
  </broker-plugin>
 </broker-plugins>
```

18.7.3. プログラムによるプラグインの登録

プラグインをプログラムで登録するには、**registerBrokerPlugin()** メソッドを使用してプラグインの新規インスタンスを渡します。以下の例は、**UserPlugin** プラグインの登録を示しています。

```
Configuration config = new ConfigurationImpl();

config.registerBrokerPlugin(new UserPlugin());
```

18.7.4. 特定のイベントのロギング

デフォルトでは、AMQ ブローカーは **LoggingActiveMQServerPlugin** プラグインを提供し、特定のブローカーイベントをログに記録します。**LoggingActiveMQServerplugin** プラグインはデフォルトではコメントアウトされ、情報はログに記録されません。

以下の表は、各プラグインプロパティーについて説明しています。設定プロパティーの値を **true** に設定してイベントをログに記録します。

プロパティー	説明
LOG_CONNECTION_EVENTS	接続が作成または破棄されたときに情報を記録します。
LOG_SESSION_EVENTS	セッションの作成時または終了時に情報をログに記録します。
LOG_CONSUMER_EVENTS	コンシューマーが作成または閉じられたときの情報をログに記録します。
LOG_DELIVERING_EVENTS	メッセージがコンシューマーに配信され、メッセージがコンシューマーによって確認されると、情報を記録します。
LOG_SENDING_EVENTS	メッセージがアドレスに送信され、メッセージがブローカー内にルーティングされたときの情報をログに記録します。

LOG_INTERNAL_EVENTS	キューが作成または破棄されたとき、メッセージが期限切れになったとき、ブリッジのデプロイ時、および重大な障害が発生するときに、情報をログに記録します。
LOG_ALL_EVENTS	上記のすべてのイベントの情報をログに記録します。

接続イベントをログに記録するように **LoggingActiveMQServerPlugin** プラグインを設定するには、**broker.xml** 設定ファイルの **<broker-plugins>** セクションのコメントを解除します。すべてのイベントの値は、コメントされたデフォルト例では **true** に設定されます。

```
<configuration ...>
...
<!-- Uncomment the following if you want to use the Standard LoggingActiveMQServerPlugin plugin
to log in events -->
         <broker-plugins>
        <broker-plugin class-
name="org.apache.activemq.artemis.core.server.plugin.impl.LoggingActiveMQServerPlugin">
          <property key="LOG_ALL_EVENTS" value="true"/>
          <property key="LOG_CONNECTION_EVENTS" value="true"/>
          <property key="LOG_SESSION_EVENTS" value="true"/>
          <property key="LOG_CONSUMER_EVENTS" value="true"/>
          <property key="LOG_DELIVERING_EVENTS" value="true"/>
          <property key="LOG_SENDING_EVENTS" value="true"/>
          <property key="LOG_INTERNAL_EVENTS" value="true"/>
        </broker-plugin>
      </broker-plugins>
...
</configuration>
```

<broker-plugins> セクション内で設定パラメーターを変更した場合は、設定の更新を再ロードするためにブローカーを再起動する必要があります。これらの設定変更は、**configuration-file-refresh-period** 設定に基づいてリロード **されません**。

ログレベルを **INFO** に設定すると、イベントの発生後にエントリーがログに記録されます。ログレベルが **DEBUG** に設定されている場合、イベントの前後でログエントリーが生成されます (例 : **beforeCreateConsumer()** および **afterCreateConsumer())**。ログレベルが **DEBUG** に設定されている場合、ロガーは利用可能な場合に通知の詳細情報をログに記録します。

付録A アクセプターおよびコネクター設定パラメーター

以下の表は、Netty ネットワーク接続の設定に使用される利用可能なパラメーターの一部を示しています。パラメーターとその値は、接続文字列の URI に追加されます。詳細は、Configuring acceptors and connectors in network connections を参照してください。各テーブルは、名前別にパラメーターを一覧表示し、アクセプターまたはコネクターと使用できるか、またはその両方とともに使用するかをメモします。たとえば、アクセプターでしか使用するなど、一部のパラメーターを使用できます。

注記

すべての Netty パラメーターは **org.apache.activemq.artemis.core.remoting.impl.netty.TransportConstants** クラスで定義されます。カスタマーポータル では、ソースコードをダウンロードできます。

表A.1 Netty TCP パラメーター

パラメーター	用途	説明
batchDelay	両方	パケットをアクセプターまたはコネクターに書き込む前に、ブローカーは **batchDelay** ミリ秒の書き込みをバッチ処理するよう設定できます。これにより、非常に小さなメッセージで全体的なスループットが増える可能性があります。これは、メッセージ転送の平均レイテンシーが増加するため、経費します。デフォルト値は **0** ミリ秒です。
connectionsAllowed	アクセプター	アクセプターが許可する接続の数を制限します。この制限に達すると、DEBUG レベルのメッセージがログに出力され、接続は拒否されました。使用中のクライアントのタイプによって、接続が拒否されたときに何が起こるかが決まります。
directDeliver	両方	メッセージがサーバーに到達し、待機しているコンシューマーに配信されると、デフォルトでは、メッセージが到達した同じスレッドで配信が実行されます。これにより、メッセージが比較的小さく、コンシューマーの数が少ない環境では適切な待ち時間が発生しますが、特にマルチコアマシンではスループットとスケーラビリティー全体のコストが発生します。レイテンシーを最小限に抑え、スループットが低い場合は、**directDeliver** のデフォルト値 (**true**) を使用できます。レイテンシーに若干ヒットするが、スループットが最も高い場合は **directDeliver** を **false** に設定します。

パラメーター	用途	説明
handshake-timeout	アクセプター	承認されていないクライアントが多数の接続を開かないようにし、開いた状態にします。各接続にはファイルハンドルが必要なため、他のクライアントでは利用できないリソースを消費します。 このタイムアウトにより、接続が認証されずにリソースを消費できる時間を制限します。接続が認証されると、リソース制限設定を使用してリソース消費を制限できます。 デフォルト値は **10** 秒に設定されます。これは、他の整数値に設定できます。このオプションをオフにするには、0 または負の整数に設定します。 タイムアウト値を編集したら、ブローカーを再起動する必要があります。
localAddress	コネクター	リモートアドレスへの接続時にクライアントが使用するローカルアドレスを指定します。通常、これはアプリケーションサーバーで使用され、Embeddent 接続に使用されるアドレスを制御するために Embedded を実行する場合に使用されます。local-address が設定されていない場合、コネクターは利用可能なローカルアドレスを使用します。
localPort	コネクター	リモートアドレスへの接続時にクライアントが使用するローカルポートを指定します。通常、これはアプリケーションサーバーで使用され、Embeddent 接続に使用されるポートを制御するために Embedded を実行する場合に使用されます。デフォルトに (0) が使用される場合、コネクターによりシステムで一時ポートを取得することが許可されます。有効なポートは 0 から 65535 です。
nioRemotingThreads	両方	NIO を使用するように設定されている場合には、 ブローカーはデフォルトで受信パケットを処理するために **Runtime.getRuntime().availableProcessors()** によって報告されるコア (または hyper-threads) の数の 3 倍のスレッドを使用します。この値をオーバーライドする場合は、このパラメーターを指定してスレッド数を設定できます。このパラメーターのデフォルト値は **-1** です。これは、**Runtime.getRuntime().availableProcessors()** * 3 から派生する値を使用することを意味します。
tcpNoDelay	両方	**true** の場合、Nagle アルゴリズム が有効になります。これは、Java(クライアント) ソケットオプション です。デフォルト値は **true** です。
tcpReceiveBufferSize	両方	TCP 受信バッファーのサイズ (バイト単位) を決定します。デフォルト値は **32768** です。

パラメーター	用途	説明
tcpSendBufferSize	両方	TCP 送信バッファーのサイズ (バイト単位) を決定します。デフォルト値は **32768** です。 TCP バッファーサイズは、ネットワークの帯域幅およびレイテンシーに従って調整する必要があります。 つまり、TCP の送信/受信バッファーサイズは以下のように計算する必要があります。 buffer_size = bandwidth * RTT 帯域幅とは秒単位で、ネットワークラウンドトリップタイム (RTT) は秒単位になります。RTT は、**ping** ユーティリティーを使用して簡単に測定できます。 高速ネットワークでは、デフォルトからバッファーサイズを増やす必要がある場合があります。

表A.2 Netty HTTP パラメーター

パラメーター	用途	説明
httpClientIdleTime	アクセプター	接続を維持するために空の HTTP 要求を送信する前にクライアントがアイドル状態でいられる期間。
httpClientIdleScanPeriod	アクセプター	アイドル状態のクライアントに対してスキャンを行う頻度 (ミリ秒単位)。
httpEnabled	アクセプター	不要になりました。単一ポートがサポートされる場合、ブローカーは HTTP が使用されているかどうかを自動的に検出し、それ自体を設定するようになりました。
httpRequiresSessionId	両方	**true** の場合、クライアントは最初の呼び出し後にセッション ID を受け取るまで待機します。HTTP コネクターがサーブレットアクセプターに接続する場合に使用されます。この設定は推奨されません。
httpResponseTime	アクセプター	接続を維持するために空の HTTP 応答を送信する前にサーバーが待機する時間。
httpServerScanPeriod	アクセプター	応答が必要なクライアントに対してスキャンを行う頻度 (ミリ秒単位)。

表A.3 Netty TLS/SSL パラメーター

パラメーター	用途	説明

パラメーター	用途	説明
enabledCipherSuites	両方	SSL 通信に使用される暗号スイートのコンマ区切りリスト。デフォルト値は空で、JVM のデフォルトが使用されます。
enabledProtocols	両方	SSL 通信に使用されるプロトコルのコンマ区切りリスト。デフォルト値は空で、JVM のデフォルトが使用されます。
forceSSLParameters	コネクター	このコネクターの SSL コンテキストを設定するために、JVM システムプロパティー (**javax.net.ssl** および AMQ Broker システムプロパティーの両方を含む) ではなく、コネクターのパラメーターとして設定される SSL 設定を使用するかどうかを制御します。 有効な値は **true** または **false** です。デフォルト値は **false** です。
keyStorePassword	両方	アクセプターで使用されると、サーバー側のキーストアのパスワードになります。 コネクターで使用されると、クライアント側のキーストアのパスワードになります。双方向 SSL(つまり相互認証) を使用している場合は、これはコネクターにのみ関係します。この値はサーバー上で設定可能ですが、ダウンロードしてクライアントで使用します。クライアントでサーバーの設定と異なるパスワードを使用する必要がある場合は、カスタムの **javax.net.ssl.keyStorePassword** システムプロパティーまたは ActiveMQ 固有の **org.apache.activemq.ssl.keyStorePassword** システムプロパティーを使用してサーバー側の設定をオーバーライドできます。ActiveMQ 固有のシステムプロパティーは、クライアントの別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に便利です。
keyStorePath	両方	アクセプターで使用される場合は、サーバーの証明書を保持するサーバーの SSL キーストアへのパスになります (自己署名または認証局によって署名されているかどうか)。 コネクターで使用される場合、これはクライアント証明書を保持するクライアント側の SSL キーストアへのパスとなります。双方向 SSL(つまり相互認証) を使用している場合は、これはコネクターにのみ関係します。この値はサーバー上で設定されますが、ダウンロードしてクライアントで使用します。クライアントでサーバーの設定と異なるパスを使用する必要がある場合は、カスタムの **javax.net.ssl.keyStore** システムプロパティーまたは ActiveMQ 固有の **org.apache.activemq.ssl.keyStore** システムプロパティーのいずれかを使用してサーバー側の設定をオーバーライドできます。ActiveMQ 固有のシステムプロパティーは、クライアントの別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に便利です。

パラメーター	用途	説明
needClientAuth	アクセプター	このプロパティーは、このアクセプターに接続するクライアントに双方向 SSL が必要であることを伝えます。有効な値は **true** または **false** です。デフォルト値は **false** です。
sslEnabled	両方	SSL を有効にするには **true** にする必要があります。デフォルト値は **false** です。
trustManagerFactoryPlugin	両方	**org.apache.activemq.artemis.api.core.Trust Manager Factory Plugin**を実装するクラスの名前を定義します。 これは、**javax.net.ssl.TrustManagerFactory** を返す単一のメソッドを持つ簡単なインターフェイスです。**TrustManagerFactory** は、基礎となる **javax.net.ssl.SSLContext** が初期化されるときに使用されます。これにより、ブローカーおよびクライアントの信頼について詳細にわたるカスタマイズが可能になります。 **trustManagerFactoryPlugin** の値は、トラストマネージャーに適用される他のすべての SSL パラメーターよりも優先されます (例 : **trustAll**、**trustStoreProvider**、**trustStorePath**、**trustStorePassword**、および **crlPath**)。 ブローカーの Java クラスパスに、指定したプラグインを配置する必要があります。**<broker_instance_dir>/lib** ディレクトリーは、デフォルトでクラスパスに含まれているため、使用することができます。
trustStorePassword	両方	アクセプターで使用されると、サーバー側のトラストストアのパスワードになります。双方向 SSL(つまり相互認証) を使用している場合、アクセプターにのみ関係します。 コネクターで使用されると、クライアント側のトラストストアのパスワードになります。この値はサーバー上で設定可能ですが、ダウンロードしてクライアントで使用します。クライアントがサーバーで設定されているものとは異なるパスワードを使用する必要がある場合は、通常の**javax.net.ssl.trust Store Password**システムプロパティーまたは ActiveMQ 固有の**org.apache.activemq.ssl.trust Store Password**システムプロパティーを使用して、サーバー側の設定を上書きできます。ActiveMQ 固有のシステムプロパティーは、クライアントの別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に便利です。

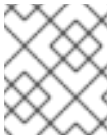
パラメーター	用途	説明
sniHost	両方	アクセプターで使用される場合、**sniHost** は受信 SSL 接続の **server_name** 拡張と一致するために使用される正規表現です (この拡張機能に関する詳細は、https://tools.ietf.org/html/rfc6066 を参照してください)。名前が一致しない場合、アクセプターへの接続は拒否されます。この場合、WARN メッセージが記録されます。 受信接続に **server_name** 拡張子が含まれていない場合、接続は受け入れられます。 コネクターで使用されると、SSL 接続の **server_name** 拡張子に **sniHost** 値が使用されます。
sslProvider	両方	**JDK** と **OPENSSL** の間で SSL プロバイダーを変更するために使用されます。デフォルトは **JDK** です。 **OPENSSL** に設定した場合は、クラスパスに **netty-tcnative** を追加して、ネイティブにインストールした OpenSSL を使用できます。 このオプションは、OpenSSL でサポートされ、JDK プロバイダーでサポートされていない、特別な ciphersuite-elliptic 曲線の組み合わせを使用する場合に便利です。
trustStorePath	両方	アクセプターで使用される場合、これはサーバーが信頼するすべてのクライアントのキーを保持するサーバー側の SSL キーストアへのパスとなります。双方向 SSL(つまり相互認証) を使用している場合、アクセプターにのみ関係します。 コネクターで使用される場合は、クライアント側の SSL/TLS キーストアへのパスとなります。これは、クライアントが信頼するすべてのサーバーの公開鍵を保持します。この値はサーバー上で設定可能ですが、ダウンロードしてクライアントで使用します。クライアントでサーバーの設定と異なるパスを使用する必要がある場合は、カスタムの **javax.net.ssl.trustStore** システムプロパティーまたは ActiveMQ 固有の **org.apache.activemq.ssl.trustStore** システムプロパティーのいずれかを使用してサーバー側の設定をオーバーライドできます。ActiveMQ 固有のシステムプロパティーは、クライアントの別のコンポーネントがすでに標準の Java システムプロパティーを使用している場合に便利です。
useDefaultSslContext	コネクター	コネクターが (**SSLContext.getDefault()** を介して) 「default」SSL コンテキストを使用できるようにします。これは、(**SSLContext.setDefault(SSLContext)** を介して) クライアントによってプログラム的に設定できます。 このパラメーターが **true** に設定されている場合、**sslEnabled** 以外の SSL 関連のパラメーターはすべて無視されます。有効な値は **true** または **false** です。デフォルト値は **false** です。

パラメーター	用途	説明
verifyHost	両方	コネクターで使用されると、サーバーの SSL 証明書の CN または Subject Alternative Name の値は、一致することを確認するために、接続先のホスト名と比較されます。これは一方向および双方向 SSL の両方に役立ちます。 アクセプターで使用されると、接続しているクライアントの SSL 証明書の CN または Subject Alternative Name の値がホスト名と比較され、それらが一致することを確認します。これは双方向 SSL でのみ便利です。 有効な値は **true** または **false** です。デフォルト値はコネクターの場合は **true**、アクセプターの場合は **false** です。
wantClientAuth	アクセプター	このアクセプターに接続するクライアントに対して、双方向 SSL が要求されているが、必須ではないことを伝えます。有効な値は **true** または **false** です。デフォルト値は **false** です。 **needClientAuth** を **true** に設定すると、そのプロパティーが優先され **wantClientAuth** は無視されます。

付録B アドレス設定設定要素

以下の表は、**address-setting** のすべての設定要素の一覧です。一部の要素は DEPRECATED とマークされていることに注意してください。潜在的な問題を回避するには、推奨される代替手段を使用してください。

表B.1 アドレス設定要素

名前	説明
address-full-policy	**max-size-bytes** で設定したアドレスが満杯になるとどうなるかを決定します。利用可能なポリシーは以下のとおりです。 **PAGE** : 完全なアドレスに送信されたメッセージは、ディスクにページングされます。 **DROP** : 完全なアドレスに送信されたメッセージは警告なしで破棄されます。 **FAIL** : 完全なアドレスに送信されたメッセージはドロップされ、メッセージプロデューサーは例外を受け取ります。 **BLOCK**: メッセージプロデューサーは、それ以上メッセージを送信しようとするとブロックします。  **注記** BLOCK ポリシーは、AMQP、OpenWire、および Core Protocol プロトコルでのみ機能します。
auto-create-addresses	マッピング先のキューからキューの存在しないアドレスにメッセージを送信するか、消費しようとした場合にアドレスを自動作成するかどうか。デフォルト値は **true** です。
auto-create-dead-letter-resources	ブローカーがデッドレターアドレスおよびキューを自動的に作成し、未配信メッセージを受信するかどうかを指定します。デフォルト値は **false** です。 パラメーターが **true** に設定されている場合、ブローカーはデッドレターアドレスと関連するデッドレターキューを定義する **<address>** 要素を自動的に作成します。自動作成された **<address>** 要素の名前は、**<dead-letter-address>** に指定する name の値と一致します。
auto-create-jms-queues	非推奨: 代わりに **auto-create-queues** を使用してください。JMS プロデューサーまたはコンシューマーがこのようなキューを使用しようとするときに、このブローカーが、アドレス設定に対応する JMS キューを自動的に作成するかどうかを決定します。デフォルト値は **false** です。
auto-create-jms-topics	非推奨: 代わりに **auto-create-queues** を使用してください。JMS プロデューサーまたはコンシューマーがこのようなキューを使用しようとするときに、このブローカーが、アドレス設定に対応する JMS トピックを自動的に作成するかどうかを決定します。デフォルト値は **false** です。

名前	説明
auto-create-queues	クライアントがキューに対してメッセージを送信するとき、またはキューからメッセージを消費しようとするときにキューを自動的に作成するかどうか。デフォルト値は **true** です。
auto-delete-addresses	ブローカーにキューがなくなったときに自動作成されたアドレスを削除するかどうか。デフォルト値は **true** です。
auto-delete-jms-queues	非推奨: 代わりに **auto-delete-queues** を使用してください。自動作成された JMS キューにコンシューマーもメッセージもない場合は、AMQ Broker が自動的に削除するかどうかを決定します。デフォルト値は **false** です。
auto-delete-jms-topics	非推奨: 代わりに **auto-delete-queues** を使用してください。自動作成された JMS トピックにコンシューマーもメッセージもない場合は、AMQ Broker が自動的に削除するかどうかを決定します。デフォルト値は **false** です。
auto-delete-queues	キューにコンシューマーがなく、メッセージがない場合に自動作成されたキューを削除するかどうか。デフォルト値は **true** です。
config-delete-addresses	設定ファイルを再読み込みすると、この設定で、設定ファイルから削除されたアドレス (とそのキュー) を処理する方法を指定します。以下の値を指定できます。 **OFF (デフォルト)** 設定ファイルを再読み込みすると、アドレスは削除されません。 **FORCE** 設定ファイルが再ロードされると、アドレスとそのキューが削除されます。キューにメッセージがある場合は、それらも削除されます。
config-delete-queues	設定ファイルを再読み込みすると、この設定は、設定ファイルから削除されたキューを処理する方法を指定します。以下の値を指定できます。 **OFF (デフォルト)** 設定ファイルを再読み込みすると、キューは削除されません。 **FORCE** キューは、設定ファイルが再ロードされると削除されます。キューにメッセージがある場合は、それらも削除されます。
dead-letter-address	ブローカーがデッドメッセージを送信するアドレス。
dead-letter-queue-prefix	ブローカーにより、自動作成されたデッドレターキューの名前に適用される接頭辞。デフォルト値は **DLQ** です。
dead-letter-queue-suffix	ブローカーにより、自動作成されたデッドレターキューに適用される接尾辞。デフォルト値は定義されていません (つまり、ブローカーは接尾辞を適用しません)。

名前	説明
default-address-routing-type	自動作成されたアドレスで使用されるルーティングタイプ。デフォルト値は **MULTICAST** です。
default-max-consumers	このキューで一度に許可されるコンシューマーの最大数。デフォルト値は **200** です。
default-purge-on-no-consumers	コンシューマーがない場合にキューの内容をパージするかどうか。デフォルト値は **false** です。
default-queue-routing-type	自動作成されたキューで使用されるルーティングタイプ。デフォルト値は **MULTICAST** です。
enable-metrics	Prometheus プラグインなどの設定されたメトリクスプラグインが一致するアドレスまたはアドレスの**セット**のメトリクスを収集するかどうかを指定します。デフォルト値は **true** です。
expiry-address	期限切れのメッセージを受信するアドレス。
expiry-delay	デフォルトの有効期限を使用してメッセージに使用される有効期限 (ミリ秒単位) を定義します。デフォルト値は **-1** で、有効期限がないことを意味します。
last-value-queue	キューが最後の値のみを使用するかどうかを指定します。デフォルト値は **false** です。
management-browse-page-size	管理リソースが参照できるメッセージの数を指定します。デフォルト値は **200** です。
max-delivery-attempts	デッドレターアドレスに送信する前にメッセージの配信を試行する回数。デフォルトは **10** です。
max-redelivery-delay	再配信遅延の最大値 (ミリ秒単位)。
max-size-bytes	このアドレスの最大メモリーサイズ (バイト単位)。**address-full-policy** が **PAGING**、**BLOCK**、または **FAIL** の場合、この値は "K"、"Mb"、および "GB" などのバイト表記で指定されます。デフォルト値は **-1** で、無限のバイトを示します。このパラメーターは、特定のアドレス領域によって消費されるメモリー量を制限してブローカーメモリーを保護するために使用されます。この設定は、現在ブローカーアドレス空間に保存されているクライアントによって送信されるバイトの合計量を表しません。これは、ブローカーのメモリー使用率の推定値です。この値は、ランタイムの状態と特定のワークロードによって異なります。アドレス空間ごとに使用できる最大メモリー容量を割り当てることが推奨されます。通常のワークロードでは、ブローカーはメモリーの未処理のメッセージのペイロードサイズの約 150% から 200% が必要になります。

名前	説明
max-size-bytes-reject-threshold	**address-full-policy** が **BLOCK** の場合に使用されます。ブローカーがメッセージを拒否する前にアドレスが到達できる最大サイズ (バイト単位)。AMQP プロトコルの場合のみ **max-size-bytes** と組み合わせて動作します。デフォルト値は **-1** で、制限なしを意味します。
message-counter-history-day-limit	このアドレスのメッセージカウンター履歴を保持する日数。デフォルト値は **0** です。
page-max-cache-size	ページングナビゲーション中に I/O を最適化するためにメモリー内に保持するページファイルの数。デフォルト値は **5** です。
page-size-bytes	ページングサイズ (バイト単位)。**K**、**Mb**、**GB** などのバイト表記にも対応します。デフォルト値は **10485760** バイト (約 10.5 MB) です。
redelivery-delay	キャンセルされたメッセージを再配信するまでの待機時間 (ミリ秒単位)。デフォルト値は **0** です。
redelivery-delay-multiplier	redelivery-delay パラメーターに適用する乗数。デフォルト値は **1.0** です。
redistribution-delay	キューの最後のコンシューマーが閉じられてから残りのメッセージを再分配するまでブローカーが待機する時間 (ミリ秒単位) を定義します。デフォルト値は **-1** です。
send-to-dla-on-no-route	**true** に設定すると、キューにルーティングされないメッセージは、設定済みのデッドレターアドレスアドレスに送信されます。デフォルト値は **false** です。
slow-consumer-check-period	低速なコンシューマーについてチェックする頻度 (秒単位)。デフォルト値は **5** です。
slow-consumer-policy	低速なコンシューマーが特定されたときにどうするのかを決定します。有効なオプションは **KILL** または **NOTIFY** です。**KILL** はコンシューマーの接続を強制終了します。これは、同じ接続を使用するすべてのクライアントスレッドに影響を与えます。**NOTIFY** は **CONSUMER_SLOW** 管理通知をクライアントに送信します。デフォルト値は **NOTIFY** です。
slow-consumer-threshold	最小限許可されるメッセージ消費率。この値を下回るとコンシューマーは遅いと見なされます。1 秒あたりのメッセージで測定されます。デフォルト値は **-1** で、バインドされません。

付録C クラスター接続設定要素

以下の表は、**cluster-connection** のすべての設定要素の一覧です。

表C.1 クラスター接続設定要素

名前	説明
address	各クラスター接続は、**address** フィールドで指定された値と一致するアドレスにのみ適用されます。アドレスが指定されていない場合、すべてのアドレスは負荷分散されます。 **address** フィールドは、アドレスのコンマ区切りリストもサポートします。アドレスが一致しないようにするには、除外構文 (**!**) を使用します。以下は、アドレスの例です。 **jms.eu** **jms.eu** で始まるすべてのアドレスと一致させます。 **!jms.eu** **jms.eu** で始まるアドレス以外のすべてのアドレスに一致させます。 **jms.eu.uk,jms.eu.de** **jms.eu.uk** または **jms.eu.de** で始まるすべてのアドレスと一致させます。 **jms.eu,!jms.eu.uk** **jms.eu** で始まるすべてのアドレスと一致させ、**jms.eu.uk** で始まるアドレスには一致させません。  **注記** 重複アドレス (例 : "europe" および "europe.news") を持つ複数のクラスター接続を持つべきではありません。複数のクラスター接続間で同じメッセージが分散され、配信が重複してしまう可能性があるためです。
call-failover-timeout	フェイルオーバーの試行中に呼び出しが行われる場合に使用します。デフォルトは **-1** で、タイムアウトなしです。
call-timeout	パケットがクラスター接続上で送信され、ブロッキング呼び出しである場合、**call-timeout** は例外を出力する前にブローカーが応答を待つ時間 (ミリ秒単位) を決定します。デフォルトは **30000** です。
check-period	クラスター接続が別のブローカーから ping を受信しなかったかどうかを確認する間隔 (ミリ秒単位)。デフォルトは **30000** です。
confirmation-window-size	接続先のブローカーから確認の送信に使用されるウインドウのサイズ (バイト単位)。ブローカーが **confirmation-window-size** バイトを受信すると、クライアントに通知します。デフォルトは **1048576** です。**-1** の値は、ウィンドウがないことを意味します。
connector-ref	適切なクラスタートポロジーを持つようにクラスター内の他のブローカーに送信される **コネクター** を特定します。このパラメーターは必須です。

名前	説明
connection-ttl	クラスター内の特定のブローカーからメッセージを受信しなくなった場合に、クラスター接続が有効である期間を決定します。既定値は **60000** です。
discovery-group-ref	クラスター内の他のブローカーとの通信に使用される **discovery-group** を参照します。この要素には **discovery-group-name** 属性を含める必要があります。これは、以前に設定した **discovery-group** の **name** 属性と一致する必要があります。
initial-connect-attempts	クラスターでシステムがブローカーへの接続を試行する回数を設定します。max-retry が達成されると、このブローカーは永続的にダウンしているとみなされ、システムはメッセージをこのブローカーにルーティングしません。デフォルトは **-1** で、再試行が無限を意味します。
max-hops	チェーンの中間として他のブローカーにのみ接続される可能性のあるブローカーへのメッセージの負荷分散を行うようにブローカーを設定します。これにより、メッセージ負荷分散を提供しながらより複雑なトポロジーが可能になります。デフォルト値は **1** です。つまり、メッセージはこのブローカーに直接接続された他のブローカーにのみ分散されます。このパラメーターは任意です。
max-retry-interval	再試行の最大遅延 (ミリ秒単位)。既定値は **2000** です。
message-load-balancing	クラスターの他のブローカー間でメッセージを分散するかどうか、およびその方法を決定します。負荷分散を有効にするために **message-load-balancing** 要素を含めます。デフォルト値は **ON_DEMAND** です。値を指定することもできます。有効な値は以下のとおりです。 **OFF** 負荷分散を無効にします。 **STRICT** キューにアクティブなコンシューマーまたは一致するセレクターがあるかどうかに関係なく、負荷分散を有効にし、一致するキューを持つすべてのブローカーにメッセージを転送します。 **ON_DEMAND** 負荷分散を有効にし、メッセージが一致するセレクターを持つアクティブなコンシューマーを持つブローカーにのみ転送されるようにします。 **OFF_WITH_REDISTRIBUTION** 負荷分散を無効にしますが、適切なローカルコンシューマーが利用できない場合に、メッセージが一致するセレクターを持つアクティブなコンシューマーを持つブローカーにのみ転送されるようにします。
min-large-message-size	メッセージのサイズ (バイト単位) が **min-large-message-size** を超える場合には、ネットワーク上で他のクラスターメンバーへの送信時に複数のセグメントに分割されます。デフォルトは **102400** です。
notification-attempts	クラスターへの接続時にクラスター接続がそれ自体をブロードキャストする回数を設定します。デフォルトは **2** です。

名前	説明
notification-interval	クラスターへの接続時にクラスター接続がそれ自体をブロードキャストする頻度 (ミリ秒単位) を設定します。既定値は **1000** です。
producer-window-size	クラスター接続に対するプロデューサーフロー制御のサイズ (バイト単位)。デフォルトでは無効になっていますが、クラスターで実際に大きなメッセージを使用している場合は、値を設定します。**-1** の値は、ウィンドウがないことを意味します。
reconnect-attempts	システムがクラスターのブローカーへの再接続を試行する回数を設定します。max-retry が達成されると、このブローカーは永続的にダウンしていると見なされ、システムはこのブローカーへのメッセージのルーティングを停止します。デフォルトは **-1** で、再試行が無限を意味します。
retry-interval	再試行の間隔 (ミリ秒単位) を指定します。クラスター接続が作成され、ターゲットブローカーが起動または起動されていない場合、他のブローカーからのクラスター接続は、バックアップされるまでターゲットへの接続を再試行します。このパラメーターは任意です。デフォルト値は 500 ミリ秒です。
retry-interval-multiplier	それぞれの再接続試行後に **retry-interval** を増やすために使用される乗数。デフォルトでは 1 回です。
use-duplicate-detection	クラスター接続はブリッジを使用してブローカーをリンクし、ブリッジを設定して転送される各メッセージに複製 ID プロパティーを追加できます。ブリッジのターゲットブローカーがクラッシュし、復旧すると、メッセージがソースブローカーから再送信される可能性があります。**use-duplicate-detection** を **true** に設定すると、重複メッセージがフィルターされ、ターゲットブローカーで受信時に無視されます。デフォルトは **true** です。

付録D コマンドラインツール

AMQ Broker にはコマンドラインインターフェイス (CLI) ツールのセットが含まれるため、メッセージングジャーナルを管理できます。以下の表は、各ツールの名前と説明を一覧表示しています。

ツール	説明
exp	特別な XML 形式および独立した XML 形式を使用して、メッセージデータをエクスポートします。
imp	**exp** によって提供された出力を使用して、ジャーナルを稼働中のブローカーにインポートします。
data	ジャーナルレコードとデータの圧縮に関するレポートを出力します。
encode	String にエンコードされるジャーナルの内部形式を示しています。
decode	エンコードから内部ジャーナル形式をインポートします。

各ツールで利用可能なコマンドの全一覧については、**help** パラメーターの後にツール名を使用してください。たとえば、以下の例で CLI 出力には、ユーザーが **./artemis help data** コマンドを入力すると、 **data** ツールで利用可能なコマンドがすべて表示されます。

```
$ ./artemis help data

NAME
        artemis data - data tools group
        (print|imp|exp|encode|decode|compact) (example ./artemis data print)

SYNOPSIS
        artemis data
        artemis data compact [--broker <brokerConfig>] [--verbose]
                [--paging <paging>] [--journal <journal>]
                [--large-messages <largeMessges>] [--bindings <binding>]
        artemis data decode [--broker <brokerConfig>] [--suffix <suffix>]
                [--verbose] [--paging <paging>] [--prefix <prefix>] [--file-size <size>]
                [--directory <directory>] --input <input> [--journal <journal>]
                [--large-messages <largeMessges>] [--bindings <binding>]
        artemis data encode [--directory <directory>] [--broker <brokerConfig>]
                [--suffix <suffix>] [--verbose] [--paging <paging>] [--prefix <prefix>]
                [--file-size <size>] [--journal <journal>]
                [--large-messages <largeMessges>] [--bindings <binding>]
        artemis data exp [--broker <brokerConfig>] [--verbose]
                [--paging <paging>] [--journal <journal>]
                [--large-messages <largeMessges>] [--bindings <binding>]
        artemis data imp [--host <host>] [--verbose] [--port <port>]
                [--password <password>] [--transaction] --input <input> [--user <user>]
        artemis data print [--broker <brokerConfig>] [--verbose]
                [--paging <paging>] [--journal <journal>]
                [--large-messages <largeMessges>] [--bindings <binding>]

COMMANDS
```

```
        With no arguments, Display help information

        print
            Print data records information (WARNING: don't use while a
            production server is running)

        ...
```

各ツールのコマンドを実行する方法の詳細については、ツールでヘルプを使用できます。たとえば、CLI は、ユーザーが **./artemis help data print** の入力後に **data print** コマンドに関する詳細情報を一覧表示します。

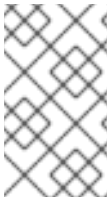
```
$ ./artemis help data print

NAME
        artemis data print - Print data records information (WARNING: don't use
        while a production server is running)

SYNOPSIS
        artemis data print [--bindings <binding>] [--journal <journal>]
                [--paging <paging>]

OPTIONS
        --bindings <binding>
            The folder used for bindings (default ../data/bindings)

        --journal <journal>
            The folder used for messages journal (default ../data/journal)

        --paging <paging>
            The folder used for paging (default ../data/paging)
```

付録E メッセージングジャーナル設定要素

以下の表は、AMQ Broker メッセージングジャーナルに関連する設定要素の一覧です。

表E.1 アドレス設定要素

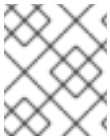
名前	説明
journal-directory	メッセージジャーナルが置かれているディレクトリー。デフォルト値は **<broker_instance_dir>/data/journal** です。 最適なパフォーマンスを得るには、ディスクヘッドの移動を最小限に抑えるために、ジャーナルを独自の物理ボリュームに置く必要があります。ジャーナルが、バインディングジャーナル、データベース、トランザクションコーディネーターなど、他のファイルを書き込む可能性のある他のプロセスと共有するボリュームにあるとします。その場合、書き込み時にディスクヘッドがこれらのファイル間で素早く移動するため、パフォーマンスが大幅に低下する可能性があります。 SAN を使用する場合、各ジャーナルインスタンスに独自の LUN (論理ユニット) を指定する必要があります。
create-journal-dir	**true** に設定すると、ジャーナルディレクトリーがまだ存在しない場合は、**journal-directory** で指定された場所にジャーナルディレクトリーが自動的に作成されます。デフォルト値は **true** です。
journal-type	有効な値は **NIO** または **ASYNCIO** です。 **NIO** に設定すると、ブローカーは Java NIO インターフェイスをそのジャーナルに使用します。**ASYNCIO** に設定され、ブローカーは Linux 非同期 IO ジャーナルを使用します。**ASYNCIO** を選択していても Linux を実行していない場合や、libaio がインストールされていない場合、ブローカーはこれを検出し、**NIO** の使用に自動的にフォールバックします。
journal-sync-transactional	**true** に設定すると、ブローカーはすべてのトランザクションデータをトランザクション境界のディスクにフラッシュします (つまり、コミット、準備、およびロールバック)。デフォルト値は **true** です。
journal-sync-non-transactional	**true** に設定すると、ブローカーは非トランザクションメッセージデータ (送信および確認応答) を毎回ディスクにフラッシュします。デフォルト値は **true** です。
journal-file-size	各ジャーナルファイルのサイズ (バイト単位)。デフォルト値は **10485760** バイト (10MiB) です。
journal-min-files	起動時にブローカーが事前作成するファイルの最小数。既存のメッセージデータがない場合にのみ、ファイルが事前に作成されます。 定常状態でキューに格納する予定のデータ量に応じて、データ全体の量と一致するようにこのファイルの数を調整する必要があります。

名前	説明
journal-pool-files	システムは必要な数だけファイルを作成します。ただし、ファイルを回収すると、**journal-pool-files** に縮小されます。 デフォルト値は **-1** です。つまり、作成後はジャーナルのファイルは削除されません。ただし、システムは無限に拡張することができませんが、永久に拡張できる宛先のページングを使用する必要があるため、システムを拡張する必要があります。
journal-max-io	常時 IO キューに格納できる書き込み要求の最大数を制御します。キューが満杯になると、領域が解放されるまで書き込みがブロックされます。 NIO を使用する場合、この値は常に **1** である必要があります。AIO を使用する場合、デフォルト値は **500** です。最大 AIO の合計は、OS レベルに設定された値 (**/proc/sys/fs/aio-max-nr**) より大きくすることはできません。通常、65536 になります。
journal-buffer-timeout	バッファーがフラッシュされるタイミングのタイムアウトを制御します。AIO は通常 NIO よりもフラッシュ率が高いため、システムは NIO と AIO の両方で異なるデフォルト値を維持します。 NIO のデフォルト値は **3333333** ナノ秒 (300 回 / 秒) で、AIO のデフォルト値は **50000** ナノ秒 (2000 回 / 秒) です。  **注記** タイムアウト値を長くすると、レイテンシーを代償にシステムのスループットを増やすことができる可能性があり、デフォルト値はスループットと待ち時間のバランスをうまくとるように選択されています。
journal-buffer-size	AIO でのタイムアウトバッファーのサイズ。デフォルト値は **490KiB** です。
journal-compact-min-files	ブローカーがジャーナルを圧縮する前に必要なファイルの最小数。少なくとも **journal-compact-min-files** が設定されない限り、圧縮アルゴリズムは開始されません。デフォルト値は **10** です。  **注記** 値を **0** に設定すると、ジャーナルが無限に増大するため、圧縮は無効になり危険になる可能性があります。
journal-compact-percentage	圧縮を開始するしきい値。**journal-compact-percentage** 未満がライブデータであると判断されると、ジャーナルデータが圧縮されます。また、少なくとも **journal-compact-min-files** のデータファイルがジャーナルに存在しなければ、圧縮は起動されません。デフォルト値は **30** です。

付録F レプリケーション高可用性設定要素

以下の表は、レプリケーション HA ポリシーを使用する場合の有効な **ha-policy** 設定要素の一覧です。

表F.1 レプリケーションの高可用性を使用する場合に利用可能な設定要素

名前	説明
check-for-live-server	マスターブローカーとして設定されたブローカーにのみ適用されます。元のマスターブローカーが起動時に独自のサーバー ID を使用して別のライブブローカーのクラスターをチェックするかどうかを指定します。**true** に設定すると、元のマスターブローカーに戻り、2 つのブローカーが同時に存続するスプリットブレインの状況を回避します。このプロパティーのデフォルト値は **false** です。
cluster-name	レプリケーションに使用するクラスター設定の名前。この設定は、複数のクラスター接続を設定する場合にのみ必要です。設定された場合、クラスターへの接続時にこの名前のクラスター設定が使用されます。未設定の場合は、設定に定義された最初のクラスター接続が使用されます。
group-name	これが設定されている場合、バックアップブローカーは **group-name** の一致する値を持つライブブローカーとのみペアになります。
initial-replication-sync-timeout	レプリカの最初のレプリケーションプロセスが完了すると、レプリカが必要なデータをすべて受け取ったことを確認するため、レプリケートブローカーが待機する時間。このプロパティーのデフォルト値は 30,000 ミリ秒です。  **注記** この間隔の間、その他のジャーナル関連の操作はブロックされます。
max-saved-replicated-journals-size	バックアップブローカーにのみ適用されます。バックアップブローカーが保持するバックアップジャーナルファイルの数を指定します。この値に達すると、ブローカーは最も古いジャーナルファイルを削除して、新しいバックアップジャーナルファイルごとに領域を作成します。このプロパティーのデフォルト値は **2** です。
allow-failback	バックアップブローカーにのみ適用されます。ライブブローカーなどの別のブローカーが原因で、バックアップブローカーが元のロールを再開するかどうかを決定します。このプロパティーのデフォルト値は **true** です。
restart-backup	バックアップブローカーにのみ適用されます。別のブローカーにフェイルバックした後にバックアップブローカーが自動的に再起動するかどうかを決定します。このプロパティーのデフォルト値は **true** です。

改訂日時：2022-10-24 16:04:23 +1000