9.4

コンテナー内の *IBM MQ*

注記

本書および本書で紹介する製品をご使用になる前に、177 ページの『特記事項』に記載されている情報をお読みください。

本書は、 IBM® MQ バージョン 9 リリース 4、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様が IBM に情報を送信する場合、お客様は IBM に対し、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で情報を使用または配布する非独占的な権利を付与します。

目次

コンテナー内の IBM MQ と IBM Cloud Pak for Integration

コンテナーを使用すると、IBM MQ キュー・マネージャーや IBM MQ クライアント・アプリケーションをすべての依存関係とともに、ソフトウェア開発のために標準化された単位でパッケージ化できます。

Red Hat® OpenShift®で IBM MQ Operator を使用して IBM MQ を実行できます。 このテストは、IBM Cloud Pak® for Integration、IBM MQ Advanced、または IBM MQ Advanced for Developers を使用して行うことができます。

また、IBM MQ をお客様が作成した独自のコンテナーで実行することもできます。

IBM MQ Operator について詳しくは、以下のリンクを参照してください。

コンテナー内の IBM MQ について

コンテナー内の IBM MQ の使用を開始するにあたって役に立つ情報を紹介します。

コンテナーは、ランタイム環境でコードのパッケージ化と分離を可能にするテクノロジーであり、同じインフラストラクチャー上の他のソフトウェアから分離された方法で実行できます。 これにより、キュー・マネージャーまたはアプリケーションを環境 (開発、テスト、実動など) 間で簡単に移動できます。 最新のコンテナー・オーケストレーター (Red Hat OpenShift Container Platform や Kubernetes など) は、同じマシン上で多くのタイプのコンテナーを実行できます。各コンテナーは、リソース、セキュリティー、および障害に関して互いに分離されています。

IBM MQ キュー・マネージャーまたは IBM MQ アプリケーションをコンテナー内で実行できます。

関連情報
コンテナーとは

IBM MQ Operator のリリース履歴

注:

- 以前の IBM MQ オペレーターについては、 IBM MQ 9.3 資料の IBM MQ Operator のリリース履歴 を参照してください。
- 今後の IBM MQ の更新については、「IBM MQ 推奨フィックスおよび計画メンテナンス・リリース日」ページ全体を参照してください。

IBM MQ Operator 3.2.1

IBM Cloud Pak for Integration バージョン
IBM Cloud Pak for Integration 16.1.0

オペレーター・チャネル
`v3.2-sc2`

`.spec.version` に許可される値
9.4.0.0-r1

マイグレーション中に許可される `.spec.version` の値
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2, 9.3.0.17-r3, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1, 9.3.5.0-r2, 9.3.5.1-r1, 9.3.5.1-r2

Red Hat OpenShift Container Platform のバージョン
OpenShift Container Platform 4.12 以上。

IBM Cloud Pak foundational services のバージョン
IBM Cloud Pak foundational services バージョン 4.6 のみ。

変更点

- 問題を解決する OpenShift Container Platform4.12 アップグレードする場合 v3.2-sc2 チャネルが予期しない動作を引き起こす可能性があります IBM Cloud Pak for Integration ユーザー。 詳細については、アップグレード 2023.4 の中に IBM Cloud Pak for Integration ドキュメンテーション。

IBM MQ Operator 3.2.0

IBM Cloud Pak for Integration バージョン
IBM Cloud Pak for Integration 16.1.0

オペレーター・チャネル
`v3.2-sc2`

`.spec.version` に許可される値
9.4.0.0-r1

マイグレーション中に許可される `.spec.version` の値
9.3.0.0-r1, 9.3.0.0-r2, 9.3.0.0-r3,9.3.3.2-r3 9.3.0.1-r1, 9.3.0.1-r2, 9.3.0.1-r3, 9.3.0.1-r4, 9.3.0.3-r1, 9.3.0.4-r1, 9.3.0.4-r2, 9.3.0.5-r1, 9.3.0.5-r2, 9.3.0.5-r3, 9.3.0.6-r1, 9.3.0.10-r1, 9.3.0.10-r2, 9.3.0.11-r1, 9.3.0.11-r2, 9.3.0.15-r1, 9.3.0.16-r1, 9.3.0.16-r2, 9.3.0.17-r1, 9.3.0.17-r2, 9.3.0.17-r3, 9.3.1.0-r1, 9.3.1.0-r2, 9.3.1.0-r3, 9.3.1.1-r1, 9.3.2.0-r1, 9.3.2.0-r2, 9.3.2.1-r1, 9.3.2.1-r2, 9.3.3.0-r1, 9.3.3.0-r2, 9.3.3.1-r1, 9.3.3.1-r2, 9.3.3.2-r1, 9.3.3.2-r2, 9.3.3.2-r3, 9.3.3.3-r1, 9.3.3.3-r2, 9.3.4.0-r1, 9.3.4.1-r1, 9.3.5.0-r1, 9.3.5.0-r2, 9.3.5.1-r1, 9.3.5.1-r2

Red Hat OpenShift Container Platform のバージョン
OpenShift Container Platform 4.12 以上。

IBM Cloud Pak foundational services のバージョン
IBM Cloud Pak foundational services バージョン 4.6 のみ。

新機能

- 100 ページの『永続ボリュームの拡張』 がサポートされるようになりました。
- `mq.ibm.com/stop` アノテーションを追加して `true` に設定することで、キュー・マネージャーを停止できるようになりました。 104 ページの『キュー・マネージャーの停止 (mq.ibm.com/stop)』 を参照してください。

  注:

  - 停止したキュー・マネージャーの `StatefulSet` 内の *.replicas* フィールドは、0 に設定されています。
  - IBM MQ Operator は現在、 `StatefulSet` 内の *.replicas* フィールドをアクティブに管理しているため、このフィールドを変更すると、オペレーターによって即時に元に戻されます。
  - 古いバージョンの IBM MQ では、 *.replicas* フィールドを変更した場合、「Failed」状態になりますが、変更した値は保持されます。 既存の操作手順がこの動作に依存している場合は、 IBM MQ 9.4 以降、 `mq.ibm.com/stop` アノテーションを使用する必要があります。

変更点

- Red Hat OpenShift Container Platform の奇数番号のリリースがサポートされるようになりました。
- IBM MQ カタログ・イメージが SQLite データベース・フォーマットからファイル・ベースのカタログ・フォーマットに移動されました。
- Red Hat Universal Base Image 9.4-949.1716471857 に基づきます。 **注:** UBI 9 には保留中の FIPS 140-3 認証があります。 UBI 9 は Power® 8 アーキテクチャーではサポートされていません。
- 対処された脆弱性の詳細については、このセキュリティー情報を参照してください。

OpenShift CP4I IBM MQ Operator で使用するキュー・マネージャー・コンテナー・イメージのリリース履歴

注 : 以前のキュー・マネージャー・コンテナー・イメージについては、IBM MQ 9.3 資料の IBM MQ Operator のリリース履歴 を参照してください。

9.4.0.0-r1

CP4I-SC2 CD

必要なオペレーター・バージョン
3.2.0 以上

サポートされているアーキテクチャー
amd64, s390x, ppc64le

イメージ

- `cp.icr.io/cp/ibm-mqadvanced-server-integration:9.4.0.0-r1`
- `cp.icr.io/cp/ibm-mqadvanced-server:9.4.0.0-r1`
- `icr.io/ibm-messaging/mq:9.4.0.0-r1`

新機能

- IBM MQ 9.4.0 for Multiplatforms の新機能-基本ライセンスと Advanced ライセンス

変更点

- IBM MQ 9.4.0 の変更内容
- Deprecated IBM MQ Advanced for Developers を使用する場合、環境変数を使用して `admin` ユーザーおよび `app` ユーザーのパスワードを設定することは推奨されません。 代わりにシークレットを使用してください。
- 環境変数 *MQ_LOGGING_CONSOLE_SOURCE* に新しいオプション値 `mqsc` が追加されました。 このオプションは、コンテナー・ログ内の `autocfgmqsc.LOG` の内容を反映するために使用できます。
- Red Hat Universal Base Image 9.4-949.1716471857 に基づきます。 **注:** UBI 9 には保留中の FIPS 140-3 認証があります。 UBI 9 は Power 8 アーキテクチャーではサポートされていません。

コンテナー内の IBM MQ の計画

コンテナー内の IBM MQ の計画を立てるときには、高可用性の実現方法、キュー・マネージャーの保護方法など、さまざまなアーキテクチャー・オプションのために IBM MQ が提供しているサポートについて考慮してください。

このタスクについて

コンテナー・アーキテクチャーで IBM MQ を計画する前に、基本的な IBM MQ 概念 (IBM MQ 技術の概要を参照) 、および基本的な Kubernetes/Red Hat OpenShift の概念を理解しておく必要があります (OpenShift Container Platform のアーキテクチャーを参照してください) 。

手順

- 8 ページの『コンテナー内の IBM MQ の使用方法の選択』.
- 8 ページの『コンテナーでの IBM MQ のサポート』.
- 15 ページの『IBM MQ Operator のストレージの計画』.
- 17 ページの『コンテナー内の IBM MQ の高可用性の計画』.
- 23 ページの『コンテナー内の IBM MQ の災害復旧』.
- 23 ページの『コンテナー内の IBM MQ でのユーザーの認証と許可』.

コンテナー内の IBM MQ の使用方法の選択

コンテナー内の IBM MQ の使用方法としては、いくつもの選択肢があります。プリパッケージされているコンテナー・イメージを使用する IBM MQ Operator を使用することも、独自のイメージとデプロイメント・コードをビルドすることもできます。

IBM MQ Operator の使用

OpenShift

Red Hat OpenShift Container Platform にデプロイする場合は、おそらく、IBM MQ Operator を使用したいはずです。

IBM MQ Operator は、 Red Hat OpenShift Container Platform API を拡張して、新しい `QueueManager` カスタム・リソースを追加します。 オペレーターは、新しいキュー・マネージャー定義を監視し、それを `StatefulSet` リソースや `Service` リソースなどの必要な下位リソースに変換します。 Native HA の場合、オペレーターはキュー・マネージャー・インスタンスの複雑なローリング更新を実行することもできます。 以下を参照してください。 21 ページの『ネイティブ HA キュー・マネージャーの独自ローリング更新を実行する場合の考慮事項』

IBM MQ の機能の中には、IBM MQ Operator を使用する場合にはサポートされないものもあります。 IBM MQ Operator の使用時にサポートされる内容について詳しくは、 8 ページの『コンテナーでの IBM MQ のサポート』 を参照してください。

独自のイメージおよびデプロイメント・コードのビルド

これは最も柔軟なコンテナソリューションですが、コンテナの設定に強いスキルが必要であり、結果としてのコンテナを"所有する"必要があります。 Red Hat OpenShift Container Platform を使用しない場合は、独自のイメージとデプロイメント・コードをビルドする必要があります。

独自のイメージをビルドするためのサンプルが用意されています。 55 ページの『独自のコンテナー・イメージのビルドによる IBM MQ の準備』 を参照してください。

独自のイメージおよびデプロイメント・コードのビルド時にサポートされる内容について詳しくは、 8 ページの『コンテナーでの IBM MQ のサポート』 を参照してください。

関連資料

8 ページの『コンテナーでの IBM MQ のサポート』
コンテナーでは、すべての IBM MQ 機能が同じ方法で使用可能およびサポートされているわけではありません。

OpenShift CP4I CP4I-SC2 CD コンテナーでの IBM MQ のサポート

コンテナーでは、すべての IBM MQ 機能が同じ方法で使用可能およびサポートされているわけではありません。

以下の表は、 IBM MQ Operator で IBM MQ 機能がどのようにサポートされているか、または独自のコンテナーとデプロイメント・コードをビルドするときにどのようにサポートされているかを示しています。

注 :

- IBM Container Registry (icr.io および cp.icr.io) 上の事前作成された IBM MQ コンテナー・イメージは、IBM MQ Operator で使用される場合にのみサポートされ、フィックスに適格です。
- IBM MQ Operator チャネル v3.2 以降、 Long Term Support (LTS) は Support Cycle 2 (SC2) に名前変更されました。 これは、コンテナー内の IBM MQ に使用できる唯一の LTS パスが IBM Cloud Pak for Integration 資格の下での 2 年間のサポートであり、 IBM Cloud Pak for Integration が SC2 という用語を採用しているためです。 以下に、資格の全体像を示します。
  - IBM MQ ライセンスを使用すると、IBM MQ Operator は IBM MQ Continuous Delivery (CD) イメージのみをデプロイできます。
  - IBM Cloud Pak for Integration ライセンスを使用すると、IBM MQ Operator は CD イメージまたは SC2 (formerly LTS) イメージをデプロイできます。

事前作成された IBM MQ Advanced for Developers イメージのライセンスを別のライセンスに「アップグレード」することはできません。 IBM MQ Operator は、選択されているライセンスに応じて異なるイメージをデプロイします。

この表では、以下の用語が適用されます。

"コンテナー・イネーブルメント・コード"
実行可能ファイル **runmqserver**、**runmqintegrationserver**、**chkmqhealthy**、**chkmqready** および **chkmqstarted**。 このコードはサンプルとして提供されており、IBM MQ Operator で使用される場合に事前作成コンテナーの一部としてのみサポートされます。

	IBM MQ Operator および IBM Cloud Pak for Integration ライセンスの使用	**IBM MQ Operator および IBM MQ Advanced ライセンスの使用**	**IBM MQ Operator および IBM MQ Advanced for Developers ライセンスの使用**	**事前作成 IBM MQ Advanced for Developers イメージ**	**Build-your-own コンテナー**
サポートされるプラットフォーム	Red Hat OpenShift Container Platform でのみサポート。 Red Hat OpenShift Container Platform のリリースは、 Red Hat がサポートを停止すると IBM MQ でサポートされなくなります。 詳しくは、13 ページの『IBM MQ Operator のバージョン・サポート』を参照してください。		Red Hat OpenShift Container Platform でのみ使用可能ですが、サポートされていません。	すべての Docker、containerd、または cri-o プラットフォームで機能しますが、サポートされません。 詳細は IBM MQ のシステム要件 を参照してください。	任意の Docker、containerd または cri-o プラットフォーム。 詳細は IBM MQ のシステム要件 を参照してください。 ネイティブ HA は、Kubernetes または Red Hat OpenShift Container Platform でのみサポートされます。 サンプル・コンテナー・イメージは、 Red Hat Universal Base Image (UBI) を使用します。 これには、 IBM MQ で使用される Linux® ライブラリーとユーティリティーが含まれています。 UBI は、 Red Hat OpenShift での実行時に Red Hat によってサポートされます。 コンテナー・イネーブルメント・コード はサポートされていません。

	IBM MQ Operator および IBM Cloud Pak for Integration ライセンスの使用	IBM MQ Operator および IBM MQ Advanced ライセンスの使用	IBM MQ Operator および IBM MQ Advanced for Developers ライセンスの使用	事前作成 IBM MQ Advanced for Developers イメージ	Build-your-own コンテナー
CPU アーキテクチャー	amd64 および s390x z/Linux でサポートされます。 ppc64le Power Systems バージョン 9 以上のシステムでもサポートされます。 Red Hat OpenShift Container Platform クラスター内のすべてのノードが同じ CPU アーキテクチャーを使用する必要があることに注意してください。		amd64 および s390x z/Linux で使用可能ですが、サポートされていません。 ppc64le Power Systems バージョン 9 以上のシステムでも使用可能ですが、サポートされていません。 Red Hat OpenShift Container Platform クラスター内のすべてのノードが同じ CPU アーキテクチャーを使用する必要があることに注意してください。		IBM MQ ソフトウェアに従います。
サポート期間	IBM Cloud Pak for Integration - Support Cycle 2 (formerly Long Term Support) または Continuous Delivery。[1] CD オペレーターおよびキュー・マネージャーは、次の IBM Cloud Pak for Integration CD または CP4I-SC2 リリースまでサポートされます。 CP4I-SC2 オペレーターおよびキュー・マネージャーは、次の IBM Cloud Pak for Integration CP4I-SC2 リリースまで、およびアップグレードを許可する猶予期間までサポートされます。	Continuous Delivery ストリームのみ (IBM MQ Operator とキュー・マネージャーの両方)。 各 IBM MQ Operator およびキュー・マネージャーのバージョンは、次の CD リリースまでのみサポートされます。	サポート対象外		IBM MQ ソフトウェアに従います。 長期サポートおよび継続的デリバリーのリリースに関する IBM MQ の FAQ を参照してください。 コンテナー・イネーブルメント・コード はサポートされていません。

	IBM MQ Operator および IBM Cloud Pak for Integration ライセンスの使用	**IBM MQ Operator および IBM MQ Advanced ライセンスの使用**	**IBM MQ Operator および IBM MQ Advanced for Developers ライセンスの使用**	**事前作成 IBM MQ Advanced for Developers イメージ**	**Build-your-own コンテナー**
セキュリティー・フィックスの可用性	IBM Container Registry でコンテナー・イメージとして使用可能な定期フィックス				IBM MQ ソフトウェアに対するフィックスは、Fix Central 上でソフトウェアとして入手できます。 コンテナー・イネーブルメント・コードはサポートされていません。
暫定修正の可用性	ソフトウェアとして使用可能なキュー・マネージャーのフィックス、およびカスタム・イメージのビルドが必要です。 IBM MQ Operator フィックスは、インテリム・フィックスとしては使用できません。		使用可能なインテリム・フィックスがありません。		IBM MQ ソフトウェアに対するフィックスは、Fix Central または IBM サポートからソフトウェアとして入手できます。 *container enablement code* はサポートされていません。
機能: Advanced Message Security	サポート対象。 サーバー・サイドの暗号化を使用することは容易ではないことに注意してください。 これは、 IBM MQ Operator では、Advanced Message Security に独自の鍵ストアを直接指定することはできないためです。		使用可能ですが、サポートされていません。		IBM MQ ソフトウェアによってサポートされますが、使用可能なサンプルはありません。
機能: Managed File Transfer	使用不可で、サポートされていません。 ただし、IBM MQ Operator を使用して、1 つ以上の調整キュー・マネージャー、コマンド・キュー・マネージャー、またはエージェント・キュー・マネージャーを提供することができます。			使用不可で、サポートされていません。	エージェント用の サンプル を使用して、 IBM MQ ソフトウェアに従ってサポートされます。

[1] IBM MQ Operator は、 IBM MQ CD リリースとして、または IBM Cloud Pak for Integration - Support Cycle 2 (formerly Long Term Support) リリースとしてサポートされます。

- IBM MQ Operator 3.2.x を使用してデプロイされた IBM MQ 9.4.0.x コンテナー・イメージは、 IBM Cloud Pak for Integration 16.1.0 の一部として使用される場合、CP4I-LTS サポートの対象となります。 IBM MQ Operator の最新の Support Cycle 2 (SC2) リリースは 3.2.1 であり、最新の SC2 コンテナー・イメージは 9.4.0.0-r1 です。
- IBM MQ Operator 3.2.x を使用してデプロイされた IBM MQ 9.4.0.x コンテナー・イメージは、 IBM Cloud Pak for Integration 16.1.0 の一部として使用される場合、 CD サポートの対象となります。 IBM MQ Operator の最新の Continuous Delivery (CD) リリースは 3.2.1 であり、最新の CD コンテナー・イメージは 9.4.0.0-r1 です。

	IBM MQ Operator および IBM Cloud Pak for Integration ライセンスの使用	**IBM MQ Operator および IBM MQ Advanced ライセンスの使用**	**IBM MQ Operator および IBM MQ Advanced for Developers ライセンスの使用**	**事前作成 IBM MQ Advanced for Developers イメージ**	**Build-your-own コンテナー**
機能: MQTT	使用不可で、サポートされていません。				IBM MQ ソフトウェアによってサポートされますが、使用可能なサンプルはありません。
機能: AMQP	使用不可で、サポートされていません。				IBM MQ ソフトウェアによってサポートされますが、使用可能なサンプルはありません。
機能: REST API	使用可能で、サポートされています。				IBM MQ ソフトウェアによって提供され、サポートされます。
機能: 複製データ・キュー・マネージャー	使用不可で、サポートされていません。 複製データ・キュー・マネージャー (RDQM) は、 Linux カーネルと密結合されており、コンテナーではサポートされません。				
機能: ネイティブ HA	使用可能で、サポートされています。		使用可能ですが、サポートされていません。		Kubernetes および Red Hat OpenShift Container Platform でのみ使用可能です。 IBM MQ ソフトウェアに従ってサポートされます。
機能: 複数インスタンス・キュー・マネージャー	使用可能で、サポートされています。		使用可能ですが、サポートされていません。		IBM MQ ソフトウェアによって提供され、サポートされます。
機能: リカバリー・ログのタイプ	循環ロギングまたは複製ログのみ。 リニア・ロギングはサポートされていません。				IBM MQ ソフトウェアによって提供され、サポートされます。 **crtmqm** オプションを構成する必要があります。

	IBM MQ Operator および IBM Cloud Pak for Integration ライセンスの使用	IBM MQ Operator および IBM MQ Advanced ライセンスの使用	IBM MQ Operator および IBM MQ Advanced for Developers ライセンスの使用	事前作成 IBM MQ Advanced for Developers イメージ	Build-your-own コンテナー
機能: `crtmqdir`、`crtmqm`、`strmqm` 、および `endmqm` のカスタム・コマンド行オプションの指定	使用不可で、サポートされていません。 ほとんどのオプションは INI ファイルを使用して構成できますが、リニア・ロギングの使用など、一部のオプションは構成できません。				オプション。 コンテナー使用可能化コードの実装方法によって異なります。
機能: オペレーティング・システム (OS) ユーザー	使用不可で、サポートされていません。				RPM を使用して IBM MQ をインストールしたが、使用可能なサンプルがない場合は、 IBM MQ ソフトウェアによって可能となり、サポートされます。 セキュリティー・リスクのため、推奨されません。

注 : 「supported as per IBM MQ software」という表現は、 IBM 技術サポートが、コンテナー内で実行されているコア IBM MQ ソフトウェアに制限されていることを意味します。

関連概念

IBM MQ FAQ for Long Term Support and Continuous Delivery リリース

関連資料

IBM Cloud Pak for Integration ソフトウェア・サポート・ライフサイクルの補足

OpenShift CP4I CP4I-SC2 CD IBM MQ Operator のバージョン・サポート

IBM MQ、OpenShift Container Platform および IBM Cloud Pak for Integration のサポート対象バージョンの対応関係。

- 14 ページの『使用可能な IBM MQ のバージョン』
- 14 ページの『互換性のある Red Hat OpenShift Container Platform のバージョン』
- 14 ページの『IBM Cloud Pak for Integration のバージョン』
- 14 ページの『以前ので使用可能な IBM MQ バージョン』
- 14 ページの『以前のオペレーターの互換性のある OpenShift Container Platform バージョン』

使用可能な IBM MQ のバージョン

オペレーター・チャネル	Operator バージョン	IBM MQ のバージョン						
		9.4.0	9.3.5	9.3.4	9.3.3	9.3.2	9.3.1	9.3.0
v32-sc2	3.2	CD および SC2	DEP	DEP	DEP	DEP	DEP	MIG

キー

- CD: Continuous Delivery サポートが使用可能です。
- SC2: IBM Cloud Pak for Integration - Support Cycle 2 (formerly Long Term Support) が使用可能です。
- MIG: IBM Cloud Pak for Integration - Support Cycle 2 (formerly Long Term Support) オペランドから Continuous Delivery オペランドへのマイグレーション時にのみ使用可能です。
- DEP: Deprecated 非推奨。 IBM MQ リリースがサポートから外れると、それらのリリースは引き続きオペレーターで構成可能になる可能性がありますが、サポートには適格ではなくなり、将来のリリースで除去される可能性があります。

各バージョンの詳細機能、変更点、フィックスなど、各バージョンの全詳細については、5 ページの『IBM MQ Operator のリリース履歴』を参照してください。

互換性のある Red Hat OpenShift Container Platform のバージョン

オペレーター・チャネル	Operator バージョン	OpenShift Container Platform のバージョン [2]		
		4.15	4.14	4.12
v3.2-sc2	3.2.0 以降	SC2	SC2	SC2

キー

- CD: Continuous Delivery サポートが使用可能です。
- SC2: IBM Cloud Pak for Integration - Support Cycle 2 (formerly Long Term Support) が使用可能です。
- EOS: サポートされなくなりました。 より新しい OpenShift Container Platform バージョンにマイグレーションしてください。

IBM Cloud Pak for Integration のバージョン

IBM Cloud Pak for Integration バージョン 16.1.0 の一部として、または単独での使用がサポートされます。

- IBM MQ Operator 3.2.x

以前ので使用可能な IBM MQ バージョン

IBM MQ 9.3 資料の 使用可能な IBM MQ バージョン を参照してください。

以前のオペレーターの互換性のある OpenShift Container Platform バージョン

IBM MQ 9.3 資料の 互換性のある OpenShift Container Platform バージョン を参照してください。

OpenShift MQ Adv. IBM MQ Operator によって作成されたリソースの編集

IBM MQ Operator は、ネイティブ Kubernetes リソースを作成および管理することによって、QueueManager カスタム・リソースを調整します。 これらの管理対象リソースを直接編集しては **なりません**。

[2] OpenShift Container Platform のバージョンは、それぞれのサポート日に影響を受けます。 詳しくは、OpenShift Container Platform ライフ・サイクル・ポリシー を参照してください。

通常、 ownerReferences を調べることによって、あるリソースが別の上位レベルのリソースによって所有されているかどうかを判別できます。 例えば、 StatefulSet から取得された以下のメタデータは、それが QueueManager リソース「qm1」によって所有されていることを示しています。

```
metadata:
  ownerReferences:
    - apiVersion: mq.ibm.com/v1beta1
      kind: QueueManager
      name: qm1
      uid: 60fda34c-9f7c-42d2-a293-78fec4315c62
      controller: true
      blockOwnerDeletion: true
```

すべてのリソースにこのメタデータがあるわけではないことに注意してください。

基礎となるリソース (StatefulSet、 Service 、 Route など) を管理するのは、 IBM MQ Operator の責任です。 これらの基礎となるリソースのいずれかを変更すると、 IBM MQ Operator はそれらを元に戻し、その変更にローリング更新が必要な場合はダウン時間が発生する可能性があります。

キュー・マネージャーの重要な設定のほとんどは、 QueueManager リソースで使用可能です。 ただし、基礎となるリソースを完全に制御する必要がある場合は、いくつかのオプションがあります。

- IBM MQ Operator によって作成されたポッドの設定をオーバーライドする必要がある場合は、 QueueManager YAML の .spec.template セクションにポッド・オーバーライド・テンプレートを追加できます。
- IBM MQ Operator によって作成されたキュー・マネージャー Route の設定をオーバーライドする必要がある場合は、経路全体で .spec.route.enabled 設定を「false」に設定してから、独自の経路を作成する必要があります。
- ラベルやアノテーションなどの設定や、 security Context などの Pod 設定は、すべて QueueManager リソースで設定できます。
- また、完全な制御が必要な場合は、 IBM MQ Operator がお客様のユース・ケースに適していないことがあります。

コンテナーでの IBM MQ のライセンス交付の計画

コンテナー・ライセンスにより、コンテナーが実行されているサーバー全体のライセンス交付を必要とするのではなく、個々の IBM MQ コンテナーの使用可能な容量のみのライセンス交付を受けることができます。 コンテナー・ライセンスを利用するには、IBM License Service を使用してライセンス使用状況を追跡し、必要なライセンスを判別する必要があります。

関連資料

163 ページの『独自の IBM MQ コンテナー・イメージを作成する時のライセンス・アノテーション』
ライセンス・アノテーションを使用すると、基礎になっているマシンではなくコンテナーで定義した制限に基づいて使用量を追跡管理できます。 クライアントで特定のアノテーションを付けてコンテナーをデプロイするための構成を行うと、IBM License Service はそのアノテーションに基づいて使用量を追跡管理します。

関連情報

IBM コンテナー・ライセンス

コンテナーのライセンス交付に関する FAQ

ライセンス・サービスのインストール

ライセンス使用の表示および追跡

OpenShift CP4I Kubernetes IBM MQ Operator のストレージの計画

IBM MQ Operator は、次の 2 つのストレージ・モードで稼働します。

- **一時ストレージ**は、コンテナーの再始動時にコンテナーのすべての状態情報を破棄してよい場合に使用します。 これは、デモンストレーション用の環境を作成する場合や、スタンドアロンのキュー・マネージャーを使用して開発する場合によく使用されます。

- **永続ストレージ**は IBM MQ の一般的な構成であり、コンテナーが再始動されても、既存の構成、ログ、永続メッセージを再始動後のコンテナーで使用することができます。

IBM MQ Operator は、環境によってかなり異なるものになることがあるストレージ特性と、必要なストレージ・モードをカスタマイズする機能を備えています。

一時ストレージ

IBM MQ はステートフル・アプリケーションであるため、再始動時にリカバリーできるように、自身の状態をストレージに保存します。 一時ストレージを使用している場合は、キュー・マネージャーのすべての状態情報が再始動時に失われます。 これには、以下が含まれます。

- すべてのメッセージ
- すべてのキュー・マネージャー間通信の状態 (チャネルのメッセージ・シーケンス番号)
- キュー・マネージャーの MQ クラスター ID
- すべてのトランザクション状態
- すべてのキュー・マネージャー構成
- ローカルにあるすべての診断データ

このため、実稼働、テスト、または開発のシナリオにとって一時ストレージが適したアプローチであるかどうか検討する必要があります。 例えば、すべてのメッセージが非永続メッセージであると認識され、キュー・マネージャーが MQ クラスターのメンバーでない場合は、 再始動時にすべてのメッセージング状態が廃棄されるだけでなく、キュー・マネージャーの構成も廃棄されます。 完全に一時的であるコンテナーを有効にするには、コンテナー・イメージ自体に IBM MQ 構成を追加する必要があります (詳しくは、93 ページの『Red Hat OpenShift CLI を使用した、カスタム MQSC および INI ファイルを使用したイメージの作成』を参照してください)。 これを行わない場合は、コンテナーが再始動するたびに IBM MQ を構成する必要があります。

OpenShift CP4I 例えば、IBM MQ に一時ストレージを構成するには、`QueueManager` のストレージ・タイプに以下を指定する必要があります。

```
queueManager:
  storage:
    queueManager:
      type: ephemeral
```

永続ストレージ

OpenShift CP4I

IBM MQ は通常、永続ストレージを使用して実行され、キュー・マネージャーが再始動後も永続メッセージと構成を保持するようにします。 これはデフォルトの動作です。 さまざまなストレージ・プロバイダーがあり、それぞれが異なる機能をサポートしているため、多くの場合、構成のカスタマイズが必要になります。 以下の例は、 v1beta1 API の IBM MQ ストレージ構成をカスタマイズする共通フィールドの概要を示しています。

- **spec.queueManager.availability** は、可用性モードを制御します。 `SingleInstance` または `NativeHA` を使用している場合は、 `ReadWriteOnce` ストレージのみが必要です。 `multiInstance` には、正しいファイル・ロック特性を持つ `ReadWriteMany` をサポートするストレージ・クラスが必要です。 IBM MQ は、サポートに関するステートメントとテストに関するステートメントを提示しています。 可用性モードは、永続ボリュームのレイアウトにも影響します。 詳しくは、17 ページの『コンテナー内の IBM MQ の高可用性の計画』を参照してください。
- **spec.queueManager.storage** は、個々のストレージ設定を制御します。 キュー・マネージャーは、1 つから 4 つの永続ボリュームを使用するように構成できます。

次の例は、単一インスタンスのキュー・マネージャーを使用する単純な構成のスニペットを示しています。

```
spec:
  queueManager:
    storage:
```

```
      queueManager:
        enabled: true
```

次の例は、マルチインスタンスのキュー・マネージャー構成のスニペットを示しており、デフォルトではないストレージ・クラスを指定し、補助グループを必要とするファイル・ストレージを指定しています。

```
spec:
  queueManager:
    availability:
      type: MultiInstance
    storage:
      queueManager:
         class: ibmc-file-gold-gid
      persistedData:
        enabled: true
        class: ibmc-file-gold-gid
      recoveryLogs:
        enabled: true
        class: ibmc-file-gold-gid
  securityContext:
    supplementalGroups: [65534] # Change to 99 for clusters with RHEL7 or earlier worker nodes
```

ネイティブ HA キュー・マネージャーのストレージに関する考慮事項については、19 ページの『ネイティブ HA』を参照してください。

注: また、単一インスタンス・キュー・マネージャーを使用して、補足グループを構成することもできます。

ストレージ容量

OpenShift CP4I

IBM MQ Operator を使用する場合は、継続的なニーズに十分な大きさのボリュームを要求するようにしてください。 ただし、1 つ以上のボリュームのストレージ容量を増やす必要がある場合、ご使用のストレージ・クラスがボリューム拡張をサポートしていれば、これらのボリュームを拡張することができます。 ボリュームは、オンラインまたはオフラインのいずれかの手順で拡張できます。 オフライン手順では QueueManager ポッドを再始動する必要がありますが、オンライン手順では再始動する必要はありません。 ご使用のストレージ・クラスがボリューム拡張をサポートしているかどうか、およびボリューム拡張がどの手順に従うかを判別するには、ご使用のストレージ・プロバイダーの資料を参照してください。 ストレージ・クラスを選択する際には、この情報を考慮する必要があります。 ボリューム拡張のガイドについては、100 ページの『永続ボリュームの拡張』を参照してください。

暗号化

OpenShift CP4I

IBM MQ は、保存データをアクティブに暗号化しません。 したがって、メッセージを暗号化するには、パッシブに暗号化されたストレージまたは IBM MQ Advanced Message Security、あるいはその両方を使用する必要があります。 IBM Cloud® では、ブロック・ストレージとファイル・ストレージの両方で、保存時にパッシブ暗号化を使用できます。

OpenShift Kubernetes コンテナー内の IBM MQ の高可用性の計画

IBM MQ Operator での高可用性には 3 つの選択肢があります。 **ネイティブ HA キュー・マネージャー** (アクティブなレプリカと 2 つのスタンバイ・レプリカを持つ)、 **複数インスタンス・キュー・マネージャー** (共有ネットワーク・ファイル・システムを使用するアクティブ/スタンバイ・ペア)、または **単一回復力キュー・マネージャー** (ネットワーク・ストレージを使用する HA の単純なアプローチを提供する) です。 後者の 2 つは、リカバリー可能データを確実に使用できるかどうかは、ファイル・システムが鍵を握りますが、ネイティブ HA ではそうではありません。 そのため、ネイティブ HA を使用しない場合、ファイル・システムの可用性はキュー・マネージャーの可用性にとって非常に重要となります。 データ・リカバリーが重要となる場合は、複製を行ってファイル・システムの冗長性を確保する必要があります。

メッセージの可用性と**サービス**の可用性は分けて考える必要があります。 IBM MQ for Multiplatforms を使用する場合、メッセージは厳密に 1 つのキュー・マネージャーに保管されます。 そのため、そのキュー・マネージャーが使用不可になると、その中に保管されているメッセージに一時的にアクセスできなくなり

ます。 メッセージの可用性を高めるためには、できるだけ速やかにキュー・マネージャーを復旧できなければなりません。 サービスの可用性を高めるには、IBM MQ 均一クラスターを使用するなど、クライアント・アプリケーションが使用するキューのインスタンスを複数用意しておくことができます。

キュー・マネージャーは、ディスク上に保管されるデータとそのデータへのアクセスを可能にする実行プロセスの 2 つの部分に分けて考えることができます。 キュー・マネージャーは、同じデータ (Kubernetes Persistent Volumes によって提供されたもの) を保持し、クライアント・アプリケーションによってネットワーク上で引き続きアドレス可能である限り、別の Kubernetes ノードに移動することができます。 Kubernetes では、ネットワークにおける同一性を維持するために 1 つのサービスが一貫して使用されます。

IBM MQ は、永続ボリュームのデータの可用性に依存しています。 このため、IBM MQ の可用性は使用するストレージの可用性を上回ることができないので、永続ボリュームを提供するストレージの可用性はキュー・マネージャーの可用性にとって非常に重要となります。 可用性ゾーン全体の障害を許容する場合は、ディスク書き込みを別のゾーンに複製するボリューム・プロバイダーを使用することが必要です。

ネイティブ HA キュー・マネージャー

MQ Adv.

ネイティブ HA キュー・マネージャーには、1 つの **アクティブ** と 2 つの **レプリカ** Kubernetes ポッドが含まれます。これらのポッドは、 Kubernetes StatefulSet の一部として実行され、それぞれに独自の Kubernetes 永続ボリューム・セットを持つ正確に 3 つのレプリカが含まれます。 ネイティブ HA キュー・マネージャーを使用する場合、IBM MQ での共有ファイル・システムの要件も適用されますが (リース・ベースのロックを除く)、共有ファイル・システムを使用する必要はありません。 上部に適切なファイル・システムを配置することで、ブロック・ストレージを使用できます。 例えば、*xfs* や *ext4* を配置します。 ネイティブ HA キュー・マネージャーが復旧に要する時間は、以下の要因によって左右されます。

1. アクティブ・インスタンスに障害が発生したことをレプリカ・インスタンスが検出するのにどれほどの時間がかかるか。 これは構成可能です。
2. 作動可能コンテナーが変更されてネットワーク・トラフィックがリダイレクトされたことを Kubernetes ポッドの Readiness Probe が検出するまでにかかる時間。 これは構成可能です。
3. IBM MQ クライアントが再接続するまでにかかる時間。

詳細については、19 ページの『ネイティブ HA』を参照してください。

複数インスタンス・キュー・マネージャー

複数インスタンス・キュー・マネージャーには**アクティブ**で**スタンバイ状態の** Kubernetes ポッドが必要で、これらは厳密に 2 つのレプリカと Kubernetes 永続ボリューム一式と共に Kubernetes ステートフル・セットの一部として稼働します。 キュー・マネージャーのトランザクション・ログとトランザクション・データは、共用ファイル・システムを使用して、2 つの永続ボリュームに保管されます。

複数インスタンス・キュー・マネージャーには、永続ボリュームへの同時アクセスを可能にするために、**アクティブな**ポッドと**スタンバイ状態の**ポッドの両方が必要です。 これを構成するには、 **access mode** を ReadWriteMany に設定した Kubernetes 永続ボリュームを使用します。 これらのボリュームは、IBM MQ の共有ファイル・システムの要件も満たしていなければなりません。IBM MQ がキュー・マネージャー・フェイルオーバーの実施をファイル・ロックの自動解除に依存しているからです。 IBM MQ はテスト対象ファイル・システムのリストを作成します。

複数インスタンス・キュー・マネージャーが復旧に要する時間は、以下の要因によって左右されます。

1. 障害が発生した後、もともとアクティブ・インスタンスによって実行されたロックを共用ファイル・システムが解除するためにかかる時間。
2. スタンバイ状態のインスタンスがロックを取得してから起動するまでにかかる時間。
3. 作動可能コンテナーが変更されてネットワーク・トラフィックがリダイレクトされたことを Kubernetes ポッドの Readiness Probe が検出するまでにかかる時間。 これは構成可能です。
4. IBM MQ クライアントが再接続するまでにかかる時間。

シングル・レジリエント・キュー・マネージャー

シングル・レジリエント・キュー・マネージャーは、1 つの Kubernetes ポッド内で実行されるキュー・マネージャーの単一のインスタンスのことで、ここで Kubernetes はキュー・マネージャーをモニタリングし、必要に応じてこのポッドを置き換えます。

シングル・レジリエント・キュー・マネージャーを使用する場合、IBM MQ での共有ファイル・システムの要件も適用されますが (リース・ベースのロックを除く)、共有ファイル・システムを使用する必要はありません。 上部に適切なファイル・システムを配置することで、ブロック・ストレージを使用できます。 例えば、 *xfs* や *ext4* を配置します。

シングル・レジリエント・キュー・マネージャーが復旧に要する時間は、以下の要因によって左右されます。

1. Liveness プローブの実行にかかる時間、および Liveness プローブが許容する失敗の数。 これは構成可能です。
2. Kubernetes スケジューラーが失敗したポッドを新規ノードに再スケジュールするためにかかる時間。
3. コンテナー・イメージを新規ノードにダウンロードするためにかかる時間。 `IfNotPresent` に **imagePullPolicy** 値を使用している場合は、すでにそのノードで画像が利用可能になっている可能性があります。
4. 新規キュー・マネージャー・インスタンスが起動するのにかかる時間。
5. コンテナーが作動可能であることを Kubernetes ポッドの Readiness Probe が検出するまでにかかる時間。 これは構成可能です。
6. IBM MQ クライアントが再接続するまでにかかる時間。

重要 :

シングル・レジリエント・キュー・マネージャー・パターンにはいくつかの利点がありますが、ノードの障害に関連した制限がある状態で、目標とする可用性に達するかどうかについて十分に理解しておく必要があります。

Kubernetes では、障害が発生したポッドは通常迅速に復旧しますが、ノード全体で障害が発生した場合は対応が異なります。 IBM MQ のようなステートフル・ワークロードを Kubernetes StatefulSet で使用する場合、 Kubernetes マスター・ノードは、ワーカー・ノードとの接続を失うと、ノードに障害が発生したかどうか、または単にネットワーク接続が失われたかどうかを判別できません。 そのため、このような場合、次のいずれかのイベントが発生するまで、Kubernetes は**何も対応しません**。

1. ワーカー・ノードが Kubernetes マスター・ノードと通信できる状態に復旧する。
2. 管理上の処置として、Kubernetes マスター・ノード上のポッドを明示的に削除する。 この場合、必ずしもポッドの実行を停止するわけではなく、単に Kubernetes ストアから削除します。 したがって、この管理上の処置は慎重に行う必要があります。

注 : IBM MQ Operator を使用してキュー・マネージャーを作成する場合、 IBM MQ キュー・マネージャーの StatefulSet の詳細 (レプリカの数を含む) の変更はサポートされません。

関連概念

高可用性の構成

関連タスク

75 ページの『IBM MQ Operator を使用したキュー・マネージャーの高可用性の構成』

CP4I MQ Adv. ネイティブ HA

ネイティブ HA は、IBM MQ 用のネイティブ (組み込み) 高可用性ソリューションであり、クラウド・ブロック・ストレージで使用するときに適しています。

ネイティブ HA 構成によって、高可用性キュー・マネージャーを実行できます。このキュー・マネージャーは、リカバリー可能な MQ データ (メッセージなど) のレプリケーションをストレージの複数セットにまたがって行うことにより、ストレージの障害によるデータの損失を防ぎます。 このキュー・マネージャーには実行中のインスタンスが複数あり、そのうちの 1 つがリーダーになります。他のキュー・マネージャー

は、障害発生時にすぐにテークオーバーできるように準備を整えているので、キュー・マネージャーとメッセージへのアクセスが最大化されます。

ネイティブ HA 構成は、3 つの Kubernetes ポッドから成り、その個々にキュー・マネージャーのインスタンスがあります。 1 つのインスタンスがアクティブ・キュー・マネージャーとして機能し、メッセージはそこで処理されてリカバリー・ログに書き込まれます。 そのリカバリー・ログへの書き込みが行われると、アクティブ・キュー・マネージャーはレプリカと呼ばれる他の 2 つのインスタンスにデータを送信します。 各レプリカは、個別に所有するリカバリー・ログへの書き込みを行い、データを認知し、複製されたリカバリー・ログからキュー・データをそれぞれ更新します。 アクティブ・キュー・マネージャーを実行しているポッドに障害が発生すると、キュー・マネージャーのレプリカ・インスタンスの 1 つがアクティブの役割を引き継ぎ、このインスタンスにある最新データで運用が行われます。

ログ・タイプは「複製ログ」と呼ばれます。 複製されたログは基本的にリニア・ログであり、自動ログ管理と自動メディア・イメージが有効になっています。 ログのタイプを参照してください。 リニア・ログの管理に使用するものと同じ手法を使用して、複製されたログを管理します。

ネットワーク・トラフィックを扱う準備ができている唯一のポッドであると識別された現行アクティブ・インスタンスに TCP/IP クライアント接続をルーティングするために、Kubernetes サービスが使用されます。 この処理を行うために、クライアント・アプリケーションがさまざまなインスタンスを認識しておく必要はありません。

3 つのポッドを使用すると、スプリット・ブレーンという状態になる可能性が大幅に減少します。 2 ポッドの高可用性システムでは、2 つのポッド間の接続が切断されるとスプリット・ブレーンが発生する可能性があります。 接続のない状態だと、両方のポッドでキュー・マネージャーが同時に実行され、別々のデータが累積される可能性があります。 そうなると、接続が復元された時に 2 つの別々のバージョンのデータ (「スプリット・ブレーン」) が存在することになるので、保持するデータ・セットと破棄するデータ・セットを決定するために手操作による介入が必要になります。

ネイティブ HA では、スプリット・ブレーン状態を回避するために、クォーラムを設定した 3 ポッド・システムを使用します。 1 つのポッドが他の 1 つ以上のポッドと通信できる場合は、その通信可能なポッド同士がクォーラムを形成します。 キュー・マネージャーは、クォーラムを形成するポッド上にある場合にのみ、アクティブ・インスタンスになることができます。 キュー・マネージャーは、他の 1 つ以上のポッドと接続していないポッド上ではアクティブになることはできないので、2 つのアクティブ・インスタンスが同時に存在することは絶対にありません。

- 1 つのポッドで障害が発生しても、他の 2 つのポッドのいずれかにあるキュー・マネージャーが引き継ぐことができます。 2 つのポッドで障害が発生すると、残りの 1 つのポッドにあるキュー・マネージャーはアクティブ・インスタンスになることができません。そのポッドはクォーラムを形成していないからです (その残りのポッドは、他の 2 つのポッドで障害が発生したのか、それとも自分の接続が失われていて他の 2 つのポッドはまだ実行されているのかの違いを判別できません)。
- 1 つのポッドが接続を失うと、そのポッドにあるキュー・マネージャーはアクティブになることができません。そのポッドはクォーラムを形成していないからです。 残りの 2 つのポッドでは、いずれか 1 つのキュー・マネージャーが引き継ぎを実行できます。クォーラムを形成しているからです。 すべてのポッドが接続を失うと、どのポッドのキュー・マネージャーもアクティブになることができません。どのポッドもクォーラムを形成していないからです。

アクティブ・ポッドに障害が発生し、その後復旧すると、レプリカの役割でグループに再参加することができます。

パフォーマンスと信頼性のために、ネイティブ HA 構成では RWO (ReadWriteOnce) 永続ストレージを使用することをお勧めします。 すべてのストレージ・プロバイダーからの RWO ボリュームは、以下の条件を満たしている場合にサポートされます。

- ブロック・ストレージ・プロバイダーから取得されます。
- ext4 または XFS としてフォーマットされます (これにより、 POSIX 準拠が保証されます)。
- 動的ボリューム・プロビジョニングと「volumeBinding モード: WaitForFirstConsumer」をサポートします。

以下のプロバイダーは、明示的に禁止されています。

- NFS
- GlusterFS

- その他の非ブロック・プロバイダー。

以下の図に、1 つのキュー・マネージャーの 3 つのインスタンスが 3 つのコンテナー内にデプロイされている、標準的なデプロイメントを示します。

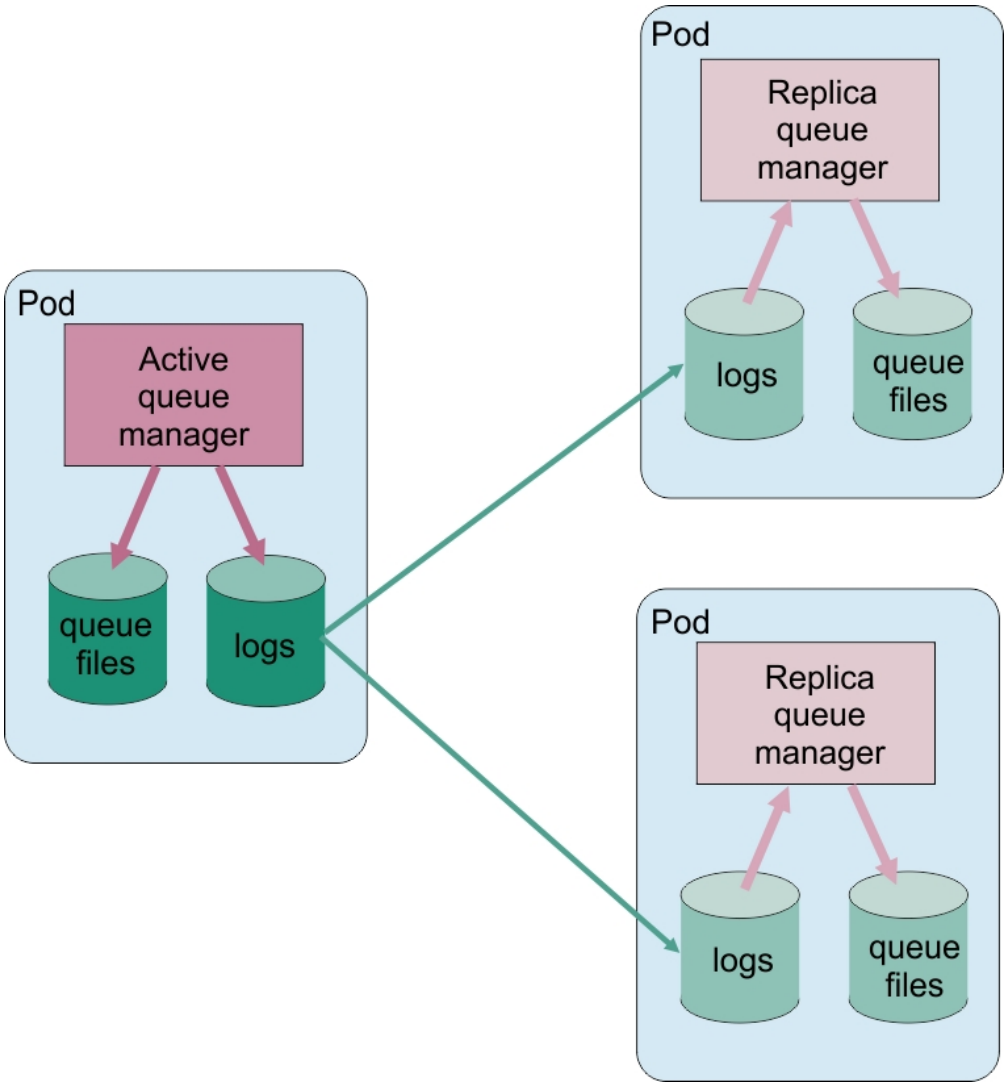


図 *1.* ネイティブ *HA* 構成の例

MQ Adv. ネイティブ HA キュー・マネージャーの独自ローリング更新を実行する場合の考慮事項

ネイティブ HA キュー・マネージャーの IBM MQ バージョンまたはポッド仕様を更新する場合は、キュー・マネージャー・インスタンスのローリング更新を実行する必要があります。 これは IBM MQ Operator によって自動的に処理されますが、独自のデプロイメント・コードを作成する場合は、いくつかの重要な考慮事項があります。

注 : サンプル Helm チャートには、ローリング更新を実行するためのシェル・スクリプトが含まれていますが、このスクリプトは、このトピックにおける考慮事項には対応していないため、実動での使用には適し**ていません**。

Kubernetes Kubernetes では、`StatefulSet` リソースは、順序付けられた始動およびローリング更新を管理するために使用されます。 始動手順の一環として、各ポッドを個別に開始し、そのポッドが作動可能になるまで待ってから、次のポッドに移動します。 すべてのポッドを開始してリーダー選出を実行できるようにする必要があるため、これはネイティブ HA では機能しません。 したがって、`.spec.podManagementPolicy` フィールド (`StatefulSet` 上) を `Parallel` に設定する必要があり

ます。 これはすべてのポッドが並行して更新されることも意味しますが、これは特に望ましくありません。 このため、 StatefulSet は OnDelete 更新方針も使用する必要があります。

StatefulSet ローリング更新コードを使用できないため、カスタム・ローリング更新コードが必要になります。以下の点を考慮してください。

- 一般的なローリング更新手順
- 最適な順序でポッドを更新することによるダウン時間の最小化
- クラスター状態の変更を処理
- エラーの処理
- タイミングの問題を処理

一般的なローリング更新手順

ローリング更新コードは、各インスタンスが REPLICA の状況を dspmq から示すまで待ちます。 つまり、インスタンスは何らかのレベルの始動を行った (例えば、コンテナーが開始され、MQ プロセスが実行されている) が、必ずしもその他のインスタンスと対話するようにはなっていません。 例えば、ポッド A が再始動され、 REPLICA 状態になるとすぐにポッド B が再始動されます。 ポッド B は新しい構成で開始されると、ポッド A と対話できるようになり、クォーラムを形成できます。A または B のいずれかが新しいアクティブ・インスタンスになります。

その一環として、各ポッドが REPLICA 状態になった後に遅延を設定して、そのポッドがピアに接続してクォーラムを確立できるようにすると便利です。

最適な順序でポッドを更新することによるダウン時間の最小化

ローリング更新コードは、既知のエラー状態にあるポッドから、正常に開始されなかったポッドまで、一度に 1 つずつポッドを削除する必要があります。 通常、アクティブなキュー・マネージャー・ポッドは最後に更新する必要があります。

また、前回の更新でポッドが既知のエラー状態になった場合は、ポッドの削除を一時停止することも重要です。 これにより、すべてのポッドにわたって、中断された更新がロールアウトされなくなります。 例えば、これが行われる可能性があるのは、アクセスできない (または誤植が含まれる) 新しいコンテナー・イメージを使用するようにポッドが更新される場合です。

クラスター状態の変更を処理

ローリング更新コードは、クラスター状態のリアルタイム変更に適切に対応する必要があります。 例えば、キュー・マネージャーのポッドの 1 つが、ノード・リブートまたはノード圧力が原因で排除されることがあります。 排除されたポッドは、クラスターがビジーだと即時に再スケジュールされない可能性があります。 この場合、ローリング更新コードは、他のすべてのポッドを再始動する前に適切に待機する必要があります。

エラーの処理

ローリング更新コードは、Kubernetes API の呼び出し時や他の予期しないクラスター動作時の障害に対して堅牢でなければなりません。

さらに、ローリング更新コード自体は、再始動を許容できなければなりません。 ローリング更新は長時間実行される可能性があり、コードの再始動が必要になる可能性があります。

タイミングの問題を処理

ローリング更新コードは、ポッドが再始動したことを確認できるように、ポッドの更新改訂を検査する必要があります。 これにより、ポッドが「開始済み」であることを示していても実際はまだ終了していないというタイミングの問題が回避されます。

関連概念

8 ページの『コンテナー内の IBM MQ の使用方法の選択』

コンテナー内の IBM MQ の使用方法としては、いくつもの選択肢があります。プリパッケージされているコンテナー・イメージを使用する IBM MQ Operator を使用することも、独自のイメージとデプロイメント・コードをビルドすることもできます。

OpenShift CP4I Kubernetes コンテナー内の IBM MQ の災害復旧

どのような種類の災害に備えるのかを検討する必要があります。 クラウド環境では、複数のアベイラビリティー・ゾーンを使用すると、災害に対して一定レベルの耐障害性を確保できる上、利用方法も簡単です。奇数個のデータ・センター (クォーラムの場合) があり、ネットワーク・リンクの待ち時間が短い場合は、単一の Red Hat OpenShift Container Platform クラスターまたは Kubernetes クラスターを、別々の物理的な場所にある複数のアベイラビリティー・ゾーンで実行することもできます。 このトピックでは、これらの基準を満たすことができない場合 (つまり、データ・センターが偶数個の場合やネットワーク・リンクの待ち時間が長い場合) の災害復旧に関する考慮事項を説明します。

災害復旧では、以下の点を考慮する必要があります。

- 災害復旧ロケーションへの IBM MQ データ (1 つ以上の `PersistentVolume` リソースで保持されている) の複製
- 複製されたデータを使用してキュー・マネージャーを再作成すること
- IBM MQ クライアント・アプリケーションおよびその他のキュー・マネージャーに表示されるキュー・マネージャーのネットワーク ID。 例えば、この ID は DNS 項目になります。

永続データを災害復旧サイトに同期的または非同期的に複製する必要があります。 通常、これはストレージ・プロバイダーに固有ですが、`VolumeSnapshot` を使用して行うこともできます。 ボリュームのスナップショットについて詳しくは、CSI volume snapshots を参照してください。

災害から復旧する場合には、複製されたデータを使用して、新しい Kubernetes クラスター上でキュー・マネージャー・インスタンスを再作成する必要があります。 IBM MQ Operator を使用している場合は、`QueueManager` YAML が必要なほか、`ConfigMap` や `Secret` など、他のサポート・リソース用の YAML も必要になります。

関連情報

ha_for_ctr.dita

OpenShift CP4I コンテナー内の IBM MQ のセキュリティーの計画

コンテナー構成で IBM MQ を計画する際のセキュリティーに関する考慮事項。

手順

- 23 ページの『コンテナー内の IBM MQ でのユーザーの認証と許可』
  - 24 ページの『コンテナーでのオペレーティング・システム・ユーザーの使用に関するセキュリティー制約』
- 24 ページの『コンテナー内の IBM MQ へのネットワーク・トラフィックを制限する際の考慮事項』

コンテナー内の IBM MQ でのユーザーの認証と許可

コンテナー内の IBM MQ は、LDAP、相互 TLS、またはカスタム MQ プラグインを使用してユーザーを認証するように構成できます。

IBM MQ Operator では、コンテナー・イメージ内でのオペレーティング・システムのユーザーおよびグループの使用は許可されないことに注意してください。 詳細については、24 ページの『コンテナーでのオペレーティング・システム・ユーザーの使用に関するセキュリティー制約』を参照してください。

LDAP

LDAP ユーザー・リポジトリーを使用するように IBM MQ を構成する方法については、 接続認証: ユーザー・リポジトリー および LDAP 許可を参照してください。

相互 TLS

TLS 証明書 (相互 TLS) を必要とするようにキュー・マネージャーへの着信接続を構成する場合は、証明書の識別名をユーザー名にマップできます。 以下の 2 つのことを行う必要があります。

- SSLPEER を使用して、ユーザー名へのマッピングを作成するようにチャネル認証レコードを構成します。 詳しくは、 MCAUSER ユーザー ID への SSL または TLS 識別名のマッピングを参照してください。
- キュー・マネージャーを構成して、システムに認識されていないユーザー名の権限レコードを定義できるようにします。 詳しくは、 qm.ini ファイルの Service スタンザを参照してください。

JSON Web トークン

JSON Web トークン (JWT) を使用するように IBM MQ を構成する方法については、 認証トークンの処理を参照してください。

カスタム MQ プラグイン

これは高度な手法であり、さらに多くの作業を必要とします。 詳しくは、 カスタム許可サービスの使用を参照してください。

関連タスク

69 ページの『例: 相互 TLS 認証を使用したキュー・マネージャーの構成』
この例では、 IBM MQ Operator を使用して、キュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

コンテナーでのオペレーティング・システム・ユーザーの使用に関するセキュリティー制約

コンテナーでのオペレーティング・システム・ユーザーの使用は推奨されておらず、 IBM MQ Operator では禁止されています。

マルチテナントのコンテナー環境では、潜在的なセキュリティー問題を防ぐために、通常は以下の例のようなセキュリティー制約が適用されます。

- **コンテナー内での「root」ユーザーの使用の防止**
- **ランダム UID の使用の強制**。 例えば Red Hat OpenShift Container Platform では、`SecurityContextConstraints` のデフォルト (つまり `restricted`) を使用すると、コンテナーごとにランダムなユーザー ID が使用されます。
- **特権エスカレーションの使用の防止**。 IBM MQ on Linux は、特権エスカレーションを使用してユーザーのパスワードを検査します。つまり、「root」ユーザーになるために「setuid」プログラムを使用します。

OpenShift CP4I これらのセキュリティー手段に確実に準拠するために、 IBM MQ Operator は、コンテナー内のオペレーティング・システム・ライブラリーで定義されている ID の使用を許可しません。 コンテナー内に `mqm` というユーザー ID やグループは定義されていません。

コンテナー内の IBM MQ へのネットワーク・トラフィックを制限する際の考慮事項

OpenShift Container Platform および Kubernetes で、クラスター内のポッドへのトラフィックを制限するためのネットワーク・ポリシーを定義できます。 このトピックでは、ネットワーク・ポリシーを IBM MQ に適用する方法に関するいくつかの考慮事項について説明します。

キュー・マネージャーへのネットワーク入口の場合、考慮すべきポートがいくつかあります。

- キュー・マネージャー・トラフィック用のポート 1414
- ネイティブ HA 用のポート 9414
- メトリック用のポート 9157
- Web コンソールおよび REST API 用のポート 9443

ネットワーク出口はより複雑です。 考慮すべきネットワーク Egress の例を以下に示します。

- DNS-DNS 名を使用するチャネルまたはその他の構成がある場合
- 他のキュー・マネージャー
- Online Certificate Status Protocol (OCSP) および証明書失効リスト (CRL)-証明書プロバイダーによって決定されます。
- 認証プロバイダー:
  - LDAP
  - IBM MQ Web サーバー用の Open ID Connect またはその他の構成済みログイン・プロバイダー。 これには、 IBM Cloud Pak Keycloak が含まれます。
- トレース・プロバイダー:
  - IBM Instana

  注 : 以前のバージョンの IBM MQ では、 IBM Cloud Pak for Integration Operations Dashboard もトレース・プロバイダーとして使用できました。 ただし、Operations Dashboard は IBM MQ 9.3.3 CD および IBM MQ 9.4.0 LTS で削除されました。

Ingress NetworkPolicy の例

Red Hat OpenShift Container Platform で使用するために、「myqm」というキュー・マネージャーの Ingress を制御するネットワーク・ポリシーの例を以下に示します。

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: myqm
spec:
  podSelector:
    matchLabels:
      app.kubernetes.io/instance: myqm
      app.kubernetes.io/name: ibm-mq
  ingress:
    # Allow access to queue manager listener from anywhere
    - ports:
        - protocol: TCP
          port: 1414
    # Allow access to Native HA port from other instances of the same queue manager
    - from:
        - podSelector:
            matchLabels:
              app.kubernetes.io/instance: myqm
              app.kubernetes.io/name: ibm-mq
      ports:
        - protocol: TCP
          port: 9414
    # Allow access to metrics from monitoring project
    - from:
        - namespaceSelector:
            matchLabels:
              network.openshift.io/policy-group: monitoring
      ports:
        - protocol: TCP
          port: 9157
    # Allow access to web server via Route
    - from:
        - namespaceSelector:
            matchLabels:
              network.openshift.io/policy-group: ingress
      ports:
        - protocol: TCP
          port: 9443
```

コンテナー内の IBM MQ の FIPS 準拠

始動時に、コンテナー内の IBM MQ は、コンテナーが始動するオペレーティング・システムが FIPS に準拠しているかどうかを検出し、準拠している場合は、FIPS サポートを自動的に構成します。 ここでは、要件と制限について説明します。

連邦情報処理標準

米国政府は、データ暗号化など、IT システムおよびセキュリティーに関する技術的助言を行っています。 米国連邦情報・技術局 (NIST) は、IT システムとセキュリティーに関する政府機関です。 NIST は、連邦情報処理標準 (FIPS) などの勧告や規格を策定しています。

重要な FIPS 標準は FIPS 140-2 であり、強力な暗号アルゴリズムを使用する必要があります。 FIPS 140-2 では、転送中のパケットが変更されることを防ぐためにハッシュ・アルゴリズムを使用することも規定しています。

IBM MQ は、FIPS 140-2 サポートを提供します (そのように構成されている場合)。

注 : AIX®, Linux, and Windows では、 IBM MQ は IBM Crypto for C (ICC) 暗号モジュールを介して FIPS 140-2 準拠を提供します。 このモジュールの証明書は「履歴」ステータスに移動されました。 お客様は、IBM Crypto for C (ICC) 証明書 を表示し、NIST から提供されたアドバイスに注意する必要があります。 交換用の FIPS 140-3 モジュールが現在進行中であり、その状況を表示するには、 「NIST CMVP modules in process list」でそのモジュールを検索します。

IBM MQ Operator 3.2.0 およびキュー・マネージャー・コンテナー・イメージ 9.4.0.0 以降は、UBI 9 に基づいています。 FIPS 140-3 準拠は現在保留中であり、その状況を表示するには、 「NIST CMVP modules in process list」で「Red Hat Enterprise Linux 9- OpenSSL FIPS Provider」を検索します。

要件

クラスターのセットアップおよびその他の考慮事項に関連する要件については、 FIPS Wall: Current IBM approach to FIPS compliance を参照してください。

コンテナー内の IBM MQ は、FIPS 140-2 準拠モードで実行できます。 始動時に、コンテナー内の IBM MQ は、コンテナーが開始されているホスト・オペレーティング・システムが FIPS に準拠しているかどうかを検出します。 ホスト・オペレーティング・システムが FIPS 準拠であり、秘密鍵と証明書が提供されている場合、 IBM MQ コンテナーは、キュー・マネージャー、 IBM MQ Web サーバー、およびネイティブ高可用性デプロイメント内のノード間のデータ転送を FIPS 準拠モードで実行するように構成します。

IBM MQ Operator を使用してキュー・マネージャーをデプロイする場合、オペレーターは終了タイプ **Passthrough** の経路を作成します。 これは、ルーターが TLS 終端を提供することなく、トラフィックが宛先に直接送信されることを意味します。 この場合、IBM MQ キュー・マネージャーと IBM MQ Web サーバーは宛先であり、既に FIPS 準拠のセキュア通信を提供しています。

主な要件:

1. キュー・マネージャーおよび Web サーバーにシークレットで提供される秘密鍵および証明書。これにより、外部クライアントはキュー・マネージャーおよび Web サーバーに安全に接続できます。
2. ネイティブ高可用性構成内の異なるノード間でのデータ転送用の秘密鍵および証明書。

制限

コンテナー内の IBM MQ の FIPS 準拠デプロイメントの場合は、以下の点を考慮してください。

- コンテナー内の IBM MQ は、メトリックを収集するためのエンドポイントを提供します。 現在、このエンドポイントは HTTP のみです。 メトリック・エンドポイントをオフにして、残りの IBM MQ を FIPS 準拠にすることができます。
- コンテナー内の IBM MQ は、カスタム・イメージのオーバーライドを許可します。 つまり、 IBM MQ コンテナー・イメージをベース・イメージとして使用してカスタム・イメージをビルドできます。 FIPS 準拠は、このようなカスタマイズされたイメージには適用されない可能性があります。
- IBM Instana を使用したメッセージ・トラッキングの場合、 IBM MQ と IBM Instana の間の通信は HTTP または HTTPS であり、FIPS に準拠していません。
- IBM の ID およびアクセス管理 (IAM)/禅サービスへの IBM MQ Operator アクセスは、FIPS 準拠ではありません。

FIPS 準拠が検出され、*FIPS* サポートが自動的に構成される方法

コンテナーが開始されるオペレーティング・システムが FIPS 準拠である場合、FIPS サポートは自動的に構成されます。

注 : AIX, Linux, and Windows では、 IBM MQ は IBM Crypto for C (ICC) 暗号モジュールを介して FIPS 140-2 準拠を提供します。 このモジュールの証明書は「履歴」ステータスに移動されました。 お客様は、IBM Crypto for C (ICC) 証明書 を表示し、NIST から提供されたアドバイスに注意する必要があります。 交換用の FIPS 140-3 モジュールが現在進行中であり、その状況を表示するには、 「NIST CMVP modules in process list」でそのモジュールを検索します。

IBM MQ Operator 3.2.0 およびキュー・マネージャー・コンテナー・イメージ 9.4.0.0 以降は、UBI 9 に基づいています。 FIPS 140-3 準拠は現在保留中であり、その状況を表示するには、 「NIST CMVP modules in process list」で「Red Hat Enterprise Linux 9- OpenSSL FIPS Provider」を検索します。

始動時に、コンテナー内の IBM MQ は、コンテナーが開始されているオペレーティング・システムが FIPS に準拠しているかどうかを検出します。 その場合、以下のアクションが自動的に実行されます。

キュー・マネージャー
ホスト・オペレーティング・システムが FIPS に準拠しており、秘密鍵と証明書が提供されている場合、キュー・マネージャー属性 **SSLFIPS** は YES に設定されます。 それ以外の場合、 **SSLFIPS** 属性は NO に設定されます。

IBM MQ Web サーバー
IBM MQ Web サーバーは、 IBM MQ を管理するための HTTP/HTTPS インターフェースを提供します。 ホスト・オペレーティング・システムが FIPS 準拠の場合、Web サーバーが FIPS 準拠の暗号方式を使用するように JVM オプションが更新されます。 FIPS を使用できるようにするには、コンテナーの開始時に秘密鍵と証明書を指定する必要があります。

ネイティブ HA
ノード間で複製されるデータのセキュリティーは、qm.ini ファイルの **NativeHALocalInstance** スタンザによって制御されます。 以下に例を示します。

```
NativeHALocalInstance:
    KeyRepository=/run/runmqserver/ha/tls/key.kdb
    CertificateLabel=NHAQM
    CipherSpec=ECDHE_RSA_AES_256_GCM_SHA384
```

FIPS が有効になっている場合、**SSLFipsRequired** 属性がスタンザに追加され、値が Yes に設定されます。

```
NativeHALocalInstance:
    KeyRepository=/run/runmqserver/ha/tls/key.kdb
    CertificateLabel=NHAQM
    CipherSpec=ECDHE_RSA_AES_256_GCM_SHA384
    SSLFipsRequired=Yes
```

FIPS がサポートされていない OpenShift クラスターでコンテナーが実行されている場合、キュー・マネージャー、 IBM MQ Web サーバー、およびネイティブ HA コンポーネントでは、FIPS が自動的にサポートされません。 現在、FIPS 用の OpenShift プラットフォームでは、 x86-64 アーキテクチャーのみがサポートされています。 Power および Linux for IBM Z® アーキテクチャーの場合、 OpenShift は FIPS サポートを提供しません。 これらのアーキテクチャーの IBM MQ コンポーネントで FIPS サポートを明示的に有効にするには、キュー・マネージャー YAML で *MQ_ENABLE_FIPS* 環境変数を true に設定します。 以下の YAML スニペットは、 *MQ_ENABLE_FIPS* 環境変数の使用法を説明しています。

```
template:
    pod:
      containers:
        - env:
            - name: MQ_ENABLE_FIPS
              value: "true"
          name: qmgr
```

コンテナー内の *IBM MQ* の自動 *FIPS* モードのオーバーライド

コンテナー内の IBM MQ コンポーネントに対して FIPS モードを明示的に有効または無効にするには、環境変数 *MQ_ENABLE_FIPS* を使用します。

始める前に

注 : AIX, Linux, and Windows では、 IBM MQ は IBM Crypto for C (ICC) 暗号モジュールを介して FIPS 140-2 準拠を提供します。 このモジュールの証明書は「履歴」ステータスに移動されました。 お客様は、IBM Crypto for C (ICC) 証明書 を表示し、NIST から提供されたアドバイスに注意する必要があります。 交換用の FIPS 140-3 モジュールが現在進行中であり、その状況を表示するには、 「NIST CMVP modules in process list」 でそのモジュールを検索します。

IBM MQ Operator 3.2.0 およびキュー・マネージャー・コンテナー・イメージ 9.4.0.0 以降は、UBI 9 に基づいています。 FIPS 140-3 準拠は現在保留中であり、その状況を表示するには、 「NIST CMVP modules in process list」 で「Red Hat Enterprise Linux 9- OpenSSL FIPS Provider」を検索します。

このタスクについて

MQ_ENABLE_FIPS は、以下の 3 つの値をサポートします。

auto
これがデフォルト値です。

ホスト・オペレーティング・システムで FIPS が有効になっている場合は、すべてのコンポーネント (キュー・マネージャー、 IBM MQ Web サーバー、およびネイティブ HA) が FIPS モードで実行されます。

ホスト・オペレーティング・システムで FIPS が有効になっていない場合、すべてのコンポーネントが FIPS モードで実行されるわけではありません。

true
この値は、コンテナー内の選択されたコンポーネントに対して FIPS をオンにします。

コンテナー内の IBM MQ が FIPS 準拠でないホスト・オペレーティング・システムで実行されている場合でも、キュー・マネージャー属性 **SSLFIPS** は YES に設定されます。 つまり、 IBM MQ キュー・マネージャー、Web サーバー、およびネイティブ HA は FIPS 準拠ですが、コンテナーのオペレーティング・システムは FIPS 準拠ではありません。

false
この値は、FIPS 準拠をオフにします。

コンテナー内の IBM MQ が FIPS 準拠のホスト・マシンで実行されている場合でも、キュー・マネージャー属性 **SSLFIPS** は NO に設定されます。 ただし、秘密鍵と証明書が提供されている場合でも、 IBM MQ は接続を保護します。

IBM MQ Web サーバーの JVM オプションは更新されません。 ただし、秘密鍵と証明書が指定されている場合、 IBM MQ Web サーバーは引き続き HTTPS エンドポイントを実行します。

ネイティブ HA でのデータ複製では、FIPS 暗号化は使用されません。

例

キュー・マネージャー・コンポーネントの TLS および FIPS を有効にする方法を説明するサンプル・キュー・マネージャー YAML を以下に示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  namespace: ibm-mq-fips
  name: ibm-mq-qm-ppcle
spec:
  license:
    accept: true
    license: L-EHXT-MQCRN9
    use: Production
  queueManager:
    name: PPCLEQM
    storage:
      queueManager:
        type: ephemeral
  template:
    pod:
      containers:
        - env:
            - name: MQ_ENABLE_FIPS
              value: "true"
```

```
        name: qmgr
version: 9.4.0.0-r1
web:
  enabled: false
pki:
  keys:
    - name: ibm-mq-tls-certs
      secret:
        secretName: ibm-mq-tls-secret
        items:
        - tls.key
        - tls.crt
```

コンテナー内の IBM MQ のスケーラビリティーとパフォーマンスの計画

ほとんどの場合、コンテナー内の IBM MQ のスケーリングとパフォーマンスは、IBM MQ for Multiplatforms と同じです。 ただし、コンテナー・プラットフォームによって課される可能性がある追加の制限がいくつかあります。

このタスクについて

コンテナー内の IBM MQ のスケーラビリティーとパフォーマンスを計画する場合は、以下のオプションを考慮してください。

手順

- **スレッドおよびプロセスの数を制限します。**

  IBM MQ はスレッドを使用して並行性を管理します。 Linux では、スレッドはプロセスとして実装されるため、コンテナー・プラットフォームまたはオペレーティング・システムによって課される、プロセスの最大数に関する制限を検出することができます。 Red Hat OpenShift Container Platform 4.11 以降では、コンテナーごとに 4096 プロセスというデフォルトの制限があります。 これは大多数のシナリオに適していますが、キュー・マネージャーのクライアント接続の数に影響を与える可能性があります。

  Kubernetes のプロセス制限は、クラスター管理者が kubelet 構成設定 **podPidsLimit** を使用して構成できます。 Kubernetes 資料の プロセス ID の制限と予約 を参照してください。 Red Hat OpenShift Container Platform では、 **ContainerRuntimeConfig** カスタム・リソースを作成して CRI-O パラメーターを編集することもできます。

  IBM MQ 構成では、キュー・マネージャーのクライアント接続の最大数を設定することもできます。 個々のサーバー接続チャネルに制限を適用する場合は サーバー接続チャネルの制限 を、キュー・マネージャー全体に制限を適用する場合は MAXCHANNELS INI 属性 を参照してください。

- **ボリューム数を制限します。**

  クラウド・システムおよびコンテナー・システムでは、Network Attached Storage ボリュームが一般的に使用されます。 Linux ノードに接続できるボリュームの数には制限があります。 例えば、 AWS EC2 は、VM 当たりのボリューム数を 30 以下に制限します。 Red Hat OpenShift Container Platform 類似した制限がある(Microsoft Azure および Google Cloud Platform と同様)。

  ネイティブ HA キュー・マネージャーは、3 つのインスタンスごとに 1 つのボリュームを必要とし、インスタンスをノード間に分散させます。 ただし、インスタンスごとに 3 つのボリューム (キュー・マネージャー・データ、リカバリー・ログ、および永続データ) を使用するようにキュー・マネージャーを構成できます。

- **IBM MQ のスケーリング手法を使用します。**

  少数の大規模なキュー・マネージャーではなく、IBM MQ 均一クラスターなどの IBM MQ スケーリング手法を使用して、同じ構成で複数のキュー・マネージャーを実行することをお勧めします。 これにより、単一コンテナーの再始動 (例えば、コンテナー・プラットフォームの保守の一環として) の影響が軽減されるという利点が追加されます。

コンテナー内の IBM MQ 用の環境の準備、インストール、およびアップグレード

IBM MQ 用に環境を準備するために、さまざまなタスクを実行します。

このタスクについて

IBM MQ Operator を使用している場合は、オペレーターをインストールして Red Hat OpenShift Container Platform クラスターを準備します。 30 ページの『IBM MQ Operator のインストールおよびアップグレード』 を参照してください。

そうでない場合は、独自のコンテナー・イメージをビルドしてコンテナー環境を準備します。 55 ページの『独自のコンテナー・イメージのビルドによる IBM MQ の準備』を参照

IBM MQ Operator のインストールおよびアップグレード

IBM MQ Operator をインストール、アンインストール、およびアップグレードするには、さまざまなタスクを実行します。

このタスクについて

Red Hat OpenShift Container Platform での IBM MQ Operator のインストールおよびアップグレードを開始するには、以下のトピックを参照してください。

手順

OpenShift CP4I IBM MQ Operator の依存関係

IBM MQ Operator のインストール時に他のオペレーターが自動的にインストールされることはありません。

IBM Licensing Operator は、ライセンス使用量を追跡するために別個にインストールする必要があります。 IBM Cloud Pak for Integration 資料の License Service を参照してください。

IBM Cloud Pak for Integration ライセンスを使用して `QueueManager` を作成する場合、 Keycloak の IBM Cloud Pak for Integration インスタンスでシングル・サインオンを使用するかどうかを選択できます。 IBM Cloud Pak for Integration ライセンスでは、 Keycloak の使用はデフォルトで有効になっていますが、インストールされていない場合、 `QueueManager` は、正しい依存関係がインストールされるまで「ブロック」状態になります。 依存関係について詳しくは、 31 ページの『IBM MQ Operator のインストール』 を参照してください。

OpenShift CP4I IBM MQ Operator に必要なクラスター・スコープ許可

IBM MQ Operator には、アドミッション Webhook やサンプルを管理したり、ストレージ・クラスやクラスター・バージョンの情報を読み取ったりするためのクラスター・スコープの権限が必要です。

IBM MQ Operator は、以下のクラスター・スコープ許可を必要とします。

- アドミッション Webhook を管理する権限。 オペレーターが提供するコンテナーの作成と管理のプロセスで使用される特定の Webhook の作成、取得、更新が可能になります。
  - API グループ: **`admissionregistration.k8s.io`**

  - リソース: **validatingwebhookconfigurations**
  - verbs: **get, delete**
- カスタム・リソースの作成時にサンプルおよびスニペットを提供するために、Red Hat OpenShift コンソールで使用されるリソースを作成および管理する権限です。
  - API グループ: **console.openshift.io**
  - リソース: **consoleyamlsamples**
  - verbs: **create, get, update, delete**
- クラスター・バージョンを読み取る権限。 オペレーターがクラスター環境に関する問題をフィードバックすることが可能になります。
  - API グループ: **config.openshift.io**
  - リソース: **clusterversions**
  - verbs: **get, list, watch**
- クラスター上のストレージ・クラスを読み取る権限。 オペレーターがコンテナー内の選択したストレージ・クラスに関する問題をフィードバックすることが可能になります。
  - API グループ: **storage.k8s.io**
  - リソース: **storageclasses**
  - verbs: **get, list**

注 : IBM MQ Operator には、名前空間を有効範囲とする許可も必要です。 IBM MQ Operator がクラスター・スコープでインストールされている場合、名前空間スコープの許可はすべての名前空間に存在します。

OpenShift CP4I イメージ署名の検証

IBM MQ Operator および IBM MQ のキュー・マネージャー・コンテナー・イメージはデジタル署名されています。

このタスクについて

デジタル署名により、コンテンツの利用者は、ダウンロードしたものが本物 (期待されるソースからのもの) であり、整合性があること (期待されるもの) を確認することができます。

手順

- IBM MQ Operator および IBM MQ キュー・マネージャー・コンテナー・イメージの署名を検査します。
  - IBM Cloud Pak for Integration (CP4I) 16.1.0 資料の「イメージ署名の検証」を参照してください。

OpenShift CP4I IBM MQ Operator のインストール

IBM MQ Operator は、 OpenShift コンソールまたはコマンド・ライン・インターフェース (CLI) を使用して Red Hat OpenShift にインストールできます。

始める前に

重要 :

- このトピックでは、スタンドアロンで使用するための IBM MQ Operator のインストールについて **のみ**説明します。 1 つ以上のキュー・マネージャーで IBM Cloud Pak for Integration または Keycloak SSO を使用する場合は、 39 ページの『CP4I で使用するための IBM MQ Operator のインストール』を参照してください。
- IBM MQ Operator をインストールする前に、 デプロイメントの構造化 に関するガイダンスを確認してください。

インストールができるだけスムーズに行われるようにするには、インストールを開始する前に、すべての前提条件と要件を理解しておく必要があります。 7 ページの『コンテナー内の IBM MQ の計画』 を参照してください。

このタスクについて

以下のステップは、 IBM MQ Operator をインストールするための標準的な作業フローを示しています。

1. Red Hat OpenShift Container Platform をインストールします。
2. ストレージを構成する。
3. ミラー・イメージ (エア・ギャップのみ)。
4. IBM MQ Operator カタログを追加します。
5. IBM MQ Operator をインストールします。
6. ライセンス・キー・シークレットを作成します (オンライン・インストールのみ)。
7. License Service をデプロイします。
8. キュー・マネージャーをデプロイします。

手順

1. Red Hat OpenShift Container Platform をインストールします。

   OpenShift をインストールする詳細なステップについては、 Red Hat ソフトウェア 4.6 以降のインストールを参照してください。

   重要 : サポートされているバージョンの OpenShift Container Platform がインストールされていることを確認してください。 例えば、 IBM MQ Operator 3.2 以降を使用するには、 OpenShift Container Platform 4.12 以降をインストールする必要があります。 詳しくは、 IBM Cloud Pak と Red Hat OpenShift Container Platform の互換性を参照してください。

   Red Hat OpenShift Container Platform CLI を使用するすべてのステップで、 `oc login` を使用して OpenShift クラスターにログインする必要があります。 CLI をインストールするには、OpenShift CLI の概要を参照してください。

   OpenShift をインストールした後、 ライセンス・キー・シークレットの作成で作成した IBM ライセンス・キーを使用して、コンテナー・ソフトウェアを検証し、アクセス権限を取得できます。
2. ストレージを構成します。

   Red Hat OpenShift Container Platform でストレージ・クラスを定義し、サイジング要件を満たすようにストレージ構成を設定する必要があります。

   重要 : IBM MQ 単一インスタンスおよびネイティブ HA キュー・マネージャーは RWO アクセス・モードを使用できますが、複数インスタンス・キュー・マネージャーは、 15 ページの『IBM MQ Operator のストレージの計画』で説明されているように RWX を必要とします。 IBM MQ 複数インスタンス・キュー・マネージャーには、特定のファイル・システム特性が必要です。これは、 IBM MQ の共有ファイル・システムのテストの手順を使用して検証できます。

   既知の準拠ファイル・システムと非準拠ファイル・システムのリスト、およびその他の制限や制約事項については、 IBM MQ ファイル・システムのテスト・ステートメントを参照してください。

   推奨されるストレージ・プロバイダーについては、 CP4I 「ストレージに関する考慮事項」 ページを参照してください。
3. イメージをミラーリングします (エア・ギャップのみ)。

   クラスターが制限付き (エアギャップ) ネットワーク環境にある場合は、以下の値を使用して IBM MQ イメージをミラーリングする必要があります。

   ```
   export OPERATOR_PACKAGE_NAME=ibm-mq
   export OPERATOR_VERSION=3.2.1
   ```

ミラー・イメージを作成するには、 エアギャップ・クラスターのミラーリング・イメージを参照してください。

4. IBM MQ Operator カタログ・ソースを追加します。

   オペレーターをクラスターで使用できるようにするカタログ・ソースを追加します。 34 ページの『IBM MQ Operator カタログ・ソースの追加』 を参照してください。

5. IBM MQ Operator のインストール

   以下の 2 つのオプションのいずれかを選択します (コンソールを使用するか、CLI を使用します)。

   - オプション 1: OpenShift コンソールを使用して IBM MQ Operator をインストールします。
   - オプション 2: OpenShift CLI を使用して IBM MQ Operator をインストールします。

6. 使用権キー・シークレットを作成します (オンライン・インストールのみ)。

   IBM MQ Operator は、ライセンス資格検査を実行するコンテナー・レジストリーからプルされたキュー・マネージャー・イメージをデプロイします。 この検査には、 `docker-registry` プル・シークレットに保管されているライセンス・キーが必要です。 キュー・マネージャーをインストールする名前空間にまだライセンス・キーがない場合は、以下の手順に従ってライセンス・キーを取得し、プル・シークレットを作成します。

   注 : IBM MQ Advanced for Developers (非警告) キュー・マネージャーのみをデプロイする場合は、ライセンス・キーは必要ありません。

   OpenShift コンソールまたは CLI を使用して、使用権キー・シークレットを作成できます。 以下の例では、CLI を使用します。

   a. IBM ID に割り当てられているライセンス・キーを取得します。 ライセンスが付与されているソフトウェアに関連付けられた IBM ID とパスワードを使用して、 MyIBM Container Software Library にログインします。

   b.「**使用権キー (Entitlement keys)**」セクションで「**キーのコピー (Copy key)**」を選択して、使用権キーをクリップボードにコピーします。

   c. OpenShift CLI から以下のコマンドを実行して、 `ibm-entitlement-key` という名前のイメージ・プル・シークレットを作成します。

   ```
   oc create secret docker-registry ibm-entitlement-key \
   --docker-server=cp.icr.io \
   --docker-username=cp \
   --docker-password=entitlement_key \
   --docker-email=user_email
   \--namespace=namespace
   ```

   ここで、 *entitlement_key* はステップ b でコピーしたライセンス・キー、 *user_email* はライセンスが付与されているソフトウェアに関連付けられた IBM ID、 *namespace* は IBM MQ Operator をインストールした名前空間です。

7. License Service をデプロイします。

   これは、キュー・マネージャーのライセンス使用状況をモニターするために必要です。 License Service の手順に従います。

8. キュー・マネージャーをデプロイします。

   サンプルの "クイック・スタート" ・キュー・マネージャーのデプロイ手順については、 63 ページの『IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ』 を参照してください。

関連タスク

53 ページの『IBM MQ Operator のアンインストール』
Red Hat OpenShift コンソールまたは CLI を使用して、Red Hat OpenShift から IBM MQ Operator をアンインストールできます。

OpenShift *IBM MQ Operator カタログ・ソースの追加*

IBM MQ Operator カタログ・ソースを OpenShift クラスターに追加して、 IBM MQ Operator をインストールできるようにします。 このタスクは、アップグレードを完了する前にカタログ・ソースのフィックスパックを適用する場合にも必要です。

このタスクについて

オペレーター・カタログは、 Red Hat OpenShift Container Platform クラスターの API を拡張して IBM ソフトウェア製品を使用可能にするために使用できるオペレーターの索引です。

以下のカタログ・ソースが使用可能です。

オプション 1: IBM MQ Operator の特定のカタログ・ソース。

特定の IBM MQ Operator カタログ・ソースを使用することにより、クラスター上でのソフトウェアのバージョン管理と、アップグレードがいつ行われるかを完全に制御できます。 新しい IBM MQ Operator バージョンが OpenShift クラスターで使用可能になるのは、カタログ・ソースを更新した後 **のみ** です。 このプロセスにより、アップグレードを手動で制御できるため、オペレーターの **Update approval** 設定に 「手動」 オプションを使用する必要はありません。 「**手動**」 オプションを選択すると、可能なすべてのアップグレードが同時に強制的に実行され、アップグレードがブロックされる可能性があるため、 「**自動**」 オプションのみを使用してください。 詳しくは、 Red Hat OpenShift コンソールを使用したオペレーターのインストールの「承認戦略による自動更新の制限」セクションを参照してください。

アップグレードを実行していて、新しいバージョンの IBM MQ Operator カタログ・ソースを追加する必要がある場合は、このオプションを選択します。

このオプションを使用するには、「 オプション 1: IBM MQ Operator の特定のカタログ・ソースの追加」にスキップします。

オプション 2: IBM オペレーター・カタログ。

このオプションを使用すると、新しいオペレーター・バージョンが使用可能になり、ユーザーの介入を **必要とせずに** 適用されます。 そのため、このオプションは、 IBM MQ Operator の **自動** アップグレードが必要で、確定的インストールが必要ないオンライン・インストールに **のみ** 使用してください。

注 : このオプションは PoC (概念検証) 環境には役立ちますが、 **実稼働環境には適していません。**

このオプションを使用するには、「 オプション 2: IBM オペレーター・カタログの追加」にスキップします。

手順

- **オプション 1: IBM MQ Operator の特定のカタログ・ソースを追加します。**

  このタスクでは、 31 ページの『IBM MQ Operator のインストール』 の最初の 3 つのステップが完了していることを前提としています。

  このタスクは、クラスター管理者が実行する必要があり、CLI を使用して実行する必要があります。

  a) アップグレードのみ: アップグレード前にカタログ・ソースのフィックスパックを適用する場合は、以下の手順を実行します。

  - オペレーターが正しく実行されていることを確認します。
  - 手動による承認が必要な保留中の IBM MQ Operator 更新がある場合は、この手順を開始する前にそれらを承認してください。 詳しくは、 Red Hat OpenShift コンソールを使用したオペレーターのインストールの「承認戦略による自動更新の制限」を参照してください。

  b) まだインストールしていない場合、または更新が必要な場合は、GitHub から IBM カタログ管理プラグイン (バージョン 1.6.0 以降) をダウンロードします。

  このプラグインを使用すると、クラスターに対して **oc ibm-pak** コマンドを実行できます。

  c) **oc login** コマンドとユーザー資格情報を使用して、クラスターにログインします。

```
oc login openshift_url -u username -p password -n namespace
```

d) IBM MQ Operator の以下の環境変数をエクスポートします。

```
export OPERATOR_PACKAGE_NAME=ibm-mq
export OPERATOR_VERSION=3.2.1
export ARCH=ARCHITECTURE
```

ここで、*ARCHITECTURE* は、IBM MQ Operator をデプロイしているシステムのアーキテクチャーを表し、値は amd64、 ppc64le、または s390x です。

重要 : IBM オペレーター・カタログから IBM MQ Operator の特定のカタログ・ソースに移動する場合は、 OPERATOR_VERSION を IBM MQ Operator のデプロイメントのバージョンに設定します。

e) IBM MQ Operator 用のファイルをダウンロードします。

注 : エアギャップ ・インストールを実行する場合は、 「IBM MQ Operator のインストール」の「ミラー・イメージ」ステップの完了後に必要なファイルが既にあるはずです。この場合は、ステップ 35 ページの『8』「IBM MQ Operator カタログ・ソースをクラスターに適用する」にスキップできます。

```
oc ibm-pak get ${OPERATOR_PACKAGE_NAME} --version ${OPERATOR_VERSION}
```

f) IBM MQ Operator に必要なカタログ・ソースを生成します。

```
oc ibm-pak generate mirror-manifests ${OPERATOR_PACKAGE_NAME} icr.io --version $
{OPERATOR_VERSION}
```

g) オプション: カタログ・ソースを生成し、別のディレクトリーに保存します。

a. カタログ・ソースを取得します。

```
cat ~/.ibm-pak/data/mirror/${OPERATOR_PACKAGE_NAME}/${OPERATOR_VERSION}/catalog-
sources.yaml
```

b. (オプション) ファイル・ブラウザーでディレクトリーにナビゲートして、これらの成果物を再使用またはパイプライン用に保持できるファイルにコピーします。

h) IBM MQ Operator カタログ・ソースをクラスターに適用します。

```
oc apply -f ~/.ibm-pak/data/mirror/${OPERATOR_PACKAGE_NAME}/${OPERATOR_VERSION}/catalog-
sources.yaml
```

i) openshift-marketplace 名前空間に IBM MQ Operator カタログ・ソースが作成されたことを確認します。

```
oc get catalogsource -n openshift-marketplace
```

出力例:

```
oc get catalogsource -n openshift-marketplace

NAME                            DISPLAY               TYPE   PUBLISHER   AGE
ibmmq-operator-catalogsource    ibm-mq-3.1.3          grpc   IBM         23h
```

これで、 IBM MQ Operator のインストールのステップ 5 を実行する準備ができました。

- **オプション 2: IBM オペレーター・カタログを追加します。**

重要 : IBM オペレーター・カタログ **は、** IBM MQ Operator の **自動** アップグレードが必要で、確定的インストールが不要なオンライン・インストールにのみ使用してください。 このオプションは PoC (概念検証) 環境には役立ちますが、 **実稼働環境には適していません。**

IBM オペレーター・カタログは、 Red Hat OpenShift Container Platform クラスターの API を拡張して IBM ソフトウェア製品を使用可能にするために使用できるオペレーターの索引です。 カタログ・ソースを OpenShift クラスターに追加すると、インストール可能なオペレーターのリストに IBM オペレーターが追加されます。

このタスクでは、 31 ページの『IBM MQ Operator のインストール』の最初の 3 つのステップが完了していることを前提としています。

このタスクは、CLI または OpenShift Web コンソールを使用して実行できます。

CLI の使用

1. IBM オペレーター用の以下のリソース定義を、ご使用のコンピューター上のローカル・ファイルにコピーします。

```
apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: ibm-operator-catalog
  namespace: openshift-marketplace
spec:
  displayName: IBM Operator Catalog
  publisher: IBM
  sourceType: grpc
  image: icr.io/cpopen/ibm-operator-catalog:latest
  updateStrategy:
    registryPoll:
      interval: 45m
```

2. 次のコマンドを実行します。 *filename*.yaml を、前のステップで作成したファイルの名前に置き換えます。

```
oc apply -f filename.yaml
```

OpenShift Web コンソールの使用

1. OpenShift クラスター管理者の資格情報を使用して OpenShift Web コンソールにログインします。
2. バナーで、プラス記号 (「+」) をクリックします。「**YAML のインポート**」ダイアログ・ボックスを開くためのアイコン。

   注 :「**プロジェクト**」の値を選択する必要はありません。 次のステップの YAML コードには、`metadata:namespace` の正しい値が既に含まれています。これにより、カタログ・ソースが正しいプロジェクト (名前空間) にインストールされます。
3. 以下のリソース定義をダイアログ・ボックスに貼り付けます。

```
apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: ibm-operator-catalog
  namespace: openshift-marketplace
spec:
  displayName: IBM Operator Catalog
  image: 'icr.io/cpopen/ibm-operator-catalog:latest'
  publisher: IBM
  sourceType: grpc
  updateStrategy:
    registryPoll:
      interval: 45m
```

4.「**作成**」 をクリックします。

これで、 IBM MQ Operator のインストールのステップ 5 を実行する準備ができました。

OpenShift CP4I *OpenShift コンソールを使用した IBM MQ Operator のインストール*

IBM MQ Operator は、 OperatorHub を使用して Red Hat OpenShift にインストールできます。

始める前に

このタスクは、 31 ページの『IBM MQ Operator のインストール』のステップ 1 から 4 を完了していることを前提としています。

手順

1. Red Hat OpenShift クラスター・コンソールにログインします。
2. ナビゲーション・ペインで、「**オペレーター (Operators)**」 > 「**OperatorHub**」をクリックします。
   「OperatorHub」ページが表示されます。
3. 「**All Items**」フィールドで、「IBM MQ」と入力します。
   IBM MQ カタログ・エントリーが表示されます。
4. 「**IBM MQ**」を選択します。
   「IBM MQ」ウィンドウが表示されます。
5. 「**インストール**」をクリックします。
   「Install Operator」ページが表示されます。
6. 以下の値を入力します。
   a) 「**チャネル**」 を、選択したバージョンに設定します。

      13 ページの『IBM MQ Operator のバージョン・サポート』を確認して、選択するオペレーター・チャネルを判別します。

   b) 「**インストール・モード**」 を「クラスター上の特定の名前空間」(次のステップで作成できます) またはクラスター全体の有効範囲のいずれかに設定します。

      異なるバージョンのオペレーターを異なる名前空間にインストールすると問題が発生する可能性があるため、クラスター全体の有効範囲を選択することをお勧めします。 オペレーターは、コントロール・プレーンの拡張機能となるように設計されています。

   c) オプション: 「クラスター上の特定の名前空間」を選択した場合は、 「**名前空間**」 を、オペレーターのインストール先のプロジェクト (名前空間) の値に設定します。

      注 : コンソールを使用してオペレーターをインストールする場合は、既存の名前空間を使用するか、オペレーターによって提供されるデフォルトの名前空間を使用するか、新しい名前空間を作成することができます。 このフォームから新しい名前空間を作成する場合は、以下のようにします。ナビゲーション・ペインで **ホーム** > 「**プロジェクト**」をクリックし、 「**プロジェクトの作成**」を選択し、作成するプロジェクトの **名前** (名前空間) を指定して、 「**作成**」をクリックします。

   d) 「**承認戦略**」 を「自動」に設定します。
7. 「**インストール**」 をクリックし、オペレーターがインストールするまで待ちます。

   インストールが完了すると、確認が表示されます。

   インストールを検証するには、 **オペレーター** > 「**インストール済みオペレーター (Installed Operators)**」にナビゲートし、 「**プロジェクト (Projects)**」 ドロップダウン・リストからプロジェクトを選択します。 インストールが完了すると、オペレーターの状況が「成功」に変わります。

次のタスク

これで、 ライセンス・キー・シークレットを作成 する準備ができました (31 ページの『IBM MQ Operator のインストール』のステップ 6)。

OpenShift CP4I *Red Hat OpenShift CLI を使用した IBM MQ Operator のインストール*

IBM MQ Operator は、コマンド・ライン・インターフェース (CLI) を使用して Red Hat OpenShift にインストールできます。

始める前に

このタスクは、 31 ページの『IBM MQ Operator のインストール』のステップ 1 から 4 を完了していることを前提としています。

手順

1. **oc login** を使用して、Red Hat OpenShift コマンド・ライン・インターフェース (CLI) にログインします。
2. オプション: IBM MQ Operator に使用する名前空間を作成します。

   IBM MQ Operator は、単一の名前空間またはすべての名前空間を範囲としてインストールできます。 このステップは、まだ存在しない特定の名前空間にインストールする場合にのみ必要です。

   CLI で新しい名前空間を作成するには、以下のコマンドを実行します。

   ```
   oc create namespace namespace_name
   ```

   ここで、 *namespace_name* は、作成する名前空間の名前です。
3. OperatorHub から、クラスターで使用可能なオペレーターのリストを表示します。

   ```
   oc get packagemanifests -n openshift-marketplace
   ```

4. IBM MQ Operator を調べて、サポートされている **InstallModes** かつ使用可能な **Channels** ことを確認します。

   ```
   oc describe packagemanifests ibm-mq -n openshift-marketplace
   ```

5. オプション: **OperatorGroup** を作成します。

   OperatorGroup は、**OperatorGroup** と同じ名前空間におけるすべてのオペレーターに必要となる RBAC アクセス権限を生成するターゲット名前空間を選択する OLM リソースです。

   オペレーターのサブスクライブ先となる名前空間には **OperatorGroup** が必要です。これは、オペレーターの **InstallMode** (AllNamespaces モードまたは SingleNamespace モードのいずれか) に適合するものです。

   インストールするオペレーターが AllNamespaces モードを使用する場合は、 openshift-operators 名前空間に適切な **OperatorGroup** が既に設定されているため、このステップをスキップできます。

   オペレーターが SingleNamespace モードを使用し、適切な **OperatorGroup** がまだ設定されていない場合は、以下のコマンドを実行して作成します。

   ```
   cat << EOF | oc apply -f -
   apiVersion: operators.coreos.com/v1
   kind: OperatorGroup
   metadata:
     name: operatorgroup_name
     namespace: namespace_name
   spec:
     targetNamespaces:
     - namespace_name
   EOF
   ```

6. 13 ページの『IBM MQ Operator のバージョン・サポート』を確認して、選択するオペレーター・チャネルを判別します。
7. オペレーターをインストールします。

   以下のコマンドを使用して、インストールする IBM MQ Operator のバージョンに合わせて *ibm-mq-operator-channel* を変更し、「AllNamespaces」モードを使用している場合は 名前空間名 を **openshift-operators** に変更し、「SingleNamespace」モードを使用している場合は IBM MQ Operator をデプロイする名前空間に変更します。

   ```
   cat << EOF | oc apply -f -
   apiVersion: operators.coreos.com/v1alpha1
   kind: Subscription
   metadata:
     name: ibm-mq
     namespace: namespace_name
   spec:
     channel: ibm-mq-operator-channel
   ```

```
  installPlanApproval: Automatic
  name: ibm-mq
  source: ibm-operator-catalog
  sourceNamespace: openshift-marketplace
EOF
```

8. 数分後に、オペレーターがインストールされます。 以下のコマンドを実行して、すべてのコンポーネントが「成功」状態であることを確認します。

```
oc get csv -n namespace_name | grep ibm-mq
```

   ここで、 *namespace_name* は、「AllNamespaces」モードを使用している場合は **openshift-operators** 、「SingleNamespace」モードを使用している場合はプロジェクト (名前空間) 名です。

次のタスク

これで、 ライセンス・キー・シークレットを作成 する準備ができました (31 ページの『IBM MQ Operator のインストール』のステップ 6)。

OpenShift CP4I CP4I で使用するための IBM MQ Operator のインストール

IBM Cloud Pak for Integration (CP4I) で使用する場合、 OpenShift コンソールまたはコマンド・ライン・インターフェース (CLI) を使用して、 IBM MQ Operator を Red Hat OpenShift にインストールできます。

始める前に

重要 :

- このトピックでは、 CP4I で使用するために IBM MQ Operator をインストールする場合、または CP4I ライセンス **のみ**を使用して少なくとも 1 つのキュー・マネージャーをデプロイする場合について説明します。 スタンドアロンで使用するための IBM MQ Operator のインストール手順については、 31 ページの『IBM MQ Operator のインストール』を参照してください。
- IBM MQ Operator をインストールする前に、 デプロイメントの構造化 に関するガイダンスを確認してください。

インストールが可能な限り円滑に行われるようにするには、インストールを開始する前に、すべての前提条件および要件を理解しておく必要があります。 7 ページの『コンテナー内の IBM MQ の計画』 を参照してください。

このタスクについて

以下のステップは、IBM MQ Operator をインストールするための標準的なタスク・フローを示しています。

1. Red Hat OpenShift Container Platform をインストールします。
2. ストレージを構成する。
3. ミラー・イメージ (エア・ギャップのみ)。
4. IBM MQ Operator カタログを追加 し、クラスターを準備します。
5. IBM MQ Operator をインストールします。
6. ライセンス・キー・シークレットを作成します (オンライン・インストールのみ)。
7. オプション: IBM Cloud Pak for Integration (CP4I) とその依存関係をインストールします。
8. License Service をデプロイします。
9. キュー・マネージャーをデプロイします。

手順

1. Red Hat OpenShift Container Platform をインストールします。

   OpenShift をインストールする詳しい手順については、 Red Hat ソフトウェアのインストール 4.6 以降 を参照してください。

重要 : サポートされているバージョンの OpenShift Container Platform がインストールされていることを確認してください。 例えば、 IBM MQ Operator 3.2 以降を使用するには、 OpenShift Container Platform 4.12 以降をインストールする必要があります。 詳しくは、 IBM Cloud Pak と Red Hat OpenShift Container Platform の互換性を参照してください。

Red Hat OpenShift Container Platform CLI を使用するすべてのステップで、 `oc login` を使用して OpenShift クラスターにログインする必要があります。 CLI をインストールするには、OpenShift CLI の概要を参照してください。

OpenShift をインストールした後、使用権キーの秘密の作成で作成した IBM 使用権キーを使用して、コンテナー・ソフトウェアを検証し、アクセス権限を取得することができます。

2. ストレージを構成します。

   Red Hat OpenShift Container Platform でストレージ・クラスを定義し、サイズ設定要件を満たすようにストレージ構成を設定する必要があります。

   重要 : IBM MQ の単一インスタンス・キュー・マネージャーおよびネイティブ HA キュー・マネージャーは RWO アクセス・モードを使用できますが、複数インスタンス・キュー・マネージャーは 15 ページの『IBM MQ Operator のストレージの計画』で説明されているように RWX を必要とします。 IBM MQ 複数インスタンス・キュー・マネージャーには、特定のファイル・システム特性が必要です。 この特性は、IBM MQ の共有ファイル・システムのテストの手順を使用して確認できます。

   既知の準拠および非準拠のファイル・システムのリスト、およびその他の制限または制約事項に関する注記は、 Testing statement for IBM MQ file systems に記載されています。

   推奨されるストレージ・プロバイダーについては、 CP4I Storage considerations ページを参照してください。

3. イメージをミラーリングします (エア・ギャップのみ)。

   クラスターが制限付き (エアギャップ) ネットワーク環境にある場合は、IBM MQ イメージをミラーリングする必要があります。 構成によっては、いくつかの追加コンポーネントのミラーリングが必要になる場合もあります。 以下の情報を読み、必要に応じてイメージをミラーリングします。

   - IBM MQ イメージをミラーリングする必要があります。 以下の値を使用します。

     ```
     export OPERATOR_PACKAGE_NAME=ibm-mq
     export OPERATOR_VERSION=3.2.1
     ```

   - また、以下の **すべて** の記述が当てはまるキュー・マネージャーを少なくとも 1 つデプロイする予定の場合は、いくつかの追加の必須コンポーネントもミラーリングする必要があります。
     - CP4I ライセンスを使用している。
     - IBM MQ Console が使用可能になります。
     - IBM MQ Console シングル・サインオン (SSO) 認証および許可に IBM Cloud Pak for Integration Keycloak サービスを使用している (デフォルト)。

     上記の記述がすべて当てはまる場合、SSO は Keycloak によって提供されます。 したがって、IBM MQ Operator カタログ・ソースの場合と同様に、以下の追加の必須コンポーネントのそれぞれについてもステップを繰り返す必要があります。

     - IBM Cloud Pak foundational services
     - IBM Cloud Pak for Integration
     - Keycloak (Red Hat OpenShift 演算子)

   ミラー・イメージを作成するには、 エアギャップ・クラスターのミラーリング・イメージを参照してください。

4. IBM MQ Operator カタログ・ソースを追加します。

以下の値を使用して、IBM MQ Operator をクラスターで使用できるようにするカタログ・ソースを追加します。

```
export OPERATOR_PACKAGE_NAME=ibm-mq
export OPERATOR_VERSION=3.2.1
export ARCH=ARCHITECTURE
```

ここで、 *ARCHITECTURE* はご使用のシステム・アーキテクチャーを表し、値は amd64、 ppc64le、または s390x です。

少なくとも 1 つのキュー・マネージャーをデプロイするときに、以下の **すべて** の記述が当てはまる場合は、いくつかの追加の必須コンポーネントがあります。

- CP4I ライセンスを使用している。
- IBM MQ Console が使用可能になります。
- IBM MQ Console シングル・サインオン (SSO) 認証および許可に IBM Cloud Pak for Integration Keycloak サービスを使用している (デフォルト)。

上記の記述がすべて当てはまる場合、SSO は Keycloak によって提供されます。 したがって、 IBM MQ Operator カタログ・ソースの場合と同様に、以下の追加の必須コンポーネントのそれぞれについてもステップを繰り返す必要があります。

- IBM Cloud Pak foundational services
- IBM Cloud Pak for Integration
- Keycloak (Red Hat OpenShift 演算子)

クラスターへのカタログ・ソースの追加に記載されている、必要なカタログ・ソースの手順に従います。

5. IBM MQ Operator のインストール

   以下の 2 つのオプションのいずれかを選択します (コンソールを使用するか、CLI を使用します)。

   - オプション 1: OpenShift コンソールを使用して IBM MQ Operator をインストールします。
   - オプション 2: OpenShift CLI を使用して IBM MQ Operator をインストールします。

6. 使用権キー・シークレットを作成します (オンライン・インストールのみ)。

   IBM MQ Operator は、ライセンス資格検査を実行するコンテナー・レジストリーからプルされるキュー・マネージャー・イメージをデプロイします。 このチェックには、 docker-registry プル・シークレットに保管されている使用権キーが必要です。 キュー・マネージャーをインストールする名前空間にまだ使用権キーがない場合は、以下の手順に従って使用権キーを取得し、プル・シークレットを作成します。

   注 : IBM MQ Advanced for Developers (非保証) キュー・マネージャーのみをデプロイする場合、ライセンス・キーは必要ありません。

   OpenShift コンソールまたは CLI を使用して、使用権キー・シークレットを作成できます。 以下の例では、CLI を使用します。

   a. IBM ID に割り当てられているライセンス・キーを取得します。 ライセンス契約済みソフトウェアに関連付けられている IBM ID とパスワードを使用して、 MyIBM Container Software Library にログインします。

   b.「**使用権キー (Entitlement keys)**」セクションで「**キーのコピー (Copy key)**」を選択して、使用権キーをクリップボードにコピーします。

   c. OpenShift CLI から、以下のコマンドを実行して、ibm-entitlement-key という名前のイメージ・プル・シークレットを作成します。

   ```
   oc create secret docker-registry ibm-entitlement-key \
   --docker-server=cp.icr.io \
   --docker-username=cp \
   --docker-password=entitlement_key \
   --docker-email=user_email
   \--namespace=namespace
   ```

ここで、 *entitlement_key* はステップ b でコピーした使用権キー、 *user_email>* は使用権付きソフトウェアに関連付けられた IBM ID、 *namespace* は IBM MQ Operator をインストールした名前空間です。

7. オプション: CP4I とその依存関係をインストールします。

   少なくとも 1 つのキュー・マネージャーをデプロイするときに、以下の **すべて** の記述が当てはまる場合は、いくつかの追加の必須コンポーネントがあります。

   - CP4I ライセンスを使用している。
   - IBM MQ Console が使用可能になります。
   - IBM MQ Console シングル・サインオン (SSO) 認証および許可に CP4I Keycloak サービスを使用している (デフォルト)。

   上記の記述がすべて当てはまる場合、SSO は Keycloak によって提供されるため、以下の追加ステップを実行する必要があります。

   - CP4I Operator と同じインストール・モードで IBM Cloud Pak foundational services Operator をインストールします。 サポートされるバージョンについては、 このリリースのオペレーター・チャネルのバージョンを参照してください。
   - CP4I Operator をインストールします。
   - オプション: プラットフォーム UI をデプロイします。

     a. `ibm-common-services` 名前空間を作成します。 CLI を使用して OpenShift クラスターにログインしたら、以下のコマンドを実行します。

     ```
     oc new-project ibm-common-services
     ```

     b. プラットフォーム UI をデプロイします。

8. License Service をデプロイします。

   これは、キュー・マネージャーのライセンス使用状況をモニターするために必要です。 License Service の手順に従います。

9. キュー・マネージャーをデプロイします。

   サンプルの "クイック・スタート" ・キュー・マネージャーのデプロイ手順については、 63 ページの『IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ』 を参照してください。

関連タスク

53 ページの『IBM MQ Operator のアンインストール』
Red Hat OpenShift コンソールまたは CLI を使用して、Red Hat OpenShift から IBM MQ Operator をアンインストールできます。

OpenShift Operator2.0.0 CP4I IBM MQ Operator とキュー・マネージャーのアップグレード

IBM MQ Operator のユーザーには、 IBM MQ ライセンスを使用するか、 IBM Cloud Pak for Integration (CP4I) ライセンスを使用するかに応じて、さまざまなアップグレード・プロセスがあります。 ご使用のデプロイメント・タイプのアップグレード・ステップを実行します。

このタスクについて

IBM MQ Operator およびキュー・マネージャーをアップグレードするには、以下のいずれかのステップを実行します。

手順

- オプション 1: **現在のオペレーター・チャネルでデプロイメントを最新バージョンにアップグレードします。**

現在のオペレーター・チャネルで IBM MQ Operator のデプロイメントを最新バージョンにアップグレードするには、 43 ページの『IBM MQ Operator チャネルの最新セキュリティー・リリースへのアップグレード』を参照してください。

- オプション 2: **IBM MQ Operator for IBM MQ ライセンスをアップグレードします。**

  IBM MQ ライセンス **のみ** を使用する IBM MQ Operator のデプロイメントをアップグレードするには、 43 ページの『IBM MQ Operator のアップグレード』を参照してください。

- オプション 3: **CP4I ユーザーのために IBM MQ Operator をアップグレードします。**

  IBM Cloud Pak for Integration のユーザーのために IBM MQ Operator のデプロイメントをアップグレードします。 これには、 CP4I ライセンスの下に少なくとも 1 つのキュー・マネージャーをデプロイした場合が含まれます。 48 ページの『CP4I ユーザーのための IBM MQ Operator のアップグレード』を参照してください。

OpenShift *IBM MQ Operator のアップグレード*

IBM MQ ライセンス **のみ** が使用されている IBM MQ Operator のデプロイメントをアップグレードします。

始める前に

重要 : このタスクは、 IBM MQ Operator および **のみ** の IBM MQ ライセンスのユーザーを対象としています。 IBM Cloud Pak for Integration (CP4I) ユーザーである場合、または CP4I ライセンスを使用して少なくとも 1 つのキュー・マネージャーをデプロイした場合は、 48 ページの『CP4I ユーザーのための IBM MQ Operator のアップグレード』を参照してください。

このタスクについて

以下のいずれかのステップを、必要なアップグレードに合わせて実行します。

注 : IBM MQ Operator のバージョン 3.2.x は、 CD と SC2 の両方のリリースとしてリリースされました。

手順

- オプション 1:43 ページの『IBM MQ Operator チャネルの最新セキュリティー・リリースへのアップグレード』
- オプション 2:45 ページの『3.2.x SC2/CD チャネルへの 2.0.x LTS IBM MQ Operator のアップグレード』
- オプション 3: 46 ページの『3.2.x SC2/CD チャネルへの CD IBM MQ Operator のアップグレード』

OpenShift CP4I *IBM MQ Operator* チャネルの最新セキュリティー・リリースへのアップグレード

IBM MQ Operator をアップグレードすると、キュー・マネージャーをアップグレードできます。

始める前に

重要 : このトピックでは、 IBM MQ Operator のデプロイメントを、デプロイメントのチャネル上の最新のセキュリティー・リリースにアップグレードします。 これがご使用のデプロイメントに該当しない場合は、 42 ページの『IBM MQ Operator とキュー・マネージャーのアップグレード』で説明されている代替アップグレード・パスを参照してください。

このタスクについて

まずカタログ・ソースをアップグレードしてから、キュー・マネージャーをアップグレードします。 アップグレード対象の IBM MQ Operator のデプロイに使用されるカタログ・ソースに応じて、2 つのオプションがあります。

オプション 1: IBM MQ Operator の特定のカタログ・ソース

新しい IBM MQ Operator バージョンが OpenShift クラスターで使用可能になるのは、カタログ・ソースを更新した後 **のみ** です。 このプロセスにより、アップグレードを手動で制御できるため、オペレー

ターの **Update approval** 設定に 「**手動**」 オプションを使用する必要はありません。 「**手動**」 オプションを選択すると、可能なすべてのアップグレードが同時に強制的に実行され、アップグレードがブロックされる可能性があるため、 「**自動**」 オプションのみを使用してください。 詳しくは、 Red Hat OpenShift コンソールを使用したオペレーターのインストールの「承認戦略による自動更新の制限」セクションを参照してください。

このオプションを使用するには、 IBM MQ Operator の特定のカタログ・ソースを使用したアップグレードにスキップします。

オプション 2: IBM オペレーター・カタログ

このオプションを使用すると、新しいオペレーター・バージョンが使用可能になり、ユーザーの介入を **必要とせずに** 適用されます。 そのため、このオプションは、 IBM MQ Operator の **自動** アップグレードが必要で、確定的インストールが必要ないオンライン・インストールに **のみ** 使用してください。 このオプションは PoC (概念検証) 環境には役立ちますが、 **実稼働環境には適していません**。

このオプションを使用するには、 IBM オペレーター・カタログを使用したアップグレードにスキップしてください。

IBM オペレーター・カタログの使用から、アップグレードをより詳細に制御できる IBM MQ Operator の特定のカタログ・ソースの使用に移行するには、 47 ページの『IBM MQ Operator の特定のカタログ・ソースへの移動』を参照してください。

手順

- **IBM MQ Operator の特定のカタログ・ソースを使用したアップグレード**

  a) 最新のカタログ・ソースを適用します。

  「IBM MQ Operator カタログ・ソースの追加」の「IBM MQ Operator の特定のカタログ・ソースの追加」の説明に従ってください。

  b) IBM MQ Operator の 「**承認の更新**」 状況が 「**自動**」に設定されている場合、オペレーターはアップグレードします。 「**承認の更新**」 が 「**手動**」に設定されている場合は、以下の手順に従って IBM MQ Operator をアップグレードします。

  a. ナビゲーション・ペインで、「**オペレーター (Operators)**」 > 「**インストール済みのオペレーター (Installed Operators)**」をクリックします。

  指定したプロジェクトにインストールされているすべてのオペレーターが表示されます。

  b.「**IBM MQ Operator**」を選択します。

  c.「**サブスクリプション**」タブにナビゲートします。

  d.「**アップグレード可能**」 をクリックします。

  e.「**プレビュー**」 **InstallPlan をクリックします**。

  f.「**承認**」 をクリックして、アップグレードを完了します。

  オペレーターが新しいバージョンにアップグレードします。

  c) すべての IBM MQ キュー・マネージャーをアップグレードします。

  IBM MQ キュー・マネージャーのアップグレードの手順に進みます。

- **IBM オペレーター・カタログを使用したアップグレード**

  a) IBM MQ Operator を新しいバージョンにアップグレードします。

  自動アップグレードが設定されている場合、新しいセキュリティー・リリースがリリースされると、IBM MQ Operator はアップグレードを完了します。 自動アップグレードが設定されていない場合は、 IBM MQ Operator のアップグレードを手動で承認します。

  – 使用可能なアップグレードがある場合、 **Upgrade Status** は「`Upgrade available`」の可能性があります。

  – この場合、 IBM MQ Operator をアップグレードする **InstallPlan** を承認するために使用できる制御が存在する可能性があります。

b) すべての IBM MQ キュー・マネージャーのアップグレード

IBM MQ キュー・マネージャーのアップグレードの手順に進みます。

- **IBM MQ キュー・マネージャーをアップグレードします。**

  IBM MQ Operator のアップグレード後に、すべての IBM MQ キュー・マネージャーを新しいバージョンにアップグレードする必要があります。

  以下の表に、アクティブなオペレーター・チャネルごとの IBM MQ キュー・マネージャーの最新バージョンを示します。 関連するバージョンを使用して、 51 ページの『Red Hat OpenShift を使用した IBM MQ キュー・マネージャーのアップグレード』の手順に従います。

オペレーター・チャネル	最新の IBM MQ キュー・マネージャー
v3.2 (SC2/CD)	9.4.0.0-r1

3.2.x SC2/CD チャネルへの 2.0.x LTS IBM MQ Operator のアップグレード

IBM MQ Operator をアップグレードすると、キュー・マネージャーをアップグレードできます。

始める前に

重要 :

- このタスクは、 IBM MQ Operator および **のみ** の IBM MQ ライセンスのユーザーを対象としています。 IBM Cloud Pak for Integration (CP4I) ユーザーである場合、または CP4I ライセンスを使用して少なくとも 1 つのキュー・マネージャーをデプロイした場合は、 48 ページの『CP4I ユーザーのための IBM MQ Operator のアップグレード』を参照してください。
- このトピックは、 2.0.x Long Term Support (LTS) IBM MQ Operator を IBM MQ Operator 3.2.x **のみ**の Support Cycle 2 (SC2) チャネルにアップグレードするためのものです。 これがご使用のデプロイメントに該当しない場合は、 42 ページの『IBM MQ Operator とキュー・マネージャーのアップグレード』で説明されている代替アップグレード・パスを参照してください。

IBM MQ Operator 3.2.1 にアップグレードするには、 Red Hat OpenShift Container Platform 4.12 以降を実行している必要があります。 各 IBM MQ Operator チャネルの互換性のあるバージョンを確認するには、 14 ページの『互換性のある Red Hat OpenShift Container Platform のバージョン』を参照してください。 プラットフォームをアップグレードするには、 Red Hat OpenShift のアップグレードを参照してください。

手順

1. **ミラー・イメージ (エア・ギャップのみ)。**

   IBM MQ イメージをミラーリングする必要があります。 これらの値のみを使用して、以下のリンクでステップを実行します。

   ```
   export OPERATOR_PACKAGE_NAME=ibm-mq
   export OPERATOR_VERSION=3.2.1
   ```

   以前のインストールまたはアップグレード時にイメージ・レジストリーへの接続がセットアップされている必要があるため、セクション 3.5 「クラスターの構成」を省略する必要があります。

   リンク: エアギャップ・クラスター用のミラーリング・イメージ。

2. **IBM MQ Operator を 3.2.1 にアップグレードします。**

   49 ページの『Red Hat OpenShift を使用した IBM MQ Operator のアップグレード』 を参照してください。

3. **インスタンスをアップグレードします。**

   最新の機能とセキュリティー・フィックスを入手するには、IBM MQ Operand (キュー・マネージャー・コンテナー・イメージ) を最新の CD バージョン (9.4.0.0-r1) にアップグレードします。 51 ページの

『Red Hat OpenShift を使用した IBM MQ キュー・マネージャーのアップグレード』を参照してください。

3.2.x SC2/CD チャネルへの CD IBM MQ Operator のアップグレード

IBM MQ Operator をアップグレードすると、キュー・マネージャーをアップグレードできます。

始める前に

重要 :

- このタスクは、 IBM MQ Operator および **のみ** の IBM MQ ライセンスのユーザーを対象としています。 IBM Cloud Pak for Integration (CP4I) ユーザーである場合、または CP4I ライセンスを使用して少なくとも 1 つのキュー・マネージャーをデプロイした場合は、 48 ページの『CP4I ユーザーのための IBM MQ Operator のアップグレード』を参照してください。
- このトピックでは、バージョン 3.2.0 より前の IBM MQ Operator の Continuous Delivery (CD) デプロイメントをバージョン 3.2.1 **のみ**にアップグレードします。 これがご使用のデプロイメントに該当しない場合は、 42 ページの『IBM MQ Operator とキュー・マネージャーのアップグレード』で説明されている代替アップグレード・パスを参照してください。

IBM MQ Operator 3.2.1 にアップグレードするには、 Red Hat OpenShift Container Platform 4.12 以降を実行している必要があります。 各 IBM MQ Operator チャネルの互換性のあるバージョンを確認するには、 14 ページの『互換性のある Red Hat OpenShift Container Platform のバージョン』を参照してください。 プラットフォームをアップグレードするには、 Red Hat OpenShift のアップグレードを参照してください。

手順

1. オプション: **3.0.0 より前の CD バージョンである IBM MQ Operator をアップグレードします。**

   ご使用の IBM MQ Operator が現在 3.0.0 より前の CD バージョンである場合は、IBM MQ Operator (IBM MQ 9.3 資料) の現行 CD チャネルへのマイグレーションの関連ステップに従ってから、ここに戻って最新の CD バージョンにアップグレードしてください。 これは、バージョン 3.2.1 にアップグレードする前の必須の前提条件ステップであることに注意してください。
2. **ミラー・イメージ (エア・ギャップのみ)。**

   IBM MQ イメージをミラーリングする必要があります。 これらの値のみを使用して、以下のリンクでステップを実行します。

   ```
   export OPERATOR_PACKAGE_NAME=ibm-mq
   export OPERATOR_VERSION=3.2.1
   ```

   以前のインストールまたはアップグレード時にイメージ・レジストリーへの接続がセットアップされている必要があるため、セクション 3.5 「クラスターの構成」を省略する必要があります。

   リンク: エアギャップ・クラスター用のミラーリング・イメージ。
3. **IBM MQ Operator を 3.2.1 にアップグレードします。**

   49 ページの『Red Hat OpenShift を使用した IBM MQ Operator のアップグレード』を参照してください。
4. **インスタンスをアップグレードします。**

   最新の機能とセキュリティー・フィックスを入手するには、IBM MQ Operand (キュー・マネージャー・コンテナー・イメージ) を最新の CD バージョン (9.4.0.0-r1) にアップグレードします。 51 ページの『Red Hat OpenShift を使用した IBM MQ キュー・マネージャーのアップグレード』を参照してください。

OpenShift CP4I V 9.4.0 V 9.4.0 *IBM MQ Operator* の特定のカタログ・ソースへの移動

以前のリリースの IBM MQ Operator がインストールされていて、IBM オペレーター・カタログを使用している場合、特定のカタログ・ソースを適用することが、クラスター上のソフトウェアのバージョン管理を完全に制御するための最も効果的な方法です。

始める前に

重要 : このタスクは、クラスター管理者が実行する必要があります。 OpenShift の役割と権限を参照してください。

CLI を使用して、以下のステップを実行します。

このタスクについて

IBM オペレーター・カタログは、Red Hat OpenShift Container Platform クラスターの API を拡張して IBM ソフトウェア製品を使用可能にするために使用できるオペレーターの索引です。

この手順では、 IBM オペレーター・カタログから IBM MQ Operator のインストールを移動して、 IBM MQ Operator の特定のカタログ・ソースを使用できるようにします。

手順

1. IBM MQ Operator カタログを追加します。

   「IBM MQ Operator カタログ・ソースの追加」の「IBM MQ Operator の特定のカタログ・ソースの追加」の説明に従ってください。
2. IBM MQ Operator カタログ・ソースが `openshift-marketplace` 名前空間に作成されたことを確認します。

   以下のコマンドを実行します。

   ```
   oc get catalogsource -n openshift-marketplace
   ```

   出力例:

   ```
   oc get catalogsource -n openshift-marketplace

   NAME                            DISPLAY                TYPE   PUBLISHER   AGE
   ibm-operator-catalog            IBM Operator Catalog   grpc   IBM         23h
   ibmmq-operator-catalogsource    ibm-mq-3.1.3           grpc   IBM         23h
   ```
3. オプション: IBM Operator カタログ・ソースを削除します。

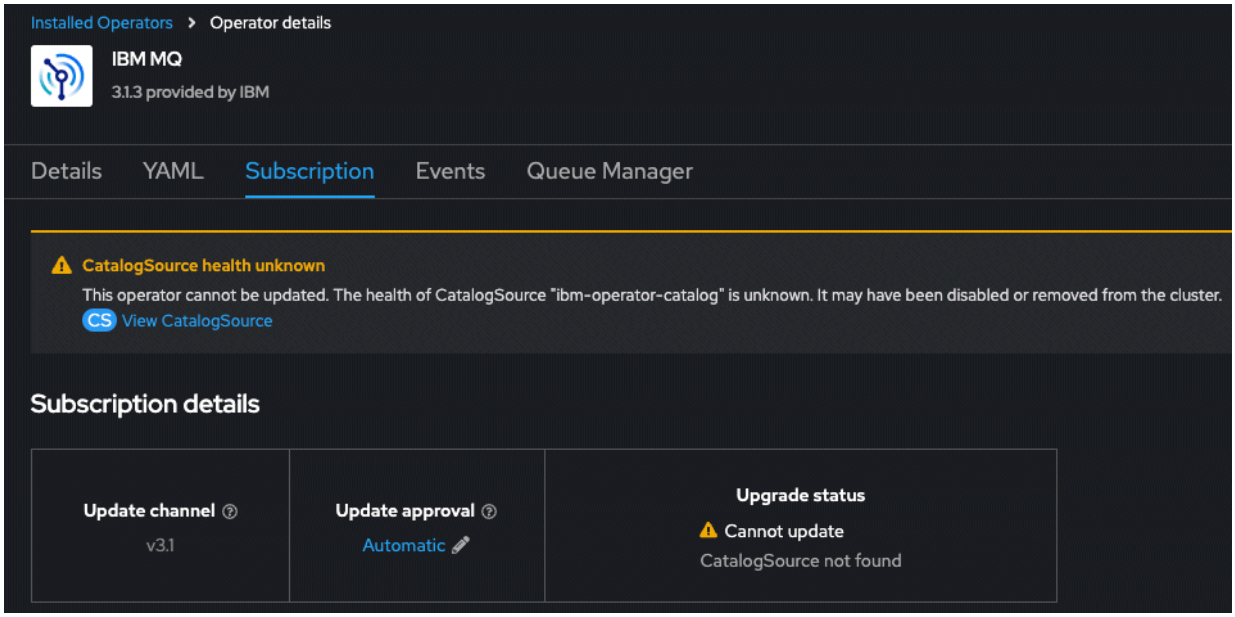
   

   警告 : このステップは、IBM オペレーター・カタログを使用しているオペレーターが他にないことが確実な場合にのみ実行してください。

   以下のコマンドを実行します。

   ```
   oc delete catalogsource ibm-operator-catalog -n openshift-marketplace
   ```

   IBM MQ Operator の状況が `CatalogSource not found` に変わります。 これは、予期されていることです。



4. IBM MQ Operator のサブスクリプションを、新しい特定の IBM MQ Operator カタログ・ソースを指すように変更します。

   a) サブスクリプションを編集します。

   以下のコマンドを実行します。 *OPERATOR-NAMESPACE* は、 IBM MQ Operator のクラスター全体のインストール済み環境の場合は `openshift-operators` に、 IBM MQ Operator がデプロイされている特定の名前空間に置き換えてください。

   ```
   oc edit subscription ibm-mq -n OPERATOR-NAMESPACE
   ```

   b) `spec.source` 値を `ibm-operator-catalog` から、ステップ 47 ページの『1』 で作成したカタログ・ソースの名前に変更します。

   以下に例を示します。

   ```
   spec:
     channel: v3.1
     installPlanApproval: Automatic
     name: ibm-mq
     source: ibm-operator-catalog # CHANGE --> ibmmq-operator-catalogsource
     sourceNamespace: openshift-marketplace
   ```

   c) 変更を保存します。

   これで、 IBM MQ Operator のインストール済み環境が IBM MQ Operator カタログ・ソースを指すようになりました。 IBM オペレーター・カタログを削除した場合、状況は「CatalogSource not found」から「Succeeded」に戻ります。

タスクの結果

これで、 IBM MQ Operator のインストール済み環境は、 IBM MQ Operator の特定のカタログ・ソースを指すようになります。 これにより、オペレーターのアップグレードを完全に制御できます。

OpenShift CP4I *CP4I ユーザーのための IBM MQ Operator のアップグレード*

IBM Cloud Pak for Integration (CP4I) ライセンスが使用されている IBM MQ Operator のデプロイメントをアップグレードします。

始める前に

重要 : このタスクは、 CP4I ユーザーを対象としています。 これには、 CP4I ライセンスの下に少なくとも 1 つのキュー・マネージャーをデプロイした場合が含まれます。 これが該当しない場合は、 43 ページの『IBM MQ Operator のアップグレード』 を参照してください。

このタスクについて

以下のいずれかのオプションを実行します。

手順

- **オプション 1:** 2.0.x のデプロイメントのアップグレード Long Term Support (LTS) IBM MQ Operator

  アップグレード計画の生成による 2022.2 からのアップグレードの手順に従います。
- **オプション 2:** IBM MQ Operator の 3.0.x または 3.1.x デプロイメントのアップグレード

  アップグレード計画の生成による 2023.4 からのアップグレードの手順に従います。
- **オプション 3:** IBM MQ Operator の他のデプロイメントをアップグレードする

  IBM MQ Operator の現行 CD チャネルへのマイグレーション (IBM MQ 9.3 資料)の関連ステップに従ってから、ここに戻り、 **オプション 2** に進みます。 これは必須の前提条件ステップであることに注意してください。

OpenShift CP4I *Red Hat OpenShift を使用した IBM MQ Operator のアップグレード*

Red Hat OpenShift Web コンソールまたは CLI を使用して、IBM MQ Operator をアップグレードできます。

手順

Red Hat OpenShift を使用して IBM MQ Operator をアップグレードするには、以下のいずれかのタスクを実行します。

- 49 ページの『Red Hat OpenShift コンソールを使用した IBM MQ Operator のアップグレード』
- 50 ページの『Red Hat OpenShiftCLI を使用して IBM MQ Operator をアップグレードする』

OpenShift CP4I *Red Hat OpenShift コンソールを使用した IBM MQ Operator のアップグレード*

Operator Hub を使用して、IBM MQ Operator をアップグレードできます。

始める前に

注 : 最新の CD バージョンの IBM MQ Operator は 3.2.1 であり、 SC2 と CD の両方のバージョンです。 最新の IBM MQ Operator リリース・ノートについては、 IBM MQ Operator のリリース・ヒストリーを参照してください。

Red Hat OpenShift クラスター・コンソールにログインします。

手順

1. 13 ページの『IBM MQ Operator のバージョン・サポート』を確認して、どのオペレーター・チャネルにアップグレードすべきかを判別します。
2. 最新のカタログ・ソースを適用します。

   `ibm-operator-catalog` ではなく、 IBM MQ Operator の特定のカタログ・ソースを使用する場合は、新しい IBM MQ バージョンのカタログ・ソースを適用する必要があります。

   IBM オペレーター・カタログの使用から IBM MQ Operator の特定のカタログ・ソースの使用に移行し、アップグレードをより詳細に制御するには、ステップ 49 ページの『3』に戻る前に、47 ページの『IBM MQ Operator の特定のカタログ・ソースへの移動』 のステップを参照してください。

   IBM オペレーター・カタログ (一部のオンライン・インストールのみ) を使用している場合は、ステップ 49 ページの『3』に進みます。

   34 ページの『IBM MQ Operator カタログ・ソースの追加』 の指示に従ってください。
3. IBM MQ Operator をアップグレードします。 IBM MQ Operator の新規のメジャー/マイナーのバージョンは、新しいサブスクリプション・チャネルを介して配信されます。 Operator を新規のメジャー/マイ

ナーのバージョンにアップグレードするには、IBM MQ Operator の「サブスクリプション」で、選択したチャネルを更新する必要があります。

a) ナビゲーション・ペインで、「**オペレーター (Operators)**」 > 「**インストール済みのオペレーター (Installed Operators)**」をクリックします。
   指定したプロジェクトにインストールされているすべてのオペレーターが表示されます。

b) 「**IBM MQ Operator**」を選択します。

c) 「**サブスクリプション**」タブにナビゲートします。

d) 「**チャネル**」をクリックします。
   「**サブスクリプション更新チャネルの変更 (Change Subscription Update Channel)**」ウィンドウが表示されます。

e) 必要なチャネルを選択して、「**保存**」をクリックします。
   新しいチャネルで使用できる最新バージョンに Operator がアップグレードされます。 13 ページの『IBM MQ Operator のバージョン・サポート』 を参照してください。

OpenShift CP4I *Red Hat OpenShiftCLI を使用して IBM MQ Operator をアップグレードする*

IBM MQ Operator はコマンド・ラインからアップグレードできます。

始める前に

注 : 最新の CD バージョンの IBM MQ Operator は 3.2.1 であり、 SC2 と CD の両方のバージョンです。 最新の IBM MQ Operator リリース・ノートについては、 IBM MQ Operator のリリース・ヒストリーを参照してください。

oc login を使用してクラスターにログインします。

手順

1. 13 ページの『IBM MQ Operator のバージョン・サポート』を確認して、どのオペレーター・チャネルにアップグレードすべきかを判別します。
2. 最新のカタログ・ソースを適用します。

   `ibm-operator-catalog` ではなく、 IBM MQ Operator の特定のカタログ・ソースを使用する場合は、新しい IBM MQ バージョンのカタログ・ソースを適用する必要があります。

   IBM オペレーター・カタログの使用から IBM MQ Operator の特定のカタログ・ソースの使用に移行し、アップグレードをより詳細に制御するには、ステップ 50 ページの『3』に戻る前に、47 ページの『IBM MQ Operator の特定のカタログ・ソースへの移動』 のステップを参照してください。

   IBM オペレーター・カタログ (一部のオンライン・インストールのみ) を使用している場合は、ステップ 50 ページの『3』に進みます。

   34 ページの『IBM MQ Operator カタログ・ソースの追加』 の指示に従ってください。
3. IBM MQ Operator をアップグレードします。 IBM MQ Operator の新規のメジャー/マイナーのバージョンは、新しいサブスクリプション・チャネルを介して配信されます。 オペレーターを新規メジャー/マイナー・バージョンにアップグレードするには、IBM MQ Operator サブスクリプションで、選択したチャネルを更新する必要があります。

   a) 必要な IBM MQ Operator アップグレード・チャネルが使用可能であることを確認します。

   ```
   oc get packagemanifest ibm-mq -o=jsonpath='{.status.channels[*].name}'
   ```

   b) `Subscription` にパッチを適用して目的の更新チャネルに移動します (*vX.Y* は前のステップで識別された目的の更新チャネルです)。

   ```
   oc patch subscription ibm-mq --patch '{"spec":{"channel":"vX.Y"}}' --type=merge
   ```

OpenShift CP4I *Red Hat OpenShift を使用した IBM MQ キュー・マネージャーのアップグレード*

始める前に

IBM MQ キュー・マネージャーをアップグレードするプロセスの一環として、 IBM Cloud Pak for Integration の資料からこのトピックに移動した可能性があります。

手順

Red Hat OpenShift を使用して IBM MQ キュー・マネージャーをアップグレードするには、以下のいずれかのタスクを実行します。

- 51 ページの『Red Hat OpenShift コンソールを使用した IBM MQ キュー・マネージャーのアップグレード』
- 52 ページの『Red Hat OpenShift CLI を使用した IBM MQ キュー・マネージャーのアップグレード』
- 52 ページの『プラットフォーム UI を使用した Red Hat OpenShift での IBM MQ キュー・マネージャーのアップグレード』

次のタスク

IBM Cloud Pak for Integration のアップグレードを完了するには、 IBM Cloud Pak for Integration の資料に戻らなければならない場合があります。

OpenShift CP4I *Red Hat OpenShift コンソールを使用した IBM MQ キュー・マネージャーのアップグレード*

IBM MQ Operator を使用してデプロイされた IBM MQ キュー・マネージャーは、オペレーター・ハブを使用して Red Hat OpenShift でアップグレードすることができます。

始める前に

注 : IBM MQ キュー・マネージャーの最新バージョンは 9.4.0.0-r1 であり、SC2 と CD の両方のバージョンです。 最新の IBM MQ キュー・マネージャーのリリース・ノートについては、IBM MQ Operator で使用するためのキュー・マネージャー・コンテナー・イメージのリリース履歴を参照してください。

- Red Hat OpenShift クラスターのウェブコンソールにログインします。
- IBM MQ Operator で対象の更新チャネルを使用していることを確認してください。 49 ページの『Red Hat OpenShift を使用した IBM MQ Operator のアップグレード』を参照してください。

エア・ギャップ環境でキュー・マネージャーをアップグレードする前に、 CD IBM MQ Operator の 3.2.x SC2/CD チャネルへのアップグレードのエアー・ギャップ固有のステップを使用して、最新の IBM Cloud Pak for Integration イメージをミラーリングする必要があります。

手順

1. ナビゲーション・ペインで、「**オペレーター (Operators)**」 > 「**インストール済みのオペレーター (Installed Operators)**」をクリックします。
   指定したプロジェクトにインストールされているすべてのオペレーターが表示されます。
2. 「**IBM MQ Operator**」を選択します。
   「**IBM MQ Operator**」ウィンドウが表示されます。
3. 「**キュー・マネージャー**」タブにナビゲートします。
   「**キュー・マネージャーの詳細**」ウィンドウが表示されます。
4. アップグレードするキュー・マネージャーを選択します。
5. YAML タブに移動します。
6. 以下のフィールドを更新します。必要に応じて、対象の IBM MQ キュー・マネージャーのバージョン・アップグレードに合わせてください。

- spec.version
- spec.license.licence

IBM MQ Operator バージョンと IBM MQ キュー・マネージャー・コンテナー・イメージのマッピングについては、7 ページの『IBM MQ Operator で使用するキュー・マネージャー・コンテナー・イメージのリリース履歴』 を参照してください。

7. 更新したキュー・マネージャー YAML を保存します。

OpenShift CP4I *Red Hat OpenShift CLI を使用した IBM MQ キュー・マネージャーのアップグレード*

IBM MQ Operator を使用してデプロイされた IBM MQ キュー・マネージャーは、コマンド行を使用して Red Hat OpenShift にアップグレードすることができます。

始める前に

注 : IBM MQ キュー・マネージャーの最新バージョンは 9.4.0.0-r1 であり、SC2 と CD の両方のバージョンです。 最新の IBM MQ キュー・マネージャーのリリース・ノートについては、IBM MQ Operator で使用するためのキュー・マネージャー・コンテナー・イメージのリリース履歴を参照してください。

以下の手順は、クラスター管理者でないと実行できません。

- `oc login` を使用して、 Red Hat OpenShift コマンド・ライン・インターフェース (CLI) にログインします。
- IBM MQ Operator で対象の更新チャネルを使用していることを確認してください。42 ページの『IBM MQ Operator とキュー・マネージャーのアップグレード』を参照してください。

エア・ギャップ環境でキュー・マネージャーをアップグレードする前に、CD IBM MQ Operator の 3.2.x SC2/CD チャネルへのアップグレードのエアー・ギャップ固有のステップを使用して、最新の IBM Cloud Pak for Integration イメージをミラーリングする必要があります。

手順

QueueManager リソースを編集して以下のフィールドを更新します。必要に応じて、対象の IBM MQ キュー・マネージャーのバージョン・アップグレードに合わせてください。

- spec.version
- spec.license.licence

チャネルから IBM MQ Operator バージョンおよび IBM MQ キュー・マネージャー・バージョンへのマッピングについては、13 ページの『IBM MQ Operator のバージョン・サポート』 を参照してください。

以下のコマンドを使用します。

```
oc edit queuemanager my_qmgr
```

ここで、*my_qmgr* は、アップグレードする QueueManager リソースの名前です。

CP4I *プラットフォーム UI を使用した Red Hat OpenShift での IBM MQ キュー・マネージャーのアップグレード*

IBM MQ Operator を使用してデプロイされた IBM MQ キュー・マネージャーは、 IBM Cloud Pak for Integration Platform UI を使用して Red Hat OpenShift でアップグレードすることができます。

始める前に

注 : IBM MQ キュー・マネージャーの最新バージョンは 9.4.0.0-r1 であり、SC2 と CD の両方のバージョンです。 最新の IBM MQ キュー・マネージャーのリリース・ノートについては、IBM MQ Operator で使用するためのキュー・マネージャー・コンテナー・イメージのリリース履歴を参照してください。

- アップグレードするキュー・マネージャーが含まれている名前空間内の IBM Cloud Pak for Integration Platform UI にログインします。

- IBM MQ Operator で対象の更新チャネルを使用していることを確認してください。 42 ページの『IBM MQ Operator とキュー・マネージャーのアップグレード』を参照してください。

エア・ギャップ環境でキュー・マネージャーをアップグレードする前に、 CD IBM MQ Operator の 3.2.x SC2/CD チャネルへのアップグレードのエアー・ギャップ固有のステップを使用して、最新の IBM Cloud Pak for Integration イメージをミラーリングする必要があります。

手順

1. IBM Cloud Pak for Integration Platform UI ホーム・ページで「**ランタイム (Runtimes)**」タブをクリックします。
2. アップグレードが可能なキュー・マネージャーには、「**バージョン**」の隣に青色の **i** マークが付いています。 **i** マークをクリックすると、「**利用できる新しいバージョン (New version available)**」が表示されます。
3. アップグレードするキュー・マネージャーの右端にある 3 点メニューをクリックして、「**バージョンの変更 (Change version)**」をクリックします。
4. 「**新しいチャネルまたはバージョンの選択 (Select a new channel or version)**」の下で、必要なアップグレード・バージョンを選択します。
5. 「**バージョンの変更 (Change version)**」をクリックします。

タスクの結果
キュー・マネージャーがアップグレードされます。

OpenShift CP4I IBM MQ Operator のアンインストール

Red Hat OpenShift コンソールまたは CLI を使用して、Red Hat OpenShift から IBM MQ Operator をアンインストールできます。

手順

- オプション 1: OpenShift コンソールを使用して IBM MQ Operator をアンインストールします。

  注 : クラスター上のすべてのプロジェクト/名前空間に IBM MQ Operator がインストールされている場合は、キュー・マネージャーを削除するプロジェクトごとに、以下の手順のステップ 2 から 6 を繰り返します。

  a) Red Hat OpenShift Container Platform クラスター管理者資格情報を使用して、 Red Hat OpenShift Container Platform Web コンソールにログインします。

  b) 「**プロジェクト**」 を、 IBM MQ Operator をアンインストールする名前空間に変更します。 「**プロジェクト**」 ドロップダウン・リストから名前空間を選択します。

  c) ナビゲーション・ペインで、 「**オペレーター**」 > 「**インストール済みオペレーター**」をクリックします。

  d) 「**IBM MQ**」オペレーターをクリックします。

  e) 「**キュー・マネージャー**」タブをクリックして、この IBM MQ Operator によって管理されているキュー・マネージャーを表示します。

  f) 1 つ以上のキュー・マネージャーを削除します。

  これらのキュー・マネージャーは引き続き稼働しますが、IBM MQ Operator がない状態では正常に機能しない場合があることに注意してください。

  g) オプション: 必要に応じて、キュー・マネージャーを削除するプロジェクトごとにステップ 2 から 6 を繰り返します。

  h) 「**オペレーター (Operators)**」 > 「**インストール済みのオペレーター (Installed Operators)**」に戻ります。

  i) 「**IBM MQ**」オペレーターの横にある 3 点メニューをクリックし、「**オペレーターのアンインストール (Uninstall Operator)**」を選択します。

- オプション 2: OpenShift CLI を使用して IBM MQ Operator をアンインストールする

  a) `oc login` を使用して Red Hat OpenShift クラスターにログインします。

  b) IBM MQ Operator が 1 つの名前空間にインストールされている場合は、以下のサブステップを実行します。

  a. アンインストールする IBM MQ Operator が含まれているプロジェクトにいることを確認します。

  ```
  oc project project_name
  ```

  b. プロジェクトにインストールされているキュー・マネージャーを表示します。

  ```
  oc get qmgr
  ```

  c. 1 つ以上のキュー・マネージャーを削除します。

  ```
  oc delete qmgr qmgr_name
  ```

  これらのキュー・マネージャーは引き続き稼働しますが、IBM MQ Operator がない状態では正常に機能しない場合があることに注意してください。

  d. **ClusterServiceVersion** インスタンスを表示します。

  ```
  oc get csv
  ```

  e. IBM MQ **ClusterServiceVersion** を削除します。

  ```
  oc delete csv ibm_mq_csv_name
  ```

  f. サブスクリプションを表示します。

  ```
  oc get subscription
  ```

  g. すべてのサブスクリプションを削除します。

  ```
  oc delete subscription ibm_mq_subscription_name
  ```

  h. 共通サービスを使用しているものがほかにない場合は、共通サービス・オペレーターをアンインストールし、オペレーター・グループを削除できます。

  i) IBM Cloud Pak foundational services 製品資料の「Uninstalling foundational services」の説明に従って、共通サービス・オペレーターをアンインストールします。

  ii) オペレーター・グループを表示します。

  ```
  oc get operatorgroup
  ```

  iii) オペレーター・グループを削除します。

  ```
  oc delete OperatorGroup operator_group_name
  ```

  c) IBM MQ Operator がクラスター上のすべての名前空間にインストールされて使用可能な状態になっている場合は、以下のサブステップを実行します。

  a. インストールされているすべてのキュー・マネージャーを表示します。

  ```
  oc get qmgr -A
  ```

  b. 1 つ以上のキュー・マネージャーを削除します。

  ```
  oc delete qmgr qmgr_name -n namespace_name
  ```

  これらのキュー・マネージャーは引き続き稼働しますが、IBM MQ Operator がない状態では正常に機能しない場合があることに注意してください。

c. **ClusterServiceVersion** インスタンスを表示します。

```
oc get csv -A
```

d. クラスターから IBM MQ **ClusterServiceVersion** を削除します。

```
oc delete csv ibm_mq_csv_name -n openshift-operators
```

e. サブスクリプションを表示します。

```
oc get subscription -n openshift-operators
```

f. サブスクリプションを削除します。

```
oc delete subscription ibm_mq_subscription_name -n openshift-operators
```

g. オプション: 共通サービスを使用しているものが他にない場合は、共通サービス・オペレーターをアンインストールすることができます。 これを行うには、 IBM Cloud Pak foundational services 製品資料の「 基本サービスのアンインストール 」の説明に従ってください。

独自のコンテナー・イメージのビルドによる IBM MQ の準備

自作コンテナーを開発します。 これは最も柔軟なコンテナソリューションですが、コンテナの設定に強いスキルが必要であり、結果としてのコンテナを"所有する"必要があります。

始める前に

独自のコンテナーを開発する前に、代わりに IBM MQ Operator を使用できるかどうかを検討してください。 8 ページの『コンテナー内の IBM MQ の使用方法の選択』 を参照してください。

このタスクについて

手順

- 55 ページの『独自のキュー・マネージャー・イメージを作成する際の一般的な考慮事項』
- 56 ページの『サンプルの IBM MQ キュー・マネージャーのコンテナー・イメージのビルド』
- 58 ページの『別々のコンテナーでのローカル・バインディング・アプリケーションの実行』
- IBM MQ サンプルの Helm チャートを確認します。

独自のキュー・マネージャー・イメージを作成する際の一般的な考慮事項

コンテナーで IBM MQ キュー・マネージャーを実行するには、考慮すべき要件がいくつかあります。 サンプルのコンテナー・イメージは、これらの要件に対応できるようになっていますが、独自のイメージを使用する場合は、これらの要件に対応する方法を検討する必要があります。

プロセス監視

コンテナーを実行することは、基本的に単一のプロセス (コンテナー内部の PID 1) を実行することになります。この単一のプロセスは、後で子プロセスを spawn することができます。

メインプロセスが終了すると、コンテナー・ランタイムがコンテナーを停止します。 IBM MQ キュー・マネージャーでは、複数のプロセスをバックグラウンドで実行する必要があります。

このため、キュー・マネージャーの実行中は、メインプロセスがアクティブな状態であることを確認する必要があります。 グッド・プラクティスとして、例えば管理照会などを実行して、キュー・マネージャーがアクティブであることをこのプロセスから確認してください。

/var/mqm への移植

コンテナーは、 /var/mqm をボリュームとして構成する必要があります。

これを行うと、コンテナーが最初に始動したときに、このボリュームのディレクトリーは空の状態です。通常、このディレクトリーにはインストール時に内容が取り込まれますが、コンテナーを使用する場合は、インストールとランタイムが別々の環境になります。

これを解決するために、コンテナーが始動して初めて実行されるときに、**crtmqdir** コマンドを使用して、/var/mqm にデータを取り込みます。

コンテナーのセキュリティー

ランタイムのセキュリティー要件を最小限にするために、サンプルのコンテナー・イメージは、unzip 可能な IBM MQ インストールを使用してインストールされます。 これにより、setuid ビットが設定されなくなり、コンテナーは特権エスカレーションを使用する必要がなくなります。 コンテナー・システムの中には、使用できるユーザー ID を定義したものもありますが、この unzip 可能なインストールでは、使用可能なオペレーティング・システム・ユーザーについて一切想定されていません。

サンプルの IBM MQ キュー・マネージャーのコンテナー・イメージのビルド

コンテナーで IBM MQ キュー・マネージャーを実行するためにサンプルのコンテナー・イメージをビルドするには、この情報を活用してください。

このタスクについて

まず、Red Hat Universal Base Image ファイル・システムと IBM MQ のクリーン・インストールが含まれているベース・イメージをビルドします。

次に、そのベースの上に、ユーザー ID とパスワードによる基本的なセキュリティーを可能にする IBM MQ 構成を追加するための別のコンテナー・イメージ層をビルドします。

最後に、このイメージをファイル・システムとして使用し、ホスト・ファイル・システム上のコンテナー固有のボリュームによって提供される /var/mqm の内容を使用してコンテナーを実行します。

手順

- コンテナーで IBM MQ キュー・マネージャーを実行するためにサンプルのコンテナー・イメージをビルドする方法については、以下のサブトピックを参照してください。
  - 56 ページの『サンプルの IBM MQ キュー・マネージャーのベース・イメージのビルド』
  - 57 ページの『サンプルの構成済みの IBM MQ キュー・マネージャーのイメージのビルド』

サンプルの *IBM MQ* キュー・マネージャーのベース・イメージのビルド

独自のコンテナー・イメージの IBM MQ を使用するためには、まず、IBM MQ クリーン・インストールを含むベース・イメージをビルドする必要があります。 以下の手順は、GitHub でホストされているサンプル・コードを使用してサンプルのベース・イメージをビルドする方法を示しています。

手順

- mq-container GitHub リポジトリーで提供されている Make ファイルを使用して実稼働用のコンテナー・イメージをビルドします。

  GitHub の コンテナー・イメージの作成の指示に従います。
- オプション: Red Hat OpenShift Container Platform "restricted" Security Context Constraint (SCC) を使用してセキュア・アクセスを構成する予定の場合は、 IBM MQ 非インストール・イメージの 1 つを使用してください。

  これらのイメージをダウンロードするためのリンクは、 IBM MQ ダウンロードの「コンテナー」セクションにあります。

タスクの結果

IBM MQ がインストールされたベース・コンテナー・イメージができました。

これで、構成済みのサンプル IBM MQ キュー・マネージャー・イメージを作成する準備ができました。

サンプルの構成済みの *IBM MQ* キュー・マネージャーのイメージのビルド

汎用的なベースの IBM MQ コンテナー・イメージをビルドしたら、セキュアなアクセスを可能にするために独自の構成を適用する必要があります。 これを行うには、汎用イメージを親として使用して、独自のコンテナー・イメージ層を作成します。

始める前に

このタスクは、サンプルの基本 IBM MQ キュー・マネージャー・イメージの作成時に "インストールなし" の IBM MQ パッケージを使用したことが前提になっています。 そうでない場合は、Red Hat OpenShift Container Platform の "制限付き" のセキュリティー・コンテキスト制約 (SCC) を使用してセキュア・アクセスを構成することができなくなります。 デフォルトで使用される "制限付き" の SCC では、ランダムのユーザー ID が使用され、別のユーザーへの変更による特権のエスカレーションが不可になります。 IBM MQ の従来の RPM ベースのインストーラーは、mqm のユーザーとグループに依存していて、実行可能プログラムで setuid ビットを使用します。 現行バージョンの IBM MQ では、 "No-Install" IBM MQ パッケージを使用すると、 mqm ユーザーも mqm グループも存在しなくなります。

手順

1. 新しいディレクトリーを作成し、以下を内容とする config.mqsc というファイルを追加します。

```
DEFINE QLOCAL(EXAMPLE.QUEUE.1) REPLACE
```

   上記の例では、ユーザー ID とパスワードによる単純な認証が使用されることに注意してください。 ただし、企業が必要とする任意のセキュリティー構成を適用できます。

2. 以下を内容とする Dockerfile というファイルを作成します。

```
FROM mq
COPY config.mqsc /etc/mqm/
```

3. 次のコマンドを使用して、カスタム・コンテナー・イメージをビルドします。

```
docker build -t mymq .
```

   「.」は、先ほど作成した 2 つのファイルが含まれているディレクトリーです。

   Docker はそのイメージを使用して一時コンテナーを作成し、残りのコマンドを実行します。

   注 : Red Hat Enterprise Linux (RHEL) では、コマンド **docker** (RHEL V7) または **podman** (RHEL V7 または RHEL V8) を使用します。 Linux では、コマンドの先頭に **sudo** を指定して **docker** コマンドを実行し、追加の特権を取得する必要があります。

4. カスタマイズした新しいイメージを実行して、先ほど作成したディスク・イメージを含む新しいコンテナーを作成します。

   新しいイメージ層では、実行する特定のコマンドを指定しなかったので、親イメージから継承されています。 親のエントリー・ポイント (このコードは GitHub で提供されています):

   - キュー・マネージャーを作成する
   - キュー・マネージャーを開始する
   - デフォルトのリスナーを作成する
   - 次に、 /etc/mqm/config.mqsc.から MQSC コマンドを実行します

   以下のコマンドを発行して、カスタマイズした新しいイメージを実行します。

```
docker run \
  --env LICENSE=accept \
  --env MQ_QMGR_NAME=QM1 \
  --volume /var/example:/var/mqm \
  --publish 1414:1414 \
```

```
--detach \
mymq
```

説明:

最初の env パラメーター
IBM IBM WebSphere® MQ のライセンスに同意したことを知らせる環境変数をコンテナーに渡しています。 LICENSE 変数を view に設定してライセンスを表示することもできます。

IBM MQ ライセンスについて詳しくは、 IBM MQ ライセンス情報 を参照してください。

2 番目の env パラメーター
使用するキュー・マネージャー名を設定しています。

volume パラメーター
MQ が `/var/mqm` 上で実際に `/var/example` に書き込む必要があることをコンテナーに指示します。

このオプションは、後で永続データを保持したままコンテナーを簡単に削除できることを意味します。 このオプションにより、ログ・ファイルの表示も簡単になります。

publish パラメーター
ホスト・システムのポートをコンテナーのポートにマップしています。 デフォルトでは、コンテナーはコンテナー自身の内部 IP アドレスを使用して実行されます。つまり、ポートを公開するには、具体的にポートをマップする必要があります。

この例では、ホストのポート 1414 をコンテナーのポート 1414 にマップしています。

detach パラメーター
バックグラウンドでコンテナーを実行します。

タスクの結果

構成したコンテナー・イメージをビルドしたので、**docker ps** コマンドを使用して、実行中のコンテナーを表示できます。 **docker top** コマンドを使用して、コンテナーで実行されている IBM MQ プロセスを表示できます。

重要 :

docker logs ${CONTAINER_ID} コマンドを使用して、コンテナーのログを表示できます。

次のタスク

- **docker ps** コマンドを使用してもコンテナーが表示されない場合は、コンテナーが失敗している可能性があります。 **docker ps -a** コマンドを使用して、失敗したコンテナーを表示できます。
- **docker ps -a** コマンドを使用すると、コンテナー ID が表示されます。 この ID は、**docker run** コマンドを発行したときにも表示されたものです。
- **docker logs ${CONTAINER_ID}** コマンドを使用して、コンテナーのログを表示できます。

別々のコンテナーでのローカル・バインディング・アプリケーションの実行

コンテナー間でプロセス名前空間を共有することにより、 IBM MQ キュー・マネージャーとは別のコンテナーにある IBM MQ へのローカル・バインディング接続を必要とするアプリケーションを実行できます。

このタスクについて

以下の制約事項に従う必要があります。

- `--pid` 引数を使用して、各コンテナーの PID 名前空間を共有する必要があります。
- `--ipc` 引数を使用して、各コンテナーの IPC 名前空間を共有する必要があります。
- 以下のいずれかが必要です。
  1. `--uts` 引数を使用して、各コンテナーの UTS 名前空間をホストと共有する。

2. -h 引数または --hostname 引数を使用して、各コンテナーを同じホスト名にする。

- IBM MQ データディレクトリは、 /var/mqm ディレクトリの下にあるすべてのコンテナが利用可能なボリュームにマウントする必要があります。

以下の例では、サンプルの IBM MQ コンテナー・イメージを使用しています。 このイメージの詳細については、Github を参照してください。

手順

1. 次のコマンドを発行して、ボリュームとして機能する一時ディレクトリーを作成します。

```
mkdir /tmp/dockerVolume
```

2. 次のコマンドを発行して、1 つのコンテナー内にキュー・マネージャー (QM1) を作成し、名前 sharedNamespace を指定します。

```
docker run -d -e LICENSE=accept -e MQ_QMGR_NAME=QM1 --volume /tmp/dockerVol:/mnt/mqm
--uts host --name sharedNamespace ibmcom/mq
```

3. 次のコマンドを発行して、ibmcom/mq をベースとする secondaryContainer という 2 つ目のコンテナーを始動します。ただし、キュー・マネージャーは作成しません。

```
docker run --entrypoint /bin/bash --volumes-from sharedNamespace --pid
container:sharedNamespace --ipc container:sharedNamespace --uts host --name
secondaryContainer -it --detach ibmcom/mq
```

4. 次のコマンドを発行して、2 つ目のコンテナーに対して **dspmq** コマンドを実行し、両方のキュー・マネージャーの状況を調べます。

```
docker exec secondaryContainer dspmq
```

5. 次のコマンドを実行して、もう一方のコンテナーで実行されているキュー・マネージャーに対する MQSC コマンドを処理します。

```
docker exec -it secondaryContainer runmqsc QM1
```

タスクの結果

これで、別々のコンテナーでローカル・アプリケーションが実行されるようになりました。**dspmq**、**amqsput**、**amqsget**、**runmqsc** などのコマンドを、QM1 キュー・マネージャーへのローカル・バインディングとして、2 つ目のコンテナーから正常に実行することができます。

予期した結果にならない場合は、59 ページの『名前空間アプリケーションのトラブルシューティング』で詳細を参照してください。

名前空間アプリケーションのトラブルシューティング

共有の名前空間を使用する場合は、すべての名前空間 (IPC、PID、UTS/ホスト名) およびマウント・ボリュームを共有する必要があります。そうしないと、アプリケーションは機能しません。

従う必要がある制約事項のリストについては、58 ページの『別々のコンテナーでのローカル・バインディング・アプリケーションの実行』を参照してください。

リストされているすべての制約事項をアプリケーションが満たしていないと、コンテナーが始動しても、予期したように機能しないという問題が発生する可能性があります。

以下のリストに、一般的な原因と、制約事項のいずれかを満たすことを忘れた場合に見られる動作をまとめています。

- コンテナーの名前空間 (UTS/PID/IPC)、またはホスト名のいずれかを共有することを忘れた状態でボリュームをマウントした場合、コンテナーは、キュー・マネージャーを認識できますが、キュー・マネージャーと対話することができません。

- **dspmq** コマンドの場合は、以下のようになります。

```
docker exec container dspmq

QMNAME(QM1)                       STATUS(Status not available)
```

- **runmqsc** コマンドなど、キュー・マネージャーに接続しようとするコマンドの場合は、AMQ8146 エラー・メッセージを受け取るはずです。

```
docker exec -it container runmqsc QM1
5724-H72 (C) Copyright IBM Corp. 1994, 2024.
Starting MQSC for queue manager QM1.
AMQ8146: IBM MQ queue manager not available
```

- すべての必要な名前空間を共有しているが、共有ボリュームを /var/mqm ディレクトリーにマウントせず、有効な IBM MQ データ・パスを持っている場合は、コマンドも アンキ 8146 のエラー・メッセージを受け取ります。

  しかし、**dspmq** は、キュー・マネージャーをまったく認識できないので、代わりに空の応答を返します。

```
docker exec container dspmq
```

- 必要なすべての名前空間を共有しているが、共有ボリュームを /var/mqm ディレクトリーにマウントせず、有効な IBM MQ データ・パス (または IBM MQ データ・パスなし) を持っていない場合は、データ・パスが IBM MQ インストールのキー・コンポーネントであるため、さまざまなエラーが表示されます。データ・パスがなければ、IBM MQ は動作できません。

  以下のコマンドのいずれかを実行したときに、これらの例に示すような応答が表示される場合は、ディレクトリーをマウントしたこと、または IBM MQ データ・ディレクトリーを作成したことを確認する必要があります。

```
docker exec container dspmq
'No such file or directory' from /var/mqm/mqs.ini
AMQ6090: IBM MQ was unable to display an error message FFFFFFFF.
AMQffff

docker exec container dspmqver
AMQ7047: An unexpected error was encountered by a command. Reason code is 0.

docker exec container mqrc
<file path>/mqrc.c[1152]
lpiObtainQMDetails --> 545261715

docker exec container crtmqm QM1
AMQ8101: IBM MQ error (893) has occurred.

docker exec container strmqm QM1
AMQ6239: Permission denied attempting to access filesystem location '/var/mqm'.
AMQ7002: An error occurred manipulating a file.

docker exec container endmqm QM1
AMQ8101: IBM MQ error (893) has occurred.

docker exec container dltmqm QM1
AMQ7002: An error occurred manipulating a file.

docker exec container strmqweb
<file path>/mqrc.c[1152]
lpiObtainQMDetails --> 545261715
```

MQ Adv. 独自のコンテナーを作成する場合のネイティブ HA グループの作成

ネイティブ HA グループを作成するには、3 つのキュー・マネージャーを作成、構成、および開始する必要があります。

このタスクについて

ネイティブ HA ソリューションを作成するために推奨される方法は、 IBM MQ 演算子を使用することです (ネイティブ HA を参照)。 あるいは、独自のコンテナーを作成する場合は、以下の手順に従うことができます。

ネイティブ HA グループを作成するには、ログ・タイプを log replication に設定して、3 つのノードに 3 つのキュー・マネージャーを作成します。 次に、各キュー・マネージャーの qm.ini ファイルを編集して、3 つのノードのそれぞれの接続の詳細を追加し、ログ・データを相互に複製できるようにします。

その後、3 つすべてのキュー・マネージャーを開始して、3 つすべてのインスタンスが相互に通信できることを確認し、どのインスタンスがアクティブ・インスタンスになり、どのインスタンスがレプリカになるかを判別できるようにする必要があります。

注 : この方法で独自のコンテナーにネイティブ HA グループを作成できるのは、 Kubernetes または Red Hat OpenShift を実行している場合のみです。

手順

1. 3 つのノードのそれぞれで、ログ・レプリカのログ・タイプを指定し、各ログ・インスタンスに固有の名前を指定して、キュー・マネージャーを作成します。 各キュー・マネージャーの名前は同じです。

   ```
   crtmqm -lr instance_name qmname
   ```

   以下に例を示します。

   ```
   node 1> crtmqm -lr qm1_inst1 qm1

   node 2> crtmqm -lr qm1_inst2 qm1

   node 3> crtmqm -lr qm1_inst3 qm1
   ```

2. 各キュー・マネージャーが正常に作成されると、 NativeHALocalInstance という名前のスタンザがキュー・マネージャー構成ファイル qm.ini に追加されます。 指定されたインスタンス名を指定する Name 属性がスタンザに追加されます。

   オプションで、以下の属性を qm.ini ファイルの NativeHALocalInstance スタンザに追加できます。

   KeyRepository
   ログ複製トラフィックの保護のために、使用するデジタル証明書を保持する鍵リポジトリーのロケーション。 位置は語幹形式で指定されます。つまり、拡張子なしの絶対パスとファイル名が含まれます。 KeyRepository スタンザ属性を省略すると、インスタンス間でログ複製データがプレーン・テキストで交換されます。

   CertificateLabel
   ログ複製トラフィックの保護に使用するデジタル証明書を識別する証明書ラベル。 KeyRepository が指定されているが、 CertificateLabel が省略されている場合は、デフォルト値 ibmwebspheremq*queue_manager* が使用されます。

   CipherSpec
   ログ複製トラフィックを保護するために使用する MQCipherSpec。 このスタンザ属性を指定する場合は、 KeyRepository も指定する必要があります。 KeyRepository が指定されているが、 CipherSpec が省略されている場合は、デフォルト値 ANY が使用されます。

   LocalAddress
   ログ複製トラフィックを受け入れるローカル・ネットワーク・インターフェース・アドレス。 このスタンザ属性が指定されている場合は、「[addr] [(port)]」の形式を使用してローカル・ネットワーク・インターフェースまたはポート (あるいはその両方) を識別します。 ネットワーク・アドレスは、ホスト名、 IPv4 小数点付き 10 進数、または IPv6 16 進形式で指定できます。 この属性を省略すると、キュー・マネージャーはすべてのネットワーク・インターフェースへのバインドを試行し、ローカル・インスタンス名と一致する NativeHAInstances スタンザの ReplicationAddress に指定されているポートを使用します。

HeartbeatInterval
ハートビート間隔は、ネイティブ HA キュー・マネージャーのアクティブ・インスタンスがネットワーク・ハートビートを送信する頻度をミリ秒単位で定義します。 ハートビート間隔値の有効範囲は 500 (0.5 秒) から 60000 (1 分) で、この範囲外の値を使用するとキュー・マネージャーの開始が失敗します。 この属性を省略すると、デフォルト値の 5000 (5 秒) が使用されます。 各インスタンスで同じハートビート間隔を使用する必要があります。

HeartbeatTimeout
ハートビート・タイムアウトは、ネイティブ HA キュー・マネージャーのレプリカ・インスタンスが、アクティブ・インスタンスが応答しないと判断するまで待機する時間の長さを定義します。 ハートビート間隔タイムアウト値の有効範囲は 500 (0.5 秒) から 120000 (2 分) です。 ハートビート・タイムアウトの値は、ハートビート間隔以上でなければなりません。

無効な値を指定すると、キュー・マネージャーの開始が失敗します。 この属性が省略されると、レプリカは、新しいアクティブ・インスタンスを選択するプロセスを開始する前に 2 x HeartbeatInterval 待機します。 各インスタンスで同じハートビート・タイムアウトを使用する必要があります。

RetryInterval
再試行間隔は、障害が発生した複製リンクがネイティブ HA キュー・マネージャーで再試行される頻度をミリ秒単位で定義します。 再試行間隔の有効範囲は 500 (0.5 秒) から 120000 (2 分) です。 この属性が省略されると、レプリカは、障害が発生した複製リンクを再試行する前に 2 x HeartbeatInterval 待機します。

3. 各キュー・マネージャーの qm.ini ファイルを編集し、接続の詳細を追加します。 ネイティブ HA グループ内のキュー・マネージャー・インスタンス (ローカル・インスタンスを含む) ごとに 1 つずつ、合計 3 つの NativeHAInstance スタンザを追加します。 以下の属性を追加します。

名前
キュー・マネージャー・インスタンスの作成時に使用したインスタンス名を指定します。

ReplicationAddress
インスタンスのホスト名、IPv4 ドット 10 進または IPv6 16 進形式のアドレスを指定します。 アドレスは、ホスト名、 IPv4 小数点付き 10 進数、または IPv6 16 進形式のアドレスとして指定できます。 複製アドレスは、グループ内の各インスタンスから解決可能かつルーティング可能でなければなりません。 ログ複製に使用するポート番号は、大括弧で囲んで指定する必要があります。以下に例を示します。

```
ReplicationAddress=host1.example.com(4444)
```

注: NativeHAInstance スタンザはすべてのインスタンスで同じであり、自動構成 (**crtmqm -ii**) を使用して提供できます。

4. 以下の 3 つのインスタンスのそれぞれを開始します。

```
strmqm QMgrName
```

インスタンスが開始されると、3 つのインスタンスがすべて実行中であることを確認するために通信が行われます。次に、3 つのインスタンスのうちどちらがアクティブ・インスタンスであるかを決定し、残りの 2 つのインスタンスは引き続きレプリカとして実行されます。

例

以下の例は、3 つのインスタンスのいずれかに必要なネイティブ HA の詳細を指定する qm.ini ファイルのセクションを示しています。

```
NativeHALocalInstance:
  LocalName=node-1

NativeHAInstance:
  Name=node-1
  ReplicationAddress=host1.example.com(4444)
NativeHAInstance:
  Name=node-2
  ReplicationAddress=host2.example.com(4444)
NativeHAInstance:
```

```
Name=node-3
ReplicationAddress=host3.example.com(4444)
```

コンテナーでのキュー・マネージャーのデプロイおよび構成

IBM MQ キュー・マネージャーをデプロイおよび構成するには、さまざまなタスクを実行します。

このタスクについて

キュー・マネージャーのデプロイおよび構成を開始するには、以下のトピックを参照してください。

手順

- 63 ページの『IBM MQ Operator を使用したキュー・マネージャーのデプロイおよび構成』
- 104 ページの『Helm を使用したキュー・マネージャーのデプロイおよび構成』

OpenShift IBM MQ Operator を使用したキュー・マネージャーのデプロイおよび構成

構成例: HA の構成、 OpenShift クラスターの外部からの接続、 CP4i ダッシュボードとの統合、Instana トレースとの統合、カスタム MQSC ファイルおよび INI ファイルを使用したイメージの作成、カスタム・アノテーションおよびラベルの追加。

このタスクについて

手順

- 66 ページの『キュー・マネージャーの構成例』.
- 75 ページの『IBM MQ Operator を使用したキュー・マネージャーの高可用性の構成』.
- 84 ページの『Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成』.
- 86 ページの『IBM MQ と IBM Instana トレースの統合』.
- 93 ページの『Red Hat OpenShift CLI を使用した、カスタム MQSC および INI ファイルを使用したイメージの作成』.
- 95 ページの『キュー・マネージャー・リソースへのカスタム・アノテーションとカスタム・ラベルの追加』.
- 95 ページの『実行時 Webhook チェックの無効化』.
- 96 ページの『キュー・マネージャー仕様に対するデフォルト値更新の無効化』.

OpenShift CP4I IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ

この例では、一時 (非永続) ストレージを使用する「クイック・スタート」キュー・マネージャーをデプロイし、 IBM MQ セキュリティーをオフにします。 メッセージは、キュー・マネージャーの再始動後は保持されません。 構成を調整することで、キュー・マネージャーのさまざまな設定を変更できます。

このタスクについて

このタスクには、キュー・マネージャーを OpenShift にデプロイするための 3 つのオプションが用意されています。

1. OpenShift コンソールを使用してキュー・マネージャーをデプロイします。
2. OpenShift CLI を使用してキュー・マネージャーをデプロイします。
3. IBM Cloud Pak for Integration Platform UI を使用してキュー・マネージャーをデプロイします。

手順

- **オプション 1: OpenShift コンソールを使用してキュー・マネージャーをデプロイする。**

  a) キュー・マネージャーをデプロイします。

  a. Red Hat OpenShift Container Platform クラスター管理者資格情報を使用して、 OpenShift コンソールにログインします。

  b.「**プロジェクト**」 を、 IBM MQ Operator をインストールした名前空間に変更します。 「**プロジェクト**」 ドロップダウン・リストから名前空間を選択します。

  c. ナビゲーション・ペインで、 「**オペレーター**」 >「**インストール済みオペレーター**」をクリックします。

  d.「インストール済みオペレーター (Installed Operators)」パネルのリストで、 **IBM MQ** を見つけてクリックします。

  e.「**キュー・マネージャー (Queue Manager)**」タブをクリックします。

  f.「**QueueManager の作成 (Create QueueManager)**」ボタンをクリックします。 インスタンス作成パネルが表示され、リソースを構成するための 2 つの方法 (**フォーム・ビュー** と **YAML ビュー**) が示されます。 デフォルトでは、 「**フォーム・ビュー**」 が選択されています。

  b) キュー・マネージャーを構成します。

  ステップ 2 オプション 1: **フォーム・ビュー**で構成します。

  「**フォーム・ビュー**」 は、リソース構成を表示または変更するために使用できるフォームを開きます。

  a.「**ライセンス**」の横にある矢印をクリックして、ライセンス承諾セクションを展開します。

  b. ご使用条件に同意する場合は、 「**ライセンスの受諾**」 を **true** に設定します。

  c. 矢印をクリックしてドロップダウン・リストを開き、ライセンスを選択します。 IBM MQ は、複数の異なるライセンスで提供されています。 有効なライセンスについて詳しくは、139 ページの『mq.ibm.com/v1beta1 のライセンスのリファレンス』を参照してください。 キュー・マネージャーをデプロイするには、ライセンスに同意する必要があります

  d.「**作成**」 をクリックします。 現在のプロジェクト (名前空間) 内のキュー・マネージャーのリストが表示されます。 新しい `QueueManager` が `Pending` の状態になっているはずです。

  ステップ 2 オプション 2: **YAML ビュー**で構成します。

  YAML ビュー は、`QueueManager` の YAML ファイルの例を含むエディターを開きます。 以下の手順に従って、ファイル内の値を更新します。

  a. `metadata.namespace` をプロジェクト (名前空間) 名に変更します。

  b. `spec.license.license` の値を、要件に一致するライセンス・ストリングに変更します。 ライセンスの詳細については、 139 ページの『mq.ibm.com/v1beta1 のライセンスのリファレンス』を参照してください。

  c. ご使用条件に同意する場合は、 `spec.license.accept` を `true` に変更します。

  d.「**作成**」 をクリックします。 現在のプロジェクト (名前空間) 内のキュー・マネージャーのリストが表示されます。 新しい `QueueManager` が `Pending` の状態になっているはずです。

  c) キュー・マネージャーの作成を確認してください。

  キュー・マネージャーが作成されたことを確認するには、以下の手順を実行します。

  a. IBM MQ Operator を作成した名前空間内にいることを確認します。

  b.「**ホーム**」 画面で、 **オペレーター** >「**インストール済みオペレーター**」をクリックし、キュー・マネージャーを作成した対象のインストール済み IBM MQ Operator を選択します。

  c.「**キュー・マネージャー (Queue Manager)**」タブをクリックします。 `QueueManager` の状況が `Running` になったら、作成は完了です。

- **オプション 2: OpenShift CLI を使用してキュー・マネージャーをデプロイする。**

  a) `QueueManager` YAML ファイルの作成

例えば、IBM Cloud Pak for Integration に基本的なキュー・マネージャーをインストールするには、以下を内容とするファイル「mq-quickstart.yaml」を作成します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
spec:
  version: 9.4.0.0-r1
  license:
    accept: false
    license: L-BMSF-5YDSLR
    use: NonProduction
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
      queueManager:
        type: ephemeral
```

重要 : ご使用条件に同意する場合は、`accept: false` を `accept: true` に変更します。 ライセンスについて詳しくは、139 ページの『mq.ibm.com/v1beta1 のライセンスのリファレンス』を参照してください。

この例には、キュー・マネージャーとともにデプロイされ、 IBM Cloud Pak for Integration 内でシングル・サインオンを使用して Web コンソールが使用可能になっている Web サーバーも含まれています。 シングル・サインオンを機能させるには、最初に他の IBM Cloud Pak for Integration コンポーネントをインストールする必要があります。 39 ページの『CP4I で使用するための IBM MQ Operator のインストール』を参照してください。

IBM Cloud Pak for Integration とは別に、基本的なキュー・マネージャーをインストールするには、以下を内容とするファイル「mq-quickstart.yaml」を作成します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart
spec:
  version: 9.4.0.0-r1
  license:
    accept: false
    license: L-EHXT-MQCRN9
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
      queueManager:
        type: ephemeral
```

重要: MQ のご使用条件に同意する場合は、 `accept: false` を `accept: true` に変更してください。 ライセンスについて詳しくは、139 ページの『mq.ibm.com/v1beta1 のライセンスのリファレンス』を参照してください。

b) `QueueManager` オブジェクトを作成します。

```
oc apply -f mq-quickstart.yaml
```

c) キュー・マネージャーの作成を確認してください。

以下の手順を実行して、キュー・マネージャーが作成されたことを確認します。

a. デプロイメントを検証します。

```
oc describe queuemanager Queue_Manager_Resource_Name
```

b. 状況を確認します。

```
oc describe queuemanager quickstart
```

- **オプション 3: IBM Cloud Pak for Integration Platform UI を使用してキュー・マネージャーをデプロイする。**

  プラットフォーム UI を使用したインスタンスのデプロイの手順に従います。

関連タスク

84 ページの『Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成』
Red Hat OpenShift クラスターの外部から IBM MQ キュー・マネージャーにアプリケーションを接続するには、 Red Hat OpenShift 経路が必要です。 IBM MQ キュー・マネージャーおよびクライアント・アプリケーションで TLS を有効にする必要があります。SNI は、TLS 1.2 以上のプロトコルが使用されている場合にのみ TLS プロトコルで使用できるためです。 Red Hat OpenShift Container Platform Router では、IBM MQ キュー・マネージャーへの要求のルーティングに SNI が使用されます。

129 ページの『IBM MQ Console クラスターにデプロイされた Red Hat OpenShift への接続』
Red Hat OpenShift Container Platform クラスターにデプロイされているキュー・マネージャーの IBM MQ Console に接続する方法について説明します。

66 ページの『キュー・マネージャーの構成例』
QueueManager カスタム・リソースの内容を調整することによってキュー・マネージャーを構成できます。

OpenShift CP4I キュー・マネージャーの構成例

QueueManager カスタム・リソースの内容を調整することによってキュー・マネージャーを構成できます。

このタスクについて

QueueManager YAML ファイルを使用してキュー・マネージャーを構成するのに役立つ例を以下に挙げます。

手順

- 66 ページの『例: MQSC ファイルと INI ファイルの提供』
- 69 ページの『例: 相互 TLS 認証を使用したキュー・マネージャーの構成』

OpenShift CP4I 例: *MQSC* ファイルと *INI* ファイルの提供

この例では、2 つの MQSC ファイルと 1 つの INI ファイルを組み込んだ Kubernetes ConfigMap を作成します。 その後、それらの MQSC ファイルと INI ファイルを処理するキュー・マネージャーをデプロイします。

このタスクについて

MQSC ファイルと INI ファイルは、キュー・マネージャーのデプロイ時に提供できます。 MQSC と INI のデータは、1 つ以上の Kubernetes ConfigMap とシークレットで定義する必要があります。 キュー・マネージャーをデプロイする名前空間 (プロジェクト) 内にそれらを作成してください。

注 : MQSC ファイルや INI ファイルに機密データを組み込む場合は、Kubernetes シークレットを使用してください。

例

2 つの MQSC ファイルと 1 つの INI ファイルを組み込んだ Kubernetes ConfigMap を作成する例を以下に示します。 その後、それらの MQSC ファイルと INI ファイルを処理するキュー・マネージャーをデプロイします。

ConfigMap の例 - 以下の YAML をクラスターに適用します。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: mqsc-ini-example
data:
  example1.mqsc: |
    DEFINE QLOCAL('DEV.QUEUE.1') REPLACE
```

```
    DEFINE QLOCAL('DEV.QUEUE.2') REPLACE
  example2.mqsc: |
    DEFINE QLOCAL('DEV.DEAD.LETTER.QUEUE') REPLACE
  example.ini: |
    Channels:
       MQIBindType=FASTPATH
```

QueueManager の例-コマンド行または Red Hat OpenShift Container Platform Web コンソールを使用して、以下の構成でキュー・マネージャーをデプロイします。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mqsc-ini-qm
spec:
  version: 9.4.0.0-r1
  license:
    accept: false
    license: L-EHXT-MQCRN9
    use: Production
  web:
    enabled: true
  queueManager:
    name: "MQSCINI"
    mqsc:
    - configMap:
        name: mqsc-ini-example
        items:
        - example1.mqsc
        - example2.mqsc
    ini:
    - configMap:
        name: mqsc-ini-example
        items:
        - example.ini
    storage:
      queueManager:
        type: ephemeral
```

重要 : IBM MQ Advanced のご使用条件に同意する場合は、`accept: false` を `accept: true` に変更します。 ライセンスの詳細については、mq.ibm.com/v1beta1 のライセンス交付に関する参照資料を参照してください。

追加情報:

- キュー・マネージャーは、単一の Kubernetes ConfigMap またはシークレット (この例を参照) を使用するように構成することも、複数の ConfigMaps およびシークレットを使用するように構成することもできます。
- この例のように 1 つの Kubernetes ConfigMap またはシークレットから MQSC と INI のすべてのデータを使用することも、キュー・マネージャーごとに使用可能なファイルのサブセットだけを使用するように構成することも可能です。
- MQSC ファイルと INI ファイルは、それぞれのキーに基づいてアルファベット順に処理されます。 したがって、`example1.mqsc` は、キュー・マネージャー構成での表示順序に関係なく、常に `example2.mqsc` の前に処理されます。
- 複数の Kubernetes ConfigMap またはシークレットにまたがる複数の MQSC ファイルや INI ファイルが同じキーを持っている場合、その一連のファイルはそれぞれがキュー・マネージャー構成で定義されている順序に基づいて処理されます。
- キュー・マネージャー・ポッドの実行中は、 Kubernetes ConfigMap に対する変更は反映されません。これは、 IBM MQ Operator が変更を認識しないためです。 ConfigMap に変更を加えた場合 (例えば、MQSC コマンドまたは INI ファイルに変更を加えた場合)、それらの変更を有効にするには、キュー・マネージャーを手動で再始動する必要があります。 単一インスタンス・キュー・マネージャーの場合は、ポッドを削除して、必要な再始動をトリガーします。 ネイティブ HA デプロイメントの場合は、まずスタンバイ・ポッドを削除して再始動します。 再度実行状態になったら、アクティブ・ポッドを削除して再始動します。 この再始動の順序により、キュー・マネージャーのダウン時間を最小限に抑えることができます。

OpenShift CP4I *OpenSSL を使用した自己署名 PKI の作成*

IBM MQ では、認証に相互 TLS を使用できます。この場合、接続の両端で証明書が提供され、証明書の詳細を使用してキュー・マネージャーとの ID が確立されます。 このトピックでは、 OpenSSL コマンド行ツールを使用して Public Key Infrastructure (PKI) の例を作成し、他の例で使用できる 2 つの証明書を作成する方法について説明します。

始める前に

OpenSSL コマンド・ライン・ツールがインストールされていることを確認します。

IBM MQ client をインストールし、`samp/bin` と `bin` を パスに追加します。 **runmqicred** コマンドが必要です。このコマンドは、以下のように IBM MQ client の一部としてインストールできます。

- Windows Linux Windows および Linux の場合: https://ibm.biz/mq94redistclients から、ご使用のオペレーティング・システム用の IBM MQ 再配布可能クライアントをインストールします。
- macOS Mac の場合: IBM MQ MacOS Toolkit をダウンロードしてセットアップします。 https://developer.ibm.com/tutorials/mq-macos-dev/

このタスクについて

重要 : ここで説明する例は、実稼働環境には適しておらず、すぐに使用できるようにするための例としてのみ意図されています。 証明書管理は、上級者向けの複雑なサブジェクトです。 実動環境では、ローテーション、取り消し、鍵の長さ、災害復旧などを考慮する必要があります。

これらのステップは、 OpenSSL 3.1.4 を使用してテストされています。

手順

1. 内部認証局に使用する秘密鍵を作成します

   ```
   openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:4096 -out ca.key
   ```

   内部認証局の秘密鍵は、 *ca.key* というファイルに作成されます。 このファイルは、安全に秘密にしておく必要があります。内部認証局の証明書に署名するために使用されます。
2. 内部認証局の自己署名証明書の発行

   ```
   openssl req -x509 -new -nodes -key ca.key -sha512 -days 30 -subj "/CN=example-selfsigned-ca"
   -out ca.crt
   ```

   `-days` は、ルート CA 証明書が有効である日数を指定します。

   ca.crt というファイルに証明書が作成されます。 この証明書には、内部認証局に関する公開情報が含まれており、自由に共有できます。
3. キュー・マネージャーの秘密鍵と証明書の作成

   a) キュー・マネージャーの秘密鍵および証明書署名要求の作成

   ```
   openssl req -new -nodes -out example-qm.csr -newkey rsa:4096 -keyout example-qm.key -subj
   '/CN=example-qm'
   ```

   example-qm.key という名前のファイルに秘密鍵が作成され、 *example-qm.csr* という名前のファイルに証明書署名要求が作成されます。

   b) 内部認証局を使用してキュー・マネージャー鍵に署名します。

   ```
   openssl x509 -req -in example-qm.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
   example-qm.crt -days 7 -sha512
   ```

   `-days` は、証明書が有効になる日数を指定します。

   example-qm.crt というファイルに署名証明書が作成されます。

   c) キュー・マネージャーの鍵と証明書を使用して Kubernetes 秘密を作成します。

```
oc create secret generic example-qm-tls --type="kubernetes.io/tls" --from-
file=tls.key=example-qm.key --from-file=tls.crt=example-qm.crt --from-file=ca.crt
```

example-qm-tls という Kubernetes シークレットが作成されます。 この秘密には、キュー・マネージャーの秘密鍵、公開証明書、および CA 証明書が含まれています。

4. アプリケーションの秘密鍵と証明書の作成

a) アプリケーションの秘密鍵および証明書署名要求の作成

```
openssl req -new -nodes -out example-app1.csr -newkey rsa:4096 -keyout example-app1.key
-subj '/CN=example-app1'
```

example-app1.key というファイルに秘密鍵が作成され、*example-app1.csr* というファイルに証明書署名要求が作成されます。

b) 内部認証局を使用してキュー・マネージャー鍵に署名します。

```
openssl x509 -req -in example-app1.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
example-app1.crt -days 7 -sha512
```

`-days` は、証明書が有効になる日数を指定します。

署名付き証明書が *example-app1.crt* というファイルに作成されます。

c) アプリケーションの鍵と証明書を使用して PKCS#12 鍵ストアを作成します。

IBM MQ は、個々の鍵ファイルではなく、鍵データベースを使用します。 コンテナー化されたキュー・マネージャーは、シークレットからキュー・マネージャーの鍵データベースを作成しますが、クライアント・アプリケーションの場合は、鍵データベースを手動で作成する必要があります。

```
openssl pkcs12 -export -in "example-app1.crt" -name "example-app1" -certfile "ca.crt"
-inkey "example-app1.key" -out "example-app1.p12" -passout pass:PASSWORD
```

ここで、 *PASSWORD* はユーザーが選択したパスワードです。

example-app1.p12 という名前のファイルに鍵ストアが作成されます。 アプリケーションの鍵と証明書は、CA 証明書だけでなく、「example-app1」の「label」または「friendly name」という名前で内部に保管されます。

d) arm64 Apple Mac を使用している場合は、アプリケーション証明書と CA 証明書を組み合わせた追加ファイルを構成する必要があります。
以下に例を示します。

```
cat example-app1.crt ca.crt > example-app1-chain.crt
```

関連タスク

69 ページの『例: 相互 TLS 認証を使用したキュー・マネージャーの構成』
この例では、 IBM MQ Operator を使用して、キュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』
この例では、 IBM MQ Operator を使用して、ネイティブ高可用性フィーチャーを使用するキュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

81 ページの『IBM MQ Operator を使用した複数インスタンス・キュー・マネージャーの構成』
この例では、 IBM MQ Operator を使用して、複数インスタンス・キュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

OpenShift CP4I Linux 例: 相互 *TLS* 認証を使用したキュー・マネージャーの構成

この例では、 IBM MQ Operator を使用して、キュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

始める前に

この例を完了するには、まず以下の前提条件を満たしておく必要があります。

- この例のための OpenShift Container Platform (OCP) プロジェクト / 名前空間を作成します。
- コマンド・ラインで OCP クラスターにログインし、上記の名前空間に切り替えます。
- 上記の名前空間に IBM MQ Operator がインストールされ、使用可能な状態になっていることを確認します。

このタスクについて

この例では、OpenShift Container Platform にデプロイするキュー・マネージャーを定義したカスタム・リソース YAML を提供しています。 また、TLS を有効にしてキュー・マネージャーをデプロイするために必要な追加のステップも詳しく説明しています。

手順

1. 68 ページの『OpenSSL を使用した自己署名 PKI の作成』の説明に従って、証明書のペアを作成します。
2. MQSC コマンドと INI ファイルを含む構成マップを作成します。

   MQSC コマンドを含む Kubernetes ConfigMap を作成して、新しいキューと SVRCONN チャネルを作成し、チャネルへのアクセスを許可するチャネル認証レコードを追加します。

   前に作成した名前空間 (始める前にを参照) にいることを確認してから、OCP Web コンソールで、またはコマンド・ラインを使用して、以下の YAML を入力します。

   ```
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: example-tls-configmap
   data:
     example-tls.mqsc: |
       DEFINE CHANNEL('MTLS.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
   SSLCIPH('ANY_TLS13_OR_HIGHER') REPLACE
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
   ACTION(REPLACE)
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=example-app1') USERSRC(MAP)
   MCAUSER('app1') ACTION(REPLACE)
       SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(CONNECT,INQ)
       DEFINE QLOCAL('EXAMPLE.QUEUE') REPLACE
       SET AUTHREC PROFILE('EXAMPLE.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
   AUTHADD(BROWSE,PUT,GET,INQ)
     example-tls.ini: |
       Service:
           Name=AuthorizationService
           EntryPoints=14
           SecurityPolicy=UserExternal
   ```

   MQSC は、*MTLS.SVRCONN* というチャネルと、*EXAMPLE.QUEUE*。 チャネルは、「共通名」が *example-app1* の証明書を提示するクライアントにのみアクセスを許可するように構成されています。 これは、ステップ 70 ページの『1』で作成した証明書のいずれかで使用される共通名です。 この共通名を持つこのチャネル上の接続は、 *app1* というユーザー ID にマップされます。このユーザー ID は、キュー・マネージャーに接続し、サンプル・キューにアクセスすることを許可されています。 INI ファイルはセキュリティー・ポリシーを使用可能にします。これは、 *app1* ユーザー ID が外部ユーザー・レジストリーに存在する必要がないことを意味します。この ID は、この構成に名前としてのみ存在します。
3. キュー・マネージャーのデプロイ

   以下のカスタム・リソース YAML を使用して、新しいキュー・マネージャーを作成します。 このタスクを開始する前に作成した名前空間にいることを確認してから、OCP Web コンソールで、またはコマンド・ラインを使用して、以下の YAML を入力します。 正しいライセンスが指定されていることを確認し、`false` を `true` に変更してライセンスを受け入れます。

   ```
   apiVersion: mq.ibm.com/v1beta1
   kind: QueueManager
   metadata:
     name: exampleqm
   spec:
     license:
   ```

```
    accept: false
    license: L-EHXT-MQCRN9
    use: Production
  queueManager:
    name: EXAMPLEQM
    mqsc:
    - configMap:
        name: example-tls-configmap
        items:
        - example-tls.mqsc
    ini:
    - configMap:
        name: example-tls-configmap
        items:
        - example-tls.ini
    storage:
      queueManager:
        type: ephemeral
  version: 9.4.0.0-r1
  pki:
    keys:
      - name: default
        secret:
          secretName: example-qm-tls
          items:
            - tls.key
            - tls.crt
            - ca.crt
```

シークレット *example-qm-tls* がステップ 70 ページの『1』で作成され、 ConfigMap *example-tls-configmap* がステップ 70 ページの『2』 で作成されたことに注意してください。

4. キュー・マネージャーが稼働していることの確認

   キュー・マネージャーがデプロイされます。 続行する前に、Running 状態であることを確認してください。 以下に例を示します。

```
oc get qmgr exampleqm
```

5. キュー・マネージャーへの接続のテスト

   キュー・マネージャーが相互 TLS 通信用に構成されていることを確認するには、 71 ページの『ラップトップからキュー・マネージャーへの相互 TLS 接続のテスト』の手順に従います。

タスクの結果

これで、TLS が有効になっているキュー・マネージャーが正常にデプロイされ、TLS 証明書で提供された詳細を使用してキュー・マネージャーで認証を行い、ID を指定することができました。

OpenShift CP4I Linux ラップトップからキュー・マネージャーへの相互 *TLS* 接続のテスト

IBM MQ Operator を使用してキュー・マネージャーを作成した後、そのキュー・マネージャーに接続し、メッセージの書き込みと読み取りを行うことによって、そのキュー・マネージャーが機能しているかどうかをテストできます。 このタスクでは、ラップトップなどの Kubernetes クラスター外部のマシン上で IBM MQ サンプル・プログラムを実行することにより、それらのプログラムを使用して接続する方法について説明します。

始める前に

この例を完了するには、まず以下の前提条件を満たしておく必要があります。

- IBM MQ client のインストール **amqsputc** コマンドと **amqsgetc** コマンドが必要です。これらのコマンドは、以下のように IBM MQ client の一部としてインストールできます。
  - Windows Linux Windows および Linux の場合: https://ibm.biz/mq94redistclients から、ご使用のオペレーティング・システム用の IBM MQ 再配布可能クライアントをインストールします。
  - macOS Mac の場合: IBM MQ MacOS Toolkit をダウンロードしてセットアップします。 https://developer.ibm.com/tutorials/mq-macos-dev/

- 必要な鍵ファイルと証明書ファイルがマシン上のディレクトリーにダウンロードされていること、および鍵ストアのパスワードがわかっていることを確認してください。 例えば、以下のファイルが 68 ページの『OpenSSL を使用した自己署名 PKI の作成』 に作成されます。
  - `example-app1.p12`
  - `example-app1-chain.crt` (arm64 Apple Mac を使用している場合のみ)
- TLS で構成されたキュー・マネージャーを OCP クラスターにデプロイします。例えば、69 ページの『例: 相互 TLS 認証を使用したキュー・マネージャーの構成』 の手順に従います。

このタスクについて

この例では、ラップトップなどの Kubernetes クラスター外部のマシン上で実行されている IBM MQ サンプル・プログラムを使用して、TLS で構成された QueueManager に接続し、メッセージの書き込みと取得を行います。

手順

1. キュー・マネージャーが稼働していることの確認

   キュー・マネージャーがデプロイされます。 続行する前に、Running 状態であることを確認してください。 以下に例を示します。

   ```
   oc get qmgr exampleqm
   ```

2. キュー・マネージャーのホスト名の検索

   自動的に作成される経路を使用して、OCP クラスターの外部からキュー・マネージャーの完全修飾ホスト名を検索するには、次のコマンドを使用します。 `exampleqm-ibm-mq-qm`

   ```
   oc get route exampleqm-ibm-mq-qm --template="{{.spec.host}}"
   ```

3. IBM MQ クライアント・チャネル定義テーブル (CCDT) の作成

   以下の内容を含む `ccdt.json` というファイルを作成します。

   ```
   {
       "channel":
       [
           {
               "name": "MTLS.SVRCONN",
               "clientConnection":
               {
                   "connection":
                   [
                       {
                           "host": "hostname from previous step",
                           "port": 443
                       }
                   ],
                   "queueManager": "EXAMPLEQM"
               },
               "transmissionSecurity":
               {
                 "cipherSpecification": "ANY_TLS13",
                 "certificateLabel": "example-app1"
               },
               "type": "clientConnection"
           }
       ]
   }
   ```

   この接続では、Red Hat OpenShift Container Platform ルーターが listen しているポートであるため、ポート 443 が使用されます。 トラフィックは、ポート 1414 でキュー・マネージャーに転送されます。

   別のチャネル名を使用した場合は、それも調整する必要があります。 相互 TLS の例では、*MTLS.SVRCONN* という名前のチャネルを使用します。

   詳しくは、 JSON 形式の CCDT の構成 を参照してください。

4. 接続の詳細を構成するためのクライアント INI ファイルの作成

   現行ディレクトリーに mqclient.ini という名前のファイルを作成します。 このファイルは、**amqsputc** および **amqsgetc** によって読み取られます。

   ```
   Channels:
     ChannelDefinitionDirectory=.
     ChannelDefinitionFile=ccdt.json
   SSL:
     OutboundSNI=HOSTNAME
     SSLKeyRepository=example-app1.p12
     SSLKeyRepositoryPassword=password you used when creating the p12 file
   ```

   必ず、 *SSLKeyRepository*「パスワード」 を、 PKCS#12 ファイルの作成時に選択したパスワードに更新してください。 暗号化されたパスワードを使用するなど、鍵ストアのパスワードを設定する方法は他にもあります。 詳しくは、 AIX, Linux, and Windows での IBM MQ MQI client の鍵リポジトリー・パスワードの提供 を参照してください。

   Red Hat OpenShift Container Platform Router では、IBM MQ キュー・マネージャーへの要求のルーティングに SNI が使用されます。 *OutboundSNI= HOSTNAME* 属性は、ルーターが IBM MQ Operator によって構成されたデフォルト経路を処理するために必要な情報が IBM MQ クライアントに確実に含まれるようにします。 詳しくは、84 ページの『Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成』を参照してください。
5. arm64 Apple Mac を使用している場合は、追加の環境変数を構成する必要があります。

   ```
   export MQSSLTRUSTSTORE=example-app1-chain.crt
   ```

   このファイルには、アプリケーションおよび CA 証明書を含む完全な証明書チェーンが含まれています。
6. キューへのメッセージの書き込み

   以下のコマンドを実行します。

   ```
   /opt/mqm/samp/bin/amqsputc EXAMPLE.QUEUE EXAMPLEQM
   ```

   キュー・マネージャーへの接続が成功すると、以下の応答が出力されます。

   ```
   target queue is EXAMPLE.QUEUE
   ```

   任意のテキストを入力してから **Enter** を押す操作を何回か繰り返すことで、キューに複数のメッセージを書き込みます。

   書き込みを終了するには、**Enter** を 2 回押します。
7. キューからのメッセージの取得

   以下のコマンドを実行します。

   ```
   /opt/mqm/samp/bin/amqsgetc EXAMPLE.QUEUE EXAMPLEQM
   ```

   前のステップで追加したメッセージがコンシュームされ、出力されます。 数秒後にコマンドが終了します。

タスクの結果

これで、TLS が有効になっているキュー・マネージャーの接続のテストが正常に完了し、クライアントからキュー・マネージャーにメッセージを安全に書き込んだり、取得したりできることが示されました。

OpenShift CP4I 例：ライセンス・サービスの注釈のカスタマイズ

IBM MQ Operator は、デプロイ済みリソースに IBM License Service アノテーションを自動的に追加します。 これらは IBM License Service によってモニターされ、必要な資格に対応するレポートが生成されます。

このタスクについて

IBM MQ Operator によって追加される注釈は、標準シチュエーションで予期される注釈であり、キュー・マネージャーのデプロイメント中に選択されたライセンス値に基づいています。

例

License が `L-RJON-BZFQU2 (IBM Cloud Pak for Integration 2021.2.1)` に設定されていて、**Use** が `NonProduction` に設定されている場合は、次のアノテーションが適用されます:

- cloudpakId: c8b82d189e7545f0892db9ef2731b90d
- cloudpakName: IBM Cloud Pak for Integration
- productChargedContainers: qmgr
- productCloudpakRatio: '4:1'
- productID: 21dfe9a0f00f444f888756d835334909
- 実動用の製品名: IBM MQ Advanced 非実動用
- 製品メトリック：VIRTUAL_PROCESSOR_CORE
- productVersion: 9.2.3.0

IBM Cloud Pak for Integration 内で、IBM App Connect Enterprise のデプロイメントには、IBM MQ に対する制限付き使用権が含まれます。 このような状況では、これらのアノテーションをオーバーライドして、IBM License Service が正しい使用法をキャプチャーすることを確認する必要があります。 そのためには、95 ページの『キュー・マネージャー・リソースへのカスタム・アノテーションとカスタム・ラベルの追加』で説明されている方法を使用してください

例えば、IBM MQ が IBM App Connect Enterprise ライセンスの下にデプロイされている場合は、以下のコード・フラグメントに示されている方法を使用してください。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mq4ace
  namespace: cp4i
spec:
  annotations:
    productMetric: FREE
```

ライセンスアノテーションの変更が必要となる理由は、他に 2 つあります。

1. IBM MQ Advanced は、別の IBM 製品の使用権に含まれています。
   - この状態では、IBM App Connect Enterprise について前に説明したアプローチを使用してください。
2. IBM MQ は IBM Cloud Pak for Integration ライセンスの下にデプロイされます。
   - IBM Cloud Pak for Integration ライセンスがある場合は、IBM MQ または IBM MQ Advanced の比率の下にキュー・マネージャーをデプロイすることを決定できます。 IBM MQ の比率の下にデプロイする場合は、ネイティブ HA や Advanced Message Security などの高度な機能を使用しないようにする必要があります。
   - このような場合は、以下のアノテーションを使用して制作してください。

     ```
     apiVersion: mq.ibm.com/v1beta1
     kind: QueueManager
     metadata:
       name: mq4ace
       namespace: cp4i
     spec:
       annotations:
         productID: c661609261d5471fb4ff8970a36bccea
         productCloudpakRatio: '4:1'
         productName: IBM MQ for Production
         productMetric: VIRTUAL_PROCESSOR_CORE
     ```

   - 非実動使用には以下の注釈を使用します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: mq4ace
  namespace: cp4i
spec:
  annotations:
    productID: 151bec68564a4a47a14e6fa99266deff
    productCloudpakRatio: '8:1'
    productName: IBM MQ for Non-Production
    productMetric: VIRTUAL_PROCESSOR_CORE
```

OpenShift MQ Adv. IBM MQ Operator を使用したキュー・マネージャーの高可用性の構成

このタスクについて

手順

- 19 ページの『ネイティブ HA』.
- 76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』.
- 81 ページの『IBM MQ Operator を使用した複数インスタンス・キュー・マネージャーの構成』.

OpenShift MQ Adv. *IBM MQ Operator* を使用したネイティブ *HA* の構成

ネイティブ HA は QueueManager API を使用して構成され、拡張オプションは INI ファイルを使用して利用できます。

ネイティブ HA は、`.spec.queueManager.availability` (QueueManager API) を使用して構成されます。以下に例を示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
name: nativeha-example
spec:
  license:
    accept: false
    license: L-EHXT-MQCRN9
    use: Production
  queueManager:
    availability:
      type: NativeHA
  version: 9.4.0.0-r1
```

`.spec.queueManager.availability.type` フィールドは `NativeHA` に設定する必要があります。

`.spec.queueManager.availability` では、複製時にキュー・マネージャー・インスタンス間で使用する TLS シークレットと TLS 暗号を構成することもできます。 この構成を行うことを強くお勧めします。 76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』には、ステップバイステップ形式のガイドが用意されています。

関連タスク

76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』
この例では、 IBM MQ Operator を使用して、ネイティブ高可用性フィーチャーを使用するキュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

OpenShift MQ Adv. Kubernetes 例: *IBM MQ Operator* を使用したネイティブ *HA* の構成

この例では、 IBM MQ Operator を使用して、ネイティブ高可用性フィーチャーを使用するキュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

始める前に

この例を完了するには、まず以下の前提条件を満たしておく必要があります。

- この例のための OpenShift Container Platform (OCP) プロジェクト / 名前空間を作成します。
- コマンド・ラインで OCP クラスターにログインし、上記の名前空間に切り替えます。
- 上記の名前空間に IBM MQ Operator がインストールされ、使用可能な状態になっていることを確認します。

このタスクについて

この例では、OpenShift Container Platform にデプロイするキュー・マネージャーを定義したカスタム・リソース YAML を提供しています。 また、TLS を有効にしてキュー・マネージャーをデプロイするために必要な追加のステップも詳しく説明しています。

手順

1. 68 ページの『OpenSSL を使用した自己署名 PKI の作成』の説明に従って、証明書のペアを作成します。
2. MQSC コマンドと INI ファイルを含む構成マップを作成します。

   MQSC コマンドを含む Kubernetes ConfigMap を作成して、新しいキューと SVRCONN チャネルを作成し、チャネルへのアクセスを許可するチャネル認証レコードを追加します。

   前に作成した名前空間 (始める前にを参照) にいることを確認してから、OCP Web コンソールで、またはコマンド・ラインを使用して、以下の YAML を入力します。

   ```
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: example-nativeha-configmap
   data:
     example-tls.mqsc: |
       DEFINE CHANNEL('MTLS.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
   SSLCIPH('ANY_TLS13_OR_HIGHER') REPLACE
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
   ACTION(REPLACE)
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=example-app1') USERSRC(MAP)
   MCAUSER('app1') ACTION(REPLACE)
       SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(CONNECT,INQ)
       DEFINE QLOCAL('EXAMPLE.QUEUE') REPLACE
       SET AUTHREC PROFILE('EXAMPLE.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
   AUTHADD(BROWSE,PUT,GET,INQ)
     example-tls.ini: |
       Service:
           Name=AuthorizationService
           EntryPoints=14
           SecurityPolicy=UserExternal
   ```

   MQSC は、*MTLS.SVRCONN* というチャネルと、*EXAMPLE.QUEUE*。 チャネルは、「共通名」が *example-app1* の証明書を提示するクライアントにのみアクセスを許可するように構成されています。 これは、ステップ 76 ページの『1』で作成した証明書のいずれかで使用される共通名です。 この共通名を持つこのチャネル上の接続は、 *app1* というユーザー ID にマップされます。このユーザー ID は、キュー・マネージャーに接続し、サンプル・キューにアクセスすることを許可されています。 INI ファイルはセキュリティー・ポリシーを使用可能にします。これは、 *app1* ユーザー ID が外部ユーザー・レジストリーに存在する必要がないことを意味します。この ID は、この構成に名前としてのみ存在します。
3. キュー・マネージャーのデプロイ

   以下のカスタム・リソース YAML を使用して、新しいキュー・マネージャーを作成します。 このタスクを開始する前に作成した名前空間にいることを確認してから、OCP Web コンソールで、またはコマン

ド・ラインを使用して、以下の YAML を入力します。 正しいライセンスが指定されていることを確認し、`false` を `true` に変更してライセンスを受け入れます。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: exampleqm
spec:
  license:
    accept: false
    license: L-EHXT-MQCRN9
    use: Production
  queueManager:
    name: EXAMPLEQM
    availability:
      type: NativeHA
      tls:
        secretName: example-qm-tls
    mqsc:
    - configMap:
        name: example-nativeha-configmap
        items:
        - example-tls.mqsc
    ini:
    - configMap:
        name: example-nativeha-configmap
        items:
        - example-tls.ini
    storage:
      queueManager:
        type: persistent-claim
  version: 9.4.0.0-r1
  pki:
    keys:
      - name: default
        secret:
          secretName: example-qm-tls
          items:
            - tls.key
            - tls.crt
            - ca.crt
```

シークレット *example-qm-tls* がステップ 76 ページの『1』で作成され、ConfigMap *example-nativeha-configmap* がステップ 76 ページの『2』 で作成されたことに注意してください。

可用性タイプが *NativeHA* に設定され、永続ストレージが選択されます。 Kubernetes クラスターで構成されているデフォルトのストレージ・クラスが使用されます。 ストレージ・クラスがデフォルトとして構成されていない場合、または別のストレージ・クラスを使用したい場合は、`defaultClass: storage_class_name` を `spec.queueManager.storage` の下に追加します。

ネイティブ HA キュー・マネージャー内の 3 つのポッドは、ネットワークを介してデータを複製します。このリンクはデフォルトでは暗号化されませんが、この例ではトラフィックの暗号化にキュー・マネージャーの証明書を使用します。 セキュリティーを強化するために、別の証明書を指定することができます。 ネイティブ HA TLS シークレットは、特定の構造を持つ Kubernetes TLS シークレットでなければなりません (例えば、秘密鍵を *tls.key* という名前にする必要があります)。

4. キュー・マネージャーが稼働していることの確認

   キュー・マネージャーがデプロイされます。 続行する前に、`Running` 状態であることを確認してください。 以下に例を示します。

   ```
   oc get qmgr exampleqm
   ```

5. キュー・マネージャーへの接続のテスト

   キュー・マネージャーが構成済みで使用可能であることを確認するには、 71 ページの『ラップトップからキュー・マネージャーへの相互 TLS 接続のテスト』の手順に従います。

6. アクティブ・ポッドの障害の強制試行

   キュー・マネージャーの自動復旧を検証するには、ポッドの障害をシミュレートします。

   a) アクティブ・ポッドとスタンバイ・ポッドの表示

   以下のコマンドを実行します。

```
oc get pods --selector app.kubernetes.io/instance=exampleqm
```

READY フィールドでは、アクティブ・ポッドは値 1/1 を返し、レプリカ・ポッドは値 0/1 を返すことに注意してください。

b) アクティブ・ポッドの削除

アクティブ・ポッドの絶対パス名を指定して次コマンドを実行します。

```
oc delete pod exampleqm-ibm-mq-value
```

c) ポッドの状況の再表示

以下のコマンドを実行します。

```
oc get pods --selector app.kubernetes.io/instance=exampleqm
```

d) キュー・マネージャーの状況の表示

他のいずれかのポッドの絶対パス名を指定して次のコマンドを実行します。

```
oc exec -t Pod -- dspmq -o nativeha -x -m EXAMPLEQM
```

アクティブ・インスタンスが変更されたことを示す状況が表示されるはずです。以下に例を示します。

```
QMNAME(EXAMPLEQM) ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
INSTANCE(inst1) ROLE(Active) REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

e) キュー・マネージャーへの接続を再度テストします。

キュー・マネージャーが回復したことを確認するには、71 ページの『ラップトップからキュー・マネージャーへの相互 TLS 接続のテスト』の手順に従います。

タスクの結果

これで、ネイティブの高可用性と相互 TLS 認証を使用してキュー・マネージャーが正常にデプロイされ、アクティブなポッドで障害が発生したときに自動的に復旧することが確認されました。

OpenShift MQ Adv. *IBM MQ コンテナーのネイティブ HA キュー・マネージャーの状況の表示*

IBM MQ コンテナーの場合、実行中のいずれかのポッド内で **dspmq** コマンドを実行することで、ネイティブ HA インスタンスの状況を表示できます。

このタスクについて

実行中のポッドのうち 1 つで **dspmq** コマンドを使用すると、キュー・マネージャー・インスタンスの運用状況を表示できます。 返される情報は、インスタンスがアクティブとレプリカのどちらであるかに応じて異なります。 アクティブ・インスタンスで提供される情報が確定的なもので、レプリカ・ノードからの情報は古くなっている可能性があります。

以下のアクションを実行できます。

- 現行ノード上のキュー・マネージャー・インスタンスがアクティブかレプリカを表示します。
- 現行ノード上のインスタンスのネイティブ HA の運用状況を表示します。
- ネイティブ HA 構成に属する 3 つのインスタンスすべての運用状況を表示します。

以下の状況フィールドが、ネイティブ HA 構成状況の報告に使用されます。

ROLE
これは、現行インスタンス・ロールを指定します。これは、Active、Replica、または Unknown のいずれかです。

INSTANCE
このキュー・マネージャー・インスタンスの作成時に **crtmqm** コマンドの **-lr** オプションを使用してこのキュー・マネージャー・インスタンスに対して指定された名前。

INSYNC
必要な場合にインスタンスがアクティブ・インスタンスとしてテークオーバーできるかどうかを示します。

QUORUM
クォーラムの状況を *number_of_instances_in-sync*/*number_of_instances_configured* という形式でレポートします。

REPLADDR
キュー・マネージャー・インスタンスの複製アドレス。

CONNACTV
ノードがアクティブ・インスタンスに接続されているかどうかを示します。

BACKLOG
このインスタンスがどれだけ遅れているかを KB 数で示します。

CONNINST
指定されたインスタンスがこのインスタンスに接続されているかどうかを示します。

ALTDATE
この情報が最後に更新された日付を示します (更新されたことがない場合にはブランク)。

ALTTIME
この情報が最後に更新された時刻を示します (更新されたことがない場合にはブランク)。

手順

- キュー・マネージャーの一部であるポッドを見つけます。

```
oc get pod --selector app.kubernetes.io/instance=nativeha-qm
```

- いずれかのポッドで dspmq を実行します。

```
oc exec -t Pod dspmq
```

```
oc rsh Pod
```

対話式シェルの場合は、dspmq を直接実行できる場所です。

- キュー・マネージャー・インスタンスがアクティブ・インスタンスとして実行されているか、それともレプリカとして実行されているか判別するには、次のようにします

```
oc exec -t Pod dspmq -o status -m QMgrName
```

BOB という名前のキュー・マネージャーのアクティブ・インスタンスからは、次の状況が報告されます

```
QMNAME(BOB)                STATUS(Running)
```

BOB という名前のキュー・マネージャーのレプリカ・インスタンスからは、次の状況が報告されます

```
QMNAME(BOB)                STATUS(Replica)
```

非アクティブ・インスタンスからは、次の状況が報告されます

```
QMNAME(BOB)                STATUS(Ended Immediately)
```

- 指定されたポッド内のインスタンスのネイティブ HA 運用状況を判別するには、次のようにします

```
oc exec -t Pod dspmq -o nativeha -m QMgrName
```

BOB という名前のキュー・マネージャーのアクティブ・インスタンスからは、次のような状況が報告されます

```
QMNAME(BOB)               ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
```

BOB という名前のキュー・マネージャーのレプリカ・インスタンスからは、次のような状況が報告されます

```
QMNAME(BOB)               ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
```

BOB という名前のキュー・マネージャーの非アクティブ・インスタンスからは、次のような状況が報告されます

```
QMNAME(BOB)               ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
```

- ネイティブ HA 構成内のすべてのインスタンスのネイティブ HA 運用状況を判別するには、次のようにします

```
oc exec -t Pod dspmq -o nativeha -x -m QMgrName
```

キュー・マネージャー BOB のアクティブ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます

```
QMNAME(BOB)            ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

キュー・マネージャー BOB のレプリカ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます。これは、レプリカの 1 つで処理が遅れていることを示しています

```
QMNAME(BOB)            ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(No)  BACKLOG(435)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

キュー・マネージャー BOB の非アクティブ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます

```
QMNAME(BOB)            ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
 INSTANCE(inst1) ROLE(Unknown) REPLADDR(9.20.123.45) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst2) ROLE(Unknown) REPLADDR(9.20.123.46) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst3) ROLE(Unknown) REPLADDR(9.20.123.47) CONNACTV(No) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
```

どのインスタンスがアクティブでどれがレプリカになるかをまだネゴシエーションしている間にコマンドを発行すると、次の状況が表示されます

```
QMNAME(BOB)              STATUS(Negotiating)
```

関連タスク

76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』
この例では、 IBM MQ Operator を使用して、ネイティブ高可用性フィーチャーを使用するキュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

関連資料
dspmq (キュー・マネージャーの表示) コマンド

OpenShift MQ Adv. ネイティブ *HA* の詳細チューニング

タイミングと間隔のチューニングに関する詳細設定。 デフォルトがシステムの要件に適合しないことが判明している場合を除いて、これらの設定を使用する必要はないはずです。

ネイティブ HA を構成するための基本的なオプションは、QueueManager API を使用して処理されます。 IBM MQ Operator はこの API を使用して、基礎となるキュー・マネージャー INI ファイルを自動的に構成します。 NativeHALocal インスタンス・スタンザの下には、INI ファイルを使用してのみ構成可能な拡張オプションがいくつかあります。 INI ファイルの構成方法について詳しくは、 66 ページの『例: MQSC ファイルと INI ファイルの提供』 も参照してください。

HeartbeatInterval
ハートビート間隔は、ネイティブ HA キュー・マネージャーのアクティブ・インスタンスがネットワーク・ハートビートを送信する頻度をミリ秒単位で定義します。 ハートビート間隔値の有効範囲は 500 (0.5 秒) から 60000 (1 分) で、この範囲外の値を使用するとキュー・マネージャーの開始が失敗します。 この属性を省略すると、デフォルト値の 5000 (5 秒) が使用されます。 各インスタンスで同じハートビート間隔を使用する必要があります。

HeartbeatTimeout
ハートビート・タイムアウトは、ネイティブ HA キュー・マネージャーのレプリカ・インスタンスが、アクティブ・インスタンスが応答しないと判断するまで待機する時間の長さを定義します。 ハートビート間隔タイムアウト値の有効範囲は 500 (0.5 秒) から 120000 (2 分) です。 ハートビート・タイムアウトの値は、ハートビート間隔以上でなければなりません。

無効な値を指定すると、キュー・マネージャーの開始が失敗します。 この属性が省略されると、レプリカは、新しいアクティブ・インスタンスを選択するプロセスを開始する前に 2 x HeartbeatInterval 待機します。 各インスタンスで同じハートビート・タイムアウトを使用する必要があります。

RetryInterval
再試行間隔は、障害が発生した複製リンクがネイティブ HA キュー・マネージャーで再試行される頻度をミリ秒単位で定義します。 再試行間隔の有効範囲は 500 (0.5 秒) から 120000 (2 分) です。 この属性が省略されると、レプリカは、障害が発生した複製リンクを再試行する前に 2 x HeartbeatInterval 待機します。

OpenShift MQ Adv. ネイティブ *HA* キュー・マネージャーの終了

endmqm コマンドを使用して、ネイティブ HA グループの一部であるアクティブ・キュー・マネージャーまたはレプリカ・キュー・マネージャーを終了できます。

手順

- キュー・マネージャーのアクティブ・インスタンスを終了するには、この資料の「構成」セクションの「ネイティブ HA キュー・マネージャーの終了」を参照してください。

OpenShift CP4I MQ Adv. Kubernetes *IBM MQ Operator* を使用した複数インスタンス・キュー・マネージャーの構成

この例では、 IBM MQ Operator を使用して、複数インスタンス・キュー・マネージャーを OpenShift Container Platform にデプロイします。 相互 TLS は、認証に使用され、TLS 証明書からキュー・マネージャー内の ID にマップされます。

始める前に

この例を完了するには、まず以下の前提条件を満たしておく必要があります。

- この例のための OpenShift Container Platform (OCP) プロジェクト / 名前空間を作成します。
- コマンド・ラインで OCP クラスターにログインし、上記の名前空間に切り替えます。

- 上記の名前空間に IBM MQ Operator がインストールされ、使用可能な状態になっていることを確認します。

このタスクについて

この例では、OpenShift Container Platform にデプロイするキュー・マネージャーを定義したカスタム・リソース YAML を提供しています。 また、TLS を有効にしてキュー・マネージャーをデプロイするために必要な追加のステップも詳しく説明しています。

手順

1. 適切なストレージ・クラスの判別

   Kubernetes クラスター内のストレージには、複数の 永続ボリューム・アクセス・モードを使用してアクセスできます。 複数インスタンス・キュー・マネージャーは、複数の永続ボリューム (キュー・マネージャーごとに 1 つ、少なくとも 1 つの共有ボリューム) を作成します。 複数インスタンス・キュー・マネージャーの共有ボリュームでは、 `ReadWriteMany` ストレージ・クラスを使用する必要があります。 Kubernetes クラスターのデフォルトのストレージ・クラスは、通常、 `ReadWriteOnce` ストレージ・クラス (ブロック・ストレージ) 用です。 例えば、 Red Hat OpenShift Data Foundation を使用している場合、ストレージ・クラス *ocs-storagecluster-cephfs* は適切な共有ファイル・システムを提供します。 すべての共有ファイル・システムが同じ方法でファイル・ロックを処理するわけではないため、ファイル・システムの選択は非常に重要です。 Multiplatforms でのファイル・システム・サポートの計画および IBM MQ 複数インスタンス・キュー・マネージャー・ファイル・システムの テスト・ステートメントを参照してください。
2. 68 ページの『OpenSSL を使用した自己署名 PKI の作成』の説明に従って、証明書のペアを作成します。
3. MQSC コマンドと INI ファイルを含む構成マップを作成します。

   MQSC コマンドを含む Kubernetes ConfigMap を作成して、新しいキューと SVRCONN チャネルを作成し、チャネルへのアクセスを許可するチャネル認証レコードを追加します。

   前に作成した名前空間 (始める前にを参照) にいることを確認してから、OCP Web コンソールで、またはコマンド・ラインを使用して、以下の YAML を入力します。

   ```
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: example-miqm-configmap
   data:
     example-tls.mqsc: |
       DEFINE CHANNEL('MTLS.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
   SSLCIPH('ANY_TLS13_OR_HIGHER') REPLACE
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
   ACTION(REPLACE)
       SET CHLAUTH('MTLS.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=example-app1') USERSRC(MAP)
   MCAUSER('app1') ACTION(REPLACE)
       SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(CONNECT,INQ)
       DEFINE QLOCAL('EXAMPLE.QUEUE') REPLACE
       SET AUTHREC PROFILE('EXAMPLE.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
   AUTHADD(BROWSE,PUT,GET,INQ)
     example-tls.ini: |
       Service:
           Name=AuthorizationService
           EntryPoints=14
           SecurityPolicy=UserExternal
   ```

   MQSC は、 *MTLS.SVRCONN* というチャネルと、 *EXAMPLE.QUEUE*。 チャネルは、「共通名」が *example-app1* の証明書を提示するクライアントにのみアクセスを許可するように構成されています。 これは、ステップ 82 ページの『2』で作成した証明書のいずれかで使用される共通名です。 この共通名を持つこのチャネル上の接続は、 *app1* というユーザー ID にマップされます。このユーザー ID は、キュー・マネージャーに接続し、サンプル・キューにアクセスすることを許可されています。 INI ファイルはセキュリティー・ポリシーを使用可能にします。これは、 *app1* ユーザー ID が外部ユーザー・レジストリーに存在する必要がないことを意味します。この ID は、この構成に名前としてのみ存在します。
4. キュー・マネージャーのデプロイ

   以下のカスタム・リソース YAML を使用して、新しいキュー・マネージャーを作成します。 このタスクを開始する前に作成した名前空間にいることを確認してから、OCP Web コンソールで、またはコマン

ド・ラインを使用して、以下の YAML を入力します。 正しいライセンスが指定されていることを確認し、false を true に変更してライセンスを受け入れます。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: exampleqm
spec:
  license:
    accept: false
    license: L-EHXT-MQCRN9
    use: Production
  queueManager:
    name: EXAMPLEQM
    availability:
      type: MultiInstance
    mqsc:
    - configMap:
        name: example-miqm-configmap
        items:
        - example-tls.mqsc
    ini:
    - configMap:
        name: example-miqm-configmap
        items:
        - example-tls.ini
    storage:
      defaultClass: STORAGE_CLASS
  version: 9.4.0.0-r1
  pki:
    keys:
      - name: default
        secret:
          secretName: example-qm-tls
          items:
            - tls.key
            - tls.crt
            - ca.crt
```

STORAGE_CLASS を、ステップ 82 ページの『1』 で識別したストレージ・クラスに変更します。

シークレット *example-qm-tls* がステップ 82 ページの『2』 で作成され、 ConfigMap *example-miqm-configmap* がステップ 82 ページの『3』 で作成されたことに注意してください。

可用性タイプは *MultiInstance* に設定されます。これにより、永続ストレージが自動的に選択されます。

5. キュー・マネージャーが稼働していることの確認

   キュー・マネージャーがデプロイされます。 続行する前に、Running 状態であることを確認してください。 以下に例を示します。

   ```
   oc get qmgr exampleqm
   ```

6. キュー・マネージャーへの接続のテスト

   キュー・マネージャーが構成済みで使用可能であることを確認するには、 71 ページの『ラップトップからキュー・マネージャーへの相互 TLS 接続のテスト』 の手順に従います。

7. アクティブ・ポッドの障害の強制試行

   キュー・マネージャーの自動復旧を検証するには、ポッドの障害をシミュレートします。

   a) アクティブ・ポッドとスタンバイ・ポッドの表示

   以下のコマンドを実行します。

   ```
   oc get pods --selector app.kubernetes.io/instance=exampleqm
   ```

   READY フィールドでは、アクティブ・ポッドが値 1/1 を返し、スタンバイ・ポッドが値 0/1 を返すことに注意してください。

   b) アクティブ・ポッドの削除

   アクティブ・ポッドの絶対パス名を指定して次コマンドを実行します。

   ```
   oc delete pod exampleqm-ibm-mq-value
   ```

c) ポッドの状況の再表示
以下のコマンドを実行します。

```
oc get pods --selector app.kubernetes.io/instance=exampleqm
```

d) キュー・マネージャーの状況の表示
他のポッドのフルネームを指定して、以下のコマンドを実行します。

```
oc exec -t Pod -- dspmq -x
```

アクティブ・インスタンスが変更されたことを示す状況が表示されるはずです。以下に例を示します。

```
QMNAME(EXAMPLEQM)                                         STATUS(Running as standby)
    INSTANCE(exampleqm-ibm-mq-1) MODE(Active)
    INSTANCE(exampleqm-ibm-mq-0) MODE(Standby)
```

e) キュー・マネージャーへの接続を再度テストします。
キュー・マネージャーが回復したことを確認するには、71 ページの『ラップトップからキュー・マネージャーへの相互 TLS 接続のテスト』の手順に従います。

タスクの結果

これで、相互 TLS 認証を使用して複数インスタンス・キュー・マネージャーが正常にデプロイされ、アクティブなポッドで障害が発生したときに自動的に復旧することが確認されました。

OpenShift CP4I CD Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成

Red Hat OpenShift クラスターの外部から IBM MQ キュー・マネージャーにアプリケーションを接続するには、 Red Hat OpenShift 経路が必要です。 IBM MQ キュー・マネージャーおよびクライアント・アプリケーションで TLS を有効にする必要があります。SNI は、TLS 1.2 以上のプロトコルが使用されている場合にのみ TLS プロトコルで使用できるためです。 Red Hat OpenShift Container Platform Router では、IBM MQ キュー・マネージャーへの要求のルーティングに SNI が使用されます。

このタスクについて

Red Hat OpenShift Route の必要な構成は、クライアント・アプリケーションの Server Name Indication (SNI) の動作によって異なります。 IBM MQ では、構成とクライアントのタイプに応じて 2 種類の SNI ヘッダー設定がサポートされています。 SNI ヘッダーは、クライアントの宛先のホスト名に設定されるか、または IBM MQ チャネル名に設定されます。 IBM MQ でチャネル名がどのようにホスト名にマップされるかについては、IBM MQ で複数の証明書の機能を提供する方法を参照してください。

SNI ヘッダーを IBM MQ チャネル名に設定するか、ホスト名に設定するかは、 **OutboundSNI** 属性を使用して制御します。 可能な値は、 OutboundSNI=CHANNEL (デフォルト値) または OutboundSNI=HOSTNAME です。 詳しくは、クライアント構成ファイルの SSL スタンザを参照してください。 CHANNEL および HOSTNAME は、使用する正確な値です。これらは、実際のチャネル名またはホスト名に置き換える変数名ではありません。

OutboundSNI 設定が異なるクライアントの動作

OutboundSNI が HOSTNAME に設定されていて、接続名でホスト名が指定されていると、以下のクライアントではホスト名の SNI が設定されます。

- C クライアント
- 非管理対象モードの .NET クライアント
- Java/JMS クライアント

OutboundSNI が HOSTNAME に設定されていて、接続名で IP アドレスが使用されていると、以下のクライアントではブランクの SNI ヘッダーが送信されます。

- C クライアント
- 非管理対象モードの .NET クライアント
- Java/JMS クライアント (ホスト名の逆引き DNS ルックアップを実行できない)

OutboundSNI が CHANNEL に設定されている場合や、何も設定されていない場合は、ホスト名と IP アドレスのどちらの接続名が使用されていても、IBM MQ チャネル名が代わりに使用されて常に送信されます。

以下のクライアント・タイプでは、SNI ヘッダーを IBM MQ チャネル名に設定できないので、**OutboundSNI** の設定に関係なく常に SNI ヘッダーをホスト名に設定しようとします。

- AMQP クライアント
- XR クライアント

IBM MQ 管理対象 .NET クライアントは、**OutboundSNI** プロパティーが HOSTNAME に設定されている場合、SERVERNAME をそれぞれのホスト名に設定します。これにより、IBM MQ 管理対象 .NET クライアントは、 Red Hat OpenShift 経路を使用してキュー・マネージャーに接続できます。

クライアント・アプリケーションが IBM MQ Internet Pass-Thru (MQIPT) を介して Red Hat OpenShift クラスターにデプロイされたキュー・マネージャーに接続する場合、 MQIPT は、ルート定義内の SSLClientOutboundSNI プロパティーを使用して、 SNI をホスト名に設定するように構成することができます。

OutboundSNI、複数の証明書、および Red Hat OpenShift 経路

IBM MQ は、SNI ヘッダーを使用して複数の証明書機能を提供します。 アプリケーションが、CERTLABL フィールドを介して別の証明書を使用するように構成されている IBM MQ チャネルに接続する場合、アプリケーションは CHANNEL の **OutboundSNI** 設定を使用して接続する必要があります。

Red Hat OpenShift 経路構成に HOSTNAME SNI が必要な場合は、 IBM MQ の複数の証明書機能を使用できず、 IBM MQ チャネル・オブジェクトに CERTLABL 設定を設定できません。

OutboundSNI に CHANNEL 以外の設定を持つアプリケーションが、証明書ラベルが構成されたチャネルに接続すると、そのアプリケーションは MQRC_SSL_INITIALIZATION_ERROR で拒否され、キュー・マネージャーのエラー・ログに AMQ9673 メッセージが出力されます。

IBM MQ が複数の証明書機能を提供する方法について詳しくは、IBM MQ が複数の証明書機能を提供する方法 を参照してください。

例

SNI を MQ チャネルに設定するクライアント・アプリケーションには、接続先のチャネルごとに新しい Red Hat OpenShift ルートが作成されている必要があります。 また、適切なキュー・マネージャーにルーティングできるようにするには、Red Hat OpenShift Container Platform クラスターで一意のチャネル名を使用する必要があります。

IBM MQ がチャネル名を SNI ヘッダーにマップする方法により、 MQ チャネル名の末尾が小文字にならないことが重要です。

それぞれの新規 Red Hat OpenShift ルートに必要なホスト名を判別するには、各チャネル名を SNI アドレスにマップする必要があります。 詳しくは、IBM MQ で複数の証明書の機能を提供する方法を参照してください。

次に、クラスターに以下の yaml を適用して、チャネルごとに新しい Red Hat OpenShift 経路を作成する必要があります。

```
apiVersion: route.openshift.io/v1
kind: Route
metadata:
  name: unique_name_for_the_route
  namespace: namespace_of_your_MQ_deployment
spec:
  host: SNI_address_mapping_for_the_channel
  to:
    kind: Service
    name: name_of_Kubernetes_Service_for_your_MQ_deployment (for example "queue_manager_name-
```

```
ibm-mq")
  port:
    targetPort: 1414
  tls:
    termination: passthrough
```

クライアント・アプリケーション接続の詳細の構成

以下のコマンドを実行すると、クライアント接続で使用するホスト名を判別できます。

```
oc get route Name of hostname based Route (for example "queue_manager_name-ibm-mq-qm")>
-n namespace of your MQ deployment -o jsonpath="{.spec.host}"
```

クライアント接続用のポートは、Red Hat OpenShift Container Platform ルーターが使用するポート (通常は 443) に設定する必要があります。

関連タスク

129 ページの『IBM MQ Console クラスターにデプロイされた Red Hat OpenShift への接続』
Red Hat OpenShift Container Platform クラスターにデプロイされているキュー・マネージャーの IBM MQ Console に接続する方法について説明します。

OpenShift CP4I IBM MQ と IBM Instana トレースの統合

IBM Instana を使用して、 IBM Cloud Pak for Integration 内のトランザクションをトレースできます。

始める前に

本書では、 IBM Instana トレースについて説明します。これは、システムを介してメッセージをトレースするプロセスです。 このトピックでは、 IBM MQ キュー・マネージャーの状態に関する詳細を取得する IBM Instana モニターについては説明しません。 IBM Instana による IBM MQ のモニターについては、 Monitoring IBM MQ を参照してください。 認証済みモニターについて詳しくは、 88 ページの『TLS を使用した認証済み IBM Instana モニターの構成』を参照してください。

注 :

- この機能は、 IBM MQ バージョン 9.3.1.0-r2 以降のオペランドでのみサポートされます。
- IBM Instana トレースは、以前のバージョンの IBM MQ オペレーターおよびキュー・マネージャーで実行できますが、ネイティブでは実行できません。 IBM Instana 資料の IBM MQ トレースの構成 を参照してください。

IBM MQ Operator を使用して IBM Instana トレースを実行する前に、 IBM Instana バックエンド・エージェントと IBM Instana エージェントの両方をデプロイする必要があります。 デフォルトでは、 IBM MQ キュー・マネージャーは、キュー・マネージャー・ポッドと同じノードにデプロイされた IBM Instana エージェントと通信します。

このタスクについて

IBM Instana との統合を有効にすると、 IBM MQ API 出口がキュー・マネージャーにインストールされます。 API 出口は、キュー・マネージャーを流れるメッセージに関するトレース・データを IBM Instana エージェントに送信します。

API 出口は、各メッセージに RFH2 ヘッダーを追加します。 これらのヘッダーにはトレース情報が含まれます。

IBM Instana エージェントは、 IBM Instana バックエンドへのトレース・データの送信を担当します。

IBM Instana バックエンドおよび IBM Instana エージェントのデプロイについては、 IBM Instana 資料の「 プラットフォーム UI での Instana モニター・リンクの有効化 」を参照してください。

手順

標準デプロイメント

- IBM Instana トレースを有効にしてキュー・マネージャーをデプロイします。

デフォルトでは、 IBM Instana トレースは無効になっています。

IBM Cloud Pak for Integration Platform UI または OpenShift Web コンソールを使用している場合:

1.「**テレメトリー**」 > 「**トレース**」 > 「**インスタンス**」をクリックします。
2.「**Instana トレースを有効にする (Enable Instana tracing)**」 トグルを `true` に設定します。

YAML を使用してデプロイする場合は、以下のスニペットを使用します。

```
spec:
  telemetry:
    tracing:
      instana:
        enabled: true
```

拡張デプロイメント

- https 経由で IBM Instana エージェントと通信します。

  デフォルトでは、 IBM MQ の IBM Instana 出口は HTTP を介して IBM Instana エージェントと通信します。 エージェントのホスト・アドレスは、キュー・マネージャーが実行されているノードの IP アドレスに設定されます。 これは、 IBM Instana 資料の「IBM Instana モニターの使用可能化」で説明されている構成と一致します。ここで、 IBM Instana エージェントは、 IBM Instana Agent Operator によってデーモン・セットとしてデプロイされます。

  現在、 IBM MQ の IBM Instana 出口と IBM Instana エージェントの間の通信では、http プロトコルまたは https プロトコルがサポートされています。 https を使用するには、まず TLS 暗号化を使用するように IBM Instana エージェントを構成する必要があります。 IBM Instana 資料の エージェント・エンドポイントの TLS 暗号化のセットアップ を参照してください。 その後、以下のようにプロトコルを https に設定できます。

  OpenShift Web コンソールを使用している場合:

  1.「**Telemetry**」 > 「**Instana**」をクリックします。
  2.「**拡張構成**」 ドロップダウン・リストを展開します。
  3.「**Instana エージェント通信プロトコル**」 を `https` に設定します。

  YAML を使用してデプロイする場合は、以下のスニペットを使用します。

  ```
  spec:
    telemetry:
      instana:
        enabled: true
        protocol: https
  ```

- **agentHost** を設定します。

  IBM Instana エージェントが、キュー・マネージャーが実行されている OpenShift クラスターにデーモンセットとしてデプロイされていない場合は、 **agentHost** 値を、 IBM Instana エージェントが実行されているホスト名または IP アドレスに設定する必要があります。 **agentHost** 値にプロトコルまたはポートを含めることはできません。

  OpenShift Web コンソールを使用している場合:

  1.「**Telemetry**」 > 「**Instana**」をクリックします。
  2.「**拡張構成**」 ドロップダウン・リストを展開します。
  3.「**Instana エージェント・ホスト (Instana agent host)**」 テキスト・ボックスにホスト名を入力します。

  YAML を使用してデプロイする場合は、以下のスニペットを使用します。

  ```
  spec:
    telemetry:
      instana:
        enabled: true
        agentHost: 9.9.9.9
  ```

次のタスク

63 ページの『IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ』も参照してください。

OpenShift CP4I Operator2.2.0 TLS を使用した認証済み IBM Instana モニターの構成

IBM Instana エージェントを介してキュー・マネージャーをモニターできるようにするには、エージェントとキュー・マネージャーの両方を構成する必要があります。

始める前に

IBM Instana 資料の 「IBM MQ のモニター」の「構成」セクション には、 IBM Instana モニター構成に関する一般情報が記載されています。 ただし、キュー・マネージャーの構成に関する詳細は含まれていません。

IBM MQ Operator で IBM Instana トレースを実行する前に、 IBM Instana バックエンドと IBM Instana エージェントの両方をデプロイする必要があります。 これを行うには、 IBM Instana 資料の CP4I Platform UI での IBM Instana モニタリングの有効化 を参照してください。

手順

1. 証明書を生成します。
2. IBM Instana エージェントを構成します。
3. キュー・マネージャーを構成します。
4. 検証およびデバッグ。

関連タスク

86 ページの『IBM MQ と IBM Instana トレースの統合』
IBM Instana を使用して、 IBM Cloud Pak for Integration 内のトランザクションをトレースできます。

OpenShift CP4I Operator2.2.0 *IBM Instana* エージェントおよびキュー・マネージャーの証明書と鍵を生成します。

IBM Instana エージェントとキュー・マネージャーの間の TLS 通信の場合、両方に証明書とそれに対応する秘密鍵が必要です。

始める前に

これは、 TLS を使用して認証済み IBM Instana モニターを構成する 4 つのタスクのうちの最初のタスクです。

注 : これらの証明書の生成に使用される値は、デモンストレーション用です。 実稼働環境にデプロイする場合は、証明書のサブジェクトと有効期限が適切であることを確認してください。

手順

IBM MQ キュー・マネージャー

TLS を介して IBM Instana エージェントと通信するには、キュー・マネージャーに証明書とそれに対応する秘密鍵が必要です。 これらが既にある場合は、このセクションをスキップしてください。

1. キュー・マネージャーの証明書と秘密鍵を生成します。

   以下のコマンドを実行します。

```
openssl req \
       -newkey rsa:2048 -nodes -keyout server.key \
       -subj "/CN=mq queuemanager/OU=ibm mq" \
       -x509 -days 3650 -out server.crt
```

IBM Instana エージェント

エージェントが IBM MQ キュー・マネージャーとの TLS 通信を実行するには、エージェントに証明書とそれに対応する秘密鍵が必要です。 使用する JKS 鍵ストア内に秘密鍵と証明書が既にある場合は、このセクションをスキップしてください。

2. IBM Instana エージェントの証明書と秘密鍵を生成します。

   以下のコマンドを実行します。

   ```
   openssl req \
          -newkey rsa:2048 -nodes -keyout application.key \
          -subj "/CN=instana-agent/OU=app team1" \
          -x509 -days 3650 -out application.crt
   ```

3. 証明書と秘密鍵を PKCS12 鍵ストアに保管します。

   以下のコマンドを実行します。 *your_password* は、鍵ストアを保護するために使用するパスワードに置き換えてください。 この置換は、後続のすべてのステップで実行します。

   ```
   openssl pkcs12 -export -out application.p12 -inkey application.key -in application.crt
   -passout pass:your_password
   ```

4. PKCS12 鍵ストアを JKS 鍵ストアに変換します。

   以下のコマンドを実行します。

   ```
   keytool -importkeystore \
           -srckeystore application.p12 \
           -srcstoretype pkcs12 \
           -destkeystore application.jks \
           -deststoretype JKS \
           -srcstorepass your_password \
           -deststorepass your_password \
           -noprompt
   ```

5. 証明書にラベルを付けます。

   以下のコマンドを実行します。

   ```
   keytool -changealias -alias "1" -destalias "instana" -keypass your_password -keystore
   application.jks -storepass your_password -noprompt
   ```

6. キュー・マネージャー証明書を鍵ストアにインポートします。

   以下のコマンドを実行します。

   ```
   keytool -importcert -file server.crt -keystore application.jks -storepass your_password
   -alias myca -noprompt
   ```

次のタスク

これで、 IBM Instana モニター用にエージェントを構成する準備ができました。

OpenShift CP4I Operator2.2.0 *Instana* モニター: エージェントの構成

鍵ストアを IBM Instana エージェントにマウントしてから、特定のキュー・マネージャーのモニターを構成します。

始める前に

このタスクは、 IBM Instana エージェントおよびキュー・マネージャーの証明書と鍵を生成していることを前提としています。

手順

IBM Instana エージェントへの鍵ストアのマウント

1. IBM Instana エージェント名前空間内の JKS 鍵ストアから秘密を作成します。

以下のコマンドを実行します。 *keystore_secret_name* は、使用する名前に置き換えてください。 この置換は、後続のすべてのステップで実行します。

```
oc create secret generic keystore_secret_name --from-file=./application.jks -n instana-agent
```

2. instana-agent 名前空間で、 `oc edit daemonset instana-agent` コマンドを使用して instana-agent デーモン・セットを編集し、以下の追加の volumeMount とボリュームを追加します。

```
volumeMounts:
- name: mq-key-jks-name
   subPath: application.jks
   mountPath: /opt/instana/agent/etc/application.jks
volumes:
- name: mq-key-jks-name
   secret:
      secretName: keystore_secret_name
```

特定のキュー・マネージャーのモニターの構成

3. instana-agent 名前空間で、 `oc edit configmap instana-agent` コマンドを使用して instana-agent 構成マップを編集します。
4. `configuration.yaml: |`の下に以下のセクションを追加します。 このセクションを既に定義している場合は、新しいキュー・マネージャーをリストに追加するだけです。

```
    com.instana.plugin.ibmmq:
      enabled: true
      poll_rate: 60
      queueManagers:
         QUEUE_MANAGER_NAME:
            channel: 'INSTANA.A.SVRCONN'
            keystorePassword: 'your_password'
            keystore: '/opt/instana/agent/etc/application.jks'
            cipherSuite: 'TLS_RSA_WITH_AES_256_CBC_SHA256'
```

説明:

- *your_password* は JKS 鍵ストアのパスワードです。
- *QUEUE_MANAGER_NAME* は、キュー・マネージャー・オペランドの名前ではなく、デプロイする基礎となる IBM MQ キュー・マネージャーの名前です。

注 : *QUEUE_MANAGER_NAME* が基礎となるキュー・マネージャー名に設定されておらず、代わりにオペランドに設定されている場合、モニターは機能しません。 基礎となる名前は、キュー・マネージャー・オペランドの `spec.queuemanager.name` で定義されます。

5. instana-agent 名前空間内の instana-agent ポッドを削除します。 これにより、それらのユーザーは再始動し、新しい設定でモニターを開始します。

次のタスク

これで、 IBM Instana モニター用にキュー・マネージャーを構成する準備ができました。

OpenShift CP4I Operator2.2.0

Instana モニター: キュー・マネージャーの構成

TLS を使用して IBM Instana エージェントと通信するキュー・マネージャーをセットアップします。この接続の認証は、 SSLPEERMAP を使用して行われます。

始める前に

このタスクは、 IBM Instana モニター用にエージェントを構成していることを前提としています。

手順

1. MQSC と INI の両方を使用してキュー・マネージャーを構成します。

   MQSC は、新しい TLS 対応チャネルをセットアップするために使用されます。その後、必須フィールドが指定された証明書がある場合に、接続先の IBM Instana エージェントを認証するようにそのチャネルを構成します。 この場合、 `CN=instana-agent,OU=app team1` フィールドを含む証明書を持つ接続

クライアントをユーザー app1 にマップします。 次に、MQSC は、 IBM Instana モニターに必要な操作を実行する権限をユーザー app1 に付与します。

INI ファイルは、外部ユーザー app1 に許可を付与するために使用されます。

以下の構成マップには、必須の MQSC 設定と INI 設定が含まれています。 キュー・マネージャーの名前空間にデプロイします。

```
apiVersion: v1
data:
  channel.mqsc: |-
    DEFINE CHANNEL('INSTANA.A.SVRCONN') CHLTYPE(SVRCONN) SSLCAUTH(REQUIRED)
SSLCIPH('ANY_TLS12_OR_HIGHER')
    ALTER QMGR CONNAUTH(' ')
    REFRESH SECURITY
    SET CHLAUTH('INSTANA.A.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=*') USERSRC(NOACCESS)
ACTION(REPLACE)
    SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS) ACTION(REPLACE)
    SET CHLAUTH('INSTANA.A.SVRCONN') TYPE(SSLPEERMAP) SSLPEER('CN=instana-agent,OU=app
team1') USERSRC(MAP) MCAUSER('app1')
    SET AUTHREC PRINCIPAL('app1') OBJTYPE(QMGR) AUTHADD(ALL)
    SET AUTHREC PROFILE('SYSTEM.ADMIN.COMMAND.QUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE)
AUTHADD(PUT,INQ,DSP,CHG)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(TOPIC) AUTHADD(DSP)
    SET AUTHREC PROFILE('*') PRINCIPAL('app1') OBJTYPE(TOPIC) AUTHADD(DSP)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG, GET)
    SET AUTHREC PROFILE('SYSTEM.**') PRINCIPAL('app1') OBJTYPE(LISTENER) AUTHADD(DSP)
    SET AUTHREC PROFILE('AMQ.*') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG)
    REFRESH SECURITY TYPE(CONNAUTH)
  auth.ini: |-
    Service:
      Name=AuthorizationService
      EntryPoints=14
      SecurityPolicy=UserExternal
kind: ConfigMap
metadata:
  namespace: your-queue-manager-namespace
  name: qmgr-monitoring-config
```

ここで、 *your-queue-manager-namespace* は、キュー・マネージャーがデプロイされる名前空間です。

注 : ユーザー定義キューをモニターする場合は、構成マップ MQSC に追加の行を追加して、DSP、CHG、および GET 許可をそれらのキューに付与する必要があります。 以下に例を示します。

```
SET AUTHREC PROFILE('MYQUEUE') PRINCIPAL('app1') OBJTYPE(QUEUE) AUTHADD(DSP, CHG, GET).
```

この例では、MQSC データと INI データに configmap を使用しますが、追加した内容が機密情報である場合は、シークレットを使用できます。 MQSC および INI を使用したデプロイに関する一般情報については、 66 ページの『例: MQSC ファイルと INI ファイルの提供』を参照してください。

2. TLS 接続を行うには、キュー・マネージャーが IBM Instana エージェントの証明書を信頼する必要があります。 これを行うには、 IBM Instana エージェントの証明書のみを含むシークレットを作成します。

```
oc create secret generic instana-certificate-secret --from-file=./application.crt -n your-
queue-manager-namespace
```

3. キュー・マネージャーは、TLS ハンドシェーク用に独自の証明書を提示する必要があり、関連付けられた秘密鍵へのアクセスを必要とします。 以前に作成したか、既に所有している鍵と証明書を含む秘密をデプロイします。

```
oc create secret tls qm-tls-secret --cert server.crt --key server.key -n your-queue-manager-
namespace
```

構成マップとシークレットが作成されると、キュー・マネージャー自体を作成する準備が整います。

4. キュー・マネージャー YAML がキュー・マネージャー・コンテナーで環境変数 **MQSNOAUT** を設定していないことを確認します。

そうしないと、有効にした後に認証メカニズムが機能しなくなります。 デプロイメント後にこの変数を削除しても、メカニズムは再有効化されないため、キュー・マネージャーを再作成する必要があります。

5. キュー・マネージャー定義に以下のセクションを追加します。ここで、 *MYQM* はキュー・マネージャーの名前です。

```
spec:
  queueManager:
    name: MYQM   #(a)
    ini:   #(b)
      - configMap:
          items:
            - auth.ini
          name: qmgr-monitoring-config
    mqsc:   #(c)
      - configMap:
          items:
            - channel.mqsc
          name: qmgr-monitoring-config
  pki:
    keys:   #(d)
        - name: default
          secret:
            items:
            - tls.key
            - tls.crt
            secretName: qm-tls-secret
    trust:   #(e)
      - name: app
        secret:
          items:
            - application.crt
          secretName: instana-certificate-secret
```

この仕様のフラグが立てられたセクションについて、以下で説明します。

a. 基礎となるキュー・マネージャーに固有の名前を指定したことを確認してください。 基礎となるキュー・マネージャーに固有の名前がない場合は、モニターが意図したとおりに機能しない可能性があります。 この名前は、前に編集した IBM Instana エージェント構成マップ内の名前と一致している必要があります。

b. 構成マップに書き込まれた INI 情報がキュー・マネージャーに追加されます。

c. 構成マップに書き込まれた MQSC 情報がキュー・マネージャーに追加されます。

d. キュー・マネージャーの証明書と秘密鍵がキュー・マネージャーの鍵ストアに追加されます。

e. IBM Instana エージェント証明書がキュー・マネージャーのトラストストアに追加されます。

6. オプション: モニター対象キュー・マネージャーで IBM Instana トレースを有効にします。

これを行う場合は、86 ページの『IBM MQ と IBM Instana トレースの統合』を参照してください。

7. キュー・マネージャーをデプロイします。

次のタスク

これで、 IBM Instana モニターの検証とデバッグを行う準備ができました。

OpenShift CP4I Operator2.2.0 *Instana* モニター: 検証およびデバッグ

IBM Instana エージェントを介してキュー・マネージャーをモニターできるようにするには、エージェントとキュー・マネージャーの両方を構成する必要があります。

始める前に

この作業は、 IBM Instana モニター用にキュー・マネージャーが構成されていることを前提としています。

手順

の検証

1. デプロイメントが正常に完了したことを確認するには、 IBM Instana ダッシュボードでキュー・マネージャーを表示します。

キュー・マネージャーは、アプリケーション・ページのサービス・セクションと「インフラストラクチャー」ビューにも表示されます。

デバッグ

注 : これらのデバッグ手順では、デーモンセットとして実行されている IBM Instana エージェントの Openshift デプロイメントを想定しています。

IBM Instana ダッシュボードにキュー・マネージャーが表示されない場合は、キュー・マネージャーの構成が誤っている可能性があります。 調査するには、以下の手順を使用します。

2. アクティブなキュー・マネージャー・ポッドが実行されているノードを識別します。

   キュー・マネージャーの名前空間で以下のコマンドを実行します。

   ```
   oc get pods -o wide -n your-queue-manager-namespace
   ```

3. キュー・マネージャーと同じノードで実行されている IBM Instana エージェント・ポッドを判別するには、instana-agent 名前空間で同じコマンドを実行します。

   ```
   oc get pods -o wide -n instana-agent-namespace
   ```

4. IBM Instana エージェント側の問題を理解しやすくするために、 IBM Instana エージェント・ポッドのログを取得し、「mq」またはキュー・マネージャーの名前に関連する項目を探します。

   以下のコマンドを実行します。

   ```
   oc logs instana-agent-pod -c instana-agent -n instana-agent
   ```

5. キュー・マネージャーのログを確認してください。

   エージェントがキュー・マネージャーへの接続を試行した場合、キュー・マネージャーのログに、接続が失敗した理由が示されているはずです。 以下のコマンドを実行します。

   ```
   oc logs your-queue-manager-name -n your-queue-manager-namespace
   ```

タスクの結果

これで、 TLS を使用した認証済み IBM Instana モニターの構成のための 4 つのタスクがすべて完了しました。

OpenShift CP4I Red Hat OpenShift CLI を使用した、カスタム MQSC および INI ファイルを使用したイメージの作成

Red Hat OpenShift Container Platform パイプラインを使用して、新規の IBM MQ コンテナー・イメージを作成できます。このイメージを使用するキュー・マネージャーに適用する MQSC ファイルと INI ファイルも指定できます。 このタスクは、プロジェクト管理担当者が実行する必要があります。

始める前に

Red Hat OpenShift Container Platform のコマンド・ライン・インターフェースをインストールする必要があります。

cloudctl login (IBM Cloud Pak for Integration の場合) または **oc login** を使用してクラスターにログインします。

Red Hat OpenShift プロジェクトに IBM Entitled Registry の Red Hat OpenShift シークレットがない場合は、 ライセンス・キー・シークレットの作成の手順に従います。

手順

1. ImageStream の作成

   イメージ・ストリームおよびそのストリームに関連付けられたタグによって、Red Hat OpenShift Container Platform 内からコンテナー・イメージを参照するための抽象化が可能になります。 イメー

ジ・ストリームおよびそのストリームのタグによって、使用可能なイメージを確認できます。また、必要とする特定のイメージがリポジトリー内で変更されたとしても、確実にそのイメージを使用することができます。

```
oc create imagestream mymq
```

2. 新規イメージ用に BuildConfig を作成

   BuildConfig は、新しいイメージのビルドを許可します。これは、IBM 公式イメージに基づきますが、コンテナーの始動時に実行される MQSC ファイルまたは INI ファイルが追加されます。

   a) BuildConfig リソースを定義する YAML ファイルを作成します

   例えば、以下を内容とする「mq-build-config.yaml」というファイルを作成します。

```
apiVersion: build.openshift.io/v1
kind: BuildConfig
metadata:
  name: mymq
spec:
  source:
    dockerfile: |-
      FROM cp.icr.io/cp/ibm-mqadvanced-server-integration:9.4.0.0-r1
      RUN printf "DEFINE QLOCAL(foo) REPLACE\n" > /etc/mqm/my.mqsc \
        && printf "Channels:\n\tMQIBindType=FASTPATH\n" > /etc/mqm/my.ini
      LABEL summary "My custom MQ image"
  strategy:
    type: Docker
    dockerStrategy:
      from:
        kind: "DockerImage"
        name: "cp.icr.io/cp/ibm-mqadvanced-server-integration:9.4.0.0-r1"
      pullSecret:
        name: ibm-entitlement-key
  output:
    to:
      kind: ImageStreamTag
      name: 'mymq:latest-amd64'
```

   ベースの IBM MQ が指定されている 2 箇所を、使用するバージョンとフィックスを表す正しいベース・イメージを指すように置き換える必要があります (詳しくは、5 ページの『IBM MQ Operator のリリース履歴』を参照)。 フィックスが適用されたときには、この手順を繰り返してイメージを再ビルドする必要があります。

   この例では、 IBM の公式イメージに基づいて新規イメージを作成し、 "my.mqsc" および "my.ini" というファイルを /etc/mqm ディレクトリーに追加します。 このディレクトリー内にある MQSC ファイルまたは INI ファイルは、始動時にコンテナーによって適用されます。 INI ファイルは、**crtmqm -ii** オプションを使用して適用され、既存の INI ファイルとマージされます。 MQSC ファイルは、アルファベット順に適用されます。

   MQSC コマンドは、キュー・マネージャーが開始されるたびに 実行されるので、反復可能であることが重要です。 通常、これは、REPLACE パラメーターを DEFINE コマンドに追加すること、および IGNSTATE(YES) パラメーターを START コマンドまたは STOP コマンドに追加することを意味します。

   b) BuildConfig をサーバーに適用します。

```
oc apply -f mq-build-config.yaml
```

3. ビルドを実行してイメージを作成します。

   a) ビルドを開始します。

```
oc start-build mymq
```

   次のような出力が表示されます。

```
build.build.openshift.io/mymq-1 started
```

   b) ビルドの状況を確認します。

例えば、前の手順で返されたビルド ID を使用して、次のコマンドを実行します。

```
oc describe build mymq-1
```

4. 新規イメージを使用してキュー・マネージャーをデプロイします。

   63 ページの『IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ』で説明している手順に従って、新規カスタム・イメージを YAML に追加します。

   以下の YAML スニペットを通常の QueueManager YAML に追加できます。*my-namespace* は使用する Red Hat OpenShift プロジェクト/名前空間です。*image* は前に作成したイメージの名前 (例えば、「mymq:latest-amd64」) です。

```
spec:
  queueManager:
    image: image-registry.openshift-image-registry.svc:5000/my-namespace/my-image
```

関連タスク

63 ページの『IBM MQ Operator を使用した単純なキュー・マネージャーのデプロイ』
この例では、一時 (非永続) ストレージを使用する「クイック・スタート」キュー・マネージャーをデプロイし、 IBM MQ セキュリティーをオフにします。 メッセージは、キュー・マネージャーの再始動後は保持されません。 構成を調整することで、キュー・マネージャーのさまざまな設定を変更できます。

OpenShift CP4I キュー・マネージャー・リソースへのカスタム・アノテーションとカスタム・ラベルの追加

QueueManager メタデータにカスタム・アノテーションとカスタム・ラベルを追加します。

このタスクについて

PVC を除くすべてのリソースにカスタム・アノテーションとカスタム・ラベルを追加できます。 カスタム・アノテーションまたはカスタム・ラベルが既存のキーと一致する場合は、IBM MQ Operator によって設定される値が使用されます。

手順

- カスタム・アノテーションを追加します。

  ポッドなどのキュー・マネージャー・リソースにカスタム・アノテーションを追加するには、metadata の下にアノテーションを追加します。 以下に例を示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
  annotations:
    annotationKey: "value"
```

- カスタム・ラベルを追加します。

  ポッドなどのキュー・マネージャー・リソースにカスタム・ラベルを追加するには、metadata の下にラベルを追加します。 以下に例を示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
  labels:
    labelKey: "value"
```

OpenShift CP4I 実行時 Webhook チェックの無効化

実行時 Webhook チェックによって、ストレージ・クラスがキュー・マネージャーで実行可能かどうかを確認します。 パフォーマンスを向上させたい場合や、ご使用の環境で有効でない場合は、このチェックを無効にできます。

このタスクについて

実行時 Webhook チェックは、キュー・マネージャー構成に対して実行します。 選択したキュー・マネージャー・タイプにストレージ・クラスが適しているかを確認します。

キュー・マネージャーの作成にかかる時間を短縮したい場合や、ご使用の特定の環境で有効でない場合は、チェックを無効にできます。

注 : 実行時 Webhook チェックを無効にすると、すべてのストレージ・クラス値が有効になります。 その結果、キュー・マネージャーの失敗につながることもあります。

手順

- 実行時 Webhook チェックを無効にします。

  `metadata` の下に以下のアノテーションを追加します。 以下に例を示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
  annotations:
    "com.ibm.cp4i/disable-webhook-runtime-checks" : "true"
```

OpenShift Operator2.1.0 CP4I キュー・マネージャー仕様に対するデフォルト値更新の無効化

IBM MQ Operator は、キュー・マネージャー仕様内の指定されていない値をデフォルト値で更新します。 キュー・マネージャー仕様に変更を加えないようにする場合は、この動作を無効にすることができます。 キュー・マネージャー状況フィールドは引き続き更新されます。

手順

- キュー・マネージャーのデフォルト値の更新を無効にします。

  `metadata` の下に以下のアノテーションを追加します。 以下に例を示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
  annotations:
    "com.ibm.mq/write-defaults-spec" : "false"
```

  注 : クイック・スタート・サンプルには、デフォルトでこのアノテーションが適用されています。

読み取り専用ルート・ファイル・システムを使用した IBM MQ コンテナーの実行

読み取り専用のルート・ファイル・システムで実行するように IBM MQ コンテナーを構成することができます。 これにより、攻撃者はコンテナー内の悪意のあるコードをコピーして実行することができなくなります。

このタスクについて

読み取り専用ルート・ファイル・システムを有効にすると、コンテナー・ファイルが変更不可能になります。 つまり、コンテナー・ファイル・システムでは、ファイルを表示することはできますが、変更することはできず、新規ファイルを作成することはできません。 ファイルは、マウントされたファイル・システム上でのみ変更または作成することができます。

読み取り専用ルート・ファイル・システムが使用可能な場合、2 つの一時ボリューム `Scratch` および `Tmp` が作成され、それぞれコンテナー内の `/run` ディレクトリーおよび `/tmp` ディレクトリーにマウントされます。

- 「スクラッチ」 ボリュームには、キュー・マネージャーの構成に使用されるファイル、鍵ストア、およびその他のファイルが含まれています。
- Tmp ボリュームには、キュー・マネージャー RAS ファイルなどの診断ファイルが含まれています。

これらのボリュームは一時ボリュームであるため、これらのボリューム上のファイルはポッドの再始動時に失われます。

キュー・マネージャー・データ用に作成されるボリュームのタイプは、ストレージ・タイプによって異なります。 デフォルトでは、永続ボリュームがマウントされます。 あるいは、ストレージ・タイプが ephemeral の場合は、一時ボリュームがマウントされます。 ボリューム内のデータのサイズが **sizeLimit** プロパティーに指定された値を超える場合、 Kubernetes はコンテナーを排出して新しいコンテナーを作成できます。

読み取り専用ルート・ファイル・システムは、デフォルトでは使用可能になっていません。 有効にするには、以下の手順を実行します。

手順

1. spec.securityContext API を使用して、読み取り専用ルート・ファイル・システムを有効にします。

   キュー・マネージャーの場合は、152 ページの『.spec.securityContext』の **readOnlyRootFilesystem** プロパティーを true に設定します。

   IBM MQ Operator は、 Scratch および Tmp という 2 つの一時ボリュームを作成します。
2. オプション: キュー・マネージャーのデータ・ストレージ・タイプを設定または変更します。

   デフォルトでは、永続ボリューム要求は /mnt/mqm にマウントされます。 あるいは、150 ページの『.spec.queueManager.storage.queueManager』で **type** プロパティーが ephemeral に設定されている場合、一時ボリュームが作成され、マウントされます。
3. 一時ボリュームごとに、データがどの程度増大する可能性があるかを慎重に検討してください。 SI 単位を含め、 **sizeLimit** プロパティーの値を適宜設定します。
   - Scratch 一時ボリュームの場合、151 ページの『.spec.queueManager.storage.scratch』で **sizeLimit** プロパティーを設定します。 デフォルト値は「100M」です。
   - Tmp 一時ボリュームの場合は、152 ページの『.spec.queueManager.storage.tmp』で **sizeLimit** プロパティーを設定します。 デフォルト値は「2Gi」です。
   - キュー・マネージャー・ボリュームの **type** が ephemeral に設定されている場合、150 ページの『.spec.queueManager.storage.queueManager』に **sizeLimit** プロパティーを設定します。 デフォルト値は「2Gi」です。

OpenShift V 9.4.0 IBM MQ Operator を使用した基本レジストリーでの IBM MQ Console の構成

IBM MQ Console にログインするために、キュー・マネージャーに独自の構成を提供することができます。

始める前に

IBM MQ Advanced for Developers ライセンスを使用してキュー・マネージャーをデプロイする場合は、単純な構成が組み込まれています。 170 ページの『admin および app ユーザーのパスワードを指定する方法を説明するキュー・マネージャー YAML の例』を参照してください。 IBM Cloud Pak for Integration ライセンス・キュー・マネージャーをデプロイする場合は、シングル・サインオンを使用して IBM MQ Console にログインするために、 IBM Cloud Pak for Integration Keycloak との統合を有効にすることができます。 129 ページの『IBM MQ Console クラスターにデプロイされた Red Hat OpenShift への接続』を参照してください。

手順

1. **パスワードを作成し、 securityUtility を使用して暗号化します。**

   ConfigMap は、キュー・マネージャーへのアクセスに使用する資格情報を保管するために使用されます。 セキュリティーを強化するために、 securityUtility コマンドを使用してこれらの資格情報をエンコードします。

   あるいは、 Kubernetes 層で資格情報を保護するシークレットを使用することもできます。 ただし、モニター・ツールやトラブルシューティング・ツールを使用すると、基礎となるファイルがセキュアでなくなる可能性があります。

2. オプション: **Red Hat OpenShift コマンド・ライン・インターフェース (CLI) にログインします。**

   OpenShift CLI を使用している場合は、 `oc login` を使用してログインします。

   あるいは、 OpenShift コンソールを使用することもできます。

3. **ご使用の構成で ConfigMap を作成します。**

   XML 構成の作成については、 IBM MQ Console および REST API セキュリティーを参照してください。

   以下の例では、グループ MQWebAdminGroup 内にユーザーを作成します。 MQWebAdminGroup のメンバーには、MQWebAdmin 役割が割り当てられます。 この例のそれぞれの指定の意味は次のとおりです。

   - *USERNAME* および *PASSWORD* を独自の値に置き換える **必要があります** 。 この例では、 *USERNAME* が 2 回使用されていることに注意してください。

     NAMESPACE は、 IBM MQ Operator がデプロイされ、キュー・マネージャーがデプロイされる場所、または既にデプロイされている場所として指定する **必要があります** 。

   a) OpenShift コンソールまたはコマンド行を使用して、以下の ConfigMap を作成します。

   ```
   kind: ConfigMap
   apiVersion: v1
   metadata:
     name: mqwebuserconfigmap
     namespace: NAMESPACE
   data:
     mqwebuser.xml: |
       <?xml version="1.0" encoding="UTF-8"?>
       <server>
         <featureManager>
           <feature>appSecurity-2.0</feature>
           <feature>basicAuthenticationMQ-1.0</feature>
         </featureManager>
         <enterpriseApplication id="com.ibm.mq.console">
           <application-bnd>
             <security-role name="MQWebAdmin">
               <group name="MQWebAdminGroup" realm="defaultRealm"/>
             </security-role>
           </application-bnd>
         </enterpriseApplication>
         <basicRegistry id="basic" realm="defaultRealm">
           <user name="USERNAME" password="PASSWORD"/>
           <group name="MQWebAdminGroup">
             <member name="USERNAME"/>
           </group>
         </basicRegistry>
         <sslDefault sslRef="mqDefaultSSLConfig"/>
       </server>
   ```

   b) オプション: コマンド行を使用する場合は、 ConfigMap を適用します。

   ```
   oc apply -f mqwebuserconfigmap.yaml
   ```

   残りのステップでは、以下のいずれかのオプションを選択します。

   - IBM MQ Console にアクセスするための構成を使用して、新しいキュー・マネージャーをデプロイします。
   - 既存のキュー・マネージャーに対するアクセス権限を IBM MQ Console に付与する構成を適用します。

4. オプション: **IBM MQ Console にアクセスするための構成を使用して、新規キュー・マネージャーをデプロイします。**

   a) キュー・マネージャーを作成します。

   以下のいずれかのオプションを使用して、認証および許可プロバイダーを **手動** に設定し、新しく作成した ConfigMap mqwebuserconfigmap を指定します。

   - オプション 1: キュー・マネージャー YAML を使用する

     キュー・マネージャー YAML の web セクションの下に以下のコードを追加します。

```
...
web:
    enabled: true
    console:
      authentication:
        provider: manual
      authorization:
        provider: manual
    manualConfig:
      configMap:
        name: mqwebuserconfigmap
```

   - オプション 2: OpenShift コンソール・フォーム・ビューを使用して、以下の操作を行います。

     i) OpenShift コンソールで、「**オペレーター**」 > 「**インストール済みオペレーター**」を選択します。

     ii) IBM MQ Operator のデプロイメントを選択します。

     iii)「**キュー・マネージャー**」 を選択し、 「**作成**」 **QueueManager** をクリックします。

     iv) キュー・マネージャーに関連するオプションを選択します。

     v)「**Web**」 を選択し、 「**Web サーバーを使用可能にする**」 を true に設定します。

     vi)「**拡張構成**」 リスト・ボックスを開きます。

     vii)「**コンソール**」 リスト・ボックスで、 「**認証**」 と 「**許可**」 の両方の **プロバイダー** を manual に設定します。

     viii)「 **構成** 」リスト・ボックスを開きます。

     ix) **ConfigMap** リスト・ボックスを開き、ステップ 98 ページの『3』で作成した ConfigMap mqwebuserconfigmap を選択します。

     x)「**作成**」 をクリックします。

   これで、ステップ 98 ページの『3』で作成した ConfigMap で指定した資格情報を使用して、新しいキュー・マネージャーの IBM MQ Console にアクセスできるようになりました。

5. オプション: **既存のキュー・マネージャーに対して IBM MQ Console を有効にする構成を適用します。**

   IBM MQ Console を有効にするキュー・マネージャーの YAML を編集します。

   a. OpenShift コンソールで、 「**オペレーター**」 > 「**インストール済みオペレーター**」を選択します。

   b. IBM MQ Operator のデプロイメントを選択します。

   c.「**キュー・マネージャー**」 を選択し、キュー・マネージャーの名前を選択します。

   d.「**YAML**」を選択します。

   e. キュー・マネージャー YAML の既存の web セクションを以下のコードに置き換えます。

```
...
web:
    enabled: true
    console:
      authentication:
        provider: manual
      authorization:
        provider: manual
    manualConfig:
      configMap:
        name: mqwebuserconfigmap
```

f. **保存** をクリックします。

これで、ステップ 98 ページの『3』 で作成した ConfigMap で指定した資格情報を使用して、既存のキュー・マネージャーの IBM MQ Console にアクセスできるようになりました。

OpenShift V 9.4.0 V 9.4.0 永続ボリュームの拡張

ご使用のストレージ・プロバイダーがボリューム拡張をサポートしている場合は、このタスクを使用して永続ボリュームを拡張します。 ストレージ・プロバイダーによっては、拡張がオンラインまたはオフラインで行われる場合があります。

始める前に

ボリュームが正常に拡張されるには、ストレージ・プロバイダーが拡張要求を満たす必要があります。 オンライン・サイズ変更がサポートされているかどうか、およびオフライン・サイズ変更手順については、ご使用のストレージ・プロバイダーの資料を参照してください。

ストレージ・プロバイダーが拡張要求を満たすことができない場合、永続ボリューム要求は警告またはエラーのある状態になる可能性があります。 拡張が失敗した場合、 OpenShift 管理者は永続ボリューム要求の状態を手動でリカバリーし、拡張を取り消すことができます。 Red Hat OpenShift 資料の「 ボリューム拡張時の障害からのリカバリー 」を参照してください。

このタスクについて

永続ストレージの管理に役立つように、 Kubernetes では以下の 2 つの API リソースが定義されています。

- PersistentVolume (PV)。これは、管理者によってプロビジョンされたか、ストレージ・クラスを使用して動的にプロビジョンされた、クラスター内のストレージの一部です。 これは、静的または動的にプロビジョンできます。
- PersistentVolumeClaim (PVC)。これは、ユーザーによるストレージの要求です。 また、リソースに対するクレーム・チェックとしても機能します。

詳しくは、 Kubernetes 資料の 永続ボリューム を参照してください。

警告 :

- キュー・マネージャー PVC の作成に使用されるストレージ・クラスがオンライン・サイズ変更をサポートしていない場合は、オフライン・サイズ変更が行われます。 ボリューム拡張を完了するには、オフラインでのサイズ変更中にユーザー介入が必要になるため、キュー・マネージャーでダウン時間が発生します。
- 複数インスタンス・キュー・マネージャーの共有ボリュームのオフライン・サイズ変更の場合、ユーザー介入の実行時にアクティブ・ポッドとスタンバイ・ポッドの両方を同時に停止する必要があります。
- OpenShift では、PVC のサイズの縮小はサポートされていません。 永続ボリュームのサイズを削減しようとすると、キュー・マネージャーは「失敗」状態になります。
- この手順は、一時ボリュームには適用されません。

IBM MQ コンテナーによって使用される PV を展開するには、以下の手順を実行します。

手順

1. **ボリュームの拡張の準備**

   a) 拡張するボリュームを決定します。

   b) ボリュームで使用されている 1 つ以上のストレージ・クラスを判別します。

   以下に例を示します。

```
spec:
  queueManager:
    storage:
      persistedData:
        enabled: true
```

```
        type: persistent-claim
        class: ocs-storagecluster-cephfs (1)
      queueManager:
        type: persistent-claim
      recoveryLogs:
        enabled: true
        type: persistent-claim
      defaultClass: ocs-storagecluster-ceph-rbd (2)
```

注:

- (1) ボリュームが特定のストレージ・クラスを定義している場合、これはこのタイプの PVC によって使用されます。
- (2) **defaultClass** が設定されている場合、このストレージ・クラスは、特定のストレージ・クラスを持たないすべてのボリュームに使用されます。 **defaultClass** が設定されておらず、ボリューム・タイプにクラスが指定されていない場合は、クラスターのデフォルトのストレージ・クラスが使用されます。

基礎となる PVC を記述することで、使用中のストレージ・クラスを確認することもできます。 以下に例を示します。

```
oc describe pvc pvc-name
```

c) ストレージ・クラスがボリューム拡張をサポートしていることを確認します。

ストレージ・クラスには、プロパティー **.allowVolumeExpansion** が定義されている場合があります。

- このプロパティーが `true` に設定されている場合、ボリューム拡張がサポートされます。
- このプロパティーが `false` に設定されているか、このプロパティーが定義されていない場合、ストレージ・クラスはボリューム拡張を許可しません。 この場合は、ストレージ・プロバイダーの資料を参照して、この機能を有効にできるかどうかを確認してください。

また、ストレージ・クラスを記述して、そのストレージ・クラスがボリューム拡張をサポートしているかどうかを判別することもできます。 以下に例を示します。

```
oc describe sc storage-class-name
```

d) ストレージ・プロバイダーの資料を参照して、ボリューム拡張にオンラインまたはオフラインの手順が使用されているかどうかを確認してください。

オフライン手順では、キュー・マネージャー・ポッドを手動で再始動する必要がありますが、オンライン手順では再始動しません。 オフラインでのサイズ変更手順については、ご使用のストレージ・プロバイダーの資料を参照してください。

e) キュー・マネージャーに「StorageMismatch」という状況条件があるかどうかを確認します。

キュー・マネージャーがこの状況条件になっている場合、ボリューム拡張を使用可能にすると、条件にリストされているボリュームが拡張されます。 これを行わない場合は、キュー・マネージャー定義内の各ボリューム・タイプに関連付けられているサイズ・フィールドを、プロビジョンされた PVC と一致するように変更します。 一致しないすべてのボリュームに対してこれが行われると、状況条件は除去されます。

2. **ボリュームの拡張**

警告 :

- キュー・マネージャー定義のボリューム・サイズ・フィールドのいずれかを以前に変更したことがある場合は、キュー・マネージャー定義で **.allowVolumeExpansion** が `true` に設定されていると、ボリュームの拡張が開始されます。
- ストレージ・プロバイダーによっては、ファイル・システムの制限やローカル・ハードウェアの可用性のために、ボリュームの最大サイズに制限がある場合があります。 障害を回避するには、ボリュームを拡張する前に、ストレージ・プロバイダーの資料でこれらの制限を確認してください。

- PVC サイズの縮小は、OpenShift ではサポートされていません。 ボリュームのサイズを拡張する場合、縮小することはできません。 これを行おうとして失敗した場合、 IBM MQ Operator は PVC を元の状態に戻すことができません。

ボリューム拡張を示すキュー・マネージャー定義の例:

```
spec:
  queueManager:
    storage:
      allowVolumeExpansion: true (A)
      persistedData:
        enabled: true
        type: persistent-claim
        size: 3Gi (B)
      queueManager:
        type: persistent-claim
        size: 4Gi (B)
      recoveryLogs:
        enabled: true
        type: persistent-claim
        size: 3Gi (B)
```

a) キュー・マネージャーのボリューム拡張を許可するには、キュー・マネージャーのフィールド **.spec.queueManager.storage.allowVolumeExpansion** (A) を `true` に設定します。

b) これで、使用可能な任意のボリューム・タイプのサイズ・フィールド (B) を増やすことができます。 これらの変更を適用すると、ボリューム拡張が開始されます。

3. **PVC がサイズ変更されたことを確認します**。

注:

- ボリュームの拡張には時間がかかる場合があります。 検証が初めて成功しなかった場合は、数分待ってから再度検証することを検討してください。
- ボリューム拡張は、オンライン・サイズ変更が実行された場合にのみ、ユーザー・アクションなしで完了します。
- 一部のストレージ・プロバイダーは、要求したストレージ・サイズを切り上げます。 拡張ボリュームのサイズは、要求のサイズ以上でなければなりません。

a) 状況条件については、キュー・マネージャーを確認してください。 条件、説明、および推奨アクションについては、以下の表を参照してください。

表 *1.* 保管のステータス条件

CONDITION	**MESSAGE**	**EXPLANATION**
StorageMismatch	Storage sizes defined in the QueueManager resource do not match the capacity of one or more provisioned PVCs [pvc-list]. AllowVolumeExpansion is set to false in the QueueManager resource so the MQ Operator will not attempt to reconcile these differences.	キュー・マネージャー定義で **.allowVolumeExpansion** が `true` に設定されていないため、ボリューム拡張は行われません。

表 1. 保管のステータス条件 (続き)

CONDITION	MESSAGE	EXPLANATION
StorageExpansionPending	Volume expansion is pending for the following PVCs [pvc-list]	ボリューム拡張はまだ行われています。 この状況状態が長期間続く場合は、オフラインのサイズ変更またはサイズ変更の失敗が発生している可能性があるため、以下の手順に従って詳細情報を収集してください。
Failed	'Failed' 状況条件を作成する可能性のある、ストレージ関連のメッセージが多数あります。 例: 'MQ Queue Manager failed to deploy: persistentvolumeclaims "<pvc>" is forbidden: only dynamically provisioned pvc can be resized and the storageclass the provisions the pvc must support resize.'	キュー・マネージャーに、ストレージを参照するテキストを持つ 'Failed' 状況条件がある場合は、状況条件内のメッセージを参照してください。 ここに示されているメッセージの例は、拡張をサポートしていないストレージ・クラスを使用していることが原因です。

b) 拡張した PVC ごとに、キュー・マネージャー定義で指定された値以上になるように容量が増加していることを確認します。

HA キュー・マネージャーには、各タイプの複数の PVC がある場合があります。 PVC の容量を取得するには、以下のコマンドを実行します。

```
oc get pvc pvc-name -o template --template '{{.status.capacity.storage}}'
```

c) PVC に、サイズ変更の失敗を示す状況条件またはイベントがないことを確認します。

```
oc describe pvc pvc-name
```

- PVC が「Waiting for user to (re-) start a pod to finish file system resize of volume on node」というメッセージとともに状況条件 FileSystemResizePending を持っている可能性があります。 この状況条件は、オンラインとオフラインの両方のサイズ変更で発生します。 オンライン・サイズ変更の場合、この状況条件は、オンライン・サイズ変更の完了後にユーザー処置なしで表示されなくなります。
- サイズ変更が失敗したことを示すイベントまたは状況条件が PVC にある場合は、 Red Hat OpenShift 資料の ボリューム拡張時の障害からのリカバリー を参照してください。

d) キュー・マネージャーのポッドに、サイズ変更の失敗を示す状況条件やイベントがないことを確認します。 HA デプロイメントの場合は、各レプリカを確認します。

```
oc describe pod queue-manager-pod-name
```

- サイズ変更が失敗したことを示すイベントまたは状況条件がポッドにある場合は、 Red Hat OpenShift 資料の ボリューム拡張時の障害からのリカバリー を参照してください。 エラー・テキストは、問題の解決に役立つ場合があります。また、リカバリー後にサイズ変更を再試行すると、同じ問題の発生を防ぐことができます。

4. **オフラインのサイズ変更時にポッドを再始動する**

ストレージ・プロバイダーがボリュームの拡張時にオフラインのサイズ変更手順を使用する場合、ボリュームの拡張を完了するには、サイズ変更するボリュームをマウントするキュー・マネージャー・ポッドを再始動する必要があります。

複数インスタンス・キュー・マネージャーの場合、リカバリー・ログと永続データ・ボリュームは、アクティブ・ポッドとスタンバイ・ポッドの両方で共有されます。 これらのボリュームのサイズ変更を完了するには、両方のポッドを同時に停止します。

オフラインでのサイズ変更手順については、ご使用のストレージ・プロバイダーの資料を参照してください。

OpenShift V 9.4.0 V 9.4.0 キュー・マネージャーの停止 (mq.ibm.com/stop)

キュー・マネージャー定義に注釈を追加して、キュー・マネージャーを停止します。

このタスクについて

IBM MQ Operator によって作成されたキュー・マネージャーには、 StatefulSet が関連付けられています。 この StatefulSet は、「.replicas」フィールドを使用して、特定のキュー・マネージャー可用性タイプに対してデプロイされる Pods の数を宣言します。 これは、1 (単一インスタンス)、2 (複数インスタンス)、または 3 (NativeHA) の値を取ります。

注: 「.replicas」フィールドの値を手動で変更すると、キュー・マネージャーが正しく機能しなくなります。

場合によっては、キュー・マネージャーを停止して、 StatefulSet のレプリカ・カウントが 0 になり、Pods がデプロイされないようにすることができます。 これを行う必要がある場合の例としては、保守中やバックアップ手順中などがあります。

注: キュー・マネージャーの停止時にはキュー・マネージャー Pods がデプロイされていないため、キュー・マネージャーが再始動されるまで、ユーザーとアプリケーションはキュー・マネージャーにアクセスできません。

手順

- キュー・マネージャーを停止するには、「.metadata.annotations」セクションの下のキュー・マネージャー定義に以下のアノテーションを追加します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: my-qm
  annotations:
    "mq.ibm.com/stop" : "true"
```

- キュー・マネージャーを再始動して正しいレプリカ数に戻すには、キュー・マネージャーからアノテーションを削除するか、その値を「false'」に設定します。

Helm を使用したキュー・マネージャーのデプロイおよび構成

サンプルの Helm チャートを使用して、 Kubernetes にキュー・マネージャーをデプロイして構成することができます。

このタスクについて

Red Hat OpenShift Container Platform を使用していない場合、 IBM MQ Operator はサポートされません。サンプルの Helm チャートを使用して、他のタイプの Kubernetes クラスターにデプロイできます。

手順

- Helm を使用して独自の IBM MQ コンテナー・イメージをデプロイする方法については、 サンプル IBM MQ Helm チャート を参照してください。

関連資料

8 ページの『コンテナーでの IBM MQ のサポート』

コンテナーでは、すべての IBM MQ 機能が同じ方法で使用可能およびサポートされているわけではありません。

IBM MQ Operator へのマイグレーション

この一連のトピックでは、Red Hat OpenShift Container Platform の IBM MQ Operator を使用して、既存の IBM MQ キュー・マネージャーをコンテナー環境にマイグレーションするための主要なステップについて説明します。

このタスクについて

IBM MQ on Red Hat OpenShift で展開するクライアントは、以下のシナリオに分けることができる。

1. 新規アプリケーションのための新しい IBM MQ デプロイメントを Red Hat OpenShift に作成する。
2. Red Hat OpenShift 内の新規アプリケーションのために IBM MQ ネットワークを Red Hat OpenShift に拡張します。
3. 既存のアプリケーションを引き続きサポートするには、 IBM MQ デプロイメントを Red Hat OpenShift に移動します。

ご使用の IBM MQ 構成をマイグレーションする必要があるのは、シナリオ 3 の場合のみです。 その他のシナリオは、新規デプロイメントと見なされます。

この一連のトピックでは、シナリオ 3 に焦点を当て、 IBM MQ Operator を使用して既存の IBM MQ キュー・マネージャーをコンテナー環境にマイグレーションするための重要なステップについて説明します。 IBM MQ は柔軟性と拡張性に優れているため、オプションで行える手順がいくつかあります。 これらの各手順に「これを行う必要がありますか?」セクションがあります。 社内でどのようなニーズがあるかを確認しておくなら、マイグレーション時に時間を節約することができるはずです。

どのデータをマイグレーションするか検討することも必要です。

1. 同じ構成で IBM MQ をマイグレーションするが、キューに入っている既存のメッセージは含めない。
2. 同じ構成で IBM MQ をマイグレーションし、既存のメッセージも含める。

標準的なバージョン間マイグレーションでは、どちらのアプローチでも使用できます。 IBM MQ キュー・マネージャーの標準的なマイグレーションでは、マイグレーション時にキューにメッセージが保管されていたとしてもわずかなので、多くの場合はオプション 1 が適切です。 コンテナー・プラットフォームへのマイグレーションでは、それにも増してオプション 1 を使用することが一般的になっています。これは、マイグレーションの複雑な手順をなくして、ブルー・グリーン・デプロイメントを行えるようにするためです。 そのため、このシナリオに焦点を当てて説明します。

このシナリオの目的は、既存のキュー・マネージャーの定義と一致するキュー・マネージャーをコンテナー環境内に作成することです。 この方法では、ネットワークに接続された既存のアプリケーションは、新しいキュー・マネージャーを指すように再構成するだけで済みますので、他の構成やアプリケーション・ロジックを変更する必要はありません。

このマイグレーション全体を通して、新しいキュー・マネージャーに適用される複数の構成ファイルを生成します。 これらのファイルの管理を簡素化するために、ディレクトリーを 1 つ作成し、生成したファイルはそのディレクトリーに入れるようにしてください。

手順

1. 106 ページの『必要な機能を利用できることの確認』
2. 106 ページの『キュー・マネージャー構成の抽出』
3. オプション: 107 ページの『オプション: キュー・マネージャーの鍵と証明書の抽出および取得』
4. オプション: 109 ページの『オプション: LDAP の構成』
5. オプション: 117 ページの『オプション: IBM MQ 構成内の IP アドレスとホスト名の変更』
6. 118 ページの『コンテナー環境用のキュー・マネージャー構成の更新』
7. 121 ページの『コンテナーで実行されている IBM MQ のためのターゲット HA アーキテクチャーの選択』

8. 122 ページの『キュー・マネージャー用のリソースの作成』
9. 123 ページの『Red Hat OpenShift での新しいキュー・マネージャーの作成』
10. 127 ページの『新規コンテナー・デプロイメントの検証』

OpenShift CP4I-SC2 CD 必要な機能を利用できることの確認

IBM MQ Operator には、IBM MQ Advanced 内で使用可能な機能がすべて含まれているわけではないので、除外されている機能が必要ないことを確認する必要があります。 その他の機能は部分的にサポートされており、コンテナー内で使用可能なものと一致するように再構成することもできます。

始める前に

これは、105 ページの『IBM MQ Operator へのマイグレーション』の最初のステップです。

手順

1. 必要なすべての機能がターゲット・コンテナー・イメージに含まれていることを確認します。

   最新情報については、8 ページの『コンテナー内の IBM MQ の使用方法の選択』を参照してください。
2. IBM MQ Operator には、リスナーと呼ばれる IBM MQ トラフィック・ポートが 1 つあります。 複数のリスナーがある場合は、これを単純化して、コンテナーで 1 つのリスナーを使用するようにします。 これは一般的なシナリオではないため、この変更についての詳細な説明は行いません。
3. IBM MQ 出口が使用されている場合は、IBM MQ 出口バイナリー内で階層化することにより、それらをコンテナーにマイグレーションします。 これは上級のマイグレーション・シナリオであるため、ここには記載しません。 手順の概要については、93 ページの『Red Hat OpenShift CLI を使用した、カスタム MQSC および INI ファイルを使用したイメージの作成』を参照してください。
4. IBM MQ システムに高可用性が設定されている場合は、使用可能なオプションを確認します。

   17 ページの『コンテナー内の IBM MQ の高可用性の計画』 を参照してください。

次のタスク

これで、キュー・マネージャー構成を抽出する準備ができました。

OpenShift CP4I-SC2 CD キュー・マネージャー構成の抽出

構成の大部分は、キュー・マネージャー間で移植可能です。 例えば、アプリケーションが対話する内容 (キュー、トピック、およびチャネルの定義など) です。 既存の IBM MQ キュー・マネージャーから構成を抽出するには、このタスクを使用します。

始める前に

このタスクでは、必要な機能が使用可能であることを確認済みであることを前提としています。

手順

1. 既存の IBM MQ インストール済み環境があるマシンにログインします。
2. 構成のバックアップをとります。

   以下のコマンドを実行します。

   ```
   dmpmqcfg -m QMGR_NAME > /tmp/backup.mqsc
   ```

   このコマンドの使用上の注意:

   - このコマンドは、バックアップを tmp ディレクトリーに保管します。 別の場所にバックアップを保管することもできますが、このシナリオの以下のコマンドでは、tmp ディレクトリーを使用することを想定しています。

- *QMGR_NAME* は、ご使用の環境のキュー・マネージャー名に置き換えてください。 値が分からない場合は、**dspmq** コマンドを実行して、このマシンで使用可能なキュー・マネージャーを表示します。 ここでは、qm1 という名前のキュー・マネージャーの **dspmq** コマンド出力例を示します。

```
QMNAME(qm1)                   STATUS(Running)
```

dspmq コマンドを実行するには、IBM MQ キュー・マネージャーが開始している必要があります。開始していない場合は、次のエラーを受け取ります。

```
AMQ8146E: IBM MQ queue manager not available.
```

必要に応じて、次のコマンドを実行してキュー・マネージャーを開始します。

```
strmqm QMGR_NAME
```

次のタスク

これで、キュー・マネージャーの鍵と証明書を抽出して取得する準備ができました。

OpenShift CP4I-SC2 CD オプション: キュー・マネージャーの鍵と証明書の抽出および取得

IBM MQ は、TLS を使用してキュー・マネージャーへのネットワーク・トラフィックを暗号化するように構成できます。 このタスクを使用して、キュー・マネージャーが TLS を使用していることを確認し、鍵と証明書を抽出し、マイグレーションされたキュー・マネージャーで TLS を構成します。

始める前に

このタスクでは、キュー・マネージャー構成を抽出済みであることを前提としています。

このタスクについて

これを行う必要がありますか?

キュー・マネージャーへのトラフィックを暗号化するように IBM MQ を構成することができます。 この暗号化は、キュー・マネージャーで構成されている鍵リポジトリーを使用して実行されます。 IBM MQ チャネルはそれを使って TLS 通信を有効にします。 ご使用の環境で TLS 通信が構成されているかどうかが不明な場合は、以下のコマンドを実行して確認してください。

```
grep 'SECCOMM(ALL\|SECCOMM(ANON\|SSLCIPH' backup.mqsc
```

結果が表示されない場合、TLS は使用されていません。 しかし、このことはマイグレーション済みのキュー・マネージャーで TLS を構成できないことを意味するものではありません。 以下の状況では、この状態を変更することが必要となる場合があります。

- Red Hat OpenShift 環境に対するセキュリティー・アプローチは、前の環境と比較して拡張する必要があります。
- Red Hat OpenShift 環境の外部からマイグレーション済みキュー・マネージャーにアクセスする必要がある場合は、Red Hat OpenShift ルートを通過するために TLS が必要です。

注 : 発行者 (CA) 証明書と同じサブジェクト識別名 (DN) を持つキュー・マネージャー証明書はサポートされません。 証明書には固有のサブジェクト識別名が必要です。 製品は、DN が同じでないことを検査します。

手順

1. 既存のストアから信頼できる証明書をすべて抽出します。

現在、キュー・マネージャーで TLS を使用している場合、キュー・マネージャーにいくつかのトラステッド証明書が保管されている可能性があります。 これらを抽出して、新しいキュー・マネージャーにコピーする必要があります。 以下のいずれかのオプションの手順を実行します。

- 証明書の抽出を簡素化するには、ローカル・システム上で以下のスクリプトを実行します。

```
#!/bin/bash

keyr=$(grep SSLKEYR $1)
if [ -n "${keyr}" ]; then
   keyrlocation=$(sed -n "s/^.*'\(.*\)'.*$/\1/ p" <<< ${keyr})
   mapfile -t runmqakmResult < <(runmqakm -cert -list -db ${keyrlocation}.kdb -stashed)
   cert=1
   for i in "${runmqakmResult[@]:2}"
   do
      certlabel=$(echo ${i:2} | xargs)
      echo Extracting certificate $certlabel to $cert.cert
      runmqakm -cert -extract -db ${keyrlocation}.kdb -label "$certlabel" -target $
{cert}.cert -stashed
      cert=$[$cert+1]
   done
fi
```

このスクリプトを実行するときに、IBM MQ バックアップの場所を引数として指定すると、証明書が抽出されます。 例えば、スクリプトが `extractCert.sh` という名前で、IBM MQ バックアップが `/tmp/backup.mqsc` にある場合は、以下のコマンドを実行します。

```
extractCert.sh /tmp/backup.mqsc
```

- または、以下のコマンドを上から順に実行します。

  a. キュー・マネージャーの TLS キー・リポジトリーの場所を識別します。

  ```
  grep SSLKEYR /tmp/backup.mqsc
  ```

  出力例は次のとおりです。

  ```
  SSLKEYR('/run/runmqserver/tls/key') +
  ```

  ここで、鍵ストアは `/run/runmqserver/tls/key.kdb` にあります

  b. このロケーション情報に基づいて鍵ストアを照会し、保管されている証明書を判別します。

  ```
  runmqakm -cert -list -db /run/runmqserver/tls/key.kdb -stashed
  ```

  出力例は次のとおりです。

  ```
  Certificates in database /run/runmqserver/tls/key.kdb:
            default
            CN=cs-ca-certificate,O=cert-manager
  ```

  c. リストされた各証明書を抽出します。 これを行うには、以下のコマンドを実行します。

  ```
  runmqakm -cert -extract -db KEYSTORE_LOCATION -label "LABEL_NAME" -target OUTPUT_FILE
  -stashed
  ```

  上記のサンプルでは、これは以下のコマンドと同等です。

  ```
  runmqakm -cert -extract -db /run/runmqserver/tls/key.kdb -label "CN=cs-ca-
  certificate,O=cert-manager" -target /tmp/cert-manager.crt -stashed
  runmqakm -cert -extract -db /run/runmqserver/tls/key.kdb -label "default" -target /tmp/
  default.crt -stashed
  ```

2. キュー・マネージャーの新しい鍵と証明書を取得します。

マイグレーション済みのキュー・マネージャー上で TLS を構成するには、新しい鍵と証明書を生成します。 これが後でデプロイメント時に使用されます。 多くの組織では、このためにセキュリティー・チームに連絡して鍵と証明書を提供してもらうことが必要になります。 組織によっては、このオプションが使えないため、自己署名証明書を使用します。

以下の例では、有効期限を 10 年に設定して自己署名証明書を生成します。

```
openssl req \
       -newkey rsa:2048 -nodes -keyout qmgr.key \
       -subj "/CN=mq queuemanager/OU=ibm mq" \
       -x509 -days 3650 -out qmgr.crt
```

次の 2 つの新規ファイルが作成されます。

- `qmgr.key` は、キュー・マネージャーの秘密鍵です
- `qmgr.crt` はパブリック証明書です

次のタスク

これで、LDAP を構成する準備ができました。

OpenShift CP4I-SC2 CD オプション: LDAP の構成

IBM MQ Operator は、複数の異なるセキュリティー・アプローチを使用するように構成できます。 通常、LDAP はエンタープライズ・デプロイメントに最も効果的なので、このマイグレーション・シナリオでは LDAP を使用します。

始める前に

このタスクでは、キュー・マネージャーの鍵と証明書を抽出して取得済みであることを前提としています。

このタスクについて

これを行う必要がありますか?

認証と許可に LDAP を既に使用している場合は、変更する必要はありません。

LDAP を使用しているかどうかが分からない場合は、次のコマンドを実行します。

```
connauthname="$(grep CONNAUTH backup.mqsc | cut -d "(" -f2 | cut -d ")" -f1)"; grep -A 20
AUTHINFO\($connauthname\) backup.mqsc
```

出力例は次のとおりです。

```
DEFINE AUTHINFO('USE.LDAP') +
   AUTHTYPE(IDPWLDAP) +
   ADOPTCTX(YES) +
   CONNAME('ldap-service.ldap(389)') +
   CHCKCLNT(REQUIRED) +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
*  LDAPPWD('********************************') +
   SHORTUSR('uid') +
   GRPFIELD('cn') +
   USRFIELD('uid') +
   AUTHORMD(SEARCHGRP) +
*  ALTDATE(2020-11-26) +
*  ALTTIME(15.44.38) +
   REPLACE
```

出力の中に、特に注目できる 2 つの属性があります。

AUTHTYPE
ここに値 IDPWLDAP が設定されている場合は、認証に LDAP を使用しています。

この値がブランクであるか、または別の値である場合は、LDAP が構成されていません。 この場合、許可に LDAP ユーザーが使用されているかどうかを確認するために、AUTHORMD 属性を確認してください。

AUTHORMD
ここに値 OS が設定されている場合は、許可に LDAP を使用していません。

LDAP を使用するように許可と認証を変更するには、以下の作業を行います。

手順

1. LDAP サーバーの IBM MQ バックアップを更新します。
2. LDAP 許可情報の IBM MQ バックアップを更新します。

OpenShift CP4I-SC2 CD LDAP パート 1: LDAP サーバー用の IBM MQ バックアップの更新

LDAP をセットアップする方法についての包括的な説明は、このシナリオでは扱われません。 このトピックでは、プロセスの要約、サンプル、および詳細情報の参照先を示します。

始める前に

このタスクでは、キュー・マネージャーの鍵と証明書を抽出して取得済みであることを前提としています。

このタスクについて

これを行う必要がありますか?

認証と許可に LDAP を既に使用している場合は、変更する必要はありません。 LDAP を使用しているかどうかが分からない場合は、109 ページの『オプション: LDAP の構成』を参照してください。

LDAP サーバーのセットアップには 2 つの段階があります。

1. LDAP 構成を定義します。
2. LDAP 構成をキュー・マネージャー定義に関連付けます。

この構成について詳しくは、以下を参照してください。

- ユーザー・リポジトリーの概要
- AUTHINFO コマンドの参照ガイド

手順

1. LDAP 構成を定義します。

   backup.mqsc ファイルを編集して、LDAP システム用の新しい **AUTHINFO** オブジェクトを定義します。以下に例を示します。

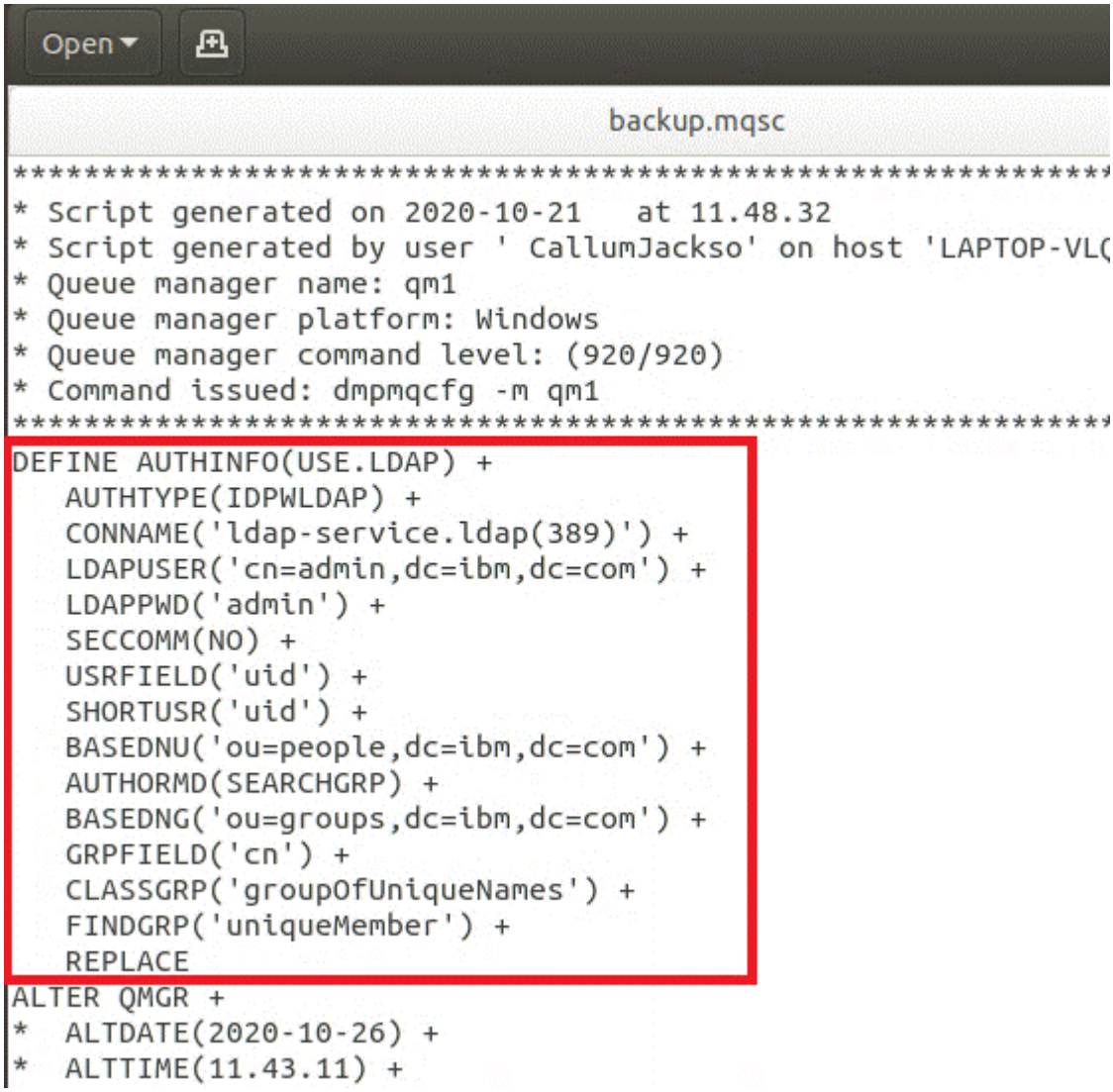
```
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
```

```
   FINDGRP('uniqueMember')
   REPLACE
```

説明:

- **CONNAME** は、LDAP サーバーに対応するホスト名とポートです。 回復力を高めるために複数のアドレスが用意されている場合は、これらをコンマ区切りリストにして構成することができます。
- **LDAPUSER** は、IBM MQ が LDAP に接続してユーザー・レコードを照会するときに使用するユーザーに対応する識別名です。
- **LDAPPWD** は、**LDAPUSER** ユーザーに対応するパスワードです。
- **SECCOM** は、LDAP サーバーへの通信に TLS を使用する必要があるかどうかを指定します。 指定可能な値:
  - YES: TLS を使用し、証明書は IBM MQ サーバーによって提供されます。
  - ANON: TLS を使用しますが、証明書は IBM MQ サーバーによって提供されません。
  - NO: 接続中に TLS を使用しません。
- **USRFIELD** は、提示されたユーザー名の突き合わせに使用する LDAP レコード内のフィールドを指定します。
- **SHORTUSR** は、LDAP レコード内の長さが 12 文字を超えないフィールドです。 認証に成功すると、このフィールド内の値は表明された ID になります。
- **BASEDNU** は、LDAP の検索に使用する必要がある基本 DN です。
- **BASEDNG** は、LDAP 内のグループの基本 DN です。
- **AUTHORMD** は、ユーザーのグループ・メンバーシップを解決するために使用するメカニズムを定義します。 次の 4 つのオプションがあります。
  - OS: 短い名前に関連付けられているグループのオペレーティング・システムを照会します。
  - SEARCHGRP: LDAP 内のグループ・エントリーから認証済みユーザーを検索します。
  - SEARCHUSR: 認証済みユーザー・レコードからグループ・メンバーシップ情報を検索します。
  - SRCHGRPSN: LDAP 内のグループ・エントリーから、認証済みユーザーの短いユーザー名 (SHORTUSR フィールドで定義する) を検索します。
- **GRPFIELD** は、単純名に対応する LDAP グループ・レコード内の属性です。 これを指定すると、許可レコードの定義に使用できます。
- **CLASSUSR** は、ユーザーに対応する LDAP オブジェクト・クラスです。
- **CLASSGRP** は、グループに対応する LDAP オブジェクト・クラスです。
- **FINDGRP** は、グループ・メンバーシップに対応する LDAP レコード内の属性です。

新しい項目はファイル内の任意の場所に置くことができますが、新しい項目をファイルの先頭に置くと便利です。



2. LDAP 構成をキュー・マネージャー定義に関連付けます。

   LDAP 構成をキュー・マネージャー定義に関連付ける必要があります。 DEFINE AUTHINFO 項目のすぐ下に ALTER QMGR 項目があります。 新しく作成された AUTHINFO 名に対応するように CONNAUTH 項目を変更します。 例えば直前の例では、AUTHINFO(USE.LDAP) が定義されています。これは、名前が USE.LDAP であることを示しています。 それで、CONNAUTH('SYSTEM.DEFAULT.AUTHINFO.IDPWOS') を CONNAUTH('USE.LDAP') に変更します。

LDAP への切り替えがすぐに行われるように、ALTER QMGR コマンドの直後に行を追加して、REFRESH SECURITY コマンドを呼び出します。

*backup.mqsc

```
************************************************************************
* Script generated on 2020-10-21   at 11.48.32
* Script generated by user ' CallumJackso' on host 'LAPTOP-VLQKJ5UH'
* Queue manager name: qm1
* Queue manager platform: Windows
* Queue manager command level: (920/920)
* Command issued: dmpmqcfg -m qm1
************************************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   REPLACE
ALTER QMGR +
*  ALTDATE(2020-10-26) +
*  ALTTIME(11.43.11) +
   CCSID(850) +
   CERTLABL('default') +
   CLWLUSEQ(LOCAL) +
*  COMMANDQ(SYSTEM.ADMIN.COMMAND.QUEUE) +
   CONNAUTH('USE.LDAP') +
*  CRDATE(2020-10-26) +
*  CRTIME(11.43.11) +
*  QMID(qm1_2020-10-26_11.43.11) +
   SSLCRYP(' ') +
   SSLKEYR('/run/runmqserver/tls/key') +
   SUITEB(NONE) +
*  VERSION(09020000) +
   FORCE
REFRESH SECURITY
```

次のタスク

これで、LDAP 許可情報の IBM MQ バックアップを更新する準備ができました。

OpenShift CP4I-SC2 CD LDAP パート 2: LDAP 許可情報の IBM MQ バックアップの更新

IBM MQ には、IBM MQ オブジェクトへのアクセスを制御する、細分化された許可規則が用意されています。 この認証および許可を LDAP に変更すると、許可規則が無効になって更新が必要になる場合があります。

始める前に

このタスクでは、LDAP サーバーのバックアップを更新済みであることを前提としています。

このタスクについて

これを行う必要がありますか?

認証と許可に LDAP を既に使用している場合は、変更する必要はありません。 LDAP を使用しているかどうかが分からない場合は、109 ページの『オプション: LDAP の構成』を参照してください。

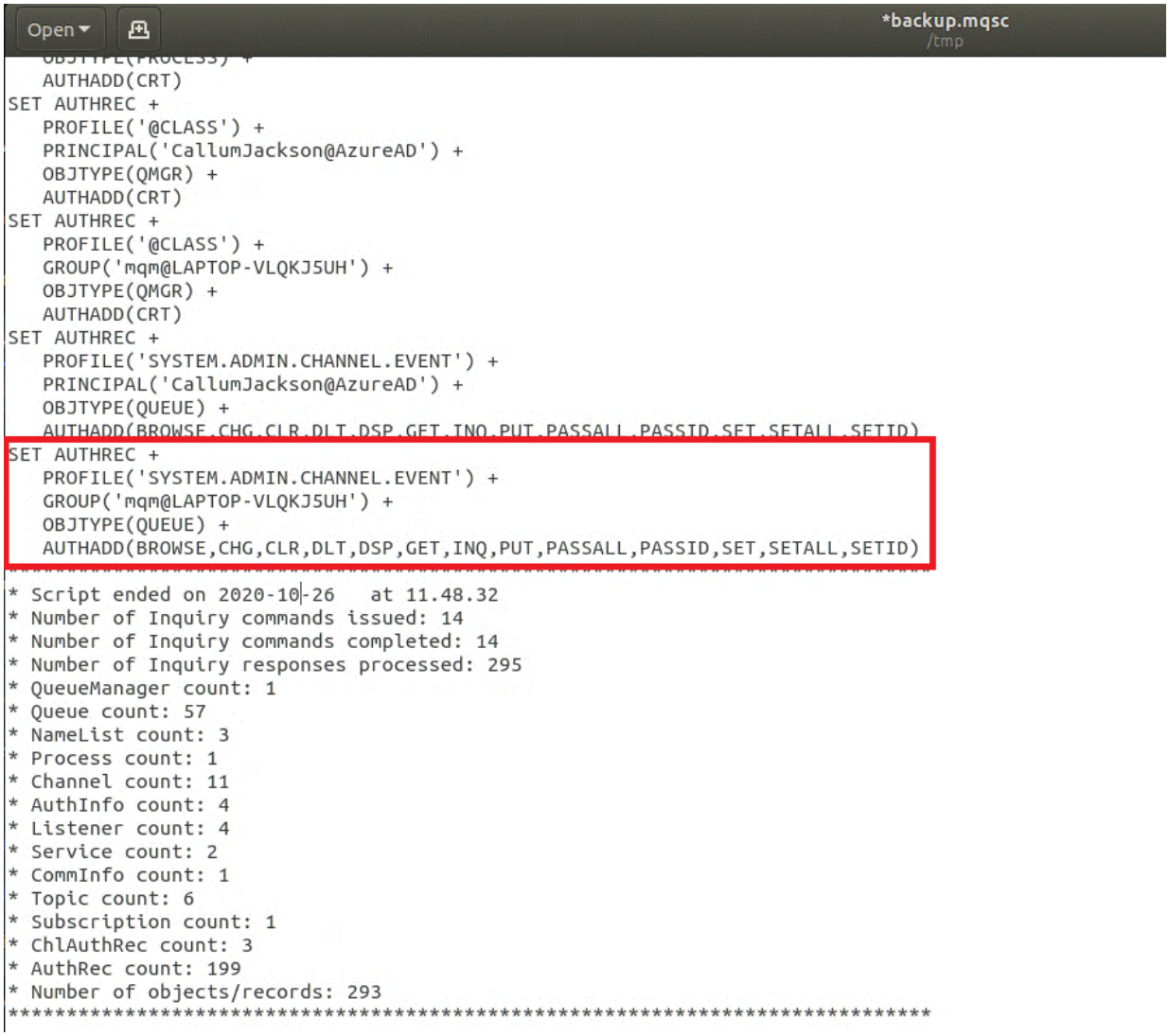
LDAP 許可情報の更新には 2 つの部分があります。

1. 既存のすべての許可をファイルから削除します。
2. LDAP 用の新しい許可情報を定義します。

手順

1. 既存のすべての許可をファイルから削除します。

   バックアップ・ファイルのファイルの終わり近くに、SET AUTHREC で始まるいくつかの項目があるはずです。



既存の項目を見つけて削除します。 一番手っ取り早い方法は、既存の SET AUTHREC ルールをすべて削除してから、LDAP 項目に基づいて新しい項目を作成する方法です。

2. LDAP 用の新しい許可情報を定義します。

   キュー・マネージャーの構成、およびリソースとグループの数によっては、この作業に時間がかかる場合もありますし、簡単にできる場合もあります。 以下の例では、キュー・マネージャーには Q1 という名前のキューが 1 つしかなく、LDAP グループ apps にアクセス権限を許可しようとしている状況を想定しています。

```
SET AUTHREC GROUP('apps') OBJTYPE(QMGR) AUTHADD(ALL)
SET AUTHREC PROFILE('Q1') GROUP('apps') OBJTYPE(QUEUE) AUTHADD(ALL)
```

   最初の AUTHREC コマンドは、キュー・マネージャーにアクセスするための権限を追加し、2 番目のコマンドはキューへのアクセス権限を設定します。 2 番目のキューにアクセスする必要がある場合は、3 番目の AUTHREC コマンドが必要になります。あるいは、ワイルドカードを使用して一般化したアクセス権限を設定することもできます。

   ここで別の例を見てみましょう。 管理者グループ (名前は admins) がキュー・マネージャーに対する全アクセス権限を必要とする場合は、以下のコマンドを追加します。

```
SET AUTHREC PROFILE('*') OBJTYPE(QUEUE) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(TOPIC) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(CHANNEL) GROUP('admins') AUTHADD(ALL)
```

```
SET AUTHREC PROFILE('*') OBJTYPE(CLNTCONN) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(AUTHINFO) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(LISTENER) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(NAMELIST) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(PROCESS) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(SERVICE) GROUP('admins') AUTHADD(ALL)
SET AUTHREC PROFILE('*') OBJTYPE(QMGR) GROUP('admins') AUTHADD(ALL)
```

次のタスク

これで、IBM MQ 構成の IP アドレスとホスト名を変更する準備ができました。

OpenShift CP4I-SC2 CD オプション: IBM MQ 構成内の IP アドレスとホスト名の変更

IBM MQ 構成には、IP アドレスとホスト名が指定されている場合があります。 状況によっては、これらをそのまま使用できる場合もありますが、更新する必要がある場合もあります。

始める前に

このタスクでは、LDAP を構成済みであることを前提としています。

このタスクについて

これを行う必要がありますか?

まず、直前のセクションで定義した LDAP 構成とは別に、IP アドレスまたはホスト名を指定したかどうかを判別します。 そのためには、以下のコマンドを実行します。

```
grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3  backup.mqsc
```

出力例は次のとおりです。

```
*****************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
--
DEFINE AUTHINFO('SYSTEM.DEFAULT.AUTHINFO.IDPWLDAP') +
   AUTHTYPE(IDPWLDAP) +
   ADOPTCTX(YES) +
   CONNAME(' ') +
--
   REPLACE
DEFINE AUTHINFO('SYSTEM.DEFAULT.AUTHINFO.CRLLDAP') +
   AUTHTYPE(CRLLDAP) +
   CONNAME(' ') +
```

この例では、検索によって 3 つの結果が返されています。 1 つの結果は、前に定義した LDAP 構成に対応しています。 LDAP サーバーのホスト名は同じままであるため、これは無視できます。 他の 2 つの結果は空の接続項目であるため、これらも無視できます。 さらに他の項目がなければ、このトピックの残りの部分をスキップできます。

手順

1. 返された項目の意味を考えます。

   IBM MQ では、構成の多くの側面に IP アドレス、ホスト名、およびポートを含めることができます。 これらは、次の 2 つのカテゴリーに分類できます。

   a. **このキュー・マネージャーのロケーション**: このキュー・マネージャーが使用またはパブリッシュするロケーション情報。IBM MQ ネットワーク内の他のキュー・マネージャーやアプリケーションはこの情報を使用して接続することができます。

b. **キュー・マネージャーの依存関係のロケーション**: このキュー・マネージャーが認識している必要がある他のキュー・マネージャーまたはシステムのロケーション。

このシナリオは、このキュー・マネージャー構成への変更のみに焦点を当てているため、カテゴリー (a) の構成の更新のみについて説明します。 ただし、このキュー・マネージャーのロケーションが他のキュー・マネージャーまたはアプリケーションによって参照されている場合は、このキュー・マネージャーの新しいロケーションと一致するように、それらの構成の更新が必要になることがあります。

更新する必要がある情報が含まれている可能性がある主なオブジェクトは、次の 2 つです。

- リスナー: これは、IBM MQ が listen するネットワーク・アドレスを表します。
- CLUSTER RECEIVER チャネル: キュー・マネージャーが IBM MQ クラスターの一部である場合、このオブジェクトが存在します。 これは、他のキュー・マネージャーが接続できるネットワーク・アドレスを指定します。

2. `grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3 backup.mqsc` コマンドからの元の出力で、CLUSTER RECEIVER チャネルが定義されているかどうかを確認します。 定義されている場合は、その IP アドレスを更新します。

   CLUSTER RECEIVER チャネルが定義されているかどうかを確認するには、オリジナルの出力の中に、次のように CHLTYPE(CLUSRCVR) を持つ項目を見つけます。

   ```
   DEFINE CHANNEL(ANY_NAME) +
      CHLTYPE(CLUSRCVR) +
   ```

   項目が存在する場合は、 IBM MQ Red Hat OpenShift 経路を使用して CONNAME を更新します。 この値は、 Red Hat OpenShift 環境に基づいており、予測可能な構文を使用します。

   ```
   queue_manager_resource_name-ibm-mq-qm-openshift_project_name.openshift_app_route_hostname
   ```

   例えば、キュー・マネージャーのデプロイメントが cp4i 名前空間内で qm1 という名前で、*openshift_app_route_hostname* が apps.callumj.icp4i.com の場合、経路 URL は次のようになります。

   ```
   qm1-ibm-mq-qm-cp4i.apps.callumj.icp4i.com
   ```

   このルートのポート番号は、通常 443 です。 Red Hat OpenShift 管理者が異なる方法で指示しない限り、これは通常、正しい値になります。 この情報を使用して、CONNAME フィールドを更新します。 以下に例を示します。

   ```
   CONNAME('qm1-ibm-mq-qm-cp4i.apps.callumj.icp4i.com(443)')
   ```

   `grep 'CONNAME\|LOCLADDR\|IPADDRV' -B 3 backup.mqsc` コマンドの元の出力で、LOCLADDR または IPADDRV の項目が存在するかどうかを確認します。 それらが存在する場合は、削除します。 それらはコンテナー環境では関係ありません。

次のタスク

これで、コンテナー環境用にキュー・マネージャー構成を更新する準備ができました。

OpenShift CP4I-SC2 CD コンテナー環境用のキュー・マネージャー構成の更新

コンテナーで実行する場合、構成の特定の側面はコンテナーによって定義され、エクスポートされた構成と対立する可能性があります。

始める前に

このタスクでは、IBM MQ 構成の IP アドレスとホスト名を変更済みであることを前提としています。

このタスクについて

以下の構成の側面は、コンテナーによって定義されます。

- リスナー定義 (公開されたポートに対応)。
- TLS ストアの候補となる場所。

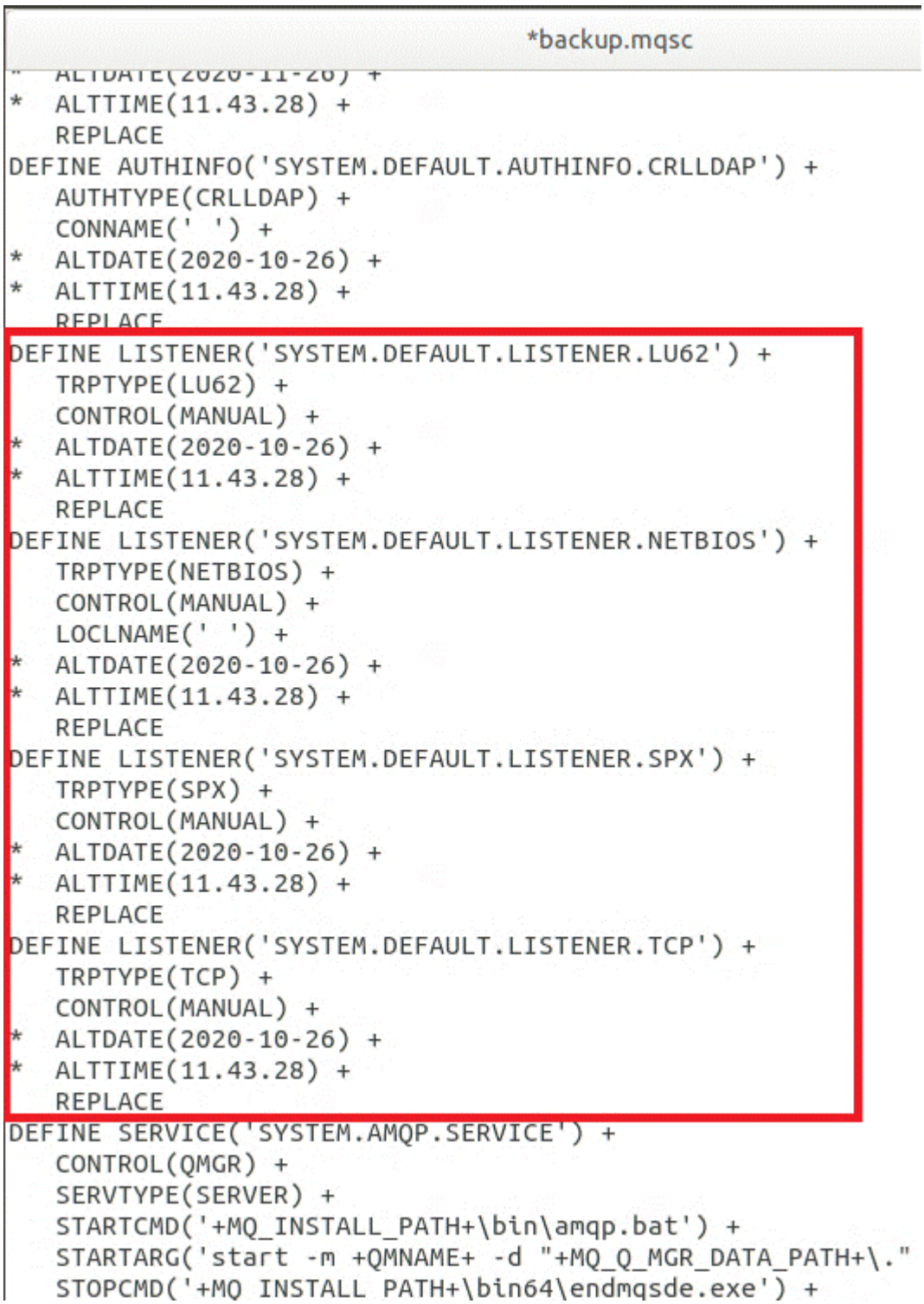
そのような理由で、エクスポートした構成を更新する必要があります。

1. リスナー定義をすべて削除します。
2. TLS 鍵リポジトリーの場所を定義します。

手順

1. リスナー定義をすべて削除します。

   バックアップ構成内で DEFINE LISTENER を検索します。 これは、AUTHINFO 定義と SERVICE 定義の間にあるはずです。 強調表示されている領域を削除します。



2. TLS 鍵リポジトリーの場所を定義します。

   キュー・マネージャーのバックアップには、元の環境の TLS 構成が含まれています。 これはコンテナー環境とは異なるため、いくつかの更新が必要です。

   - **CERTLABL** 項目を `default` に変更します
   - TLS キー・リポジトリーの場所 (**SSLKEYR**) を `/run/runmqserver/tls/key` に変更します

   ファイル内の **SSLKEYR** 属性の位置を検索するには、**SSLKEYR** を検索します。 通常は 1 つの項目のみが検出されます。 複数の項目が検出された場合は、以下の図に示すように、**QMGR** オブジェクトを編集中であるか確認します。

*backup.mqsc

```
********************************************************************************
* Script generated on 2020-10-21   at 11.48.32
* Script generated by user ' CallumJackso' on host 'LAPTOP-VLQKJ5UH'
* Queue manager name: qm1
* Queue manager platform: Windows
* Queue manager command level: (920/920)
* Command issued: dmpmqcfg -m qm1
********************************************************************************
DEFINE AUTHINFO(USE.LDAP) +
   AUTHTYPE(IDPWLDAP) +
   CONNAME('ldap-service.ldap(389)') +
   LDAPUSER('cn=admin,dc=ibm,dc=com') +
   LDAPPWD('admin') +
   SECCOMM(NO) +
   USRFIELD('uid') +
   SHORTUSR('uid') +
   BASEDNU('ou=people,dc=ibm,dc=com') +
   AUTHORMD(SEARCHGRP) +
   BASEDNG('ou=groups,dc=ibm,dc=com') +
   GRPFIELD('cn') +
   CLASSGRP('groupOfUniqueNames') +
   FINDGRP('uniqueMember') +
   REPLACE
ALTER QMGR +
*  ALTDATE(2020-10-26) +
*  ALTTIME(11.43.11) +
   CCSID(850) +
   CERTLABL('default') +
   CLWLUSEQ(LOCAL) +
*  COMMANDQ(SYSTEM.ADMIN.COMMAND.QUEUE) +
   CONNAUTH('USE.LDAP') +
*  CRDATE(2020-10-26) +
*  CRTIME(11.43.11) +
*  QMID(qm1_2020-10-26_11.43.11) +
   SSLCRYP(' ') +
   SSLKEYR('/run/runmqserver/tls/key') +
   SUITEB(NONE) +
*  VERSION(09020000) +
   FORCE
REFRESH SECURITY
```

次のタスク

これで、コンテナーで実行されている IBM MQ のためのターゲット・アーキテクチャーを選択する準備が整いました。

OpenShift CP4I-SC2 CD コンテナーで実行されている IBM MQ のためのターゲット HA アーキテクチャーの選択

高可用性の要件を満たすために、単一インスタンス (単一の Kubernetes ポッド)、複数インスタンス (2 つのポッド)、およびネイティブ HA (1 つのアクティブ・レプリカ・ポッドと 2 つのスタンバイ・レプリカ・ポッド) のいずれかを選択します。

始める前に

このタスクでは、コンテナー環境用のキュー・マネージャー構成を更新済みであることを前提としています。

このタスクについて

IBM MQ Operator には、以下の 3 つの高可用性オプションがあります。

- **単一インスタンス**: 単一のコンテナー (ポッド) が開始され、障害が発生した場合に Red Hat OpenShift が再始動するのはその責任になります。 Kubernetes 内のステートフル・セットの特性が原因で、このフェイルオーバーの際に、長い時間がかかったり管理アクションの実行が求められたりする状態がいくつかあります。
- **複数インスタンス**: 2 つのコンテナー (それぞれを別個のポッドに配置) が、1 つはアクティブ・モード、もう 1 つはスタンバイで開始します。 このトポロジーでは、フェイルオーバーの大幅な高速化が可能です。 これには、IBM MQ の要件を満たす Read Write Many ファイル・システムが必要です。
- **ネイティブ HA**: 3 つのコンテナー (それぞれが別個のポッド内にある) があり、それぞれにキュー・マネージャーのインスタンスがあります。 1 つのインスタンスがアクティブ・キュー・マネージャーとして機能し、メッセージはそこで処理されてリカバリー・ログに書き込まれます。 そのリカバリー・ログへの書き込みが行われると、アクティブ・キュー・マネージャーはレプリカと呼ばれる他の 2 つのインスタンスにデータを送信します。 アクティブ・キュー・マネージャーを実行しているポッドに障害が発生すると、キュー・マネージャーのレプリカ・インスタンスの 1 つがアクティブの役割を引き継ぎ、このインスタンスにある最新データで運用が行われます。

このタスクでは、ターゲット HA アーキテクチャーのみを選択します。 選択したアーキテクチャーを構成する手順については、このシナリオの後続のタスク (123 ページの『Red Hat OpenShift での新しいキュー・マネージャーの作成』) で説明します。

手順

1. 3 つのオプションを確認します。

   これらのオプションの包括的な説明については、 17 ページの『コンテナー内の IBM MQ の高可用性の計画』 を参照してください。
2. ターゲット HA アーキテクチャーを選択します。

   どちらのオプションを選択すべきか分からない場合、まず**単一インスタンス**のオプションで開始し、これがご使用の環境の高可用性要件を満たしているかどうかを確認します。

次のタスク

これで、キュー・マネージャー・リソースを作成する準備ができました。

OpenShift CP4I-SC2 CD キュー・マネージャー用のリソースの作成

IBM MQ 構成、TLS 証明書、および鍵を Red Hat OpenShift 環境にインポートします。

始める前に

このタスクでは、コンテナーで実行される IBM MQ 用のターゲット・アーキテクチャーを選択済みであることを前提としています。

このタスクについて

前の各セクションで、次の 2 つのリソースの抽出、更新、および定義を完了しました。

- IBM MQ 構成
- TLS 証明書および鍵

キュー・マネージャーがデプロイされる前に、これらのリソースを Red Hat OpenShift 環境にインポートする必要があります。

手順

1. IBM MQ 構成を Red Hat OpenShift にインポートします。

   以下の説明では、現行ディレクトリーの backup.mqsc というファイルに IBM MQ 構成があることを前提としています。 そうでない場合は、ご使用の環境に基づいてファイル名をカスタマイズする必要があります。

   a) oc login を使用してクラスターにログインします。

   b) IBM MQ 構成を configmap にロードします。

   以下のコマンドを実行します。

   ```
   oc create configmap my-mqsc-migrated --from-file=backup.mqsc
   ```

   c) ファイルが正常にロードされたことを確認します。

   以下のコマンドを実行します。

   ```
   oc describe configmap my-mqsc-migrated
   ```

2. IBM MQ TLS リソースをインポートします。

   107 ページの『オプション: キュー・マネージャーの鍵と証明書の抽出および取得』で説明しているように、キュー・マネージャーのデプロイメントに TLS が必要な場合があります。 その場合は、 .crt および .key で終わるファイルの数が既に存在するはずです。 キュー・マネージャーがこれらをデプロイメント時に参照するために、これらのファイルを Kubernetes シークレットに追加する必要があります。

   キュー・マネージャー用の鍵と証明書が存在する場合、それらは一例として次のような名前になります。

   - qmgr.crt
   - qmgr.key

   これらのファイルをインポートするには、以下のコマンドを実行します。

   ```
   oc create secret tls my-tls-migration --cert=qmgr.crt --key=qmgr.key
   ```

   Kubernetes では、一致する公開鍵と秘密鍵のインポート時に、この役立つユーティリティーが提供されます。 例えば、キュー・マネージャーのトラストストアに追加する証明書がさらにある場合、次のコマンドを実行します。

   ```
   oc create secret generic my-extra-tls-migration --from-file=comma_separated_list_of_files
   ```

   例えば、インポートするファイルが trust1.crt、trust2.crt と trust3.crt の場合、コマンドは次のようになります：

   ```
   oc create secret generic my-extra-tls-migration --from-file=trust1.crt,trust2.crt,trust3.crt
   ```

次のタスク

これで、Red Hat OpenShift で新しいキュー・マネージャーを作成する準備ができました。

OpenShift CP4I-SC2 CD Red Hat OpenShift での新しいキュー・マネージャーの作成

Red Hat OpenShift に単一インスタンス・キュー・マネージャーまたは複数インスタンス・キュー・マネージャーのいずれかをデプロイします。

始める前に

このタスクは、 キュー・マネージャー・リソースの作成および IBM MQ Operator を Red Hat OpenShift にインストールするがあることを前提としています。

このタスクについて

121 ページの『コンテナーで実行されている IBM MQ のためのターゲット HA アーキテクチャーの選択』で概説されているように、3 つの可能なデプロイメント・トポロジーがあります。 したがって、このトピックでは以下の 3 つの異なるテンプレートを提供します

- テンプレート 1: 単一インスタンス・キュー・マネージャーをデプロイします。
- テンプレート 2: 複数インスタンス・キュー・マネージャーをデプロイします。
- テンプレート 3: ネイティブ HA キュー・マネージャーをデプロイします。

重要 : 優先トポロジーに基づいて、3 つのテンプレートのいずれか 1 つのみを実行します。

手順

- **テンプレート 1: 単一インスタンス・キュー・マネージャーをデプロイします。**

  マイグレーションされたキュー・マネージャーは、 YAML ファイルを使用して Red Hat OpenShift にデプロイされます。 前の各トピックで使用された名前に基づいたサンプルを以下に示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1
spec:
  version: 9.4.0.0-r1
  license:
    accept: true
    license: L-BMSF-5YDSLR
    use: "Production"
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
  web:
    enabled: true
  queueManager:
    name: QM1
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

  実行した手順によっては、直前の YAML をカスタマイズする必要があります。 これを行うための手引きとして、この YAML の説明を次に示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1
```

  これは、Kubernetes のオブジェクト、タイプ、および名前を定義します。 カスタマイズが必要となるフィールドは name フィールドのみです。

```
 spec:
  version: 9.4.0.0-r1
  license:
    accept: true
```

```
    license: L-BMSF-5YDSLR
    use: "Production"
```

これは、デプロイメントのバージョン情報とライセンス情報に対応しています。 これをカスタマイズする必要がある場合は、139 ページの『mq.ibm.com/v1beta1 のライセンスのリファレンス』に記載されている情報を使用してください。

```
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
```

TLS を使用するように構成されているキュー・マネージャーの場合は、関連する証明書と鍵を参照する必要があります。 `secretName` フィールドは、Kubernetes シークレット (IBM MQ TLS リソースのインポートのセクション内で作成されたもの) を参照します。項目 (`tls.key` および `tls.crt`) のリストは、Kubernetes が `oc create secret tls` 構文の使用時に割り当てる標準名です。 トラストストアに追加する証明書がさらにある場合は、それらは同様の方法で追加できますが、各項目はインポート時に使用された対応する各ファイル名です。 例えば、トラストストア証明書を作成するために次のコードを使用できます。

```
oc create secret generic my-extra-tls-migration --from-file=trust1.crt,trust2.crt,trust3.crt
```

```
  pki:
    trust:
    - name: default
      secret:
        secretName: my-extra-tls-migration
        items:
          - trust1.crt
          - trust2.crt
          - trust3.crt
```

重要 : TLS が必要ない場合は、YAML の TLS セクションを削除します。

```
  web:
    enabled: true
```

これは、デプロイメントの Web コンソールを有効にします。

```
  queueManager:
    name: QM1
```

これは、キュー・マネージャーの名前を QM1 と定義します。 キュー・マネージャーは、お客様の要件 (例えば、元のキュー・マネージャー名) に基づいてカスタマイズします。

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

直前のコードは、IBM MQ 構成をインポートするセクションでインポートされたキュー・マネージャー構成をプルします。 別の名前を使用した場合は、`my-mqsc-migrated` と `backup.mqsc` を変更する必要があります。

サンプルの YAML では、Red Hat OpenShift 環境のデフォルトのストレージ・クラスが RWX または RWO ストレージ・クラスのいずれかとして定義されていることが前提となっていることに注意してください。 ご使用の環境内でデフォルトが定義されていない場合は、使用するストレージ・クラスを指定する必要があります。 これは、YAML を次のように拡張することで行えます。

```
  queueManager:
    name: QM1
```

```
    storage:
      defaultClass: my_storage_class
      queueManager:
        type: persistent-claim
```

強調表示されたテキストを、ご使用の環境に合わせてカスタマイズしたクラス属性を設定して追加します。 ご使用の環境内のストレージ・クラス名を検出するには、次のコマンドを実行します。

```
oc get storageclass
```

このコマンドによって返される出力例を次に示します。

```
NAME          PROVISIONER             RECLAIMPOLICY
aws-efs       openshift.org/aws-efs   Delete
gp2 (default) kubernetes.io/aws-ebs   Delete
```

以下のコードは、IBM MQ 構成 (IBM MQ 構成のインポートのセクションでインポートされたもの) を参照する方法を示しています。 別の名前を使用した場合は、`my-mqsc-migrated` と `backup.mqsc` を変更する必要があります。

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

単一インスタンス・キュー・マネージャーのデプロイが完了しました。 これにより、テンプレートが完了します。 これで、新しいコンテナー・デプロイメントを検証する準備ができました。

- **テンプレート 2: 複数インスタンス・キュー・マネージャーをデプロイします。**

  マイグレーションされたキュー・マネージャーは、 YAML ファイルを使用して Red Hat OpenShift にデプロイされます。 前の各セクションで使用された名前に基づいたサンプルを以下に示します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm1mi
spec:
  version: 9.4.0.0-r1
  license:
    accept: true
    license: L-BMSF-5YDSLR
    use: "Production"
  pki:
    keys:
    - name: default
      secret:
        secretName: my-tls-migration
        items:
          - tls.key
          - tls.crt
  web:
    enabled: true
  queueManager:
    name: QM1
    availability: MultiInstance
    storage:
      defaultClass: aws-efs
      persistedData:
        enabled: true
      queueManager:
        enabled: true
      recoveryLogs:
        enabled: true
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

ここでは、この YAML について説明します。 構成の大部分は、単一インスタンス・キュー・マネージャーをデプロイする方法と同じであるため、ここでは、キュー・マネージャーの可用性とストレージの側面についてのみ説明します。

```
queueManager:
    name: QM1
    availability: MultiInstance
```

これは、キュー・マネージャー名を QM1 として指定し、デプロイメントがデフォルトの単一インスタンスではなく MultiInstance になるように設定します。

```
    storage:
      defaultClass: aws-efs
      persistedData:
        enabled: true
      queueManager:
        enabled: true
      recoveryLogs:
        enabled: true
```

IBM MQ 複数インスタンス・キュー・マネージャーは、RWX ストレージに依存します。 デフォルトでは、キュー・マネージャーは単一インスタンス・モードでデプロイされるため、複数インスタンス・モードに変更する場合は追加のストレージ・オプションが必要になります。 直前の YAML サンプルでは、3 つのストレージ永続ボリュームと 1 つの永続ボリューム・クラスが定義されています。 この永続ボリューム・クラスは、RWX ストレージ・クラスでなければなりません。 ご使用の環境内の各ストレージ・クラス名が分からない場合は、次のコマンドを実行してそれらを検出することができます。

```
oc get storageclass
```

このコマンドによって返される出力例を次に示します。

```
NAME          PROVISIONER             RECLAIMPOLICY
aws-efs       openshift.org/aws-efs   Delete
gp2 (default) kubernetes.io/aws-ebs   Delete
```

以下のコードは、IBM MQ 構成 (IBM MQ 構成のインポートのセクションでインポートされたもの) を参照する方法を示しています。 別の名前を使用した場合は、my-mqsc-migrated と backup.mqsc を変更する必要があります。

```
    mqsc:
      - configMap:
          name: my-mqsc-migrated
          items:
            - backup.mqsc
```

複数インスタンス・キュー・マネージャーのデプロイが完了しました。 これにより、テンプレートが完了します。 これで、新しいコンテナー・デプロイメントを検証する準備ができました。

- **テンプレート 3: ネイティブ HA キュー・マネージャーをデプロイします。**

  ネイティブ HA キュー・マネージャーの作成の作業例については、 76 ページの『例: IBM MQ Operator を使用したネイティブ HA の構成』 を参照してください。

OpenShift CP4I-SC2 CD 新規コンテナー・デプロイメントの検証

IBM MQ が Red Hat OpenShift にデプロイされたので、IBM MQ サンプルを使用して環境を検査できます。

始める前に

このタスクでは、Red Hat OpenShift に新しいキュー・マネージャーを作成済みであることを前提としています。

重要 : このタスクでは、キュー・マネージャーで TLS が有効になっていないことを前提としています。

このタスクについて

このタスクでは、マイグレーション済みキュー・マネージャーのコンテナーの内部から IBM MQ サンプルを実行します。 ただし、別の環境から実行される独自のアプリケーションを使用することもできます。

以下の情報が必要になります。

- LDAP ユーザー名
- LDAP パスワード
- IBM MQ チャネル名
- キュー名

このサンプル・コードは、以下の設定を使用します。 この設定はご使用の環境によって異なることに注意してください。

- LDAP ユーザー名: mqapp
- LDAP パスワード: mqapp
- IBM MQ チャネル名: DEV.APP.SVRCONN
- キュー名: Q1

手順

1. 実行中の IBM MQ コンテナーに exec を実行します。

   以下のコマンドを使用します。

   ```
   oc exec -it qm1-ibm-mq-0 /bin/bash
   ```

   ここで `qm1-ibm-mq-0` は、123 ページの『Red Hat OpenShift での新しいキュー・マネージャーの作成』でデプロイしたポッドです。 別のデプロイメントを呼び出した場合は、この値をカスタマイズします。
2. メッセージを送信します。

   以下のコマンドを実行します。

   ```
   cd /opt/mqm/samp/bin
   export IBM MQSAMP_USER_ID=mqapp
   export IBM MQSERVER=DEV.APP.SVRCONN/TCP/'localhost(1414)'
   ./amqsputc Q1 QM1
   ```

   パスワードの入力を求めるプロンプトが表示されたら、メッセージを送信できます。
3. メッセージが正常に受信されたことを確認します。

   GET サンプルを実行します。

   ```
   ./amqsgetc Q1 QM1
   ```

タスクの結果

105 ページの『IBM MQ Operator へのマイグレーション』が完了しました。

次のタスク

より複雑なマイグレーション・シナリオについては、以下の情報を参考にしてください。

キューに入ったメッセージのマイグレーション
キューに入っている既存のメッセージをマイグレーションするには、新しいキュー・マネージャーの配置後にメッセージをエクスポートおよびインポートするために、2 つのシステム間での dmpmqmsg ユーティリティーの使用のトピックのガイドに従ってください。

Red Hat OpenShift 環境の外部からの IBM MQ への接続

デプロイされたキュー・マネージャーは、 Red Hat OpenShift 環境外の IBM MQ クライアントおよびキュー・マネージャーに公開することができます。 このプロセスは、 Red Hat OpenShift 環境に接続する IBM MQ のバージョンによって異なります。 84 ページの『Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成』を参照してください。

コンテナーでの IBM MQ の操作

コンテナーで実行されている IBM MQ キュー・マネージャーを操作または操作する必要がある場合、詳しくは以下のトピックを参照してください。

手順

- 129 ページの『IBM MQ Operator を使用した IBM MQ』.
- 136 ページの『ネイティブ HA キュー・マネージャーの状況の表示』.
- 138 ページの『ネイティブ HA キュー・マネージャー・インスタンスの手動での終了』.

OpenShift CP4I IBM MQ Operator を使用した IBM MQ

手順

- 129 ページの『IBM MQ Console クラスターにデプロイされた Red Hat OpenShift への接続』.
- 130 ページの『IBM MQ Operator 使用時のモニター』.
- 135 ページの『Red Hat OpenShift CLI を使用したキュー・マネージャー構成のバックアップおよびリストア』.

OpenShift CP4I IBM MQ Console クラスターにデプロイされた Red Hat OpenShift への接続

Red Hat OpenShift Container Platform クラスターにデプロイされているキュー・マネージャーの IBM MQ Console に接続する方法について説明します。

このタスクについて

IBM MQ Console URL は、 Red Hat OpenShift Web コンソールの QueueManager 詳細ページまたは IBM Cloud Pak for Integration Platform UI で見つけることができます。 あるいは、以下のコマンドを実行することにより、Red Hat OpenShiftCLI からそれを検出することもできます。

```
oc get queuemanager QueueManager Name -n namespace of your MQ deployment --output
jsonpath='{.status.adminUiUrl}'
```

IBM Cloud Pak for Integration ライセンスを使用している場合、IBM MQ Console は、ID およびアクセス管理に Keycloak を使用します。 IBM Cloud Pak for Integration 資料の Identity and Access management を参照してください。

IBM MQ ライセンスを使用している場合、IBM MQ Console は事前構成されていないため、自分で構成する必要があります。 詳しくは、ユーザーおよび役割の構成を参照してください。 例については、97 ページの『IBM MQ Operator を使用した基本レジストリーでの IBM MQ Console の構成』を参照してください。

関連タスク

84 ページの『Red Hat OpenShift クラスターの外部からキュー・マネージャーに接続するためのルートの構成』

Red Hat OpenShift クラスターの外部から IBM MQ キュー・マネージャーにアプリケーションを接続するには、 Red Hat OpenShift 経路が必要です。 IBM MQ キュー・マネージャーおよびクライアント・アプリケーションで TLS を有効にする必要があります。SNI は、TLS 1.2 以上のプロトコルが使用されている場合にのみ TLS プロトコルで使用できるためです。 Red Hat OpenShift Container Platform Router では、IBM MQ キュー・マネージャーへの要求のルーティングに SNI が使用されます。

OpenShift CP4I *IBM MQ Console* に対する権限の付与

IBM MQ Console の権限は、ライセンス使用状況に応じて異なる方法で管理されます。

このタスクについて

- IBM Cloud Pak for Integration ライセンスを使用している場合、IBM MQ Console は、ID およびアクセス管理に Keycloak を使用します。
  - IBM Cloud Pak for Integration 資料の Identity and Access management を参照してください。
  - 以前に旧バージョンの IBM MQ Operator で IAM を使用してユーザーを構成した場合は、IAM から Keycloak へのユーザーのマイグレーションを参照してください。
- IBM MQ ライセンスを使用している場合、IBM MQ Console は事前構成されていないため、自分で構成する必要があります。
  - ユーザーおよび役割について詳しくは、ユーザーおよび役割の構成を参照してください。
  - 簡単な例については、97 ページの『IBM MQ Operator を使用した基本レジストリーでの IBM MQ Console の構成』を参照してください。
  - あるいは、前述のように IBM Cloud Pak for Integration Operator をインストールして Keycloak を構成することもできます。

OpenShift CP4I IBM MQ Operator 使用時のモニター

IBM MQ Operator が管理するキュー・マネージャーは、Prometheus と互換性のあるメトリックを生成できます。

これらのメトリックは、Red Hat OpenShift Container Platform (OCP) モニター・スタックを使用して表示できます。 OCP の「**メトリック**」タブを開き、「**監視**」>「**メトリック**」をクリックします。 キュー・マネージャーのメトリックはデフォルトで有効になっていますが、**.spec.metrics.enabled** を `false` に設定することで無効にすることができます。

Prometheus は、データベースと規則を評価してメトリックを時系列で取得するエンジンです。 Prometheus は、IBM MQ コンテナーで公開されるメトリック・エンドポイントを利用して照会を行うことができます。 MQ システム・トピックから、モニタリングとアクティビティー・トレースを行うためのメトリックが生成されます。

OpenShift Container Platform には、Prometheus サーバーを使用する自己更新型のモニタリング・スタックが、事前インストールおよび事前構成されています。 ユーザー定義のプロジェクトをモニターするには、OpenShift Container Platform モニタリング・スタックを構成する必要があります。 詳しくは、Enabling monitoring for user-defined projects を参照してください。 IBM MQ Operator によって `ServiceMonitor` が作成されるのは、メトリックを有効にして `QueueManager` を作成するときです。 Prometheus オペレーターはこれをディスカバーできます。

OpenShift CP4I *IBM MQ Operator* の使用時にパブリッシュされるメトリック

キューマネージャーコンテナは、Red Hat OpenShift モニタリングと互換性のあるメトリクスを公開することができます。

メトリック	タイプ	説明
`ibmmq_qmgr_commit_total`	`counter`	コミット・カウント
`ibmmq_qmgr_cpu_load_fifteen_minute_average_percentage`	`gauge`	CPU 負荷 - 15 分間の平均
`ibmmq_qmgr_cpu_load_five_minute_average_percentage`	`gauge`	CPU 負荷 - 5 分間の平均

メトリック	タイプ	説明
ibmmq_qmgr_cpu_load_one_minute_average_percentage	gauge	CPU 負荷 - 1 分間の平均
ibmmq_qmgr_destructive_get_bytes_total	counter	破壊的 GET のインターバルにおける合計 - バイト数
ibmmq_qmgr_destructive_get_total	counter	破壊的 GET のインターバルにおける合計 - 数
ibmmq_qmgr_durable_subscription_alter_total	counter	永続サブスクリプション変更回数
ibmmq_qmgr_durable_subscription_create_total	counter	永続サブスクリプション作成回数
ibmmq_qmgr_durable_subscription_delete_total	counter	永続サブスクリプション削除回数
ibmmq_qmgr_durable_subscription_resume_total	counter	永続サブスクリプション再開回数
ibmmq_qmgr_errors_file_system_free_space_percentage	gauge	MQ エラー・ファイル・システム - 空き領域
ibmmq_qmgr_errors_file_system_in_use_bytes	gauge	MQ エラー・ファイル・システム - 使用中バイト数
ibmmq_qmgr_expired_message_total	counter	期限切れメッセージ数
ibmmq_qmgr_failed_browse_total	counter	失敗したブラウズの数
ibmmq_qmgr_failed_mqcb_total	counter	失敗した MQCB の数
ibmmq_qmgr_failed_mqclose_total	counter	失敗した MQCLOSE の数
ibmmq_qmgr_failed_mqconn_mqconnx_total	counter	失敗した MQCONN/MQCONNX の数
ibmmq_qmgr_failed_mqget_total	counter	失敗した MQGET - 数
ibmmq_qmgr_failed_mqinq_total	counter	失敗した MQINQ の数
ibmmq_qmgr_failed_mqopen_total	counter	失敗した MQOPEN の数
ibmmq_qmgr_failed_mqput1_total	counter	失敗した MQPUT1 の数

メトリック	タイプ	説明
ibmmq_qmgr_failed_mqput_total	counter	失敗した MQPUT の数
ibmmq_qmgr_failed_mqset_total	counter	失敗した MQSET の数
ibmmq_qmgr_failed_mqsubrq_total	counter	失敗した MQSUBRQ の数
ibmmq_qmgr_failed_subscription_create_alter_resume_total	counter	サブスクリプションの作成/変更/再開に失敗した回数
ibmmq_qmgr_failed_subscription_delete_total	counter	サブスクリプション削除に失敗した回数
ibmmq_qmgr_failed_topic_mqput_mqput1_total	counter	失敗したトピック MQPUT/MQPUT1 の数
ibmmq_qmgr_fdc_files	gauge	MQ FDC ファイル数
ibmmq_qmgr_log_file_system_in_use_bytes	gauge	ログ・ファイル・システム - 使用中バイト数
ibmmq_qmgr_log_file_system_max_bytes	gauge	ログ・ファイル・システム - 最大バイト数
ibmmq_qmgr_log_in_use_bytes	gauge	ログ - 使用中バイト数
ibmmq_qmgr_log_logical_written_bytes_total	counter	ログ - 書き込まれた論理バイト数
ibmmq_qmgr_log_max_bytes	gauge	ログ - 最大バイト数
ibmmq_qmgr_log_occupied_by_reusable_extents_bytes	gauge	ログ - 再使用可能エクステントが占有するバイト数
ibmmq_qmgr_log_physical_written_bytes_total	counter	ログ - 書き込まれた物理バイト数
ibmmq_qmgr_log_primary_space_in_use_percentage	gauge	ログ - 使用中の現行 1 次スペース
ibmmq_qmgr_log_required_for_media_recovery_bytes	gauge	ログ - メディア・リカバリーに必要なバイト数
ibmmq_qmgr_log_workload_primary_space_utilization_percentage	gauge	ログ - ワークロード 1 次スペースの使用状況

メトリック	タイプ	説明
ibmmq_qmgr_log_write_latency_seconds	gauge	ログ - 書き込み待ち時間
ibmmq_qmgr_log_write_size_bytes	gauge	ログ - 書き込みサイズ
ibmmq_qmgr_mqcb_total	counter	MQCB の数
ibmmq_qmgr_mqclose_total	counter	MQCLOSE の数
ibmmq_qmgr_mqconn_mqconnx_total	counter	MQCONN/MQCONNX の数
ibmmq_qmgr_mqctl_total	counter	MQCTL の数
ibmmq_qmgr_mqdisc_total	counter	MQDISC の数
ibmmq_qmgr_mqinq_total	counter	MQINQ の数
ibmmq_qmgr_mqopen_total	counter	MQOPEN の数
ibmmq_qmgr_mqput_mqput1_bytes_total	counter	MQPUT/MQPUT1 のバイト数のインターバルにおける合計
ibmmq_qmgr_mqput_mqput1_total	counter	MQPUT/MQPUT1 の数のインターバルにおける合計
ibmmq_qmgr_mqset_total	counter	MQSET の数
ibmmq_qmgr_mqstat_total	counter	MQSTAT の数
ibmmq_qmgr_mqsubrq_total	counter	MQSUBRQ の数
ibmmq_qmgr_non_durable_subscription_create_total	counter	非永続サブスクリプション作成回数
ibmmq_qmgr_non_durable_subscription_delete_total	counter	非永続サブスクリプション削除回数
ibmmq_qmgr_non_persistent_message_browse_bytes_total	counter	非持続メッセージのブラウズ - バイト数
ibmmq_qmgr_non_persistent_message_browse_total	counter	非持続メッセージのブラウズ - 数
ibmmq_qmgr_non_persistent_message_destructive_get_total	counter	非持続メッセージの破壊的 GET - 数

メトリック	タイプ	説明
ibmmq_qmgr_non_persistent_message_get_bytes_total	counter	取得された非持続メッセージ - バイト数
ibmmq_qmgr_non_persistent_message_mqput1_total	counter	非持続メッセージ MQPUT1 の数
ibmmq_qmgr_non_persistent_message_mqput_total	counter	非持続メッセージ MQPUT の数
ibmmq_qmgr_non_persistent_message_put_bytes_total	counter	書き込まれた非持続メッセージ - バイト数
ibmmq_qmgr_non_persistent_topic_mqput_mqput1_total	counter	非持続 - トピック MQPUT/MQPUT1 の数
ibmmq_qmgr_persistent_message_browse_bytes_total	counter	持続メッセージのブラウズ - バイト数
ibmmq_qmgr_persistent_message_browse_total	counter	持続メッセージのブラウズ - 数
ibmmq_qmgr_persistent_message_destructive_get_total	counter	持続メッセージの破壊的 GET - 数
ibmmq_qmgr_persistent_message_get_bytes_total	counter	取得された持続メッセージ - バイト数
ibmmq_qmgr_persistent_message_mqput1_total	counter	持続メッセージ MQPUT1 の数
ibmmq_qmgr_persistent_message_mqput_total	counter	持続メッセージ MQPUT の数
ibmmq_qmgr_persistent_message_put_bytes_total	counter	書き込まれた持続メッセージ - バイト数
ibmmq_qmgr_persistent_topic_mqput_mqput1_total	counter	持続 - トピック MQPUT/MQPUT1 の数
ibmmq_qmgr_published_to_subscribers_bytes_total	counter	サブスクライバーへのパブリッシュ - バイト数
ibmmq_qmgr_published_to_subscribers_message_total	counter	サブスクライバーへのパブリッシュ - メッセージ数
ibmmq_qmgr_purged_queue_total	counter	パージされたキュー数

メトリック	タイプ	説明
ibmmq_qmgr_queue_manager_file_system_free_space_percentage	gauge	キュー・マネージャー・ファイル・システム - 空き領域
ibmmq_qmgr_queue_manager_file_system_in_use_bytes	gauge	キュー・マネージャー・ファイル・システム - 使用中バイト数
ibmmq_qmgr_ram_free_percentage	gauge	RAM 空き領域パーセンテージ
ibmmq_qmgr_ram_usage_estimate_for_queue_manager_bytes	gauge	RAM 合計バイト数 - キュー・マネージャーの見積もり
ibmmq_qmgr_rollback_total	counter	ロールバック数
ibmmq_qmgr_system_cpu_time_estimate_for_queue_manager_percentage	gauge	システム CPU 時間 - キュー・マネージャーのパーセンテージ見積もり
ibmmq_qmgr_system_cpu_time_percentage	gauge	システム CPU 時間パーセンテージ
ibmmq_qmgr_topic_mqput_mqput1_total	counter	トピック MQPUT/MQPUT1 のインターバルにおける合計
ibmmq_qmgr_topic_put_bytes_total	counter	書き込まれたトピック・バイト数のインターバルにおける合計
ibmmq_qmgr_trace_file_system_free_space_percentage	gauge	MQ トレース・ファイル・システム - 空き領域
ibmmq_qmgr_trace_file_system_in_use_bytes	gauge	MQ トレース・ファイル・システム - 使用中バイト数
ibmmq_qmgr_user_cpu_time_estimate_for_queue_manager_percentage	gauge	ユーザー CPU 時間 - キュー・マネージャーのパーセンテージ見積もり
ibmmq_qmgr_user_cpu_time_percentage	gauge	ユーザー CPU 時間パーセンテージ

関連情報

システム・トピックにパブリッシュされるメトリック

OpenShift CP4I Red Hat OpenShift CLI を使用したキュー・マネージャー構成のバックアップおよびリストア

キュー・マネージャー構成をバックアップすると、キュー・マネージャー構成が失われた場合に、キュー・マネージャーをその定義から再構築することができます。 この手順を実行しても、キュー・マネージャーのログ・データはバックアップされません。 メッセージは特定の状況で出される一時的なものなので、履歴ログ・データは復元時の対象となりません。

始める前に

oc login を使用してクラスターにログインします。

手順

- キュー・マネージャー構成をバックアップします。

  dmpmqcfg コマンドを使用して、IBM MQ キュー・マネージャーの構成をダンプすることができます。

  a) キュー・マネージャーのポッドの名前を取得します。
  例えば、次のコマンドを実行します。ここで、*queue_manager_name* は QueueManager リソースの名前です。

  ```
  oc get pods --selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/
  instance=queue_manager_name
  ```

  b) 出力をローカル・マシン上のファイルに指定して、ポッド上で **dmpmqcfg** コマンドを実行します。

  dmpmqcfg がキュー・マネージャーの MQSC 構成を出力します。

  ```
  oc exec -it pod_name -- dmpmqcfg > backup.mqsc
  ```

- キュー・マネージャー構成を復元します。

  前のステップで概説したバックアップ手順に従っている場合は、キュー・マネージャー構成を含む backup.mqsc ファイルが必要になります。 このファイルを新しいキュー・マネージャーに適用することで、構成を復元できます。

  a) キュー・マネージャーのポッドの名前を取得します。
  例えば、次のコマンドを実行します。ここで、*queue_manager_name* は QueueManager リソースの名前です。

  ```
  oc get pods --selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/
  instance=queue_manager_name
  ```

  b) ポッド上で **runmqsc** コマンドを実行し、backup.mqsc ファイルの内容を読み込みます。

  ```
  oc exec -i pod_name -- runmqsc < backup.mqsc
  ```

MQ Adv. ネイティブ HA キュー・マネージャーの状況の表示

カスタムビルト・コンテナーの場合、 **dspmq** コマンドを使用してネイティブ HA インスタンスの状況を表示できます。

このタスクについて

dspmq コマンドを使用して、ノード上のキュー・マネージャー・インスタンスの操作状況を表示できます。返される情報は、インスタンスがアクティブとレプリカのどちらであるかに応じて異なります。 アクティブ・インスタンスで提供される情報が確定的なもので、レプリカ・ノードからの情報は古くなっている可能性があります。

以下のアクションを実行できます。

- 現行ノード上のキュー・マネージャー・インスタンスがアクティブかレプリカを表示します。
- 現行ノード上のインスタンスのネイティブ HA の運用状況を表示します。
- ネイティブ HA 構成に属する 3 つのインスタンスすべての運用状況を表示します。

以下の状況フィールドが、ネイティブ HA 構成状況の報告に使用されます。

ROLE
これは、現行インスタンス・ロールを指定します。これは、Active、Replica、または Unknown のいずれかです。

INSTANCE
このキュー・マネージャー・インスタンスの作成時に **crtmqm** コマンドの **-lr** オプションを使用してこのキュー・マネージャー・インスタンスに対して指定された名前。

INSYNC
必要な場合にインスタンスがアクティブ・インスタンスとしてテークオーバーできるかどうかを示します。

QUORUM
クォーラムの状況を *number_of_instances_in-sync*/*number_of_instances_configured* という形式でレポートします。

REPLADDR
キュー・マネージャー・インスタンスの複製アドレス。

CONNACTV
ノードがアクティブ・インスタンスに接続されているかどうかを示します。

BACKLOG
このインスタンスがどれだけ遅れているかを KB 数で示します。

CONNINST
指定されたインスタンスがこのインスタンスに接続されているかどうかを示します。

ALTDATE
この情報が最後に更新された日付を示します (更新されたことがない場合にはブランク)。

ALTTIME
この情報が最後に更新された時刻を示します (更新されたことがない場合にはブランク)。

手順

- キュー・マネージャー・インスタンスがアクティブ・インスタンスとして実行されているか、それともレプリカとして実行されているか判別するには、次のようにします

  ```
  dspmq -o status -m QMgrName
  ```

  BOB という名前のキュー・マネージャーのアクティブ・インスタンスからは、次の状況が報告されます

  ```
  QMNAME(BOB)                STATUS(Running)
  ```

  BOB という名前のキュー・マネージャーのレプリカ・インスタンスからは、次の状況が報告されます

  ```
  QMNAME(BOB)                STATUS(Replica)
  ```

  非アクティブ・インスタンスからは、次の状況が報告されます

  ```
  QMNAME(BOB)                STATUS(Ended Immediately)
  ```

- 現行ノード上のインスタンスのネイティブ HA 運用状況を判別するには、以下のようにします。

  ```
  dspmq -o nativeha -m QMgrName
  ```

  BOB という名前のキュー・マネージャーのアクティブ・インスタンスからは、次のような状況が報告されます

  ```
  QMNAME(BOB)              ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
  ```

  BOB という名前のキュー・マネージャーのレプリカ・インスタンスからは、次のような状況が報告されます

  ```
  QMNAME(BOB)              ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
  ```

BOB という名前のキュー・マネージャーの非アクティブ・インスタンスからは、次のような状況が報告されます

```
QMNAME(BOB)               ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
```

- ネイティブ HA 構成内のすべてのインスタンスのネイティブ HA 運用状況を判別するには、次のようにします

```
dspmq -o nativeha -x -m QMgrName
```

キュー・マネージャー BOB のアクティブ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます

```
QMNAME(BOB)            ROLE(Active) INSTANCE(inst1) INSYNC(Yes) QUORUM(3/3)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

キュー・マネージャー BOB のレプリカ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます。これは、レプリカの 1 つで処理が遅れていることを示しています

```
QMNAME(BOB)            ROLE(Replica) INSTANCE(inst2) INSYNC(Yes) QUORUM(2/3)
 INSTANCE(inst2) ROLE(Replica) REPLADDR(9.20.123.46) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst1) ROLE(Active)  REPLADDR(9.20.123.45) CONNACTV(Yes) INSYNC(Yes) BACKLOG(0)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
 INSTANCE(inst3) ROLE(Replica) REPLADDR(9.20.123.47) CONNACTV(Yes) INSYNC(No)  BACKLOG(435)
CONNINST(Yes) ALTDATE(2022-01-12) ALTTIME(12.03.44)
```

キュー・マネージャー BOB の非アクティブ・インスタンスを実行しているノード上でこのコマンドを発行すると、以下のような状況が表示されます

```
QMNAME(BOB)            ROLE(Unknown) INSTANCE(inst3) INSYNC(no) QUORUM(0/3)
 INSTANCE(inst1) ROLE(Unknown) REPLADDR(9.20.123.45) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst2) ROLE(Unknown) REPLADDR(9.20.123.46) CONNACTV(Unknown) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
 INSTANCE(inst3) ROLE(Unknown) REPLADDR(9.20.123.47) CONNACTV(No) INSYNC(Unknown)
BACKLOG(Unknown) CONNINST(No) ALTDATE() ALTTIME()
```

どのインスタンスがアクティブでどれがレプリカになるかをまだネゴシエーションしている間にコマンドを発行すると、次の状況が表示されます

```
QMNAME(BOB)              STATUS(Negotiating)
```

関連資料

dspmq (キュー・マネージャーの表示) コマンド

MQ Adv. ネイティブ HA キュー・マネージャー・インスタンスの手動での終了

endmqm コマンドを使用して、ネイティブ HA グループの一部であるアクティブ・キュー・マネージャーまたはレプリカ・キュー・マネージャーを終了できます。

手順

- キュー・マネージャーのアクティブ・インスタンスを終了するには、この資料の「構成」セクションの「ネイティブ HA キュー・マネージャーの終了」を参照してください。

OpenShift CP4I コンテナー内の IBM MQ の参照情報

IBM MQ は、Red Hat OpenShift コンテナー・プラットフォームとのネイティブ統合を提供する、Kubernetes オペレーターを提供します。

OpenShift CP4I IBM MQ Operator の API リファレンス

IBM MQ は、Red Hat OpenShift コンテナー・プラットフォームとのネイティブ統合を提供する、Kubernetes オペレーターを提供します。

OpenShift CP4I mq.ibm.com/v1beta1 の API リファレンス

v1beta1 API を使用して、QueueManager リソースを作成および管理できます。

OpenShift CP4I CP4I-SC2 CD *mq.ibm.com/v1beta1 のライセンスのリファレンス*

現行バージョンのライセンス

spec.license.license フィールドには、同意しようとしているライセンスのライセンス ID が含まれていなければなりません。 有効な値は以下のとおりです。

spec.license.license の値	**spec.license.use の値**	**ライセンス情報**	**利用可能な IBM MQ のバージョン**
L-JTPV-KYG8TF	Production または NonProduction	IBM Cloud Pak for Integration 16.1.0	9.4.0
L-BMSF-5YDSLR	Production または NonProduction	IBM Cloud Pak for Integration 限定版 16.1.0	9.4.0
L-EHXT-MQCRN9	Production	IBM MQ Advanced 9.4	9.4.0
L-CLXQ-ADXTK3	Development	IBM MQ Advanced for Developers (保証適用外) 9.4	9.4.0

ライセンスのバージョン を指定しますが、これは必ずしも IBM MQ のバージョンとは同じでないことに注意してください。

古いバージョンのライセンス

IBM MQ 9.3 資料の 旧ライセンス・バージョン を参照してください。

OpenShift CP4I *QueueManager (mq.ibm.com/v1beta1) の API リファレンス*

QueueManager

QueueManager は、アプリケーションにキューイングとパブリッシュ/サブスクライブのサービスを提供する IBM MQ サーバーです。 IBM MQ 資料: https://ibm.biz/BdPZqj。 ライセンス参照: https://ibm.biz/BdPZfq.。

フィールド	説明
apiVersion 文字列	APIVersion は、このオブジェクトの表記のスキーマのバージョンを定義します。 サーバーは、認識されたスキーマを最新の内部値に変換する必要があります。 認識されない値は拒否されることがあります。 詳細情報: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources。
kind 文字列	kind は、このオブジェクトが表している REST リソースを表す文字列の値です。 サーバーは、クライアントが要求を送信するエンドポイントからこれを推測することがあります。 更新することはできません。 キャメル・ケースの値です。 詳細情報: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds。
metadata	
specQueueManagerSpec	QueueManager について必要とする状態。
statusQueueManagerStatus	QueueManager について観測された状態。

.spec

QueueManager について必要とする状態。

以下の中に含まれます:

- 139 ページの『QueueManager』

フィールド	説明
affinity	標準的な Kubernete アフィニティー・ルール。 詳しくは、https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.17/#affinity-v1-core を参照してください。
annotations Annotations	annotations フィールドは、ポッド・アノテーションのパススルーの役目を果たします。 ユーザーはこのフィールドにアノテーションを追加することによって、ポッドにアノテーションを適用できます。 ここでアノテーションを指定すると、デフォルトのアノテーションが上書きされます。 MQ Operator 1.3.0 以上が必要です。
imagePullSecrets LocalObjectReference 配列	(オプション) この QueueManager で使用するイメージをプルするために使用する、同じ名前空間にあるシークレットへの参照のリスト。 指定すると、それらのシークレットがプル実行プログラムに渡されて使用されます。 例えば、Docker の場合は、DockerConfig タイプのシークレットだけが適用されます。 詳しくは、https://kubernetes.io/docs/concepts/containers/images#specifying-imagepullsecrets-on-a-pod を参照してください。
labels Labels	labels フィールドは、ポッド・ラベルのパススルーの役目を果たします。 ユーザーはこのフィールドにラベルを追加することによって、ポッドにラベルを適用できます。 ここでラベルを指定すると、デフォルトのラベルが上書きされます。 MQ Operator 1.3.0 以上が必要です。
license License	ライセンスの受け入れを制御する設定、および使用するライセンス・メトリック。
pki PKI	Transport Layer Security (TLS) または MQ Advanced Message Security (AMS) で使用する鍵と証明書を定義するための Public Key Infrastructure の設定。
queueManager QueueManagerConfig	キュー・マネージャーのコンテナーおよび基礎キュー・マネージャーの設定。
securityContext SecurityContext	キュー・マネージャー・ポッドの securityContext に追加するセキュリティー設定です。

フィールド	説明
telemetry テレメトリー	Open Telemetry 構成の設定。 MQ Operator 2.2.0 以上が必要です。
template テンプレート	Kubernetes リソースの拡張テンプレート。 このテンプレートは、基礎の Kubernetes リソース (StatefulSet、Pod、Service など) を IBM MQ で生成する方法をユーザーがオーバーライドすることを可能にします。 これは上級者専用です。誤って使用すると MQ の正常な動作が阻害される可能性があります。 QueueManager リソースの他の場所で指定された値は、このテンプレートの設定によってオーバーライドされます。
terminationGracePeriodSeconds 整数	(オプション) ポットの正常な終了にかかる時間 (秒単位)。 値は負以外の整数でなければなりません。 ゼロの値は、ただちに削除することを意味します。 このキュー・マネージャーの終了の目標時間を達成するために、アプリケーションの切断のフェーズが押し進められます。 必要な場合は、キュー・マネージャーの重要なメンテナンス・タスクが中断されます。 デフォルトは 30 秒です。
tracing TracingConfig	Cloud Pak for Integration Operations Dashboard とのトレースの統合のための設定。
version 文字列	使用する MQ のバージョンを制御する設定 (必須)。 例えば、9.1.5.0-r2 は、コンテナー・イメージの 2 番目のリビジョンを使用する MQ バージョン 9.1.5.0 を指します。 ベース・イメージのフィックスなどのように、コンテナー固有のフィックスが、リビジョンの中で適用されることがよくあります。
web WebServerConfig	MQ Web サーバーの設定。

.spec.annotations

annotations フィールドは、ポッド・アノテーションのパススルーの役目を果たします。 ユーザーはこのフィールドにアノテーションを追加することによって、ポッドにアノテーションを適用できます。 ここでアノテーションを指定すると、デフォルトのアノテーションが上書きされます。 MQ Operator 1.3.0 以上が必要です。

以下の中に含まれます:

- 140 ページの『.spec』

.spec.imagePullSecrets

LocalObjectReference に、同じ名前空間の内部で参照されているオブジェクトを見つけることができる十分な情報が含まれています。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
name 文字列	参照の名前。 詳細情報: https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#names TODO: その他の便利なフィールドを追加してください。 apiVersion、kind、uid など。

.spec.labels

labels フィールドは、ポッド・ラベルのパススルーの役目を果たします。 ユーザーはこのフィールドにラベルを追加することによって、ポッドにラベルを適用できます。 ここでラベルを指定すると、デフォルトのラベルが上書きされます。 MQ Operator 1.3.0 以上が必要です。

以下の中に含まれます:

- 140 ページの『.spec』

.spec.license

ライセンスの受け入れを制御する設定、および使用するライセンス・メトリック。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
accept ブール値	このソフトウェアに関連付けられているライセンスを受け入れるかどうか (必須)。
license 文字列	受け入れるライセンスの ID。 これは、使用する MQ のバージョンの正確なライセンス ID である必要があります。 有効な値については、「https://ibm.biz/BdPZfq」を参照してください。
metric 文字列	使用するライセンス・メトリックを指定する設定。 例えば、ProcessorValueUnit、VirtualProcessorCore、ManagedVirtualServer などです。 MQ ライセンスを使用する場合のデフォルトは ProcessorValueUnit、Cloud Pak for Integration ライセンスを使用する場合のデフォルトは VirtualProcessorCore です。
use 文字列	複数の使用方法をサポートするライセンスの場合に、ソフトウェアの使用方法を制御する設定。 有効な値については、「https://ibm.biz/BdPZfq」を参照してください。

.spec.pki

Transport Layer Security (TLS) または MQ Advanced Message Security (AMS) で使用する鍵と証明書を定義するための Public Key Infrastructure の設定。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
keys PKISource 配列	キュー・マネージャーの鍵リポジトリーに追加する秘密鍵です。
trust PKISource 配列	キュー・マネージャーの鍵リポジトリーに追加する証明書です。

.spec.pki.keys

PKISource は、鍵や証明書などの Public Key Infrastructure 情報のソースを定義します。

以下の中に含まれます:

- 142 ページの『.spec.pki』

フィールド	説明
name 文字列	name は鍵や証明書のラベルとして使用されます。 小文字の英数字の文字列である必要があります。
secret Secret	Kubernetes シークレットを使用して鍵を渡します。

.spec.pki.keys.secret

Kubernetes シークレットを使用して鍵を渡します。

以下の中に含まれます:

- 142 ページの『.spec.pki.keys』

フィールド	説明
items 配列	キュー・マネージャーのコンテナーに追加する必要がある Kubernetes シークレットの内部にある鍵。
secretName 文字列	Kubernetes シークレットの名前。

.spec.pki.trust

PKISource は、鍵や証明書などの Public Key Infrastructure 情報のソースを定義します。

以下の中に含まれます:

- 142 ページの『.spec.pki』

フィールド	説明
name 文字列	name は鍵や証明書のラベルとして使用されます。 小文字の英数字の文字列である必要があります。
secret Secret	Kubernetes シークレットを使用して鍵を渡します。

.spec.pki.trust.secret

Kubernetes シークレットを使用して鍵を渡します。

以下の中に含まれます:

- 143 ページの『.spec.pki.trust』

フィールド	説明
items 配列	キュー・マネージャーのコンテナーに追加する必要がある Kubernetes シークレットの内部にある鍵。
secretName 文字列	Kubernetes シークレットの名前。

.spec.queueManager

キュー・マネージャーのコンテナーおよび基礎キュー・マネージャーの設定。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
availability Availability	キュー・マネージャーの可用性の設定 (アクティブとスタンバイのペアやネイティブの高可用性を使用するかどうかなど)。
debug ブール値	コンテナー固有のコードからのデバッグ・メッセージをコンテナー・ログに記録するかどうか。 デフォルトは false です。
image 文字列	使用するコンテナー・イメージ。
imagePullPolicy 文字列	指定されたイメージのプルを Kubelet が試行するタイミングを制御する設定。 デフォルトは IfNotPresent です。
ini INISource 配列	キュー・マネージャーに INI を提供するための設定。 MQ Operator 1.1.0 以上が必要です。
livenessProbe QueueManagerLivenessProbe	Liveness プローブを制御する設定。

フィールド	説明
logFormat 文字列	このコンテナーで使用するログの形式。 JSON 形式のコンテナー・ログには、JSON を使用します。 テキスト形式のメッセージには、Basic を使用します。 デフォルトは Basic です。
metrics QueueManagerMetrics	Prometheus スタイルのメトリックの設定。
mqsc MQSCSource 配列	キュー・マネージャーに MQSC を提供するための設定。 MQ Operator 1.1.0 以上が必要です。
name 文字列	基礎 MQ キュー・マネージャーの名前 (metadata.name と異なる場合)。 名前の Kubernetes 規則に準拠しないキュー・マネージャー名 (例えば、大文字を含む名前) が必要な場合は、このフィールドを使用します。
readinessProbe QueueManagerReadinessProbe	Readiness プローブを制御する設定。
recoveryLogs RecoveryLogs	MQ リカバリー・ログの設定。 MQ Operator 2.4.0 以上が必要です。
resources Resources	リソース要件を制御する設定。
route Route	キュー・マネージャー・ルートの設定。 MQ Operator 1.4.0 以上が必要です。
startupProbe StartupProbe	始動プローブを制御する設定。 MultiInstance デプロイメントと NativeHA デプロイメントにのみ適用されます。 MQ Operator 1.5.0 以上が必要です。
storage QueueManagerStorage	キュー・マネージャーが永続ボリュームおよびストレージ・クラスを使用することを制御するストレージ設定です。

.spec.queueManager.availability

キュー・マネージャーの可用性の設定 (アクティブとスタンバイのペアやネイティブの高可用性を使用するかどうかなど)。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
tls Tls	NativeHA レプリカ間のセキュア通信を構成するためのオプションの TLS 設定。 MQ Operator 1.5.0 以上が必要です。
type 文字列	使用する可用性のタイプ。 Kubernetes が (一部の状況で) 自動的に再始動する単一ポッドには、SingleInstance を使用します。 MultiInstance は、ポッドのペア (1 つは active キュー・マネージャー、もう 1 つはスタンバイ) に使用します。 ネイティブの高可用性の複製には NativeHA を使用します (MQ Operator 1.5.0 以上が必要です)。 デフォルトは SingleInstance です。 詳しくは、http://ibm.biz/BdqAQa を参照してください。
updateStrategy 文字列	MultiInstance および NativeHA キュー・マネージャーに使用する更新方針。 RollingUpdate を使用して、キュー・マネージャーの構成が変更されるたびに自動ローリング更新を有効にします。 自動ローリング更新を無効にするには、OnDelete を使用します。キュー・マネージャーの変更は、ポッドが削除された場合にのみ適用されます (外部要因によってトリガーされたポッド削除も含む)。 デフォルトは RollingUpdate です。 MQ Operator 1.6.0 以上が必要です。

.spec.queueManager.availability.tls

NativeHA レプリカ間のセキュア通信を構成するためのオプションの TLS 設定。 MQ Operator 1.5.0 以上が必要です。

以下の中に含まれます:

- 144 ページの『.spec.queueManager.availability』

フィールド	説明
cipherSpec 文字列	NativeHA TLS 用の CipherSpec の名前。
secretName 文字列	Kubernetes シークレットの名前。

.spec.queueManager.ini

INI 構成ファイルのソース。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
configMap ConfigMapINISource	configMap は、INI 情報が入っている Kubernetes ConfigMap を表します。
secret SecretINISource	secret は、INI 情報が入っている Kubernetes シークレットを表します。

.spec.queueManager.ini.configMap

configMap は、INI 情報が入っている Kubernetes ConfigMap を表します。

以下の中に含まれます:

- 145 ページの『.spec.queueManager.ini』

フィールド	説明
items 配列	適用する必要がある、Kubernetes ソース内部の鍵。
name 文字列	Kubernetes ソースの名前。

.spec.queueManager.ini.secret

secret は、INI 情報が入っている Kubernetes シークレットを表します。

以下の中に含まれます:

- 145 ページの『.spec.queueManager.ini』

フィールド	説明
items 配列	適用する必要がある、Kubernetes ソース内部の鍵。
name 文字列	Kubernetes ソースの名前。

.spec.queueManager.livenessProbe

Liveness プローブを制御する設定。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してからプローブが開始されるまでの秒数。 SingleInstance の場合、デフォルトは 90 秒です。 MultiInstance デプロイメントと NativeHA デプロイメントの場合、デフォルトは 0 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 10 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 5 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.queueManager.metrics

Prometheus スタイルのメトリックの設定。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
enabled ブール値	Prometheus 互換のメトリックのエンドポイントを有効にするかどうか。 デフォルトは true です。

.spec.queueManager.mqsc

MQSC 構成ファイルのソース。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
configMap ConfigMapMQSCSource	configMap は、MQSC 情報が入っている Kubernetes ConfigMap を表します。
secret SecretMQSCSource	secret は、MQSC 情報が入っている Kubernetes シークレットを表します。

.spec.queueManager.mqsc.configMap

configMap は、MQSC 情報が入っている Kubernetes ConfigMap を表します。

以下の中に含まれます:

- 146 ページの『.spec.queueManager.mqsc』

フィールド	説明
items 配列	適用する必要がある、Kubernetes ソース内部の鍵。
name 文字列	Kubernetes ソースの名前。

.spec.queueManager.mqsc.secret

secret は、MQSC 情報が入っている Kubernetes シークレットを表します。

以下の中に含まれます:

- 146 ページの『.spec.queueManager.mqsc』

フィールド	説明
items 配列	適用する必要がある、Kubernetes ソース内部の鍵。
name 文字列	Kubernetes ソースの名前。

.spec.queueManager.readinessProbe

Readiness プローブを制御する設定。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してからプローブが開始されるまでの秒数。 SingleInstance の場合、デフォルトは 10 秒です。 MultiInstance デプロイメントと NativeHA デプロイメントの場合、デフォルトは 0 です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 5 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 3 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.queueManager.recoveryLogs

MQ リカバリー・ログの設定。 MQ Operator 2.4.0 以上が必要です。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
logFilePages 整数	回復ログ・データは一連のファイルに保持されます。 ログ・ファイル・サイズは、4 KB ページ単位で指定します。

.spec.queueManager.resources

リソース要件を制御する設定。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
limits Limits	CPU とメモリーの設定。

フィールド	説明
`requests` Requests	CPU とメモリーの設定。

.spec.queueManager.resources.limits

CPU とメモリーの設定。

以下の中に含まれます:

- 147 ページの『.spec.queueManager.resources』

フィールド	説明
`cpu`	
`memory`	

.spec.queueManager.resources.requests

CPU とメモリーの設定。

以下の中に含まれます:

- 147 ページの『.spec.queueManager.resources』

フィールド	説明
`cpu`	
`memory`	

.spec.queueManager.route

キュー・マネージャー・ルートの設定。 MQ Operator 1.4.0 以上が必要です。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
`enabled` ブール値	ルートを有効にするかどうか。 デフォルトは true です。

.spec.queueManager.startupProbe

始動プローブを制御する設定。 MultiInstance デプロイメントと NativeHA デプロイメントにのみ適用されます。 MQ Operator 1.5.0 以上が必要です。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
`failureThreshold` 整数	この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 24 です。
`initialDelaySeconds` 整数	コンテナーが始動してからプローブが開始されるまでの秒数。 デフォルトは 0 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
`periodSeconds` 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 5 秒です。

フィールド	説明
successThreshold 整数	この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 5 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.queueManager.storage

キュー・マネージャーが永続ボリュームおよびストレージ・クラスを使用することを制御するストレージ設定です。

以下の中に含まれます:

- 143 ページの『.spec.queueManager』

フィールド	説明
allowVolumeExpansion ブール値	ボリュームの拡張を許可するかどうか。
defaultClass 文字列	このキュー・マネージャーのすべての永続ボリュームにデフォルトで適用するストレージ・クラス。 個々の永続ボリュームで独自のストレージ・クラスを定義すると、このデフォルトのストレージ・クラス設定がオーバーライドされます。 type of availability が SingleInstance または NativeHA の場合は、ストレージ・クラスのタイプを ReadWriteOnce か ReadWriteMany にできます。 type of availability が MultiInstance の場合は、ストレージ・クラスのタイプを ReadWriteMany にしなければなりません。
defaultDeleteClaim ブール値	キュー・マネージャーの削除時にすべてのボリュームを削除するかどうか。 個々の永続ボリュームで独自の deleteClaim 値を定義すると、この defaultDeleteClaim 設定がオーバーライドされます。 デフォルトは false です。
persistedData QueueManagerOptionalVolume	構成、キュー、メッセージなどの MQ の永続データに使用する永続ボリュームの詳細。 マルチインスタンスのキュー・マネージャーを使用する場合は必須です。
queueManager QueueManagerVolume	あらゆるデータに使用するデフォルトの永続ボリューム (通常は、/var/mqm 下に置かれます)。 他のボリュームを指定しない場合は、すべての永続データとリカバリー・ログがここに格納されます。
recoveryLogs QueueManagerOptionalVolume	MQ リカバリー・ログ用の永続ボリュームの詳細。 マルチインスタンスのキュー・マネージャーを使用する場合は必須です。
scratch スクラッチ	キュー・マネージャーの Scratch 一時ボリュームの設定。 このボリュームは、「/run」フォルダーとしてコンテナーにマウントされます。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ適用されます。 MQ Operator 3.0.0 以上が必要です。
tmp 一時	キュー・マネージャーの一時一時ボリュームの設定。 このボリュームは、「/tmp」フォルダーとしてコンテナーにマウントされます。 runmqras コマンドによって作成された zip ファイルなどの診断データ・ファイルが、このボリュームに作成されます。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ適用されます。 MQ Operator 3.0.0 以上が必要です。

.spec.queueManager.storage.persistedData

構成、キュー、メッセージなどの MQ の永続データに使用する永続ボリュームの詳細。 マルチインスタンスのキュー・マネージャーを使用する場合は必須です。

以下の中に含まれます:

- 149 ページの『.spec.queueManager.storage』

フィールド	説明
class 文字列	このボリュームに使用するストレージ・クラス。 type が persistent-claim である場合にのみ有効です。 type of availability が SingleInstance または NativeHA の場合は、ストレージ・クラスのタイプを ReadWriteOnce か ReadWriteMany にできます。 type of availability が MultiInstance の場合は、ストレージ・クラスのタイプを ReadWriteMany にしなければなりません。
deleteClaim ブール値	キュー・マネージャーの削除時にこのボリュームを削除するかどうか。
enabled ブール値	このボリュームを別個のボリュームとして使用可能にするかどうか、あるいは、デフォルトの queueManager ボリュームに置くかどうか。 デフォルトは false です。
size 文字列	Kubernetes に渡す PersistentVolume のサイズ (SI 単位を含む)。 type が persistent-claim である場合にのみ有効です。 例: 2Gi。 デフォルトは 2Gi です。
sizeLimit 文字列	ephemeral ボリュームを使用する場合のサイズの制限。 ファイルは引き続き一時ディレクトリーに書き込まれるので、このオプションを使用してサイズを制限できます。 type が ephemeral で、ルート・ファイル・システムが読み取り専用に設定されている場合にのみ有効です。 MQ Operator 3.0.0 以上が必要です。
type 文字列	使用するボリュームのタイプ。 非永続ストレージを使用する場合は ephemeral を選択し、永続ボリュームを使用する場合は persistent-claim を選択します。 デフォルトは persistent-claim です。

.spec.queueManager.storage.queueManager

あらゆるデータに使用するデフォルトの永続ボリューム (通常は、/var/mqm 下に置かれます)。 他のボリュームを指定しない場合は、すべての永続データとリカバリー・ログがここに格納されます。

以下の中に含まれます:

- 149 ページの『.spec.queueManager.storage』

フィールド	説明
class 文字列	このボリュームに使用するストレージ・クラス。 type が persistent-claim である場合にのみ有効です。 type of availability が SingleInstance または NativeHA の場合は、ストレージ・クラスのタイプを ReadWriteOnce か ReadWriteMany にできます。 type of availability が MultiInstance の場合は、ストレージ・クラスのタイプを ReadWriteMany にしなければなりません。
deleteClaim ブール値	キュー・マネージャーの削除時にこのボリュームを削除するかどうか。
size 文字列	Kubernetes に渡す PersistentVolume のサイズ (SI 単位を含む)。 type が persistent-claim である場合にのみ有効です。 例: 2Gi。 デフォルトは 2Gi です。

フィールド	説明
sizeLimit 文字列	ephemeral ボリュームを使用する場合のサイズの制限。 ファイルは引き続き一時ディレクトリーに書き込まれるので、このオプションを使用してサイズを制限できます。 type が ephemeral で、ルート・ファイル・システムが読み取り専用に設定されている場合にのみ有効です。 MQ Operator 3.0.0 以上が必要です。
type 文字列	使用するボリュームのタイプ。 非永続ストレージを使用する場合は ephemeral を選択し、永続ボリュームを使用する場合は persistent-claim を選択します。 デフォルトは persistent-claim です。

.spec.queueManager.storage.recoveryLogs

MQ リカバリー・ログ用の永続ボリュームの詳細。 マルチインスタンスのキュー・マネージャーを使用する場合は必須です。

以下の中に含まれます:

- 149 ページの『.spec.queueManager.storage』

フィールド	説明
class 文字列	このボリュームに使用するストレージ・クラス。 type が persistent-claim である場合にのみ有効です。 type of availability が SingleInstance または NativeHA の場合は、ストレージ・クラスのタイプを ReadWriteOnce か ReadWriteMany にできます。 type of availability が MultiInstance の場合は、ストレージ・クラスのタイプを ReadWriteMany にしなければなりません。
deleteClaim ブール値	キュー・マネージャーの削除時にこのボリュームを削除するかどうか。
enabled ブール値	このボリュームを別個のボリュームとして使用可能にするかどうか、あるいは、デフォルトの queueManager ボリュームに置くかどうか。 デフォルトは false です。
size 文字列	Kubernetes に渡す PersistentVolume のサイズ (SI 単位を含む)。 type が persistent-claim である場合にのみ有効です。 例: 2Gi。 デフォルトは 2Gi です。
sizeLimit 文字列	ephemeral ボリュームを使用する場合のサイズの制限。 ファイルは引き続き一時ディレクトリーに書き込まれるので、このオプションを使用してサイズを制限できます。 type が ephemeral で、ルート・ファイル・システムが読み取り専用に設定されている場合にのみ有効です。 MQ Operator 3.0.0 以上が必要です。
type 文字列	使用するボリュームのタイプ。 非永続ストレージを使用する場合は ephemeral を選択し、永続ボリュームを使用する場合は persistent-claim を選択します。 デフォルトは persistent-claim です。

.spec.queueManager.storage.scratch

キュー・マネージャーの Scratch 一時ボリュームの設定。 このボリュームは、「/run」フォルダーとしてコンテナーにマウントされます。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ適用されます。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 149 ページの『.spec.queueManager.storage』

フィールド	説明
sizeLimit 文字列	一時ボリュームのサイズ制限 (SI 単位を含む)。 例えば、 2Gi などです。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ有効です。 MQ Operator 3.0.0 以上が必要です。

.spec.queueManager.storage.tmp

キュー・マネージャーの一時一時ボリュームの設定。 このボリュームは、「/tmp」フォルダーとしてコンテナーにマウントされます。 runmqras コマンドによって作成された zip ファイルなどの診断データ・ファイルが、このボリュームに作成されます。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ適用されます。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 149 ページの『.spec.queueManager.storage』

フィールド	説明
sizeLimit 文字列	一時ボリュームのサイズ制限 (SI 単位を含む)。 例えば、 2Gi などです。 ルート・ファイル・システムが読み取り専用に設定されている場合にのみ有効です。 MQ Operator 3.0.0 以上が必要です。

.spec.securityContext

キュー・マネージャー・ポッドの securityContext に追加するセキュリティー設定です。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
fsGroup 整数	ポッド内のすべてのコンテナーに適用される特殊な補助グループ。 いくつかのボリューム・タイプでは、 Kubelet がそのボリュームの所有権をポッドによって所有されるように変更することができます : 1。 所有 GID は、 FSGroup 2 になります。 setgid ビットが設定されます (ボリューム内に作成された新規ファイルは、 FSGroup が所有します) 3 です。 許可ビットは OR で rw-rw ---- 設定されていない場合、 Kubelet はボリュームの所有権と許可を変更しません。
initVolumeAsRoot ブール値	これは、PersistentVolume を初期化するコンテナーで使用されるセキュリティー・コンテキストに影響を与えます。 新しくプロビジョンしたボリュームには root ユーザーを使用してアクセスしなければならないストレージ・プロバイダーを使用する場合は、true に設定します。 これを true に設定すると、使用できるセキュリティー・コンテキスト制約 (SCC) オブジェクトが影響を受けます。 root ユーザーを許可する SCC を使用する権限を持っていないと、キュー・マネージャーの始動に失敗する可能性があります。 デフォルトは false です。 詳しくは、https://docs.openshift.com/container-platform/latest/authentication/managing-security-context-constraints.html を参照してください。
readOnlyRootFilesystem ブール値	キュー・マネージャーの読み取り専用ルート・ファイル・システム設定を有効にするかどうか。 デフォルトは false です。 MQ Operator 3.0.0 以上が必要です。
supplementalGroups 配列	コンテナーの 1 次 GID に加えて、最初のプロセスに適用されるグループのリストは、各コンテナーで実行されます。 指定しない場合は、コンテナーにグループは追加されません。

.spec.telemetry

Open Telemetry 構成の設定。 MQ Operator 2.2.0 以上が必要です。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
tracing トレース	Open Telemetry トレースの設定。

.spec.telemetry.tracing

Open Telemetry トレースの設定。

以下の中に含まれます:

- 152 ページの『.spec.telemetry』

フィールド	説明
instana インスタナ	Instana トレースの設定。

.spec.telemetry.tracing.instana

Instana トレースの設定。

以下の中に含まれます:

- 153 ページの『.spec.telemetry.tracing』

フィールド	説明
agentHost 文字列	トレース・データの送信先の Instana エージェントのホスト名。 これにプロトコルを含めることはできません。
enabled ブール値	Instana トレースを有効にするかどうか。 デフォルトは false です。
protocol 文字列	Instana エージェントとの通信で使用されるプロトコル。 http および https がサポートされています。

.spec.template

Kubernetes リソースの拡張テンプレート。 このテンプレートは、基礎の Kubernetes リソース (StatefulSet、Pod、Service など) を IBM MQ で生成する方法をユーザーがオーバーライドすることを可能にします。 これは上級者専用です。誤って使用すると MQ の正常な動作が阻害される可能性があります。 QueueManager リソースの他の場所で指定された値は、このテンプレートの設定によってオーバーライドされます。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
pod	ポッドに使用するテンプレートのオーバーライド。 https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.17/#podspec-v1-core を参照してください。

.spec.tracing

Cloud Pak for Integration Operations Dashboard とのトレースの統合のための設定。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
agent TracingAgent	Cloud Pak for Integration でのみ、オプションの Tracing Agent の設定を構成できます。
collector TracingCollector	Cloud Pak for Integration でのみ、オプションの Tracing Collector の設定を構成できます。
enabled ブール値	Cloud Pak for Integration Operations Dashboard とのトレースの統合を有効にするかどうか。 デフォルトは false です。
namespace 文字列	Cloud Pak for Integration Operations Dashboard がインストールされている名前空間。

.spec.tracing.agent

Cloud Pak for Integration でのみ、オプションの Tracing Agent の設定を構成できます。

以下の中に含まれます:

- 153 ページの『.spec.tracing』

フィールド	説明
image 文字列	使用するコンテナー・イメージ。
imagePullPolicy 文字列	指定されたイメージのプルを Kubelet が試行するタイミングを制御する設定。 デフォルトは IfNotPresent です。
livenessProbe TracingProbe	Liveness プローブを制御する設定。
readinessProbe TracingProbe	Readiness プローブを制御する設定。

.spec.tracing.agent.livenessProbe

Liveness プローブを制御する設定。

以下の中に含まれます:

- 154 ページの『.spec.tracing.agent』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してから Liveness プローブが開始されるまでの秒数。 デフォルトは 10 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 10 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 2 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.tracing.agent.readinessProbe

Readiness プローブを制御する設定。

以下の中に含まれます:

- 154 ページの『.spec.tracing.agent』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してから Liveness プローブが開始されるまでの秒数。 デフォルトは 10 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 10 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 2 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.tracing.collector

Cloud Pak for Integration でのみ、オプションの Tracing Collector の設定を構成できます。

以下の中に含まれます:

- 153 ページの『.spec.tracing』

フィールド	説明
image 文字列	使用するコンテナー・イメージ。
imagePullPolicy 文字列	指定されたイメージのプルを Kubelet が試行するタイミングを制御する設定。 デフォルトは IfNotPresent です。
livenessProbe TracingProbe	Liveness プローブを制御する設定。
readinessProbe TracingProbe	Readiness プローブを制御する設定。

.spec.tracing.collector.livenessProbe

Liveness プローブを制御する設定。

以下の中に含まれます:

- 155 ページの『.spec.tracing.collector』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してから Liveness プローブが開始されるまでの秒数。 デフォルトは 10 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 10 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。

フィールド	説明
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 2 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.tracing.collector.readinessProbe

Readiness プローブを制御する設定。

以下の中に含まれます:

- 155 ページの『.spec.tracing.collector』

フィールド	説明
failureThreshold 整数	プローブが成功した後に、この回数以上連続して失敗すると、失敗したプローブと見なされます。 デフォルトは 1 です。
initialDelaySeconds 整数	コンテナーが始動してから Liveness プローブが開始されるまでの秒数。 デフォルトは 10 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。
periodSeconds 整数	プローブを実行する間隔 (秒単位)。 デフォルトは 10 秒です。
successThreshold 整数	プローブが成功した後に、この回数以上連続して成功すると、成功したプローブと見なされます。 デフォルトは 1 です。
timeoutSeconds 整数	プローブがタイムアウトになるまでの秒数。 デフォルトは 2 秒です。 詳細情報: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes。

.spec.web

MQ Web サーバーの設定。

以下の中に含まれます:

- 140 ページの『.spec』

フィールド	説明
console コンソール	MQ Web コンソールの設定。 MQ Operator 3.0.0 以上が必要です。
enabled ブール値	Web サーバーを有効にするかどうか。 デフォルトは false です。
manualConfig ManualConfig	Web サーバー XML 構成を指定するための設定。 MQ Operator 3.0.0 以上が必要です。

.spec.web.console

MQ Web コンソールの設定。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 156 ページの『.spec.web』

フィールド	説明
authentication 認証	MQ Web コンソールの認証設定。 MQ Operator 3.0.0 以上が必要です。
authorization 許可	MQ Web コンソールの許可設定。 MQ Operator 3.0.0 以上が必要です。

.spec.web.console.authentication

MQ Web コンソールの認証設定。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 156 ページの『.spec.web.console』

フィールド	説明
provider 文字列	MQ Web コンソール用に使用する認証プロバイダー。 integration-keycloak を使用して、 Cloud Pak for Integration Platform UI (Keycloak) でシングル・サインオンを使用します。 デフォルトは、 Cloud Pak for Integration ライセンスを使用する場合は integration-keycloak 、 MQ ライセンスを使用する場合は manual です。 独自の構成を指定する場合は、 manual を使用します。

.spec.web.console.authorization

MQ Web コンソールの許可設定。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 156 ページの『.spec.web.console』

フィールド	説明
provider 文字列	MQ Web コンソール用に使用する許可プロバイダー。 integration-keycloak を使用して、 Cloud Pak for Integration Keycloak によって提供される役割を使用します。 独自の構成を指定する場合は、 manual を使用します。 デフォルトは、 Cloud Pak for Integration ライセンスを使用する場合は integration-keycloak 、 MQ ライセンスを使用する場合は manual です。

.spec.web.manualConfig

Web サーバー XML 構成を指定するための設定。 MQ Operator 3.0.0 以上が必要です。

以下の中に含まれます:

- 156 ページの『.spec.web』

フィールド	説明
configMap ConfigMap	ConfigMap は、Web サーバー XML 構成を含む Kubernetes ConfigMap を表します。
secret Secret	シークレットは、Web サーバー XML 構成を含む Kubernetes シークレットを表します。 シークレットを使用すると、 Kubernetes レイヤー内のすべての資格情報が保護されますが、モニター・ツールやトラブルシューティング・ツールによって、基礎となるファイルが非セキュアに公開される可能性があります。 セキュリティーを向上させるには、「securityUtility」を使用して資格情報をエンコードします。

.spec.web.manualConfig.configMap

ConfigMap は、Web サーバー XML 構成を含む Kubernetes ConfigMap を表します。

以下の中に含まれます:

- 157 ページの『.spec.web.manualConfig』

フィールド	説明
name 文字列	Kubernetes ソースの名前。

.spec.web.manualConfig.secret

シークレットは、Web サーバー XML 構成を含む Kubernetes シークレットを表します。 シークレットを使用すると、 Kubernetes レイヤー内のすべての資格情報が保護されますが、モニター・ツールやトラブルシューティング・ツールによって、基礎となるファイルが非セキュアに公開される可能性があります。 セキュリティーを向上させるには、「securityUtility」を使用して資格情報をエンコードします。

以下の中に含まれます:

- 157 ページの『.spec.web.manualConfig』

フィールド	説明
name 文字列	Kubernetes ソースの名前。

. 状況

QueueManager について観測された状態。

以下の中に含まれます:

- 139 ページの『QueueManager』

フィールド	説明
adminUiUrl 文字列	管理 UI の URL。
availability Availability	キュー・マネージャーの可用性状況。
conditions QueueManagerStatusCondition 配列	条件は、キュー・マネージャーの状態に関する最新の使用可能な監視を表します。
endpoints QueueManagerStatusEndpoint 配列	このキュー・マネージャーが公開しているエンドポイントに関する情報 (API エンドポイントや UI エンドポイントなど)。
metadata メタデータ	メタデータは、統合-Keycloak 状況など、キュー・マネージャーの追加情報を表します。
name 文字列	キュー・マネージャーの名前。
phase 文字列	キュー・マネージャーの状態のフェーズです。
versions QueueManagerStatusVersion	使用されている MQ のバージョン、および IBM Entitled Registry から取得できるその他のバージョン。

.status.availability

キュー・マネージャーの可用性状況。

以下の中に含まれます:

- 158 ページの『. 状況』

フィールド	説明
initialQuorumEstablished ブール値	NativeHA に初期クォーラムが確立されているかどうか。

.status.conditions

QueueManagerStatusCondition は、キュー・マネージャーの状況を示します。

以下の中に含まれます:

- 158 ページの『. 状況』

フィールド	説明
lastTransitionTime 文字列	状況のステータスが最後に遷移した時刻。
message 文字列	最後の遷移についての詳細を示す、人間が読める形式のメッセージ。
reason 文字列	最後にこのステータスに遷移した理由。
status 文字列	状況のステータス。
type 文字列	状況のタイプ。

.status.endpoints

QueueManagerStatusEndpoint は、QueueManager のエンドポイントを示します。

以下の中に含まれます:

- 158 ページの『. 状況』

フィールド	説明
name 文字列	エンドポイントの名前。
type 文字列	エンドポイントのタイプ。 UI エンドポイントの場合は「UI」、 API エンドポイントの場合は「API」、 API 資料の場合は「OpenAPI」です。
uri 文字列	エンドポイントの URI。

.status.metadata

メタデータは、統合-Keycloak 状況など、キュー・マネージャーの追加情報を表します。

以下の中に含まれます:

- 158 ページの『. 状況』

フィールド	説明
integrationKeycloak IntegrationKeycloak	QueueManagerStatusIntegrationKeycloak は、QueueManager の統合 Keycloak 状況を定義します。

.status.metadata.integrationKeycloak

QueueManagerStatusIntegrationKeycloak は、 QueueManager の統合 Keycloak 状況を定義します。

以下の中に含まれます:

- 159 ページの『.status.metadata』

フィールド	説明
clientName 文字列	

.status.versions

使用されている MQ のバージョン、および IBM Entitled Registry から取得できるその他のバージョン。

以下の中に含まれます:

- 158 ページの『. 状況』

フィールド	説明
`available` QueueManagerStatusVersionAvailable	IBM Entitled Registry から取得できるその他のバージョンの MQ。
`reconciled` 文字列	使用されている IBM MQ の具体的なバージョン。 カスタム・イメージが示されている場合は、実際に使用されている MQ のバージョンと一致していない可能性があります。

.status.versions.available

IBM Entitled Registry から取得できるその他のバージョンの MQ。

以下の中に含まれます:

- 160 ページの『.status.versions』

フィールド	説明
`channels` 配列	MQ のバージョンを自動的に更新するために使用できるチャネル。
`versions` Versions 配列	使用可能な MQ の具体的なバージョン。

.status.versions.available.versions

QueueManagerStatusVersion は MQ のバージョンを示します。

以下の中に含まれます:

- 160 ページの『.status.versions.available』

フィールド	説明
`licenses` Licenses 配列	このバージョンの QueueManager に適用可能なライセンス。
`name` 文字列	このバージョンの QueueManager のバージョン `name` 。 これは、`spec.version` フィールドで有効な値です。

.status.versions.available.versions.licenses

QueueManagerStatusLicense はライセンスを定義します。

以下の中に含まれます:

- 160 ページの『.status.versions.available.versions』

フィールド	説明
`displayName` 文字列	ライセンスの表示名。
`link` 文字列	ライセンス・コンテンツへのリンク。
`matchesCurrentType` ブール値	ライセンスが現在使用されているライセンスのタイプと一致するかどうか。
`name` 文字列	ライセンスの名前。

OpenShift CP4I *QueueManager (mq.ibm.com/v1beta1) の状況状態*

status.conditions フィールドは、QueueManager リソースの状態に合わせて更新されます。 状態は通常、異常な状況を説明するものです。 正常な作動可能状態のキュー・マネージャーは、**Error** や **Pending** の状態になりません。 通知のための **Warning** 状態になることはあります。

QueueManager リソースでは以下の状態が定義されています。

表 2. キュー・マネージャー状況状態

コンポーネント	状態タイプ	理由コード	メッセージ警告
QueueManager[3]	ブロック	OperatorDependency	このインスタンスをインストールするには、[IBM Cloud Pak for Integration] で Keycloak を構成する必要があります。 このインスタンスは、この QueueManager の Cp4iServicesBinding リソースで Keycloak が [KeycloakReady] として報告されるまで、[Pending] 状況のままになります。
			このインスタンスをインストールするには、オペレーター [IBM IAM] が必要です。 このインスタンスは、オペレーターが [IBM Cloud Pak 基本サービス] によってインストールされるまで「ブロック」状況のままになります。
	保留中	Creating	MQ キュー・マネージャーのデプロイ中です
	保留中	OidcPending	MQ キュー・マネージャーが OIDC クライアント登録を待っています。
	保留中	停止	「mq.ibm.com/stop」アノテーションが存在し、 QueueManager 定義で「true」に設定されているため、 MQ キュー・マネージャーが停止されました。 停止すると、 QueueManager StatefulSet レプリカ数がゼロに設定され、すべての MQ キュー・マネージャー・ポッドが削除されます。
	エラー	失敗	MQ キュー・マネージャーのデプロイが失敗しました
	警告	UnsupportedVersion	オペランドが、 OCP バージョン *<ocp_version>*でサポートされていないオペレーターによってインストールされました。 このオペランドはサポートされません。
	警告	CP4I-LTS のサポート	CP4I-LTS オペランド *< mq_version>* がインストールされましたが、拡張サポート期間に適格でないオペレーターによって管理されています。 このオペランドは拡張サポート期間に対応していません。
	警告	CP4I-LTS のサポート	CP4I-LTS オペランド *< mq_version>* がインストールされていますが、 OCP バージョン *< ocp_version>* が拡張サポート期間に適格ではありません。 このオペランドは拡張サポート期間に対応もしていません。

[3] 条件 Creating および Failed は、キュー・マネージャーのデプロイメントの全体的な進行状況をモニターします。 IBM Cloud Pak for Integration ライセンスを使用していて、Web コンソールが有効になっている場合、 OidcPending 条件は、OIDC クライアント登録が IAM で完了するのを待機している間のキュー・マネージャーの状況をログに記録します。

表 2. キュー・マネージャー状況状態 (続き)			
コンポーネント	**状態タイプ**	**理由コード**	**メッセージ警告**
ポッド [4]	保留中	PodPending	MQ キュー・マネージャーのポッドのデプロイ中です
	エラー	PodFailed	MQ キュー・マネージャーのポッドのデプロイ中です
記憶域 [5]	保留中	StoragePending	MQ キュー・マネージャーのストレージのプロビジョン中です
	警告	StorageEphemeral	実動 MQ キュー・マネージャーで一時ストレージを使用しています
	警告	StorageExpansion 保留中	次の PVC のボリューム拡張は保留中です [< list of pvcs>]
	警告	StorageMismatch	QueueManager リソースで定義されたストレージ・サイズが、1 つ以上のプロビジョンされた PVC [< list of pvcs>] の容量と一致しません。 QueueManager リソースで AllowVolumeExpansion が false に設定されているため、 MQ オペレーターはこれらの差分の調整を試行しません。
	エラー	StorageFailed	MQ キュー・マネージャーのストレージのプロビジョンが失敗しました

Linux 独自の IBM MQ コンテナー・イメージを作成する時のライセンス・アノテーション

ライセンス・アノテーションを使用すると、基礎になっているマシンではなくコンテナーで定義した制限に基づいて使用量を追跡管理できます。 クライアントで特定のアノテーションを付けてコンテナーをデプロイするための構成を行うと、IBM License Service はそのアノテーションに基づいて使用量を追跡管理します。

独自に作成した IBM MQ コンテナー・イメージをデプロイする場合は、ライセンス交付に関して以下の 2 つの一般的なアプローチがあります。

- コンテナーを実行するマシン全体のライセンスを取得します。
- 関連する制限に基づいてコンテナーのライセンスを取得します。

どちらのオプションもお客様が使用できます。詳細については、 Passport Advantage®の「 IBM Container Licenses 」ページを参照してください。

コンテナーの制限に基づいて IBM MQ コンテナーのライセンスを取得する場合は、使用量を追跡管理するために IBM License Service をインストールする必要があります。 サポートされている環境やインストール手順の詳細については、GitHub の ibm-licensing-operator のページを参照してください。

---

[4] POD 条件は、キュー・マネージャーのデプロイメント中にポッドの状況をモニターします。 `PodFailed` 条件が表示された場合は、キュー・マネージャー全体の条件も `Failed` に設定されます。

[5] ストレージ条件は、永続ストレージのボリュームを作成する要求の進行状況 (`StoragePending` 条件) をモニターし、バインディング・エラーおよびその他の障害を報告します。 また、ストレージ条件は、ボリューム拡張の進行状況をモニターし、キュー・マネージャー定義で定義されたストレージ・サイズとデプロイされた PVC のサイズの間の不一致のアラートもモニターします。 ストレージ・プロビジョニング中にエラーが発生した場合、 `StorageFailed` 条件が条件リストに追加され、キュー・マネージャー全体の条件が `Failed` に設定されます。

IBM MQ コンテナーがデプロイされている Kubernetes クラスターに IBM License Service がインストールされ、ポッドのアノテーションを使用して使用量が追跡されます。 そのためクライアントで、IBM License Service がその後に使用する特定のアノテーションを付けてポッドをデプロイする必要があります。 コンテナー内にデプロイされた資格および機能に基づいて、以下の 1 つ以上のアノテーションを使用します。

注 : アノテーションの多くには、以下の行のいずれかまたは両方が含まれています。

```
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
```

アノテーションを使用する前に、以下の行を編集する必要があります。

- `productChargedContainers` の場合は、`"All"`を選択するか、コンテナーの実際の名前を置き換える必要があります。
- `productMetric` の場合は、提供されている値のいずれかを選択する必要があります。

IBM MQ 製品ライセンスで使用するアノテーション

IBM MQ 製品ライセンスがある場合は、購入した使用する資格に一致する以下のアノテーションを選択します。

- 166 ページの『IBM MQ』
- 166 ページの『IBM MQ 拡張』
- 166 ページの『IBM MQ (非実稼働環境)』
- 166 ページの『IBM MQ Advanced for Non-Production Environment (非実稼働環境向け拡張)』
- 166 ページの『IBM MQ Advanced for Developers』

IBM MQ マルチインスタンス高可用性構成で使用する IBM MQ アノテーションは、以下のとおりです。 164 ページの『高可用性構成の正しいアノテーションの選択』も参照してください。

- 166 ページの『IBM MQ コンテナー・マルチインスタンス』
- 166 ページの『IBM MQ 拡張コンテナー・マルチインスタンス』
- 167 ページの『IBM MQ Container Multi Instance for Non-Production Environment』
- 167 ページの『IBM MQ Advanced Container Multi Instance for Non-Production Environment』

CP4I 製品ライセンスで使用するアノテーション

IBM Cloud Pak for Integration (CP4I) 資格がある場合は、購入して使用する資格に一致する以下の注釈を選択します。

- 167 ページの『IBM MQ with CP4I ライセンス』
- 167 ページの『IBM MQ Advanced with CP4I ライセンス』
- 167 ページの『IBM MQ for Non-Production Environment with CP4I の使用許諾』
- 167 ページの『IBM MQ Advanced for Non-Production Environment with CP4I の使用許諾』

IBM MQ マルチインスタンス高可用性構成で使用する CP4I アノテーションは、以下のとおりです。 164 ページの『高可用性構成の正しいアノテーションの選択』も参照してください。

- 167 ページの『IBM MQ Container Multi Instance with CP4I のライセンス』
- 168 ページの『IBM MQ Advanced Container Multi Instance with CP4I のライセンス』
- 168 ページの『IBM MQ Container Multi Instance for Non-Production Environment with CP4I の使用許諾』
- 168 ページの『IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I のライセンス』

高可用性構成の正しいアノテーションの選択

IBM MQ マルチインスタンス

IBM MQ 複数インスタンスの高可用性構成でキュー・マネージャーのペアをデプロイする場合は、両方のインスタンスで同じアノテーションを使用する必要があります。 購入したライセンスに応じて、以下のいずれかのアノテーションを選択する必要があります。

- IBM MQ または IBM MQ Advanced スタンドアロン・ライセンス
  - 166 ページの『IBM MQ コンテナー・マルチインスタンス』
  - 166 ページの『IBM MQ 拡張コンテナー・マルチインスタンス』
  - 167 ページの『IBM MQ Container Multi Instance for Non-Production Environment』
  - 167 ページの『IBM MQ Advanced Container Multi Instance for Non-Production Environment』
- IBM Cloud Pak for Integration 資格
  - 167 ページの『IBM MQ Container Multi Instance with CP4I のライセンス』
  - 168 ページの『IBM MQ Advanced Container Multi Instance with CP4I のライセンス』
  - 168 ページの『IBM MQ Container Multi Instance for Non-Production Environment with CP4I の使用許諾』
  - 168 ページの『IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I のライセンス』

IBM Cloud Pak for Integration 資格で使用する場合、アノテーション内の資格比率により、正しい資格使用量が記録されます。 スタンドアロンの IBM MQ または IBM MQ Advanced の資格で使用する場合は、以下のように、インスタンスごとに License Service で報告されるアノテーションを IBM MQ 資格パーツにマップする必要があります。

- IBM MQ Advanced container マルチインスタンス
  - 1 x IBM MQ Advanced **および** 1 x IBM MQ Advanced 高可用性レプリカ **または**
  - 2 つの IBM MQ Advanced[6]
- 非実稼働環境用の IBM MQ Advanced container マルチインスタンス
  - 1 x IBM MQ Advanced **および** 1 x IBM MQ Advanced 高可用性レプリカ **または**
  - 2 x IBM MQ Advanced (非実稼働環境の場合)[6]
- IBM MQ コンテナー・マルチインスタンス
  - 1 x IBM MQ **および** 1 x IBM MQ 高可用性レプリカ **または**
  - 2 つの IBM MQ[6]
- IBM MQ Container Multi Instance for Non-Production Environment
  - 1 x IBM MQ **および** 1 x IBM MQ 高可用性レプリカ **または**
  - 2 x IBM MQ (非実稼働環境の場合) [6]

IBM MQ ネイティブ HA

ネイティブ HA クォーラムに 3 つのキュー・マネージャーをデプロイする場合、アクティブ・インスタンスのみがライセンスを消費します。 すべてのインスタンスに同じアノテーションを付ける必要があります。 購入したライセンスに応じて、以下のいずれかを選択する必要があります。

- IBM MQ または IBM MQ Advanced スタンドアロン・ライセンス
  - 166 ページの『IBM MQ 拡張』
  - 166 ページの『IBM MQ Advanced for Non-Production Environment (非実稼働環境向け拡張)』
- IBM Cloud Pak for Integration 資格
  - 167 ページの『IBM MQ Advanced with CP4I ライセンス』
  - 167 ページの『IBM MQ Advanced for Non-Production Environment with CP4I の使用許諾』

[6] このライセンス・オプションは最適ではありません。関連する高可用性レプリカ・パーツのライセンスがない場合にのみ使用してください。

アノテーション

このトピックの残りの部分では、各アノテーションの内容について詳しく説明します。

IBM MQ

```
productID: "c661609261d5471fb4ff8970a36bccea"
productName: "IBM MQ"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ 拡張

```
productID: "208423bb063c43288328b1d788745b0c"
productName: "IBM MQ Advanced"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ (非実稼働環境)

```
productID: "151bec68564a4a47a14e6fa99266deff"
productName: "IBM MQ for Non-Production Environment"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Advanced for Non-Production Environment (非実稼働環境向け拡張)

```
productID: "21dfe9a0f00f444f888756d835334909"
productName: "IBM MQ Advanced for Non-Production Environment"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Advanced for Developers

```
productID: "2f886a3eefbe4ccb89b2adb97c78b9cb"
productName: "IBM MQ Advanced for Developers (Non-Warranted)"
productMetric: "FREE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ コンテナー・マルチインスタンス

```
productID: "2dea73b866b648b6b4abe2a85eb76964"
productName: "IBM MQ Container Multi Instance"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ 拡張コンテナー・マルチインスタンス

```
productID: "bd35bff411bb47c2a3f3a4590f33a8ef"
productName: "IBM MQ Advanced Container Multi Instance"
productMetric: "PROCESSOR_VALUE_UNIT" | "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Container Multi Instance for Non-Production Environment

```
productID: "af11b093f16a4a26806013712b860b60"
productName: "IBM MQ Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ Advanced Container Multi Instance for Non-Production Environment

```
productID: "31f844f7a96b49749130cd0708fdbb17"
productName: "IBM MQ Advanced Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

IBM MQ with CP4I ライセンス

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "c661609261d5471fb4ff8970a36bccea"
productName: "IBM MQ"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "4:1"
```

IBM MQ Advanced with CP4I ライセンス

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "208423bb063c43288328b1d788745b0c"
productName: "IBM MQ Advanced"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "2:1"
```

IBM MQ for Non-Production Environment with CP4I の使用許諾

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "151bec68564a4a47a14e6fa99266deff"
productName: "IBM MQ for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers:  "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "8:1"
```

IBM MQ Advanced for Non-Production Environment with CP4I の使用許諾

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "21dfe9a0f00f444f888756d835334909"
productName: "IBM MQ Advanced for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "4:1"
```

IBM MQ Container Multi Instance with CP4I のライセンス

```
productName: "IBM MQ Container Multi Instance"
productID: "2dea73b866b648b6b4abe2a85eb76964"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
```

```
productMetric: "VIRTUAL_PROCESSOR_CORE"
productCloudpakRatio: "10:3"
cloudpakName: "IBM Cloud Pak for Integration"
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
```

IBM MQ Advanced Container Multi Instance with CP4I のライセンス

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "bd35bff411bb47c2a3f3a4590f33a8ef"
productName: "IBM MQ Advanced Container Multi Instance"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "5:3"
```

IBM MQ Container Multi Instance for Non-Production Environment with CP4I の使用許諾

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "af11b093f16a4a26806013712b860b60"
productName: "IBM MQ Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "20:3"
```

IBM MQ Advanced Container Multi Instance for Non-Production Environment with CP4I のライセンス

```
cloudpakId: "c8b82d189e7545f0892db9ef2731b90d"
cloudpakName: "IBM Cloud Pak for Integration"
productID: "31f844f7a96b49749130cd0708fdbb17"
productName: "IBM MQ Advanced Container Multi Instance for Non-Production Environment"
productMetric: "VIRTUAL_PROCESSOR_CORE"
productChargedContainers: "All" | "NAME_OF_CONTAINER"
productCloudpakRatio: "10:3"
```

OpenShift CP4I Kubernetes IBM MQ Advanced for Developers コンテナー・イメージ

IBM MQ Advanced for Developers には、事前ビルドされたコンテナー・イメージが用意されています。 このイメージは、 IBM Container Registry から入手できます。 このイメージは、 Docker、 Podman、 Kubernetes、およびその他のコンテナー環境での使用に適しています。

使用可能なイメージ

IBM MQ イメージは、 IBM Container Registry に保管されます。

- IBM MQ Advanced for Developers 9.4.0.0: `icr.io/ibm-messaging/mq:9.4.0.0-r1`

クイック・リファレンス

- ライセンス:
  - mq.ibm.com/v1beta1 および Apache License 2.0 のライセンス・リファレンス。 IBM MQ Advanced for Developers ライセンスではこれ以上の配布は許可されておらず、条件によって開発者マシンへの使用が制限されていることに注意してください。
- 問題のファイリング先:
  - GitHub
- 以下の CPU アーキテクチャーで使用可能です。

- amd64
- s390x
- ppc64le

使用法

コンテナーで IBM MQ Advanced for Developers を実行します。

コンテナーの実行方法について詳しくは、 使用法の資料 を参照してください。

イメージを使用できるようにするには、**LICENSE** 環境変数を設定して IBM MQ ライセンスの条項に同意する必要があります。

サポートされる環境変数

LANG
ライセンスの印刷に使用する言語を設定します。

LICENSE
IBM MQ Advanced for Developers ライセンス条件に同意するには、 `accept` を設定します。

ライセンス条件を表示するには、 `view` を設定します。

Deprecated **MQ_ADMIN_PASSWORD**
admin ユーザーのパスワードを指定します。

長さは 8 文字以上でなければなりません。

admin ユーザーのデフォルト・パスワードはありません。

V 9.4.0 V 9.4.0 IBM MQ 9.4.0 以降、この変数は提供されなくなりました。 このトピックの YAML の例 は、この変数を自分で作成し、シークレットで保護する方法を示しています。

Deprecated **MQ_APP_PASSWORD**
アプリケーション・ユーザーのパスワードを指定します。

これを設定すると、**DEV.APP.SVRCONN** チャネルが保護され、有効なユーザー ID とパスワードを提供する接続のみが許可されます。

長さは 8 文字以上でなければなりません。

アプリケーション・ユーザーのデフォルト・パスワードはありません。

V 9.4.0 V 9.4.0 IBM MQ 9.4.0 以降、この変数は提供されなくなりました。 このトピックの YAML の例 は、この変数を自分で作成し、シークレットで保護する方法を示しています。

MQ_DEV
作成中のデフォルト・オブジェクトを停止するには、 `false` に設定します。

MQ_ENABLE_METRICS
`true` に設定すると、キュー・マネージャーの Prometheus メトリックが生成されます。

MQ_LOGGING_CONSOLE_SOURCE
コンテナーの **stdout** ロケーションにミラーリングされるログのソースのコンマ区切りリストを指定します。

有効な値は、 `qmgr`、 `web` 、および `mqsc` です。

デフォルト値は `qmgr, web` です。

オプション値は `mqsc` です。 このオプションは、コンテナー・ログ内の `autocfgmqsc.LOG` の内容を反映するために使用できます。

MQ_LOGGING_CONSOLE_FORMAT
コンテナーの **stdout** ロケーションに出力されるログのフォーマットを変更します。

単純な人間が理解できる形式を使用するには、 `basic` を設定します。 これがデフォルト値です。

JSON 形式 (各行に 1 つの JSON オブジェクト) を使用するように `json` を設定します。

MQ_LOGGING_CONSOLE_EXCLUDE_ID
除外するログ・メッセージのメッセージ ID のコンマ区切りリストを指定します。

ログ・メッセージは引き続きディスク上のログ・ファイルに表示されますが、コンテナーの **stdout** ロケーションには出力されません。

デフォルト値は AMQ5041I,AMQ5052I,AMQ5051I,AMQ5037I,AMQ5975I です。

mq_qmgr_name
キュー・マネージャーの作成に使用する名前を設定します。

IBM MQ Advanced for Developers イメージでサポートされるデフォルトの開発者構成について詳しくは、デフォルトの開発者構成の資料を参照してください。

admin および app ユーザーのパスワードを指定する方法を説明するキュー・マネージャー YAML の例

admin ユーザー ID および **app** ユーザー ID のユーザーの場合、Development ライセンスを使用してキュー・マネージャーをデプロイするときにパスワードを指定する必要があります。 以下に、IBM MQ Operator でこれを行う方法を示すキュー・マネージャー YAML の例を示します。

以下のコマンドは、 **admin** および **app** ユーザーのパスワードを含むシークレットを作成します。

```
oc create secret generic my-mq-dev-passwords --from-literal=dev-admin-password=passw0rd --from-
literal=dev-app-password=passw0rd
```

以下の YAML は、キュー・マネージャーのデプロイ時にこれらのパスワードを使用します。

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: qm-dev
spec:
  license:
    accept: false
    license: L-CLXQ-ADXTK3
    use: Development
  web:
    enabled: true
  template:
    pod:
      containers:
        - env:
            - name: MQ_DEV
              value: "true"
            - name: MQ_CONNAUTH_USE_HTP
              value: "true"
            - name: MQ_ADMIN_PASSWORD
              valueFrom:
                secretKeyRef:
                  name: my-mq-dev-passwords
                  key: dev-admin-password
            - name: MQ_APP_PASSWORD
              valueFrom:
                secretKeyRef:
                  name: my-mq-dev-passwords
                  key: dev-app-password
          name: qmgr
  queueManager:
    storage:
      queueManager:
        type: persistent-claim
    name: QUICKSTART
  version: 9.4.0.0-r1
```

コンテナー内の IBM MQ のトラブルシューティング

コンテナーでの IBM MQ の実行に問題がある場合は、ここで説明する手法を使用して、問題の診断と解決に役立てることができます。

手順

- 171 ページの『コンテナー内の IBM MQ の計画外の再始動のトラブルシューティング』.
- 172 ページの『IBM MQ Operator に関する問題のトラブルシューティング』.

OpenShift CP4I Kubernetes コンテナー内の IBM MQ の計画外の再始動のトラブルシューティング

Red Hat OpenShift Container Platform や Kubernetes などのほとんどのコンテナー管理システムでは、通常、コンテナーが再始動されます。 コンテナーが長期間存続することは通常ではありません。 このトピックでは、コンテナーのライフサイクル、再始動の調査方法、および計画外のコンテナー再始動の背後にある理由について説明します。

IBM MQ デプロイメントに問題がなく、引き続き予期したとおりに実行される場合は、ソリューションが意図したとおりに実行されている可能性があります。 コンテナー・ログに次のようなログ・メッセージが表示されることがあります。

```
Signal received: terminated
```

これは、SIGTERM シグナルが MQ コンテナーに送信され、終了を要求していることを意味します。 Linux コンテナーは、 POSIX シグナルに応答する責任があります。このシグナルは、動作をトリガーするためにプログラムに送信される標準化されたメッセージです。

IBM MQ コンテナーは、SIGTERM シグナルを受信すると、 `endmqm -w -r -tp` コマンドを発行してキュー・マネージャーを停止します。 キュー・マネージャーが停止すると、コンテナーは停止します。 キュー・マネージャーの停止に長時間かかる場合は、SIGKILL シグナルが送信される可能性があります。これにより、 Linux プロセスが即時に終了します。 SIGTERM と SIGKILL の間の時間の長さは、 Kubernetes では「終了猶予期間」と呼ばれ、 `QueueManager` リソース (IBM MQ Operator を使用している場合) またはポッド・リソースで直接構成可能です。 デフォルトは 30 秒で、そのうちの 1 秒はコンテナーをシャットダウンするために予約されており、残りは IBM MQ に指定されています。 例えば、デフォルトの場合、 `endmqm -w -tp 29` が発行されます。これにより、シャットダウンに 29 秒かかったことがキュー・マネージャーに通知されます。

ポッド排除の理由

SIGTERM シグナルは、ポッドを正常に終了するために Kubernetes (および Red Hat OpenShift Container Platform) によって使用されます。 Kubernetes 資料の Termination of Pods を参照してください。 Kubernetes は、ノード上のポッドが自発的または非自発的に強制終了されるプロセスに対して、「ポッドの中断」 および「排除」という用語を使用します。 ポッドが追い出される理由には、以下のような多くの理由があります。

- **kubelet による終了**。 これには、以下のようないくつかの理由が考えられます。
  - ノードが (おそらくローリング・クラスター更新の一部として) シャットダウンされているため、ポッドを強制終了できます。
  - ポッドは、ノードの「圧力」(kubelet がノード上のリソースを再利用するためにポッドをプロアクティブに強制終了する) が原因で終了する可能性があります。 Kubernetes クラスター管理者は、クラスター間で異なる可能性がある排除しきい値を構成できます。
  - ポッドが活性プローブに失敗したため、ポッドを強制終了することができます。 Kubernetes で Liveness プローブを構成して、ポッドがまだ正常であることを確認できます。 IBM MQ Operator は、有効な実行状態を確認するために **dspmq** コマンドを呼び出すキュー・マネージャーの活性プローブをセットアップします。 キュー・マネージャーが正常な状態でない場合、またはプローブ自体の実行に時間がかかりすぎる場合、kubelet は失敗と見なします。 許容される障害数のしきい値は、 `QueueManager` リソース (IBM MQ Operator を使用している場合) またはポッド・リソースで直接構成できます。
- **Kubernetes スケジューラーによる優先使用**。 これは、 Kubernetes スケジューラーが優先度の高いポッドを実行する必要がある場合に発生する可能性があります

- **テイント適用ノード**。 ノードは「テイント」にすることができ、テイントを許容しないポッドは排除されます。 テイントは、 Kubernetes 管理者が特定のノードからポッドを「反復」するために使用します。 例えば、 IBM MQ ポッドは、現在他のワークロード用に予約されている特別なハードウェアを持つノード上では実行されなくなります。
- **Eviction API を介した要求**。 これは、管理者がポッドを除去するために呼び出すことができます。
- **ポッド・ガーベッジ・コレクション**。 これは、ノードがサービス休止になった場合、または Kubernetes API を使用してノードが削除された場合に発生する可能性があります。

キュー・マネージャー・ポッドが除去された理由の判別

ポッドが強制排除された理由を理解するために役立つ可能性のある情報源には、以下のものがあります。

- **クラスター・イベント**。 例えば、 OpenShift Container Platform クラスター内のシステム・イベント情報の表示。
- **クラスター監査イベント**。 Red Hat OpenShift Container Platform での監査ログの表示を参照してください。
- **圧力がかかっているノード**。 CPU、ネットワーク、またはメモリーの圧力がかかっているノードを探します。 これはノード状況で確認できます。 表示するまでには、ノードに圧力がかかっていない可能性があることに注意してください。
- **Red Hat OpenShift Container Platform Monitoring** またはその他のモニター・メトリックは、ディスク待ち時間の問題などを示すことができる場合があります。 有用な Prometheus メトリックは、 `ibmmq_qmgr_log_write_latency_seconds` です。 この情報は、 MQ 統計のトピックから得られます。

関連情報

スケジューリング、優先使用、および回避に関する Kubernetes 資料

OpenShift CP4I IBM MQ Operator に関する問題のトラブルシューティング

IBM MQ Operator で問題が発生する場合、説明されている手法を使用して問題の診断と解決を実施します。

手順

- 172 ページの『IBM MQ Operator を使用してデプロイされたキュー・マネージャーのトラブルシューティング情報の収集』
- 174 ページの『トラブルシューティング: キュー・マネージャー・データへのアクセスの取得』

OpenShift CP4I IBM MQ Operator を使用してデプロイされたキュー・マネージャーのトラブルシューティング情報の収集

新しいサポート Case を提出する際に IBM サポートに提供する必要があるトラブルシューティング情報を収集する。

手順

1. クラウド・プロバイダー情報を収集します。

   これは、 Red Hat OpenShift クラスターをホストするクラウド・プロバイダーです (例えば、 IBM Cloud)。
2. アーキテクチャー情報を収集します。

   Red Hat OpenShift クラスターのアーキテクチャーは、以下のいずれかです。

   - Linux for x86-64
   - Linux on Power Systems (ppc64le)
   - Linux for IBM Z
3. IBM MQ デプロイメント情報を収集します。

a) bash/zsh シェルを使用して、 Red Hat OpenShift クラスターにログオンします。

b) 以下の環境変数を設定します。

```
export QM=QueueManager_name
export QM_NAMESPACE=QueueManager_namespace
export MQ_OPERATOR_NAMESPACE=mq_operator_namespace
```

ここで、 *QueueManager_name* は QueueManager リソースの名前、 *QueueManager_namespace* はそれがデプロイされている名前空間、 *mq_operator_namespace* は IBM MQ Operator がデプロイされている名前空間です。 これは、 QueueManager 名前空間と同じ場合があります。

c) 以下のコマンドを実行し、結果の出力ファイルをすべて IBM サポートに提供します。

```
# OCP / Kubernetes: Version
oc version -o yaml > ocversion.yaml

# QueueManager: YAML
oc get qmgr $QM -n $QM_NAMESPACE -o yaml > "queue-manager-$QM.yaml"

# MQ Queue Manager: Pods
oc get pods -n $QM_NAMESPACE -o wide --selector "app.kubernetes.io/instance=$QM" > "qm-
pods-$QM.txt"

# MQ Queue Manager: Pod YAML
oc get pods -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
pods-$QM.yaml"

# MQ Queue Manager: Pod Logs
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc logs -n $QM_NAMESPACE --previous "$p" > "qm-logs-
previous-$p.txt"; oc logs -n $QM_NAMESPACE $p > "qm-logs-$p.txt";done

# MQ Queue Manager: Describe Pods
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc describe pod $p -n $QM_NAMESPACE > "qm-pod-
describe-$p.txt"; done

# MQ Web UI: Console Log
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc cp -n $QM_NAMESPACE --retries=10 "$p:var/mqm/web/
installations/Installation1/servers/mqweb/logs/console.log" "web-$p-console.log"; done

# MQ Web UI: Messages Log
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc cp -n $QM_NAMESPACE --retries=10 "$p:var/mqm/web/
installations/Installation1/servers/mqweb/logs/messages.log" "web-$p-messages.log"; done

# MQ Queue Manager: routes defined by operator
oc get routes -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
routes-$QM.yaml"

# MQ Queue Manager: routes to QM
oc get routes -n $QM_NAMESPACE -o yaml --field-selector "spec.to.name=$QM-ibm-mq" > "qm-
routes2-$QM.yaml"

# MQ Queue Manager: stateful set
oc get statefulset -n $QM_NAMESPACE -o yaml ${QM}-ibm-mq > "qm-statefulset-$QM.yaml"

# MQ Queue Manager: revisions of the stateful set
oc get controllerrevisions.apps -o yaml -n $QM_NAMESPACE --selector "app.kubernetes.io/
instance=$QM" > "qm-statefulset-revisions-$QM.yaml"

# MQ Queue Manager: Pod events
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do oc get -o custom-columns="LAST
SEEN:.lastTimestamp,TYPE:.type,REASON:.reason,KIND:.involvedObject.kind,NAME:.involvedObje
ct.name,MESSAGE:.message" event -n $QM_NAMESPACE --field-selector
involvedObject.name="$p" > "qm-pod-events-$p.txt"; done

# MQ Queue Manager: StatefulSet events
oc get events -n $QM_NAMESPACE -o custom-columns="LAST
SEEN:.lastTimestamp,TYPE:.type,REASON:.reason,KIND:.involvedObject.kind,NAME:.involvedObje
ct.name,MESSAGE:.message" --field-selector involvedObject.name="${QM}-ibm-mq" > "qm-
statefulset-events-$QM.txt"

# MQ Queue Manager: services
oc get services -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" >
"qm-services-$QM.yaml"
```

```
# MQ Queue Manager: PVCs
oc get pvc -n $QM_NAMESPACE -o yaml --selector "app.kubernetes.io/instance=$QM" > "qm-
pvcs-$QM.yaml"

# MQ Operator: Version
oc get csv -n $QM_NAMESPACE | grep "^ibm-mq\|NAME" > mq-operator-csv.txt

# Cloud Pak Foundational Services: Version
oc get csv -n $QM_NAMESPACE | grep "^ibm-common-service-operator\|NAME" > common-services-
csv.txt

# Cloud Pak for Integration: Version (if applicable)
oc get csv -n $QM_NAMESPACE | grep "^ibm-integration-platform-navigator\|NAME" > cp4i-
csv.txt

# Output from runmqras (this may take a while to execute)
for p in $(oc get pods -n $QM_NAMESPACE --no-headers --selector "app.kubernetes.io/
instance=$QM" | cut -d ' ' -f 1); do timestamp=$(TZ=UTC date +"%Y%m%d_%H%M%S"); oc exec
-n $QM_NAMESPACE $p -- runmqras -workdirectory "/tmp/runmqras_$timestamp" -section
logger,mqweb,nativeha,trace; oc cp -n $QM_NAMESPACE --retries=10 "$p:tmp/
runmqras_$timestamp/" .; done

# MQ Operator: Pod Log
oc logs -n $MQ_OPERATOR_NAMESPACE $(oc get pods -n $MQ_OPERATOR_NAMESPACE --no-headers --
selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/managed-by=olm | cut -d ' ' -f
1) > mq-operator-log.txt
```

注:

これらのコマンドの大部分は、キュー・マネージャーがデプロイされている名前空間へのアクセス権限を必要とします。 ただし、 IBM MQ Operator が **cluster-scoped** にインストールされている場合は、IBM MQ Operator ログを収集するために、**クラスター管理者** アクセス権限が追加で必要になることがあります。

関連タスク

IBM サポートのトラブルシューティング情報の収集

OpenShift CP4I トラブルシューティング: キュー・マネージャー・データへのアクセスの取得

PVC インスペクター・ツールを使用して、キュー・マネージャー・ポッドに対してリモート・シェルを確立できないキュー・マネージャー PVC 上のファイルにアクセスできるようにします。 これは、ポッドが **Error** 状態または **CrashLoopBackOff** 状態であることが原因である可能性があります。 このツールは、IBM MQ Operator によってデプロイされたキュー・マネージャーで使用するために設計されています。

始める前に

PVC Inspector ツールを使用する場合。 キュー・マネージャーの名前空間へのアクセス権限が必要です。

このタスクについて

トラブルシューティングを支援するために、特定のキュー・マネージャーに関連付けられた永続ボリューム要求 (PVC) に保管されているデータにアクセスできます。 これを行うには、ツールを使用して、一連のインスペクター・ポッドに PVC をマウントします。 その後、リモート・シェルをインスペクター・ポッドのいずれかに取得して、ファイルを読み取ることができます。

デプロイメントのタイプに応じて、1 つから 3 つのインスペクター・ポッドが作成されます。 Native-HA キュー・マネージャーまたは複数インスタンス・キュー・マネージャーの特定のポッドに固有のボリュームは、関連付けられた PVC インスペクター・ポッドで使用可能です。 共有ボリュームはすべてのインスペクターで使用可能です。 インスペクター・ポッドの名前には、関連付けられたキュー・マネージャー・ポッドの名前が含まれます。

手順

1. MQ PVC インスペクター・ツールをダウンロードします。

このツールは、 https://github.com/ibm-messaging/mq-pvc-tool から入手できます。

2. クラスターにログインしていることを確認します。
3. キュー・マネージャーの名前と、キュー・マネージャーが実行されている名前空間を調べます。
4. キュー・マネージャーに対してインスペクター・ツールを実行します。
   a) キュー・マネージャー名とその名前空間名を指定して、以下のコマンドを実行します。

   ```
   ./pvc-tool.sh queue_manager_name queue_manager_namespace_name
   ```

   b) ツールが完了したら、以下のコマンドを実行して、作成されるインスペクター・ポッドを表示します。

   ```
   oc get pods
   ```

5. インスペクター・ポッドにマウントされたファイルを表示します。
   a) 各 PVC インスペクター・ポッドはキュー・マネージャー・ポッドに関連付けられるため、複数のインスペクター・ポッドが存在する可能性があります。 以下のコマンドを実行して、これらのポッドのいずれかにアクセスします。

   ```
   oc rsh pvc-inspector-pod-name
   ```

   マウントされた PVC ディレクトリーが入っているディレクトリーに置かれます。

   b) 以下のコマンドを実行して、PVC ディレクトリーをリストします。

   ```
   ls
   ```

   c) リモート・シェル・セッションの外部で以下のコマンドを実行して、PVC のリストを表示します。

   ```
   oc get pvc
   ```

   d) 以下のコマンドを実行して、ツールによって作成されたポッドをクリーンアップします。

   ```
   oc delete pods -l tool=mq-pvc-inspector
   ```

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

IBM 本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。 ただし、IBM 以外の製品とプログラムの操作またはサービスの 評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。 本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 103-8510
東京都中央区日本橋箱崎町 19 番 21 号
日本アイ・ビー・エム株式会社
日本アイ・ビー・エム株式会社
法務・知的財産
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
〒 103-8510
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 INTERNATIONAL BUSINESS MACHINES CORPORATION は、法律上の瑕疵担保責任、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。 "" 国または地域によっては、法律の強行規定により、保証責任の制限が 禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。 それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

東京都中央区日本橋箱崎町 19 番 21 号
日本アイ・ビー・エム株式会社
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用すること ができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他の ライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で 決定されたものです。 そのため、他の操作環境で得られた結果は、異なる可能性があります。 一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。 さらに、一部の測定値が、推定値である可能性があります。 実際の結果は、異なる可能性があります。 お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、 もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。 したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、 あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。 お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。 このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性が あることをほのめかしたり、保証することはできません。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

プログラミング・インターフェース情報 (提供されている場合) は、このプログラムで使用するアプリケーション・ソフトウェアの作成を支援することを目的としています。

本書には、プログラムを作成するユーザーが IBM MQ のサービスを使用できるようにするためのプログラミング・インターフェースに関する情報が記載されています。

ただし、この情報には、診断、修正、および調整情報が含まれている場合があります。 診断、修正、調整情報は、お客様のアプリケーション・ソフトウェアのデバッグ支援のために提供されています。

重要 : この診断、修正、およびチューニング情報は、変更される可能性があるため、プログラミング・インターフェースとして使用しないでください。

商標

IBM、 IBM ロゴ、 ibm.com®は、世界の多くの国で登録された IBM Corporation の商標です。 現時点での IBM の商標リストについては、 "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml をご覧ください。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。

Microsoft および Windows は、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標です。

この製品には、 Eclipse Project (https://www.eclipse.org/) により開発されたソフトウェアが含まれています。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

部品番号:

(1P) P/N: