9.1

IBM MQ v kontejnerech

Poznámka

Než začnete používat tyto informace a produkt, který podporují, přečtěte si informace, které uvádí “Poznámky” na stránce 51.

Toto vydání se vztahuje k verzi 9 vydání 1 produktu IBM® MQ a ke všem následujícím vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak.

Když odešlete informace do IBM, udělíte společnosti IBM nevýlučné právo použít nebo distribuovat informace libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Obsah

Linux IBM MQ v kontejnerech

Kontejnery umožňují zabalit správce front IBM MQ nebo aplikaci klienta IBM MQ se všemi závislostmi do standardizované jednotky pro vývoj softwaru.

Produkt IBM MQ lze spustit v kontejneru s předpřipraveném stavu, který je k dispozici v produktu IBM MQ Advanced a IBM MQ Advanced for Developers. Tento produkt IBM MQ Advanced certified container nabízí podporovaný obrázek a graf Helm a lze jej použít k implementaci obrazu produktu production-ready produktu IBM MQ do produktů Red Hat® OpenShift®, IBM Cloud Privatenebo IBM Cloud Kubernetes Service.

Produkt IBM MQ můžete také spustit v kontejneru IBM Cloud Pak for Integration nebo ve vámi sestaveném kontejneru.

MQ Adv. CD Další informace o IBM MQ Advanced certified container viz následující odkazy.

Linux MQ Adv. CD Plánování pro IBM MQ v kontejnerech

Když plánujete pro produkt IBM MQ v kontejnerech, zvažte podporu, kterou produkt IBM MQ poskytuje pro různé architektonické volby, jako je například způsob správy vysoké dostupnosti a jak zabezpečit správce front.

Informace o této úloze

Před plánováním architektury produktu IBM MQ v kontejnerech byste se měli seznámit se základními koncepty IBM MQ (viz Technický přehled IBM MQ) i základními koncepty Kubernetes/OpenShift (viz Architektura platformy OpenShift Container Platform).

Procedura

- “Zvolení, jak se má produkt IBM MQ používat v kontejnerech” na stránce 5.
- “Vysoká dostupnost pro IBM MQ Advanced certified container” na stránce 10.
- “Ověření uživatele a autorizace pro produkt IBM MQ Advanced certified container” na stránce 12.

Linux MQ Adv. CD Zvolení, jak se má produkt IBM MQ používat v kontejnerech

Existuje více voleb pro použití produktu IBM MQ v kontejnerech: můžete zvolit použití předem seskupených certifikovaných kontejnerů nebo můžete sestavit vlastní obrazy a kód implementace.

Použití certifikovaných kontejnerů IBM MQ Advanced

Plánujete-li implementovat v produktu Red Hat OpenShift Container Platform, pravděpodobně budete chtít používat certifikované kontejnery. K dispozici jsou tři druhy certifikovaného kontejneru:

- IBM MQ Advanced certified container pro IBM Cloud Pak for Integration. Jedná se o samostatný produkt IBM, který obsahuje verzi certifikovaného kontejneru.
- IBM MQ Advanced certified container
- Certifikovaný kontejner IBM MQ Advanced for Developers (bez záruky)

IBM MQ 9.1.4 a starší verze produktu CD byly také podporovány v systémech IBM Cloud Private a IBM Cloud Kubernetes Service.

Všimněte si, že certifikované kontejnery se vyvíjejí rychle, a proto jsou podporovány pouze pod vydáními produktu Continuous Delivery.

Certifikované kontejnery obsahují jak předem sestavené obrazy kontejneru, tak i kód implementace pro spuštění na systému Red Hat OpenShift Container Platform. Od verze IBM MQ 9.1.5 jsou správci front spravovány pomocí operátoru IBM MQ . Předchozí verze produktu IBM MQ, až do verze 9.1.5a její zahrnutí, jsou spravovány pomocí grafů Helm .

Některé funkce produktu IBM MQ nejsou při použití certifikovaných kontejnerů podporovány. Chcete-li provést některou z následujících akcí, budete muset sestavit vlastní obrazy a grafy:

- Použijte rozhraní REST API pro administraci nebo systém zpráv.
- Použijte kteroukoli z následujících komponent produktu MQ:
  - Managed File Transfer Agents a jeho prostředky. Certifikované kontejnery však můžete použít k poskytnutí jednoho nebo více správců front Coordination, Command, nebo Agent.
  - AMQP
  - IBM MQ Bridge to Salesforce
  - IBM MQ Bridge to blockchain (není podporováno v kontejnerech).
- Použijte webový server při implementaci pomocí grafů Helm (kromě produktu IBM Cloud Pak for Integration).
- Upravte volby použité s příkazy **crtmqm**, **strmqm** a **endmqm**, např. konfigurací protokolů zotavení.

Vytváření vlastních obrazů a grafů

Jedná se o nejflexibilnější řešení kontejneru, které ale od vás vyžaduje značné dovednosti v konfiguraci kontejnerů a abyste "vlastnili" výsledný kontejner. Pokud nemáte v úmyslu používat platformu Red Hat OpenShift Container Platform, budete muset sestavit vlastní obrazy a kód implementace.

K dispozici jsou ukázky pro sestavení vlastních obrazů. Viz “Sestavení vlastního kontejneru IBM MQ” na stránce 33. Grafy Helm poskytnuté jako součást certifikovaných kontejnerů jsou publikovány v systému GitHuba lze je použít jako ukázky při vytváření vlastních obrázků:

- GrafHelm pro produkt IBM MQ Advanced certified container
- GrafHelm pro certifikovaný kontejner produktu IBM MQ Advanced for Developers

Související pojmy

“Podpora certifikovaných kontejnerů produktu IBM MQ” na stránce 6
Certifikované kontejnery produktu IBM MQ jsou podporovány pouze v určitých prostředích Kubernetes

“Podpora pro sestavení vlastních kontejnerových obrazů a grafů produktu IBM MQ” na stránce 8
Informace, které je třeba vzít v úvahu, pokud používáte kontejnery v systému Linux.

Linux Podpora certifikovaných kontejnerů produktu IBM MQ

Certifikované kontejnery produktu IBM MQ jsou podporovány pouze v určitých prostředích Kubernetes

V 9.1.4 MQ Adv. CD Pro vydání CD V9.1.4 a pozdější je IBM MQ Advanced certified container podporován pro použití s Red Hat OpenShift. Viz téma “Implementace správce front pomocí rozhraní CLI Helm” na stránce 24.

Verze CD starších než V9.1.4 byly podporovány v následujících prostředích Kubernetes :

- IBM Cloud Kubernetes Service
- IBM Cloud Private
- Produkt IBM Cloud Private s produktem Red Hat OpenShift

Konkrétní podporované verze produktu Kubernetesnaleznete v souborech `qualification.yaml` a `Chart.yaml` ve staženém grafu IBM MQ Advanced Helm . Tyto verze se liší od vydání k vydání.

Produkt IBM MQ Advanced certified container je podporován pouze při implementaci pomocí operátoru IBM MQ , nebo při použití jednoho z následujících grafů Helm :

- `ibm-mqadvanced-server-prod`
- `ibm-mqadvanced-server-integration-prod` v příručce IBM Cloud Pak for Integration

Poznámka: Použití grafů Helm je zamítnuto, a to po vydání operátoru IBM MQ .

Vzhledem k tomu, že se technologie kontejnerů rychle vyvíjí, je produkt IBM MQ Advanced certified container podporován pouze na nejnovější verzi platforem, které tento graf podporuje v době vydání. Chcete-li použít starší verzi platformy, může být zapotřebí použít starší verzi produktu IBM MQ Advanced certified container.

Obraz IBM MQ Advanced certified container je založen na verzích IBM MQ Continuous Delivery (CD). Ty jsou podporovány po dobu až jednoho roku nebo pro dvě vydání CD, podle toho, která doba je delší. Long Term Support vydání produktu IBM MQ není k dispozici jako ověřený kontejner.

From IBM MQ Advanced certified container V4.0 onwards, the image provides an installation of IBM MQ on a Red Hat Universal Base Image (UBI), which includes key Linux libraries and utilities used by IBM MQ. Nástroj UBI je podporován produktem Red Hat při spuštění na hostiteli produktu Red Hat Enterprise Linux . Starší verze produktu IBM MQ Advanced certified container používaly nepodporovaný základní obraz Ubuntu .

Související pojmy

“Podpora pro sestavení vlastních kontejnerových obrazů a grafů produktu IBM MQ” na stránce 8
Informace, které je třeba vzít v úvahu, pokud používáte kontejnery v systému Linux.

Linux MQ Adv. CD Podpora verze pro IBM MQ Advanced certified container

Sada tabulek zobrazující mapování mezi podporovanými verzemi produktů IBM MQ Advanced certified container, IBM MQ, IBM Cloud Kubernetes Service, IBM Cloud Pak for Integrationa IBM Cloud Private.

IBM MQ Operátor

V 9.1.5

Operátor IBM MQ je podporován pro použití jako součást produktu IBM Cloud Pak for Integration verze 2020.2, nebo nezávisle na produktu IBM MQ verze 9.1.5 a vyšší.

Operátor IBM MQ je podporován ve verzi Red Hat OpenShift Container Platform 4.4 nebo vyšší.

IBM MQ Advanced certified container V 9.1.5 (Helm chart)-zamítnuté

Obsahuje graf Helm `ibm-mqadvanced-server-prod`.

V 9.1.5 Od verze IBM MQ Advanced certified container V5.0.x jsou prostřednictvím produktu IBM Entitled Catalog a Registry dodávány grafy a opravy Helm , obrazy a opravy. Starší verze byly dodány přes Passport Advantagea opravné verze jsou dostupné z IBM Fix Central.

Tabulka 1. Podpora pro IBM MQ Advanced certified container

Verze	Verze IBM MQ	Ukončení podpory	podporované platformy
6.0.x	9.1.5 Continuous Delivery Release	březen 2021	Podrobné systémové požadavky
5.0.x	9.1.4 Souvislé vydání doručení	Prosince 2020	Podrobné systémové požadavky

Tabulka 1. Podpora pro IBM MQ Advanced certified container (pokračování)			
Verze	**Verze IBM MQ**	**Ukončení podpory**	**podporované platformy**
4.1.x	9.1.3 Continuous Delivery Release.	červenec 2020	Podrobné systémové požadavky

IBM MQ Advanced certified container software pro IBM Cloud Pak for Integration V 9.1.5 (Helm chart)-zamítnuté

Obsahuje graf Helm `ibm-mqadvanced-server-integration-prod`.

Tabulka 2. Podpora verzí pro software IBM MQ Advanced certified container pro IBM Cloud Pak for Integration		
Verze	**Verze IBM MQ**	**Verze IBM Cloud Pak for Integration**
6.0.x	9.1.4 Souvislé vydání doručení	2020.1.1 (Systémové požadavky)
5.0.x	9.1.3 Continuous Delivery Release.	2019.4.1 (Systémové požadavky)
4.1.x	9.1.3 Continuous Delivery Release.	2019.3.2.2 (Systémové požadavky)
4.0.x	9.1.3 Continuous Delivery Release.	2019.3.2 (Systémové požadavky)
3.0.x	9.1.3 Continuous Delivery Release.	2019.3.1 (Systémové požadavky)

Informace o podporovaných verzích naleznete v poznámkách k verzi produktuIBM Cloud Pak for Integration .

Linux Podpora pro sestavení vlastních kontejnerových obrazů a grafů produktu IBM MQ

Informace, které je třeba vzít v úvahu, pokud používáte kontejnery v systému Linux.

- Základní obraz použitý kontejnerovým obrazem musí používat podporovaný operační systém Linux.
- K instalaci produktu v rámci kontejnerového obrazu musíte použít instalační programy produktu IBM MQ.
- Seznam podporovaných balíků viz komponenty IBM MQ rpm pro systémy Linux.
- V 9.1.0 Následující balíky nejsou podporovány:
  - `MQSeriesBCBridge`
  - `MQSeriesRDQM`
- Datový adresář správce front (standardně `/var/mqm`) musí být uložen na svazku kontejneru, který udržuje trvalý stav.

  Důležité: Nemůžete používat systém souborů sjednocení.

  Musíte buď připojit adresář hostitele jako datový svazek, nebo použít kontejner datového svazku. Další informace viz Správa dat v kontejnerech.
- Musíte mít možnost spouštět řídicí příkazy IBM MQ, jako např. **endmqm**, v rámci kontejneru.
- K diagnostickým účelům musíte mít možnost získat soubory a adresáře z kontejneru.
- V 9.1.0 Obor názvů můžete použít ke sdílení oborů názvů kontejneru pro správce front s ostatními kontejnery, aby byly aplikace lokálně svázány se správcem front spuštěnými v samostatných

kontejnerech. Další informace viz téma “Spuštění lokálních aplikací vazby v samostatných kontejnerech” na stránce 37.

Související pojmy

“Podpora certifikovaných kontejnerů produktu IBM MQ” na stránce 6
Certifikované kontejnery produktu IBM MQ jsou podporovány pouze v určitých prostředích Kubernetes

Linux MQ Adv. CD V 9.1.5 Aspekty úložiště pro IBM MQ Advanced certified container

IBM MQ Advanced certified container se spouští ve dvou režimech úložiště:

- **Přechodné úložiště** se používá, když je při restartování kontejneru možné celý stav kontejneru zlikvidovat. Běžně se používá při vytváření předváděcích prostředí nebo při vývoji se samostatnými správci front.
- **Trvalé úložiště** je běžná konfigurace produktu IBM MQ, která zajišťuje, že pokud je kontejner restartován, budou v restartovaném kontejneru existující konfigurace, protokoly a trvalé zprávy k dispozici.

IBM MQ Opertor poskytuje schopnost pro přizpůsobení charakteristik úložiště, které se mohou výrazně lišit v závislosti na prostředí a požadovaném režimu úložiště.

Přechodné úložiště

Produkt IBM MQ je stavová aplikace a uchovává tento stav pro úložiště pro zotavení v případě restartování. Pokud se použije přechodné úložiště, bude při restartu ztracen celý stav správce front. To zahrnuje:

- Všechny zprávy.
- Všichni správci front do stavu komunikace správce front (pořadová čísla zpráv kanálu).
- Identitu klastru MQ správce front.
- Stav všech transakcí.
- Konfiguraci všech správců front.
- Všechna lokální diagnostická data.

Z tohoto důvodu byste měli zvážit, zda přechodné úložiště je vhodný přístup pro scénář produkce, testování nebo vývoje. Například u všech zpráv, u nichž je známo, že jsou dočasné a že správce front není členem klastru MQ. Kromě likvidace veškerého stavu systému zpráv při restartu, bude také vyřazena konfigurace správce front. Chcete-li povolit úplně přechodný kontejner, musí být konfigurace produktu IBM MQ přidána do samotného kontejnerového obrazu (další informace viz “Sestavení obrazu s vlastními soubory MQSC a INI, pomocí rozhraní OpenShift CLI” na stránce 21). Není-li tento proces dokončen, bude muset být při každém restartování kontejneru nakonfigurován produkt IBM MQ.

Chcete-li např. nakonfigurovat produkt IBM MQ s přechodným úložištěm, měl by typ úložiště `QueueManager` obsahovat následující:

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

Trvalé úložiště

Produkt IBM MQ za normálních okolností pracuje s trvalým úložištěm, aby bylo zajištěno, že správce front zachová své trvalé zprávy a konfiguraci po restartu. Proto se jedná o výchozí chování. Kvůli různým poskytovatelům úložiště a různým schopnostem každé podpory to často znamená, že je nezbytné přizpůsobit konfiguraci. Níže jsou uvedena společná pole, které upravují konfiguraci úložiště MQ v rozhraní v1beta1 API:

- spec.queueManager.availability řídí režim dostupnosti. Používáte-li `SingleInstance`, vyžadujete pouze úložiště `ReadWriteOnce`, zatímco `multiInstance` vyžaduje paměťovou třídu, která podporuje `ReadWriteMany` se správnými charakteristikami zamykání souborů. IBM MQ poskytuje prohlášení o podpoře a prohlášení o testování. Režim dostupnosti má také vliv na rozvržení trvalého svazku. Další informace viz “Vysoká dostupnost pro IBM MQ Advanced certified container” na stránce 10.
- spec.queueManager.storage řídí nastavení individuálního úložiště. Správce front lze nakonfigurovat tak, aby používal jeden až čtyři trvalé svazky.

V následujícím příkladu je zobrazen úsek jednoduché konfigurace pomocí správce front s jednou instancí:

```
spec:
  queueManager:
    storage:
      queueManager:
        enabled: true
```

V následujícím příkladu je zobrazen úsek kódu konfigurace správce front s více instancemi, s jinou než výchozí třídou úložiště a s úložištěm souborů vyžadujícím doplňkové skupiny:

```
spec:
  queueManager:
    availability:
      type: MultiInstance
    storage:
      queueManager:
        enabled: true
        class: ibmc-file-gold-gid
          persistedData:
            enabled: true
            class: ibmc-file-gold-gid
          recoveryLogs:
            enabled: true
            class: ibmc-file-gold-gid
     securityContext:
       supplementalGroups: [99]
```

Linux MQ Adv. CD Vysoká dostupnost pro IBM MQ Advanced certified container

K dispozici máte dvě hlavní volby vysoké dostupnosti: IBM MQ Advanced certified container: **Správce front s více instancemi** (což je dvojice aktivní-pohotovostní, využívající sdílený síťový systém souborů) a **Jeden odolný správce front** (který nabízí jednoduchý přístup pro vysokou dostupnost používající síťové úložiště).

Měli byste zvážit mít dostupnost pro **zprávy** a **služby** odděleně. S IBM MQ for Multiplatforms je zpráva uložena přesně do jednoho správce front. Takže pokud se tento správce front stane nedostupným, dočasně ztratíte přístup ke zprávám, které obsahuje. Chcete-li dosáhnout vysoké dostupnosti `zprávy`, musíte být schopni obnovit správce front co nejrychleji. Dostupnost `služby` můžete dosáhnout tím, že budete mít více instancí front pro aplikace klienta, které se mají používat, například pomocí uniformního klastru IBM MQ.

Správce front lze považovat za dvě části: data uložená na disku a běžící procesy, které umožňují přístup k datům. Libovolného správce front lze přesunout do jiného uzlu Kubernetes, pokud uchovává stejná data (poskytovaná Trvalými svazky Kubernetes) a je stále síťově adresovatelný v aplikacemi klienta. V Kubernetes je služba použita k poskytnutí konzistentní sítě identity.

IBM MQ spoléhá na dostupnost dat na trvalých svazcích. Dostupnost úložiště poskytujícího trvalé svazky je proto rozhodující pro dostupnost správce front, neboť produkt IBM MQ nemůže být dostupnější než úložiště, které používá. Chcete-li tolerovat výpadek celé zóny dostupnosti, je třeba použít poskytovatele svazků, který replikuje zápisy na disk do jiné zóny.

Správce front s více instancemi

Správce front s více instancemi zahrnují **aktivní** a **pohotovostní** Pody Kubernetes, které se spouštějí jako součást stavové sady Kubernetes s přesně dvěma replikami a sadou trvalých svazků Kubernetes.

Protokoly a data transakcí správce front jsou drženy ve dvou trvalých svazcích za použití sdíleného systému souborů.

Správci front s více instancemi vyžadují **aktivní** i **pohotovostní** Pody, aby měli souběžný přístup k trvalému svazku. Chcete-li provést konfiguraci, použijte trvalé svazky Kubernetes s parametrem **`access mode`** nastaveným na `ReadWriteMany`. Svazky musí také splňovat IBM MQ požadavky pro sdílené systémy souborů, protože produkt IBM MQ spoléhá na automatické uvolnění zámků souborů k podněcování překonání selhání správce front. IBM MQ produkuje seznam testovaných systémů souborů.

Doby obnovy pro správce front s více instancemi jsou řízeny následujícími faktory:

1. Jak dlouho trvá, než dojde k selhání sdíleného systému souborů, aby uvolnil zámky původně provedené aktivní instancí.
2. Jak dlouho trvá, než pohotovostní instance získá zámky, a pak se spustí.
3. Jak dlouho trvá sondě připravenosti Podu Kubernetes zjistit, že je kontejner připraven. Toto lze konfigurovat v grafu Helm .
4. Jak dlouho trvá, než se klienti IBM MQ znovu připojí.

Jeden odolný správce front

Jeden odolný správce front je jedna instance správce front spuštěná v jednom podu Kubernetes, kde Kubernetes monitoruje správce front a v případě potřeby pod nahradí.

Požadavky IBM MQ pro sdílené systémů souborů také platí pro použití jednoho odolného správce front (s výjimkou zamykání na základě nájmů), u něhož ale nepotřebujete sdílený systém souborů. Úložiště bloků můžete používat s vhodným završujícím systémem souborů. Např. *xfs* nebo *ext4*.

Doby obnovy pro jednoho odolného správce front jsou řízeny následujícími faktory:

1. Jak dlouho trvá spuštění sondy živosti a kolik chyb toleruje. Toto lze konfigurovat v grafu Helm .
2. Jak dlouho trvá plánovači Kubernetes znovu na novém uzlu naplánovat nezdařený Pod.
3. Jak dlouho trvá stažení kontejnerového obrazu do nového uzlu. Použijete-li hodnotu **`imagePullPolicy`** parametru `IfNotPresent`, může tento obraz již v daném uzlu existovat.
4. Jak dlouho trvá, než se nová instance správce front spustí.
5. Jak dlouho trvá sondě připravenosti Podu Kubernetes zjistit, že je kontejner připraven. Toto lze konfigurovat v grafu Helm .
6. Jak dlouho trvá, než se klienti IBM MQ znovu připojí.

Důležité:

Ačkoli vzor jednoho odolného správce front nabízí některé výhody, je třeba porozumět tomu, zda lze dosáhnout cílů dostupnosti s omezeními v souvislosti se selháními uzlu.

V Kubernetes je selhaný Pod obvykle rychle obnoven, ale selhání celého uzlu se zpracovává jinak. Pokud hlavní uzel Kubernetes ztratí kontakt s pracovním uzlem, nemůže rozlišit, zda došlo k selhání uzlu nebo jen ke ztrátě síťové konektivity. Proto Kubernetes v tomto případě neprovede **žádnou akci**, dokud se nevyskytne jedna z následujících událostí:

1. Uzel se obnoví do stavu, v němž může hlavní uzel Kubernetes s ním komunikovat.
2. Je provedena administrativní akce, která explicitně odstraní Pod v hlavním uzlu Kubernetes. Spuštěný Pod se nemusí nutně zastavit, stačí jej odstranit z úložiště Kubernetes. Tuto administrativní akci je proto třeba velmi pečlivě zvážit.

Související pojmy

Konfigurace vysoké dostupnosti

Linux MQ Adv. CD Ověření uživatele a autorizace pro produkt IBM MQ Advanced certified container

Produkt IBM MQ může být nakonfigurován pro použití uživatelů a skupin LDAP k autorizaci. Toto je doporučený přístup pro produkt IBM MQ Advanced certified container.

V kontejnerizovaném prostředí s více nájemci, jako např. Red Hat OpenShift Container Platform, jsou zavedena omezení zabezpečení, aby se zabránilo možným problémům zabezpečení. Například v produktu Red Hat OpenShift Container Platform výchozí objekt `SecurityContextConstraints` (označovaný `restricted`) používá náhodné ID uživatele, což odrazuje všechny uživatele lokální pro samotný kontejner. Produkt IBM MQ obvykle používá eskalace oprávnění ke kontrole hesel uživatelů, což se také nedoporučuje v prostředích kontejnerů s více nájemci. Z těchto důvodů není použití uživatelů definovaných v knihovnách operačního systému uvnitř spuštěného kontejneru podporováno v certifikovaných kontejnerech produktu IBM MQ.

Je třeba nakonfigurovat správce front tak, aby používal protokol LDAP k ověření a autorizaci uživatele. Informace o konfiguraci produktu IBM MQ viz Ověření připojení: Úložiště uživatelů a Autorizace LDAP

Linux MQ Adv. CD V 9.1.5 Instalace a odinstalace produktu IBM MQ Operator on OpenShift

Produkt IBM MQ Operator lze nainstalovat do OpenShift pomocí Operator Hub.

Než začnete

Procedura

- “Instalace produktu IBM MQ Operator pomocí OpenShift CLI” na stránce 13.
- “Instalace produktu IBM MQ Operator pomocí webové konzoly OpenShift” na stránce 12.

Linux MQ Adv. CD V 9.1.5 Instalace produktu IBM MQ Operator pomocí webové konzoly OpenShift

Produkt IBM MQ Operator lze nainstalovat do OpenShift pomocí Operator Hub.

Než začnete

Přihlaste se k webové konzole klastru OpenShift.

Postup

1. Přidejte operátory IBM Common Services do seznamu instalovatelných operátorů.
   a) Klepněte na ikonu plus. Zobrazí se dialogové okno **Importovat YAML**.
   b) Vložte následující definici prostředku v dialogovém okně.

```
apiVersion: operators.coreos.com/v1alpha1
kind: CatalogSource
metadata:
  name: opencloud-operators
  namespace: openshift-marketplace
spec:
  displayName: IBMCS Operators
  publisher: IBM
  sourceType: grpc
  image: docker.io/ibmcom/ibm-common-service-catalog:latest
  updateStrategy:
    registryPoll:
      interval: 45m
```

   c) Klepněte na volbu **Vytvořit**.

2. Přidejte operátory IBM do seznamu instalovatelných operátorů.
   a) Klepněte na ikonu plus. Zobrazí se dialogové okno **Importovat YAML**.
   b) Vložte následující definici prostředku v dialogovém okně.

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

   c) Klepněte na volbu **Vytvořit**.
3. Vytvořte obor názvů, který se má použít pro IBM MQ Operator.

   IBM MQ Operator lze nainstalovat s vymezeným rozsahem do jednoho nebo všech oborů názvů. Tento krok je nezbytný pouze v případě, že chcete instalovat do konkrétního oboru názvů, který ještě neexistuje.
   a) V navigačním podokně klepněte na volbu **Domů** > **Projekty**.

      Zobrazí se stránka Projekty.
   b) Klepněte na volbu **Vytvořit projekt**. Zobrazí se oblast Vytvořit projekt.
   c) Zadejte podrobnosti o oboru názvů, který vytváříte. Např. můžete určit "ibm-mq" jako název.
   d) Klepněte na volbu **Vytvořit**. Vytvoří se obor názvů pro IBM MQ Operator.
4. Nainstalujte IBM MQ Operator.
   a) V navigačním podokně klepněte na volbu **Operators** > **OperatorHub**.

      Zobrazí se stránka OperatorHub.
   b) Do pole **Všechny položky** zadejte hodnotu "IBM MQ".

      Zobrazí se položka katalogu IBM MQ.
   c) Vyberte volbu **IBM MQ**.

      Zobrazí se okno IBM MQ.
   d) Klepněte na volbu **Instalovat**.

      Zobrazí se stránka Vytvořit odběr operátoru.
   e) Nastavte Režim instalace buď na specifický obor názvů, který jste vytvořili, nebo na rozsah celého klastru.
   f) Klepněte na volbu **Odebírat**.

      Na stránce Instalované operátory uvidíte IBM MQ.
   g) Zkontrolujte stav operátoru na stránce Instalované operátory, stav se změní po dokončení instalace na Succeeded.

Jak pokračovat dále

“Implementace certifikovaných kontejnerů produktu IBM MQ” na stránce 15

Instalace produktu IBM MQ Operator pomocí OpenShift CLI

Produkt IBM MQ Operator lze nainstalovat do OpenShift pomocí Operator Hub.

Než začnete

Přihlaste se do rozhraní příkazového řádku (CLI) OpenShift pomocí **oc login**. V rámci těchto kroků budete muset být administrátorem klastru.

Postup

1. Vytvořte OperatorSource pro operátory IBM Common Services
   a) Vytvořit soubor YAML definující prostředek OperatorSource

      Vytvořte soubor s názvem "operator-source-cs.yaml" s následujícím obsahem:

      ```
      apiVersion: operators.coreos.com/v1alpha1
      kind: CatalogSource
      metadata:
        name: opencloud-operators
        namespace: openshift-marketplace
      spec:
        displayName: IBMCS Operators
        publisher: IBM
        sourceType: grpc
        image: docker.io/ibmcom/ibm-common-service-catalog:latest
        updateStrategy:
          registryPoll:
            interval: 45m
      ```

   b) Použijte OperatorSource na server.

      ```
      oc apply -f operator-source-cs.yaml -n openshift-marketplace
      ```

2. Vytvořte OperatorSource pro operátory IBM.
   a) Vytvořit soubor YAML definující prostředek OperatorSource

      Vytvořte soubor s názvem "operator-source-ibm.yaml" s následujícím obsahem:

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

   b) Použijte OperatorSource na server.

      ```
      oc apply -f operator-source-ibm.yaml -n openshift-marketplace
      ```

3. Vytvořte obor názvů, který se má použít pro IBM MQ Operator.

   IBM MQ Operator lze nainstalovat s vymezeným rozsahem do jednoho nebo všech oborů názvů. Tento krok je nezbytný pouze v případě, že chcete instalovat do konkrétního oboru názvů, který ještě neexistuje.

   ```
   oc new-project ibm-mq
   ```

4. Zobrazte seznam operátorů dostupných pro klastr z OperatorHub.

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

5. Zkontrolujte IBM MQ Operator a ověřte jeho podporované režimy InstallModes a dostupné kanály.

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

6. Vytvořit soubor YAML objektu OperatorGroup

`OperatorGroup` je prostředek OLM, který vybírá cílové obory názvů, v nichž se má generovat požadovaný přístup RBAC pro všechny operátory ve stejném oboru názvů jako server `OperatorGroup`.

Obor názvů, k němuž se přihlašujete k odběru, musí mít `OperatorGroup` odpovídající operátoru `InstallMode`, ať už v režimu `AllNamespaces`, nebo `SingleNamespace`. Pokud operátor, který zamýšlíte instalovat, používá `AllNamespaces`, pak již má obor názvů `openshift-operators` příslušnou skupinu OperatorGroup na místě.

Pokud však operátor používá režim `SingleNamespace` a vy dosud nemáte příslušnou skupinu `OperatorGroup` na místě, je nutné ji vytvořit.

a) Vytvořte soubor s názvem "mq-operator-group.yaml" s následujícím obsahem:

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: <operatorgroup_name>
  namespace: <namespace>
spec:
  targetNamespaces:
  - <namespace>
```

b) Vytvořit objekt `OperatorGroup`

```
oc apply -f mq-operator-group.yaml
```

7. Vytvořte soubor YAML objektu odběru pro odběr oboru názvů pro MQ Operator.

a) Vytvořte soubor s názvem "mq-sub. yaml" s následujícím obsahem:

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: ibm-mq
  namespace: openshift-operators
spec:
  channel:
  name: ibm-mq
  source: ibm-operator-catalog
  sourceNamespace: openshift-marketplace
```

Pro použití prostoru `AllNamespaces` **`InstallMode`** zadejte obor názvů `openshift-operators` . Jinak uveďte jeden příslušný obor názvů pro použití `Jednoho oboru názvů` **`InstallMode`**.

b) Vytvořit objekt `Subscription`

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

8. Zkontrolovat stav operátora

Jakmile je instalace operátora úspěšná, stav podu se zobrazí jako *Spuštěný*. Pro použití `Všech oborů názvů` **`InstallMode`** uveďte jako obor názvů **`openshift-operators`**. Jinak uveďte jeden příslušný obor názvů pro použití `Jednoho oboru názvů` **`InstallMode`**.

Jak pokračovat dále

“Implementace certifikovaných kontejnerů produktu IBM MQ” na stránce 15

Linux MQ Adv. CD

Implementace certifikovaných kontejnerů produktu IBM MQ

IBM MQ verze 9.1.5 a vyšší je možné implementovat do produktu Red Hat OpenShift pomocí operátoru IBM MQ . Produkt IBM MQ verze 9.1.5 a 9.1.4 lze implementovat do produktu Red Hat OpenShift pomocí volby Helm. Starší verze CD lze implementovat do klastru IBM Cloud Private nebo do klastru IBM Cloud Kubernetes Service pomocí Helm.

Informace o této úloze

Procedura

- “Implementace správce front pomocí rozhraní CLI Helm” na stránce 24.
- “Implementace předchozích verzí CD produktu IBM MQ do klastru IBM Cloud Private” na stránce 26.
- “Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Private” na stránce 28.
- “Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Kubernetes Service” na stránce 29.

Linux MQ Adv. CD Příprava projektu OpenShift pro produkt IBM MQ pomocí rozhraní OpenShift CLI

Připravte si klastr Red Hat OpenShift Container Platform tak, aby byl připraven implementovat správce front pomocí IBM MQ Operator. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Poznámka: Plánujete-li použít produkt IBM MQ v projektu s dalšími již nainstalovanými komponentami produktu IBM Cloud Pak for Integration, nemusíte se těmito pokyny řídit.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Informace o této úloze

Obrazy IBM MQ Advanced certified container se stahují z registru kontejnerů, který provádí kontrolu licenčních oprávnění. Tato kontrola vyžaduje klíč oprávnění, který je uložen v tajném údaji stažení `docker-registry`. Nemáte-li ještě klíč oprávnění, postupujte podle těchto pokynů, abyste získali klíč oprávnění a vytvořili tajný údaj stažení.

Postup

1. Získejte klíč oprávnění, který je přiřazen k vašemu ID.
   a) Přihlaste se k MyIBM Container Software Library s ID a heslem IBM přidruženým k oprávněnému softwaru.
   b) V sekci **Klíče oprávnění** vyberte **Kopírovat klíč** ke zkopírování klíče oprávnění do schránky (clipboardu).
2. Vytvořte tajný údaj obsahující váš klíč oprávnění, v projektu, kam chcete implementovat správce front.
   Spusťte následující příkaz, kde *<entitlement-key>* je klíč načtený v kroku 1, a *<user-email>* je ID IBM přidružené k oprávněnému softwaru.

```
oc create secret docker-registry ibm-entitlement-key \
--docker-server=cp.icr.io \
--docker-username=cp \
--docker-password=<entitlement-key> \
--docker-email=<user-email>
```

Jak pokračovat dále

“Implementace správce front pomocí rozhraní OpenShift CLI” na stránce 18

Linux MQ Adv. CD V 9.1.5 Implementace správce front pomocí produktu IBM Cloud Pak for Integration Platform Navigator

Pomocí vlastního prostředku správce front implementujte správce front do klastru Red Hat OpenShift Container Platform pomocí produktu IBM Cloud Pak for Integration Platform Navigator. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

V prohlížeči spusťte produkt IBM Cloud Pak for Integration Platform Navigator.

Jedná-li se o první implementaci správce front do tohoto projektu Red Hat OpenShift, postupujte podle kroků pro “Příprava projektu OpenShift pro produkt IBM MQ pomocí rozhraní OpenShift CLI” na stránce 16.

Postup

1. Implementujte správce front.

   Následující příklad implementuje základního "quick start" správce front, který používá přechodné (dočasné) úložiště a vypíná zabezpečení MQ. Zprávy nebudou po restartu správce front zachovány. Konfiguraci můžete upravit tak, aby bylo možné změnit mnoho nastavení správce front.

   a) V produktu IBM Cloud Pak for Integration Platform Navigator klepněte na volbu **Běhové prostředí a instance**.

   b) Klepněte na volbu **Vytvořit instanci**.

   c) Vyberte **Správce front** a klepněte na tlačítko **Další**.

   Zobrazí se formulář pro vytvoření instance `QueueManager`.

   Poznámka: Můžete také klepnout na volbu **Kód** a zobrazit nebo změnit konfiguraci `QueueManager` YAML.

   d) V sekci **Podrobnosti** zkontrolujte nebo aktualizujte pole **Název** a zadejte **Obor názvů**, ve kterém se má vytvořit instance správce front.

   e) Jestliže přijmete licenční smlouvu produktu IBM Cloud Pak for Integration, změňte volbu **Přijetí licence** na hodnotu **Zapnuto**.

   Chcete-li implementovat správce front, musíte přijmout licenci.

   f) V sekci **Konfigurace správce front** zkontrolujte nebo aktualizujte **Název** základního správce front.

   Standardně se název správce front používaného aplikacemi klienta IBM MQ bude shodovat s názvem `QueueManager`, ale s odebranými neplatnými znaky (jako jsou pomlčky). Chcete-li vynutit použití určitého názvu, můžete jej upravit zde.

   g) Klepněte na volbu **Vytvořit**.

   Nyní je zobrazen seznam správců front v aktuálním projektu (obor názvů). Nový správce `QueueManager` by měl mít stav `Pending`.

2. Zkontrolujte, zda je správce front spuštěn.

   Vytvoření je dokončeno, když stav `QueueManager` je `Running`.

Související úlohy

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

Linux MQ Adv. CD V 9.1.5 Implementace správce front pomocí webové konzoly OpenShift

Pomocí vlastního prostředku správce front implementujte správce front do klastru Red Hat OpenShift Container Platform pomocí webové konzoly Red Hat OpenShift. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Přihlaste se k webové konzole klastru OpenShift. Budete muset vybrat existující projekt (obor názvů), který se má použít, nebo vytvořit nový projekt.

Jedná-li se o první implementaci správce front do tohoto projektu Red Hat OpenShift, postupujte podle kroků pro “Příprava projektu OpenShift pro produkt IBM MQ pomocí rozhraní OpenShift CLI” na stránce 16.

Postup

1. Implementujte správce front.

   Následující příklad implementuje základního "quick start" správce front, který používá přechodné (dočasné) úložiště a vypíná zabezpečení MQ. Zprávy nebudou po restartu správce front zachovány. Konfiguraci můžete upravit tak, aby bylo možné změnit mnoho nastavení správce front.

   a) V rámci webové konzoly OpenShift klepněte v navigačním podokně na nabídku **Operátory** > **Instalované operátory**.

   b) Klepněte na volbu **IBM MQ**.

   c) Klepněte na kartu **Správce front**.

   d) Klepněte na tlačítko **Vytvořit správce front**.

   Zobrazí se editor YAML obsahující příklad YAML pro prostředek `QueueManager`.

   Poznámka: Můžete také klepnout na volbu **Upravit formulář** a zobrazit nebo změnit konfiguraci `QueueManager`.

   e) Jestliže přijmete licenční smlouvu, změňte volbu **Přijetí licence** na hodnotu **Zapnuto**.

   Produkt IBM MQ je k dispozici pod několika různými licencemi. Další informace o platných licencích viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 39. Chcete-li implementovat správce front, musíte přijmout licenci.

   f) Klepněte na volbu **Vytvořit**.

   Nyní je zobrazen seznam správců front v aktuálním projektu (obor názvů). Nový správce `QueueManager` by měl být ve stavu `Pending`.

2. Zkontrolujte, zda je správce front spuštěn.

   Vytvoření je dokončeno, když stav `QueueManager` je `Running`.

Související úlohy

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

Linux MQ Adv. CD V 9.1.5 Implementace správce front pomocí rozhraní OpenShift CLI

Pomocí vlastního prostředku správce front implementujte správce front do klastru Red Hat OpenShift Container Platform pomocí rozhraní příkazového řádku (CLI). Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Musíte nainstalovat rozhraní příkazového řádku Red Hat OpenShift Container Platform.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Jedná-li se o první implementaci správce front do tohoto projektu Red Hat OpenShift, postupujte podle kroků pro “Příprava projektu OpenShift pro produkt IBM MQ pomocí rozhraní OpenShift CLI” na stránce 16.

Postup

1. Implementujte správce front.

   Následující příklad implementuje základního "quick start" správce front, který používá přechodné (dočasné) úložiště a vypíná zabezpečení MQ. Zprávy nebudou po restartu správce front zachovány. Obsah YAML můžete upravit tak, aby bylo možné změnit mnoho nastavení správce front.

   a) Vytvořit soubor YAML produktu `QueueManager`

   Chcete-li například nainstalovat základního správce front v IBM Cloud Pak for Integration, vytvořte soubor "mq-quickstart.yaml" s následujícím obsahem:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart-cp4i
spec:
  version: 9.1.5.0-r2
  license:
    accept: false
    license: L-RJON-BN7PN3
    use: NonProduction
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
      queueManager:
        type: ephemeral
  template:
    pod:
      containers:
       - name: qmgr
         env:
         - name: MQSNOAUT
           value: "yes"
```

   Důležité: Souhlasíte-li s licenční smlouvou IBM Cloud Pak for Integration, změňte `accept: false` na `accept: true`. Podrobnosti o licenci viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 39 .

   Tento příklad také zahrnuje webový server implementovaný se správcem front, s webovou konzolou povolenou pomocí jednotného přihlášení s produktem Cloud Pak Identity and Access Manager.

   Chcete-li nainstalovat základního správce front nezávisle na produktu IBM Cloud Pak for Integration, vytvořte soubor "mq-quickstart.yaml" s následujícím obsahem:

```
apiVersion: mq.ibm.com/v1beta1
kind: QueueManager
metadata:
  name: quickstart
spec:
  version: 9.1.5.0-r2
  license:
    accept: false
    license: L-APIG-BM7GDH
    use: Development
  web:
    enabled: true
  queueManager:
    name: "QUICKSTART"
    storage:
```

```
      queueManager:
        type: ephemeral
  template:
    pod:
      containers:
       - name: qmgr
         env:
         - name: MQSNOAUT
           value: "yes"
```

Důležité: Pokud přijmete licenční smlouvu produktu MQ, změňte `accept: false` na `accept: true`. Podrobnosti o licenci viz “Odkaz na licenci pro mq.ibm.com/v1beta1” na stránce 39 .

b) Vytvořit objekt `QueueManager`

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

2. Zkontrolujte, zda je správce front spuštěn.

   Implementaci můžete ověřit spuštěním

   ```
   oc describe queuemanager <QueueManagerResourceName>
   ```

   a následnou kontrolou stavu.

   Např. spusťte

   ```
   oc describe queuemanager quickstart
   ```

   a zkontrolujte, že pole `status.Phase` udává `Running`

Související úlohy

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

V 9.1.4 Linux MQ Adv. CD

Integrace s IBM Cloud Pak for Integration Operations Dashboard

Schopnost trasovat transakce pomocí produktu IBM Cloud Pak for Integration je poskytována produktem Operations Dashboard.

Informace o této úloze

Povolení integrace s produktem Operations Dashboard instaluje uživatelskou proceduru rozhraní MQ API do správce front. Uživatelská procedura rozhraní API odešle data trasování do datového úložiště Operations Dashboard; o zprávách, které jsou posílány prostřednictvím správce front.

Mějte na zřeteli, že jsou trasovány pouze zprávy, které jsou odesílány pomocí vazeb klienta MQ.

Postup

1. Implementujte správce front s povoleným trasováním.

   Standardně je funkce trasování zakázána.

   Implementujete-li pomocí produktu IBM Cloud Pak for Integration Platform Navigator, potom můžete povolit trasování při implementaci nastavením volby **Povolit trasování** na **Zapnuto** a nastavením **Obor názvů trasování** na obor názvů, kde je nainstalován produktu Operations Dashboard. Podrobnější informace o implementaci správce front viz “Implementace správce front pomocí produktu IBM Cloud Pak for Integration Platform Navigator” na stránce 17

Implementujete-li pomocí rozhraní OpenShift CLI nebo webové konzoly OpenShift, potom můžete povolit trasování s následujícím úsekem kódu YAML:

```
spec:
  tracing:
    enabled: true
    namespace: <Operations_Dashboard_Namespace
```

Pokud provádíte implementaci pomocí Helm, můžete povolit trasování nastavením od`TracingConfig.enabled=true` a od`TracingNamespace=`*<Operations_Dashboard_Namespace*. Chcete-li povolit integraci produktu Operations Dashboard do existujícího správce front, můžete toto nastavení použít při přechodu na vyšší verzi vydání Helm .

Důležité: Správce front se nespustí, dokud produkt MQ nebude registrován s produktem Operations Dashboard (viz další krok).

Mějte na zřeteli, že když je tato funkce povolena, spustí se kromě kontejneru správce front dva rozšiřující (tzv. sidecar) kontejnery ("Agent" a "Collector"). Obrazy pro tyto dva rozšiřující kontejnery budou k dispozici ve stejném registru jako hlavní obraz MQ a budou používat stejnou zásadu stažení a tajný údaj stažení. K dispozici jsou další nastavení konfigurace limitů CPU a paměti.

2. Pokud se jedná o první správce front s integrací produktu Operations Dashboard, který byl implementován v tomto oboru názvů, pak musíte Registrovat s produktem Operations Dashboard.

   Registrace vytvoří objekt Tajný údaj, který musí Pod správce front úspěšně spustit.

Linux MQ Adv. CD V 9.1.5 Sestavení obrazu s vlastními soubory MQSC a INI, pomocí rozhraní OpenShift CLI

Pomocí propojení (pipeline) vytvoříte v platformě Red Hat OpenShift Container Platform nový kontejnerový obraz IBM MQ se soubory MQSC a INI, které mají správci front používající tento obraz aplikovat. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Musíte nainstalovat rozhraní příkazového řádku Red Hat OpenShift Container Platform.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Nemáte-li v projektu Red Hat OpenShift OpenShift Secret pro produkt IBM Entitled Registry, postupujte podle kroků pro “Příprava projektu OpenShift pro produkt IBM MQ pomocí rozhraní OpenShift CLI” na stránce 16.

Postup

1. Vytvořit `ImageStream`

   Proud obrazu a jeho přidružené značky poskytují abstrakci pro odkazování na kontejnerové obrazy z produktu Red Hat OpenShift Container Platform. Proud obrazu a jeho značky vám umožňují zjistit, jaké obrazy jsou k dispozici, a ujistit se, že používáte specifický obraz, který potřebujete, i když se obraz v úložišti změní.

   ```
   oc create imagestream mymq
   ```

2. Vytvořit `BuildConfig` pro nový obraz

   Produkt `BuildConfig` umožní sestavení pro váš nový obraz, který nebude založen na oficiálních obrazech IBM, ale přidá všechny soubory MQSC nebo INI, které chcete spustit při spuštění kontejneru.

   a) Vytvořit soubor YAML definující prostředek `BuildConfig`

      Např. vytvořte soubor s názvem "mq-build-config.yaml" s následujícím obsahem:

```
apiVersion: build.openshift.io/v1
kind: BuildConfig
metadata:
  name: mymq
spec:
  source:
    dockerfile: |-
      FROM cp.icr.io/cp/ibm-mqadvanced-server-integration:9.1.5.0-r2-amd64
      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:9.1.5.0-r2-amd64"
      pullSecret:
        name: ibm-entitlement-key
  output:
    to:
      kind: ImageStreamTag
      name: 'mymq:latest-amd64'
```

Budete muset nahradit dvě místa, kde je základní produkt IBM MQ uveden, aby ukazoval na správný základní obraz pro verzi a opravu, kterou chcete použít. Při aplikování oprav budete muset tyto kroky zopakovat, abyste znovu sestavili obraz.

Tento příklad vytvoří nový obraz založený na oficiálním obrazu IBM a přidá soubory s názvem „my.mqsc“ a „my.in“ do adresáře `/etc/mqm`. Všechny soubory MQSC nebo INI nalezené v tomto adresáři budou při spuštění použity kontejnerem. Soubory INI se aplikují pomocí volby **`crtmqm -ii`** a sloučí se s existujícími soubory INI. Soubory MQSC jsou použity v abecedním pořadí.

Je důležité, aby byly vaše příkazy MQSC opakovatelné, protože budou spuštěny *vždy*, když se spustí správce front. To obvykle znamená přidání parametru `REPLACE` do všech příkazů `DEFINE` a přidání parametru `IGNSTATE(YES)` do všech příkazů `START` nebo `STOP`.

b) Použijte `BuildConfig` na server.

```
oc apply -f mq-build-config.yaml
```

3. Spusťte sestavení k vytvoření obrazu.

a) Spusťte sestavení.

```
oc start-build mymq
```

Měl by se zobrazit výstup podobný tomuto:

```
build.build.openshift.io/mymq-1 started
```

b) Zkontrolujte stav sestavení.
Můžete například spustit následující příkaz s použitím identifikátoru sestavení vráceného v předchozím kroku:

```
oc describe build mymq-1
```

4. Implementujte správce front pomocí nového obrazu.

Postupujte podle kroků popsaných v tématu “Implementace správce front pomocí rozhraní OpenShift CLI” na stránce 18 a přidejte nový vlastní obraz do YAML.

Měli byste přidat následující úsek kódu YAML do normálního `QueueManager` YAML, kde *můj-obor-názvů* je projekt/obor názvů OpenShift, který používáte, a *obraz* je název obrazu, který jste vytvořili dříve (např. "mymq:latest-amd64"):

```
spec:
  queueManager:
    image: image-registry.openshift-image-registry.svc:5000/my-namespace/my-image
```

Související úlohy

“Implementace správce front pomocí rozhraní OpenShift CLI” na stránce 18
Pomocí vlastního prostředku správce front implementujte správce front do klastru Red Hat OpenShift Container Platform pomocí rozhraní příkazového řádku (CLI). Tuto úlohu by měl dokončit administrátor projektu.

Linux MQ Adv. CD Implementace certifikovaných kontejnerů produktu IBM MQ pomocí Helm

V produktu IBM MQ 9.1.5.0je doporučeným způsobem implementace správce front používat operátor IBM MQ . Produkt IBM MQ 9.1.5.0 a předchozí vydání CD lze implementovat pomocí Helmpomocí následujících pokynů.

Informace o této úloze

Procedura

- “Příprava klastru OpenShift pro produkt IBM MQ v systému OpenShift pomocí volby Helm” na stránce 23.
- “Implementace správce front pomocí rozhraní CLI Helm” na stránce 24.

Linux MQ Adv. CD Příprava klastru OpenShift pro produkt IBM MQ v systému OpenShift pomocí volby Helm

Připravte klastr platformy kontejneru produktu Red Hat OpenShift tak, aby byl připraven k implementaci správce front pomocí volby Helm. Tato úloha by měla být dokončena administrátorem klastru.

Než začnete

Poznámka: Pokud používáte produkt IBM Cloud Pak for Integration, měl by instalační program pro vás připravit projekt OpenShift (obor názvů), který má být použit s produktem IBM MQ, takže nebudete muset postupovat podle těchto pokynů.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Postup

1. Ujistěte se, že jste přidali úložiště IBM Helm do své lokální kopie Helm.
   Můžete například spustit následující příkaz:

   ```
   helm repo add ibm-entitled-charts https://raw.githubusercontent.com/IBM/charts/master/repo/entitled
   ```

2. Ujistěte se, že máte server Helm (s názvem "Tiller") instalované ve vašem klastru.

   Postupujte podle pokynů v tématu Začínáme s Helm na OpenShift , abyste nainstalovali Helm na váš klastr.
3. Ujistěte se, že servisní účty ve vašem projektu OpenShift (obor názvů) jsou autorizovány pro použití práva SCC (Security Context Constraints).

   V 9.1.5 Produkt IBM MQ pracuje s výchozí SCC "restricted", takže tento krok může být obvykle přeskočen.

   Použití změn SCC vyžaduje, aby byl proveden administrátorem klastru OpenShift . Každá verze grafu Helm má různé požadavky pro SCC, které jsou zdokumentovány v jednotlivých souborech README pro graf Helm :

```
helm inspect readme ibm-entitled-charts/ibm-mqadvanced-server-prod
```

K dispozici jsou instrukce v každém souboru README pro nastavení autorizace pro SCC. Všimněte si, že grafy IBM MQ Helm vytvářejí servisní účet pro své vlastní použití, což znamená, že oprávnění SCC musí být použita na úrovni "group" (pro všechny servisní účty v oboru názvů).

4. Ujistěte se, že máte platný "image tag tay" pro stažení obrázků z vašeho vybraného registru kontejneru

   Obrazy IBM MQ Advanced certified container se stahují z registru kontejnerů, který provádí kontrolu licenčních oprávnění. Tato kontrola vyžaduje klíč oprávnění, který je uložen v tajném údaji stažení `docker-registry`. Nemáte-li ještě klíč oprávnění, postupujte podle těchto pokynů, abyste získali klíč oprávnění a vytvořili tajný údaj stažení.

   a) Získejte klíč oprávnění, který je přiřazen k vašemu ID.

      i) Přihlaste se k MyIBM Container Software Library s ID a heslem IBM přidruženým k oprávněnému softwaru.

      ii) V sekci *Klíče oprávnění* vyberte **Kopírovat klíč** ke zkopírování klíče oprávnění do schránky (clipboardu).

   b) Vytvořte tajný údaj v oboru názvů, do kterého chcete implementovat správce front.

   - Spusťte následující příkaz, kde *<entitlement-key>* je klíč načtený v kroku 1, a *<user-email>* je ID IBM přidružené k oprávněnému softwaru.

     ```
     oc create secret docker-registry ibm-entitlement-key \
     --docker-server=cp.icr.io \
     --docker-username=cp \
     --docker-password=<entitlement-key> \
     --docker-email=<user-email>
     ```

Jak pokračovat dále

“Implementace správce front pomocí rozhraní CLI Helm” na stránce 24

V 9.1.4 Linux MQ Adv. CD Implementace správce front pomocí rozhraní CLI Helm

Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Musíte nainstalovat Helm V2 a Red Hat OpenShift Container Platform rozhraní příkazového řádku. Pokud nepoužíváte IBM Cloud Pak for Integration, postupujte podle kroků pro “Příprava klastru OpenShift pro produkt IBM MQ v systému OpenShift pomocí volby Helm” na stránce 23.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Postup

1. Ujistěte se, že jste přidali úložiště IBM Helm do své lokální kopie Helm.
   Můžete například spustit následující příkaz:

   ```
   helm repo add ibm-entitled-charts https://raw.githubusercontent.com/IBM/charts/master/repo/
   entitled
   ```

2. Zkontrolujte volby konfigurace pro správce front

   Krok implementace zahrnuje jak instalaci, tak kroky konfigurace. Některá nastavení pro správce front musí být nastavena v době implementace a změna těchto nastavení vyžaduje opětné nasazení.

   Můžete zobrazit soubor README grafu Helm a zobrazit podrobnosti o všech dostupných volbách implementace spuštěním jednoho z následujících příkazů:

- Pro IBM MQ Advanced certified container v IBM Cloud Pak for Integration:

```
helm inspect readme ibm-entitled-charts/ibm-mqadvanced-server-integration-prod
```

- Pro produkt IBM MQ Advanced certified container:

```
helm inspect readme ibm-entitled-charts/ibm-mqadvanced-server-prod
```

Obvykle budete potřebovat alespoň následující parametry:

a. Název vydání. Například: `my-release`
b. Vzdálené úložiště Helm . Například: `ibm-entitled-charts`
c. Graf Helm : například `ibm-mqadvanced-server-prod` nebo `ibm-mqadvanced-server-integration-prod`
d. Tajný název obrazu obrazu. Například: `entitled-registry`. Všimněte si, že toto není zapotřebí, pokud provádíte implementaci do předdefinovaného projektu pro MQ v produktu IBM Cloud Pak for Integration

3. Implementujte správce front.

Všimněte si, že standardně se v grafu Helm předpokládá, že máte ve svém klastru platformy Red Hat OpenShift Container Platform nastaven výchozí Úložná třída .

Chcete-li například instalovat základního správce front v produktu IBM Cloud Pak for Integration, spusťte následující příkaz:

```
helm install \
--tls \
--name my-release \
ibm-entitled-charts/ibm-mqadvanced-server-integration-prod \
--set license=accept \
--set tls.hostname=my.cluster \
--set tls.generate=true
```

Do pole `tls.hostname` můžete zadat libovolný název hostitele (toto je povinné pole, ale nebude použito jako v tomto příkladu budeme generovat nový certifikát podepsaný svým držitelem).

Chcete-li instalovat základního správce front nezávisle na produktu IBM Cloud Pak for Integration, můžete spustit následující příkaz:

```
helm install \
--name my-release \
ibm-entitled-charts/ibm-mqadvanced-server-prod \
--set license=accept \
--set image.pullSecret=ibm-entitlement-key
```

Související úlohy

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

Implementace správce front s produktem IBM Cloud File Storagepomocí rozhraní CLI Helm

Vzorový scénář pro použití Helm k implementaci správce front do Red Hat OpenShift na klastru IBM Cloud pomocí IBM Cloud File Storage. Tuto úlohu by měl dokončit administrátor projektu.

Než začnete

Musíte nainstalovat Helm V2 a Red Hat OpenShift Container Platform rozhraní příkazového řádku. Pokud nepoužíváte IBM Cloud Pak for Integration, postupujte podle kroků pro “Příprava klastru OpenShift pro produkt IBM MQ v systému OpenShift pomocí volby Helm” na stránce 23.

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Postup

1. Ujistěte se, že jste přidali úložiště IBM Helm do své lokální kopie Helm.
   Můžete například spustit následující příkaz:

   ```
   helm repo add ibm-entitled-charts https://raw.githubusercontent.com/IBM/charts/master/repo/
   entitled
   ```

2. Implementujte správce front.

   Při použití produktu IBM Cloud File Storagese obvykle zobrazí nejlepší výsledky za použití paměťové třídy produktu `ibmc-file-gold-gid` . Tato třída ukládání umožňuje ukládání dat uživatelům ve správné skupině systémů souborů.

   Chcete-li například instalovat základního správce front v produktu IBM Cloud Pak for Integration, spusťte následující příkaz:

   ```
   helm install \
   --tls \
   --name my-release \
   ibm-entitled-charts/ibm-mqadvanced-server-integration-prod \
   --set license=accept \
   --set tls.hostname=my.cluster \
   --set tls.generate=true \
   --set dataPVC.storageClassName=ibmc-file-gold-gid \
   --set security.context.supplementalGroups={99}
   ```

   Do pole `tls.hostname` můžete zadat libovolný název hostitele (toto je povinné pole, ale zde se zde nepoužívá, protože v tomto příkladu vytváříme nový certifikát podepsaný držitelem).

   Chcete-li instalovat základního správce front nezávisle na produktu IBM Cloud Pak for Integration, můžete spustit následující příkaz:

   ```
   helm install \
   --name my-release \
   ibm-entitled-charts/ibm-mqadvanced-server-prod \
   --set license=accept \
   --set image.pullSecret=ibm-entitlement-key \
   --set dataPVC.storageClassName=ibmc-file-gold-gid \
   --set security.context.supplementalGroups={99}
   ```

Související úlohy

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

Linux MQ Adv. CD Implementace předchozích verzí CD produktu IBM MQ do klastru IBM Cloud Private

Pro verze CD produktu IBM MQ starší než 9.1.4použijte konzolu správy produktu IBM Cloud Private k implementaci správce front do produktu IBM Cloud Private.

Než začnete

Upozornění: V 9.1.4 Tato implementace není podporována v produktu IBM MQ 9.1.4 nebo v novějších verzích.

Tato úloha předpokládá, že jste již přidali obraz IBM MQ do klastru IBM Cloud Private.

Soubor Helm grafu README.md je dostupný z položky katalogu IBM Cloud Private , který se zobrazí po dokončení tohoto dílčího kroku, nebo z příkazového řádku přidáním svého úložiště IBM Cloud Private **local-charts** jako vzdáleného úložiště Helm a spuštěním následujícího příkazu:

```
helm inspect readme remote_repo_name/ibm-mqadvanced-server-prod
```

Musíte mít zásaduPodSecuritynebo SecurityContextConstraint (pro produkt IBM Cloud Private on Red Hat OpenShift), který podporuje nezbytný kontext zabezpečení. Podrobnosti, včetně příkladů, lze nalézt ze souboru Helm chart README.md .

Podrobnosti o způsobu konfigurace vydání Helm lze najít také v souboru Helm README.md grafu.

Poznámka:

- Provádíte-li implementaci do prostředí produktu IBM Cloud Private , které standardně nepodporuje požadovaná nastavení zabezpečení, povolte nasazení podle pokynů v tématu Implementace grafů Helm , které vyžadují zvýšená oprávnění v jiném než výchozím oboru názvů v dokumentaci produktu IBM Cloud Private .
- Používáte-li systém SELinux, musíte splňovat požadavky produktu IBM MQ popsané v tématu Podpora produktuIBM MQ pro systém SELinux na systému Red Hat Enterprise Linux.

Informace o této úloze

Produkt IBM Cloud Private nabízí platformu pro správu lokálně obsažených aplikací, které obsahují kontejnery. Po přidání obrazu produktu IBM MQ do klastru produktu IBM Cloud Private můžete k implementaci správce front použít konzolu pro správu produktu IBM Cloud Private nebo příkazový řádek.

Procedura

- Použití konzoly IBM Cloud Private Management Console
  a) Otevřete konzolu správy produktu IBM Cloud Private ve webovém prohlížeči a klepněte na volbu **Katalog**.

     Další informace naleznete v tématu Přístup ke klastru IBM Cloud Private pomocí konzoly pro správu v dokumentaci produktu IBM Cloud Private .
  b) Vyberte graf ibm-mqadvanced-server-prod ze seznamu.
  c) Vyberte volbu **Konfigurovat**a poté proveďte následující kroky konfigurace:
     a. Zadejte název vydání.
     b. Přečtěte si a přijměte licenční smlouvy.
     c. Pod sekcí **dataPVC** nastavte **storageclass** na požadovanou paměťovou třídu. Ponechte prázdné, chcete-li vybrat výchozí paměťovou třídu.
     d. Pod sekcí **obrázek** nastavte úložiště na úplnou cestu k obrazu. Příklad:

        ```
        mycluster.icp:8500/namespace_name/ibm-mqadvanced-server-prod
        ```

     e. Pod sekcí **obrázek** nastavte značku na značku obrázku. Příklad:

        ```
        9.1.3.0-r1
        ```

     f. Pokud potřebujete Kubernetes tahat utajený údaj pro přístup k obrazového registru, přidejte jej jako **pullSecret**.
     g. V části **queueManager** nastavte název správce front.
  d) Klepnutím na tlačítko **Instalovat** implementujte správce front jako *Helm release*.
- z příkazového řádku,
  a) Nakonfigurujte produkt **cloudctl** pro přístup ke klastru IBM Cloud Private .

Viz téma Instalace rozhraní CLI produktu IBM Cloud Private v dokumentaci produktu IBM Cloud Private .

b) Ujistěte se, že jste přidali úložiště produktu IBM Cloud Private **local-charts** jako vzdálené úložiště Helm.

c) Nainstalujte graf.

Spusťte následující příkaz a zadejte tyto parametry:

a. Název vydání (například `my-release`)

b. Název vzdáleného úložiště kormidla, které obsahuje diagram `ibm-mqadvanced-server-prod` (například `my-repo`).

c. Úložiště obrazů (například `mycluster.icp:8500/`*`namespace_name`*`/ibm-mqadvanced-server-prod`)

d. Značka obrazu (například `9.1.3.0-r1`)

```
helm install --name my-release --repo my-repo ibm-mqadvanced-server-prod --set
license=accept --set image.repository=mycluster.icp:8500/namespace_name/ibm-mqadvanced-
server-prod --set image.tag=9.1.3.0-r1 --tls
```

Související úlohy

“Implementace správce front pomocí rozhraní CLI Helm” na stránce 24
Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

“Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Private” na stránce 28
U verzí CD IBM MQ starších než 9.1.4připravte svůj klastr IBM Cloud Private , aby nasadil obraz připravený pro instalaci produktu IBM MQ.

“Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Kubernetes Service” na stránce 29
Pro verzi CD produktu IBM MQ dřívější než 9.1.4importujte obraz připravený pro produkt IBM MQ do produktu IBM Cloud Kubernetes Service.

Linux MQ Adv. CD Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Private

U verzí CD IBM MQ starších než 9.1.4připravte svůj klastr IBM Cloud Private , aby nasadil obraz připravený pro instalaci produktu IBM MQ.

Informace o této úloze

Upozornění: V 9.1.4 Tento import není podporován v produktu IBM MQ 9.1.4 nebo v novějších verzích.

Obraz produktu IBM MQ lze stáhnout z produktu Passport Advantage a importovat jej do kontejneru IBM Cloud Private .

Postup

1. Stáhněte nejnovější obraz produktu IBM MQ z Passport Advantage a Passport Advantage Express web.

   Podrobnosti o dostupných stažení získáte na webové stránce Stahování IBM MQ 9.1 a poté klepněte na kartu pro vydání, které chcete stáhnout. Název a číslo části, která se má stáhnout, jsou uvedeny v tabulce.
2. Naimportujte stažený archivní soubor do produktu IBM Cloud Private.

   Viz část Přidání softwaru IBM do katalogu IBM Cloud Private v katalogu v dokumentaci produktu IBM Cloud Private .

Jak pokračovat dále

Nyní jste připraveni Implementovat správce front do produktu IBM Cloud Private.

Související úlohy

"Implementace správce front pomocí rozhraní CLI Helm" na stránce 24
Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

"Implementace předchozích verzí CD produktu IBM MQ do klastru IBM Cloud Private" na stránce 26
Pro verze CD produktu IBM MQ starší než 9.1.4použijte konzolu správy produktu IBM Cloud Private k implementaci správce front do produktu IBM Cloud Private.

"Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Kubernetes Service" na stránce 29
Pro verzi CD produktu IBM MQ dřívější než 9.1.4importujte obraz připravený pro produkt IBM MQ do produktu IBM Cloud Kubernetes Service.

Linux MQ Adv. CD Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Kubernetes Service

Pro verzi CD produktu IBM MQ dřívější než 9.1.4importujte obraz připravený pro produkt IBM MQ do produktu IBM Cloud Kubernetes Service.

Informace o této úloze

Upozornění: V 9.1.4 Tento import není podporován v produktu IBM MQ 9.1.4 nebo v novějších verzích.

Obraz produktu IBM MQ můžete stáhnout z produktu Passport Advantage a importovat jej do klastru IBM Cloud Kubernetes Service .

Postup

1. Stáhněte nejnovější obraz produktu IBM MQ z Passport Advantage a Passport Advantage Express web.

   Podrobnosti o dostupných stažení získáte na webové stránce Stahování IBM MQ 9.1 a poté klepněte na kartu pro vydání, které chcete stáhnout. Název a číslo části, která se má stáhnout, jsou uvedeny v tabulce.
2. Naimportujte stažený archivní soubor do produktu IBM Cloud Kubernetes Service.

   Viz část Spuštění obrazů IBM Cloud Private ve veřejných kontejnerech Kubernetes.

Související úlohy

"Implementace správce front pomocí rozhraní CLI Helm" na stránce 24
Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

"Implementace předchozích verzí CD produktu IBM MQ do klastru IBM Cloud Private" na stránce 26
Pro verze CD produktu IBM MQ starší než 9.1.4použijte konzolu správy produktu IBM Cloud Private k implementaci správce front do produktu IBM Cloud Private.

"Přidání předchozích vydání CD obrazu IBM MQ do klastru IBM Cloud Private" na stránce 28
U verzí CD IBM MQ starších než 9.1.4připravte svůj klastr IBM Cloud Private , aby nasadil obraz připravený pro instalaci produktu IBM MQ.

V 9.1.4 Linux MQ Adv. CD Připojení ke správci front implementovanému v klastru OpenShift

Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

Informace o této úloze

Je zapotřebí použít OpenShift Route pro připojení aplikace ke správci front IBM MQ mimo klastr Red Hat OpenShift.

Zabezpečení TLS musíte povolit ve správci front IBM MQ a aplikaci klienta, protože Indikace názvu serveru (SNI) je k dispozici pouze v protokolu TLS. Red Hat OpenShift Container Platform Router používá SNI ke směrování požadavků na správce front IBM MQ.

Požadovaná konfigurace OpenShift Route závisí na chování SNI vaší aplikace klienta.

Chcete-li nastavit záhlaví SNI jako TLS 1.2 nebo vyšší, musí se pro komunikaci TLS použít CipherSpec nebo CipherSuite .

Rozhraní SNI je nastaveno na kanál MQ , jsou-li splněny následující podmínky:

- Klient jazyka IBM MQ jazyka C je V8 nebo novější.
- Klient Java/JMS je V9.1.1 nebo novější a instalace prostředí Java podporuje třídu `javax.net.ssl.SNIHostName` .
- Produkt .NET Client je v nespravovaném režimu.

Adaptér SNI je nastaven na název hostitele, pokud je název hostitele zadán jako název připojení a jsou splněny následující podmínky:

- Klient .NET je ve spravovaném režimu.
- Je použit klient AMQP nebo XR.
- Klienti Java/JMS se používají s **`AllowOutboundSNI`** nastaveným na `NO`.

Rozhraní SNI není nastaveno a je prázdné za následujících podmínek:

- Klient jazyka C produktu IBM MQ je V7.5 nebo starší.
- IBM MQ Klient jazyka C se používá s parametrem **`AllowOutboundSNI`** nastaveným na hodnotu `NO`.
- Klienti Java/JMS se používají s instalací Java, která nepodporuje třídu `javax.net.ssl.SNIHostName` .

Příklad

Cesty založené na názvu hostitele OpenShift Trasy: Pro aplikace klienta, které nastavují SNI na název hostitele

Následující grafy Helm automaticky vytvářejí trasu s názvem OpenShift Route pro připojení aplikace ke správci front produktu IBM MQ . Aplikace klienta, které nastaví SNI na název hostitele, mohou použít tuto trasu OpenShift .

- ibm-mqadvanced-server-dev
- ibm-mqadvanced-server-prod
- ibm-mqadvanced-server-integration-prod v IBM Cloud Pak for Integration.

Pokud tyto grafy nepoužíváte a potřebujete vytvořit vlastní název hostitele OpenShift Route, můžete ve svém klastru použít následující `yaml` :

```
apiVersion: route.openshift.io/v1
  kind: Route
  metadata:
    name: <provide a unique name for the Route>
    namespace: <namespace of your MQ deployment>
  spec:
    to:
      kind: Service
      name: <name of the Kubernetes Service for your MQ deployment (for example "<Helm Release>-ibm-
mq")>
    port:
      targetPort: 1414
    tls:
      termination: passthrough
```

MQ Cesty založené na kanálu OpenShift : Pro klientské aplikace, které nastavují SNI na kanál MQ

Aplikace klienta, které nastavují SNI na kanál MQ, vyžadují vytvoření nového OpenShift Route pro každý kanál, ke kterému se chcete připojit. Chcete-li povolit směrování ke správnému správci front, musíte také použít jedinečné názvy kanálů v rámci klastru Red Hat OpenShift .

Chcete-li určit požadovaný název hostitele pro každý z vašich nových OpenShift Route, je třeba mapovat každý název kanálu na adresu SNI, jak je zdokumentováno zde: https://www.ibm.com/support/pages/ibm-websphere-mq-how-does-mq-provide-multiple-certificates-certlabl-capability

Poté musíte vytvořit nový OpenShift Route (pro každý kanál) tak, že ve svém klastru použijete následující `yaml`:

```
  apiVersion: route.openshift.io/v1
  kind: Route
  metadata:
    name: <provide a unique name for the Route>
    namespace: <the namespace of your MQ deployment>
  spec:
    host: <SNI address mapping for the channel>
    to:
      kind: Service
      name: <the name of the Kubernetes Service for your MQ deployment (for example "<Helm Release>-
ibm-mq")>
    port:
      targetPort: 1414
    tls:
      termination: passthrough
```

Konfigurace podrobností připojení aplikace klienta

Název hostitele, který má být použit pro připojení klienta, můžete určit spuštěním následujícího příkazu:

```
oc get route <Name of hostname based Route (for example "<Helm Release>-ibm-mq-qm")>
-n <namespace of your MQ deployment> -o jsonpath="{.spec.host}"
```

Port pro připojení klienta by měl být nastaven na port používaný směrovačem OCP (OpenShift Container Platform)-obvykle 443.

Související úlohy

“Implementace správce front pomocí rozhraní CLI Helm” na stránce 24
Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

“Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift” na stránce 31
Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

V 9.1.4 Linux MQ Adv. CD

Připojení k rozhraní IBM MQ Console implementovaného v klastru OpenShift

Jak se připojit k rozhraní IBM MQ Console správce front, který byl implementován do klastru Red Hat OpenShift Container Platform.

Informace o této úloze

Pokud používáte operátor IBM MQ , lze adresu URL IBM MQ Console nalézt na stránce s podrobnostmi `QueueManager` ve webové konzole OpenShift nebo v produktu IBM Cloud Pak for Integration Platform Navigator. Volitelně lze tento příkaz nalézt z rozhraní OpenShift CLI spuštěním následujícího příkazu:

```
oc get queuemanager <QueueManager Name> -n <namespace of your MQ deployment> --output
jsonpath='{.status.adminUiUrl}'
```

Příklad

Následující grafy Helm automaticky vytvářejí trasu OpenShift Route pro přístup k produktu IBM MQ Console

- ibm-mqadvanced-server-dev
- ibm-mqadvanced-server-integration-prod v IBM Cloud Pak for Integration.

Název hostitele trasy OpenShift můžete získat spuštěním následujícího příkazu:

```
oc get route <Route Name (for example "<Helm Release>-ibm-mq-web")>
-n <namespace of your MQ deployment> --output jsonpath='{.spec.host}'
```

K produktu IBM MQ Console můžete přistupovat prostřednictvím této adresy URL:

```
https://<Route Hostname>/ibmmq/console
```

Související úlohy

“Implementace správce front pomocí rozhraní CLI Helm” na stránce 24
Použijte Helm k implementaci správce front do klastru platformy Red Hat OpenShift Container Platform. Tuto úlohu by měl dokončit administrátor projektu.

“Připojení ke správci front implementovanému v klastru OpenShift” na stránce 29
Sada příkladů konfigurace pro připojení ke správci front implementovanému v klastru Red Hat OpenShift.

Linux MQ Adv. CD Zálohování a obnova konfigurace správce front pomocí rozhraní OpenShift CLI

Záloha konfigurace správce front vám může pomoci při znovusestavení správce front z jeho definic v případě, že dojde ke ztrátě konfigurace správce front. Tento postup nezálohuje data protokolu správce front. Vzhledem k přechodné povaze zpráv je pravděpodobné, že historická data protokolu budou v době obnovy bezvýznamná.

Než začnete

Přihlaste se do svého klastru pomocí **`cloudctl login`** (pro IBM Cloud Pak for Integration) nebo **`oc login`**.

Procedura

- Zazálohujte konfiguraci správce front.

  Příkaz **dmpmqcfg** můžete použít k vypsání paměti konfigurace správce front IBM MQ.

  a) Získejte název podu pro správce front.
  Například, pokud používáte operátor, můžete spustit následující příkaz, kde *queue_manager_name* je název vašeho prostředku `QueueManager` :

  ```
  oc get pods --selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/
  instance=queue_manager_name
  ```

  Například, pokud používáte Helm, můžete spustit následující příkaz, kde *release_name* je název vašeho vydání Helm .

  ```
  oc get pods --selector release=release_name
  ```

  b) Spusťte příkaz **dmpmqcfg** na podu, směrujte výstup do souboru na svém lokálním počítači.

  Příkaz **dmpmqcfg** je výstupem konfigurace MQSC správce front.

  ```
  oc exec -it pod_name -- dmpmqcfg > backup.mqsc
  ```

- Obnovte konfiguraci správce front.

  Po provedení procedury zálohy uvedené v předchozím kroku byste měli mít soubor `backup.mqsc` obsahující konfiguraci správce front. Konfiguraci můžete obnovit tak, že tento soubor použijete pro nového správce front.

  a) Získejte název podu pro správce front.
  Například, pokud používáte operátor, můžete spustit následující příkaz, kde *queue_manager_name* je název vašeho prostředku `QueueManager` :

  ```
  oc get pods --selector app.kubernetes.io/name=ibm-mq,app.kubernetes.io/
  instance=queue_manager_name
  ```

  Například, pokud používáte Helm, můžete spustit následující příkaz, kde *release_name* je název vašeho vydání Helm .

  ```
  oc get pods --selector release=release_name
  ```

  b) Spusťte příkaz **`runmqsc`** na podu, směrovaný do obsahu souboru `backup.mqsc`.

  ```
  oc exec -i pod_name -- runmqsc < backup.mqsc
  ```

Sestavení vlastního kontejneru IBM MQ

Vytvořte si vlastní kontejner, dříve označovaný jako "obraz kontejneruDocker". Jedná se o nejflexibilnější řešení kontejneru, které ale od vás vyžaduje značné dovednosti v konfiguraci kontejnerů a abyste "vlastnili" výsledný kontejner.

Než začnete

Než začnete vyvíjet svůj vlastní kontejner, zvažte, zda nemůžete místo toho využít některý z předpřipravených zabalených kontejnerů od IBM. Viz IBM MQ v kontejnerech

Informace o této úloze

Když zabalíte IBM MQ jako kontejnerový obraz, můžete rychle a snadno implementovat změny v aplikaci tak, aby mohly být implementovány v testovacím a přechodovém systému. To může být významným přínosem pro průběžné doručování ve vašem podniku.

Procedura

- Informace o tom, jak sestavit kontejnerový obraz IBM MQ pomocí Docker, naleznete v následujících dílčích tématech:
  - Linux “Podpora pro sestavení vlastních kontejnerových obrazů a grafů produktu IBM MQ” na stránce 8
  - “Plánování vlastního obrazu správce front IBM MQ pomocí kontejneru” na stránce 33
  - “Sestavení ukázkového obrazu správce front produktu IBM MQ pomocí produktu Docker” na stránce 34
  - “Spuštění lokálních aplikací vazby v samostatných kontejnerech” na stránce 37

Související pojmy

IBM MQ v kontejnerech

Plánování vlastního obrazu správce front IBM MQ pomocí kontejneru

Při spuštění správce front produktu IBM MQ v kontejneru je třeba vzít v úvahu několik požadavků. Ukázkový kontejnerový obraz nabízí způsob, jak tyto požadavky zpracovat, ale chcete-li použít vlastní obraz, je třeba zvážit, jak jsou tyto požadavky zpracovávány.

Řízení procesu

Když spustíte kontejner, v podstatě spouštíte jeden proces (PID 1 uvnitř kontejneru), který může později vyvolat podřízené procesy.

Pokud hlavní proces skončí, běhové prostředí kontejneru zastaví kontejner. Správce front produktu IBM MQ vyžaduje, aby bylo na pozadí spuštěno více procesů.

Z tohoto důvodu se musíte ujistit, že váš hlavní proces zůstane aktivní, dokud bude spuštěn správce front. Dobrým zvykem je kontrolovat z tohoto procesu, zda je správce front aktivní, například prostřednictvím administrativních dotazů.

Naplnění `/var/mqm`

Kontejnery musí být nakonfigurovány s `/var/mqm` jako svazkem.

Provedete-li to, bude adresář svazku při prvním spuštění kontejneru prázdný. Tento adresář je obvykle naplněn v době instalace, ale instalace a běhové prostředí jsou oddělená prostředí při použití kontejneru.

V 9.1.0 Chcete-li tento problém vyřešit při spuštění kontejneru, můžete použít příkaz **crtmqdir** k naplnění `/var/mqm` při prvním spuštění.

Sestavení ukázkového obrazu správce front produktu IBM MQ pomocí produktu Docker

Tyto informace použijte k sestavení ukázkového kontejnerového obrazu pro spuštění správce front IBM MQ v kontejneru.

Informace o této úloze

Za prvé sestavíte základní obraz obsahující systém souborů Red Hat Universal Base Image a čistou instalaci produktu IBM MQ.

Za druhé sestavíte nad základní další vrstvu kontejnerového obrazu, která přidává nějakou konfiguraci produktu IBM MQ, aby bylo umožněno základní zabezpečení ID uživatele a hesla.

Nakonec spustíte kontejner tak, aby používal tento obraz jako svůj systém souborů, s obsahem `/var/mqm` poskytovaným svazkem kontejneru na systému souborů hostitele.

Procedura

- Informace, jak sestavit ukázkový kontejnerový obraz pro spuštění správce front IBM MQ v kontejneru viz následující dílčí témata:
  - “Sestavení ukázkového obrazu základního správce front produktu IBM MQ” na stránce 34
  - “Sestavení ukázkového obrazu nakonfigurovaného správce front IBM MQ” na stránce 35

Sestavení ukázkového obrazu základního správce front produktu IBM MQ

Abyste mohli používat produkt IBM MQ ve svém vlastním kontejnerovém obrazu, musíte nejprve sestavit základní obraz s čistou instalací produktu IBM MQ. Následující postup ukazuje, jak sestavit ukázkový základní obraz pomocí ukázkového kódu hostovaného na serveru GitHub.

Procedura

- Použijte soubory make dodané v úložišti mq-container GitHub k sestavení produkčního kontejnerového obrazu.

  Postupujte podle pokynů v části Sestavení kontejnerového obrazu v GitHub.

Výsledky

Nyní máte nainstalovaný základní kontejnerový obraz s nainstalovaným produktem IBM MQ.

Sestavení ukázkového obrazu nakonfigurovaného správce front IBM MQ

Jakmile sestavíte generický kontejnerový obraz základního produktu IBM MQ, musíte použít vlastní konfiguraci, abyste umožnili bezpečný přístup. Chcete-li tak učinit, vytvořte vlastní vrstvu kontejnerového obrazu s použitím generického obrazu jako nadřízeného prvku.

Než začnete

Pro obraz IBM MQ 9.1 nelze konfigurovat zabezpečený přístup pomocí Red Hat OpenShift Container Platform "restricted" Security Context Constraint Constraint Constraint Security Constraint Constraint (SCC). "Omezený" SCC používá náhodná ID uživatelů a zabraňuje eskalaci oprávnění tím, že se změní na jiného uživatele. Instalační program produktu IBM MQ 9.1 založený na RPM spoléhá na uživatele a skupinu `mqm` a na spustitelných programech také používá bity `setuid` .

Toto omezení je odebráno v produktu IBM MQ 9.2.

Postup

1. Vytvořte nový adresář a přidejte soubor s názvem `config.mqsc` s následujícím obsahem:

```
DEFINE CHANNEL(PASSWORD.SVRCONN) CHLTYPE(SVRCONN)
SET CHLAUTH(PASSWORD.SVRCONN) TYPE(BLOCKUSER) USERLIST('nobody') +
DESCR('Allow privileged users on this channel')
SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(NOACCESS) DESCR('BackStop rule')
SET CHLAUTH(PASSWORD.SVRCONN) TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(CHANNEL) CHCKCLNT(REQUIRED)
ALTER AUTHINFO(SYSTEM.DEFAULT.AUTHINFO.IDPWOS) AUTHTYPE(IDPWOS) ADOPTCTX(YES)
REFRESH SECURITY TYPE(CONNAUTH)
```

   Mějte na zřeteli, že předchozí příklad používá jednoduché ověření ID uživatele a hesla. Nicméně můžete použít jakoukoli konfiguraci zabezpečení, kterou vyžaduje váš podnik.

2. Vytvořte soubor s názvem `Dockerfile` s následujícím obsahem:

```
FROM mq
RUN useradd johndoe -G mqm && \
    echo johndoe:passw0rd | chpasswd
COPY config.mqsc /etc/mqm/
```

   kde:

   - `johndoe` je ID uživatele, které chcete přidat
   - `passw0rd` je původní heslo

3. Sestavte vlastní kontejnerový obraz pomocí následujícího příkazu:

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

   kde „`.`“ je adresář obsahující dva soubory, které jste právě vytvořili.

   Docker potom vytvoří dočasný kontejner pomocí tohoto obrazu a spustí zbývající příkazy.

   Příkaz **RUN** přidá uživatele s názvem `johndoe` s heslem `passw0rd` a příkaz **COPY** přidá soubor `config.mqsc` do specifického umístění, které je známé nadřazeným obrazem.

   Poznámka: V systému Red Hat Enterprise Linux (RHEL) můžete použít příkaz **`docker`** (RHEL V7) nebo **podman** (RHEL V7 nebo RHEL V8). V případě **podman**nepotřebujete **sudo** na začátku příkazu.

4. Spusťte nový upravený obraz a vytvořte nový kontejner s obrazem disku, který jste právě vytvořili.

   Vaše nová vrstva obrazu neurčovala žádný konkrétní příkaz ke spuštění, takže byl zděděn z nadřízeného obrazu. Vstupní bod nadřízeného prvku (kód je k dispozici v GitHub):

   - Vytvoří správce front.

- Spustí správce front.
- Vytvoří výchozí modul listener.
- Poté spustí všechny příkazy MQSC z `/etc/mqm/config.mqsc`..

Chcete-li spustit nový upravený obraz, zadejte následující příkazy:

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

Kde:

První parametr env
Předává proměnnou prostředí do kontejneru, který potvrzuje vaše přijetí licence pro IBM IBM WebSphere MQ. Můžete také nastavit proměnnou LICENSE pro zobrazení licence.

Další podrobnosti viz informace o licenci IBM MQ v licencích IBM MQ.

Druhý parametr env
Nastaví název správce front, který používáte.

Parametr svazku
Říká kontejneru, že jakékoli zápisy MQ do `/var/mqm` by měly být skutečně zapsány do `/var/example` na hostiteli.

Tato volba znamená, že lze kontejner snadno odstranit později a přesto zachovat veškerá trvalá data. Tato volba také usnadňuje zobrazení souborů protokolu.

Parametr publikování
Mapuje porty na hostitelském systému do portů v kontejneru. Kontejner se standardně spouští s vlastní interní adresou IP, což znamená, že musíte specificky mapovat všechny porty, které chcete vystavit.

V tomto příkladu to znamená mapování portu 1414 na hostiteli na port 1414 v kontejneru.

Parametr odpojení
Spustí kontejner na pozadí.

Výsledky

Postavili jste obraz konfigurovaného kontejneru a můžete prohlížet spuštěné kontejnery pomocí příkazu docker **ps** . Procesy produktu IBM MQ , které jsou spuštěny ve vašem kontejneru, lze zobrazit pomocí příkazu docker **top** .

Upozornění:

Protokoly kontejneru si můžete prohlížet pomocí příkazu docker **logs ${CONTAINER_ID}** .

Jak pokračovat dále

- Pokud se kontejner nezobrazí, když použijete příkaz docker **ps** , kontejner se možná nezdařil. Kontejnery se selháním můžete zobrazit pomocí příkazu docker **ps -a** .
- Použijete-li příkaz docker **ps -a** , zobrazí se ID kontejneru. Toto ID bylo také vytisknuto, když jste zadali příkaz docker **run** .
- Protokoly kontejneru si můžete prohlédnout pomocí příkazu docker **logs ${CONTAINER_ID}** .
- Maximální počet otevřených souborů lze nastavit pomocí příkazu **sysctl fs.file-max=524288**.

V 9.1.0 Spuštění lokálních aplikací vazby v samostatných kontejnerech

Díky sdílení oboru názvů procesu mezi kontejnery v Docker můžete spouštět aplikace, které vyžadují připojení lokální vazby k produktu IBM MQ v samostatných kontejnerech ze správce front IBM MQ.

Informace o této úloze

Tato funkce je podporována ve správcích front IBM MQ 9.0.3 a novějších.

Musíte dodržovat následující omezení:

- Musíte sdílet obor názvů PID kontejnerů pomocí argumentu `--pid`.
- Musíte sdílet obor názvů IPC kontejnerů pomocí argumentu `--ipc`.
- Musíte buď:
  1. Sdílet obor názvů UTS kontejnerů s hostitelem pomocí argumentu `--uts`, nebo
  2. zajistit, že kontejnery budou mít stejný název hostitele pomocí argumentu `-h` nebo `--hostname`.
- Datový adresář IBM MQ je třeba připojit do svazku, který je k dispozici pro všechny kontejnery v adresáři `/var/mqm`

Tuto funkčnost můžete vyzkoušet provedením následujících kroků v systému Linux, na kterém je již nainstalován Docker.

Následující příklad používá ukázkový kontejnerový obraz IBM MQ. Podrobnosti o tomto obrazu viz Github.

Postup

1. Vytvořte dočasný adresář, který bude fungovat jako váš svazek, zadáním následujícího příkazu:

```
mkdir /tmp/dockerVolume
```

2. Vytvořte správce front (`QM1`) v kontejneru, s názvem `sharedNamespace`, zadáním následujícího příkazu:

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

3. Spusťte druhý kontejner s názvem `secondaryContainer`, který je založen na produktu `ibmcom/mq`, ale nevytvářejte správce front, zadáním následujícího příkazu:

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

4. Spusťte příkaz **dspmq** ve druhém kontejneru, abyste viděli stav obou správců front, zadáním následujícího příkazu:

```
docker exec secondaryContainer dspmq
```

5. Spusťte následující příkaz ke zpracování příkazů MQSC pro správce front spuštěného na jiném kontejneru:

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

Výsledky

Nyní máte lokální aplikace spuštěné v samostatných kontejnerech a můžete úspěšně spouštět příkazy jako **dspmq**, **amqsput**, **amqsget** a **runmqsc** jako lokální vazby ke správci front `QM1` ze sekundárního kontejneru.

Pokud se nezobrazí očekávaný výsledek, přečtěte si další informace v “Odstraňování problémů s aplikacemi oboru názvů” na stránce 38.

V 9.1.0 Odstraňování problémů s aplikacemi oboru názvů

Při používání sdílených oborů názvů musíte zajistit sdílení všech oborů názvů (IPC, PID a UTS/hostname) a připojených svazků, jinak vaše aplikace nebudou fungovat.

Seznam omezení, která musíte dodržovat, viz “Spuštění lokálních aplikací vazby v samostatných kontejnerech” na stránce 37.

Pokud vaše aplikace nesplňuje všechna uvedená omezení, můžete se setkat s problémy při spuštění kontejneru, ale funkčnost, kterou očekáváte, nebude fungovat.

Následující seznam popisuje některé běžné příčiny a chování, které se pravděpodobně zobrazí, pokud jste zapomněli splnit jedno z omezení.

- Pokud zapomenete sdílet buď obor názvů (UTS/PID/IPC), nebo název hostitele kontejnerů a poté svazek připojíte, bude kontejner schopen zobrazit správce front, ale nebude se správcem front spolupracovat.
  - V případě příkazů **dspmq** uvidíte následující:

```
docker exec container dspmq

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

  - V případě příkazů **runmqsc** nebo jiných příkazů, které se pokusí připojit ke správci front, pravděpodobně obdržíte chybovou zprávu AMQ8146:

```
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
```

- Jestliže sdílíte všechny požadované obory názvů, ale nepřipojíte sdílený svazek k adresáři `/var/mqm` a máte platnou cestu k datům IBM MQ, pak vaše příkazy také přijímají chybové zprávy AMQ8146.

  Příkaz **dspmq** však není vůbec schopen zobrazit vašeho správce front, místo toho vrací prázdnou odezvu:

```
docker exec container dspmq
```

- Jestliže sdílíte všechny požadované obory názvů, ale nepřipojíte sdílený svazek k adresáři `/var/mqm` a máte platnou cestu k datům IBM MQ (nebo datovou cestu IBM MQ), zobrazí se různé chyby, protože cesta k datům je klíčovou komponentou instalace produktu IBM MQ. Bez cesty k datům produkt IBM MQ nemůže fungovat.

  Pokud spustíte kterýkoli z následujících příkazů a uvidíte odezvy podobné těm, které jsou zobrazeny v těchto příkladech, měli byste ověřit, zda jste připojili adresář nebo vytvořili datový adresář IBM MQ:

```
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
```

Linux MQ Adv. CD V 9.1.5 Odkaz rozhraní API pro IBM MQ Operator

Produkt IBM MQ poskytuje operátor Kubernetes poskytující nativní integraci s platformou OpenShift Container Platform.

Linux MQ Adv. CD V 9.1.5 Odkaz rozhraní API pro mq.ibm.com/v1beta1

Rozhraní v1beta1 API lze použít k vytvoření a správě prostředků správce front.

Linux MQ Adv. CD V 9.1.5 Odkaz na licenci pro mq.ibm.com/v1beta1

Pole `spec.license.license` musí obsahovat identifikátor licence pro licenci, kterou přijímáte. Platné hodnoty:

Hodnota `spec.license.license`	**Hodnota `spec.license.use`**	**Informace o licenci**
`L-RJON-BN7PN3`	`Production` nebo `NonProduction`	IBM Cloud Pak for Integration 2020.2
`L-RJON-BPHL2Y`		IBM Cloud Pak for Integration Limited Edition 2020.2
`L-APIG-BJAKBF`	`Production` nebo `Development`	IBM MQ Advanced 9.1.5
`L-APIG-BM7GDH`	`Development`	IBM MQ Advanced for Developers 9.1.5

Všimněte si, že je určena *verze* licence, což není vždy stejné jako verze produktu IBM MQ.

Linux MQ Adv. CD V 9.1.5 Odkaz rozhraní API pro správce front (mq.ibm.com/v1beta1)

QueueManager

Správce front je server IBM MQ, který poskytuje služby front a publikování/odebírání pro aplikace.

Pole	**Popis**
`apiVersion` string	APIVersion definuje schéma opatřené verzí této reprezentace objektu. Servery by měly převést rozpoznaná schémata na nejnovější interní hodnotu a mohou odmítnout nerozpoznané hodnoty. Další informace: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resources.

Pole	Popis
`kind` string	Kind je hodnota řetězce představující prostředek REST, který tento objekt reprezentuje. Servery mohou toto odvodit z koncového bodu, na který klient odesílá požadavky. Nelze aktualizovat. Bez mezer mezi slovy a s velkými počátečními písmeny (CamelCase). Další informace: https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds.
`metadata`	
`spec` “Specifikace QueueManager” na stránce 44	Požadovaný stav správce front.
`status` “QueueManagerStatus” na stránce 45	Pozorovaný stav správce front.

Dostupnost

Nastavení dostupnosti pro správce front, například zda má být použita dvojice aktivní-pohotovostní, či nikoli.

Zobrazí se v:

- “Konfigurace správce front QueueManager” na stránce 41

Pole	Popis
`type` string	Typ dostupnosti, který se má použít. Použijte "SingleInstance" pro jeden Pod, který bude automaticky restartován (v některých případech) programem Kubernetes. Použijte "MultiInstance" pro dvojici Pods, z nichž jeden je "aktivní" správce front a druhý z nich je záložní. Viz Vysoká dostupnost pro produkt IBM MQ v kontejnerech v nejnovější verzi produktu IBM MQ.

Licence

Nastavení, která řídí převzetí licence a které metriky licencí se mají používat.

Zobrazí se v:

- “Specifikace QueueManager” na stránce 44

Pole	Popis
`use` string	Nastavení, které řídí, jak se bude software používat, kde licence podporuje více použití. Platné hodnoty viz https://ibm.biz/BdqvCF .
`accept` boolean	Zda přijímáte licenci přidruženou k tomuto softwaru (povinné), či nikoli.
`license` string	Identifikátor licence, kterou přijímáte. Musí se jednat o správný identifikátor licence pro vámi používanou verzi produktu MQ. Platné hodnoty viz https://ibm.biz/BdqvCF .
`metric` string	Nastavení, které určuje, která metrika licence se má použít. Příklad: "ProcessorValueUnit", "VirtualProcessorCore" nebo "ManagedVirtualServer".

Limity

QueueManagerResourceList definuje nastavení CPU a paměti.

Zobrazí se v:

- “Prostředky” na stránce 47

Pole	Popis
`cpu`	
`memory`	

Odkaz LocalObject

LocalObjectReference obsahuje dostatek informací, aby bylo možné umístit odkazovaný objekt do stejného oboru názvů.

Zobrazí se v:

- "Specifikace QueueManager" na stránce 44

Pole	Popis
`name` string	Název odkazujícího objektu. Další informace: https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#names ÚKOL: Přidejte další užitečná pole. apiVersion, kind, uid?.

PKI

Nastavení Public Key Infrastructure pro definování klíčů a certifikátů pro použití se zabezpečením Transport Layer Security (TLS) nebo MQ Advanced Message Security (AMS).

Zobrazí se v:

- "Specifikace QueueManager" na stránce 44

Pole	Popis
Pole `keys` "PKISsource" na stránce 41	Soukromé klíče, které mají být přidány do úložiště klíčů správce front.
Pole `trust` "PKISsource" na stránce 41	Certifikáty pro přidání do úložiště klíčů správce front.

PKISsource

PKISsource definuje zdroj informací o Public Key Infrastructure, jako např. klíče nebo certifikáty.

Zobrazí se v:

- "PKI" na stránce 41

Pole	Popis
`name` string	Name se používá jako štítek pro klíč nebo certifikát. Musí se jednat o alfanumerický řetězec s malými písmeny.
`secret` "Tajné údaje" na stránce 47	Zadejte klíč pomocí tajného údaje Kybernetes.

Konfigurace správce front QueueManager

QueueManagerKonfigurace definuje nastavení pro kontejner správce front a základní správce front.

Zobrazí se v:

- "Specifikace QueueManager" na stránce 44

Pole	Popis
`logFormat` string	Který formát protokolu má být použit pro tento kontejner. Použijte "JSON" pro protokoly ve formátu JSON z kontejneru. Použijte "Basic" pro textově formátované zprávy.
`metrics` “Metriky QueueManager” na stránce 43	Nastavení pro metriky ve stylu Prometheus.
`readinessProbe` “QueueManagerReadinessProbe” na stránce 43	Nastavení, které řídí sondu připravenosti.
`resources` “Prostředky” na stránce 47	Nastavení, která řídí požadavky na prostředky.
`storage` “Úložiště QueueManager” na stránce 46	Nastavení úložiště pro řízení použití trvalých svazků a úložných tříd správce front.
`availability` “Dostupnost” na stránce 40	Nastavení dostupnosti pro správce front, například zda má být použita dvojice aktivní-pohotovostní, či nikoli.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz.
`livenessProbe` “QueueManagerLivenessProbe” na stránce 42	Nastavení, která řídí sondu živosti.
debug boolean	Zda protokolovat zprávy ladění z kódu specifického pro kontejner do protokolu kontejneru, či nikoli.
`image` string	Kontejnerový obraz, který bude použit.
name string	Název základního správce front MQ, pokud je odlišný od metadata.name. Toto pole použijte, pokud chcete, aby název správce front, který neodpovídá pravidlům Kubernetes, obsahoval názvy (například název, který obsahuje velká písmena).

QueueManagerLivenessProbe

Nastavení, která řídí sondu živosti.

Zobrazí se v:

- “Konfigurace správce front QueueManager” na stránce 41

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

Metriky QueueManager

Nastavení pro metriky ve stylu Prometheus.

Zobrazí se v:

- "Konfigurace správce front QueueManager" na stránce 41

Pole	Popis
`enabled` boolean	Zda se má povolit koncový bod metrik kompatibilních s Prometheus, či nikoli.

QueueManagerOptionalVolume

Podrobnosti o PersistentVolume pro protokoly zotavení produktu MQ. Povinné při použití správce front s více instancemi.

Zobrazí se v:

- "Úložiště QueueManager" na stránce 46

Pole	Popis
`class` string	Paměťová třída, která se má použít pro tento svazek. Platné pouze, je-li "typ" je "persistent-claim".
`enabled` boolean	Určuje, zda má být tento svazek povolen jako samostatný svazek nebo zda má být umístěn na výchozí svazek "queueManager".
`size` string	Velikost objektu PersistentVolume pro předání do Kubernetes. Platné pouze, je-li "typ" je "persistent-claim".
`sizeLimit` string	Omezení velikosti při použití svazku "efemérní". Soubory jsou stále zapisovány do dočasného adresáře, takže můžete tuto volbu použít k omezení velikosti. Platí pouze tehdy, je-li `type` "pomíjející".
`type` string	Typ svazku, který se má použít. Vyberte `ephemeral` , chcete-li vytvořit dočasný svazek "emptyDir", nebo `persistent-claim` pro použití trvalého svazku.

QueueManagerReadinessProbe

Nastavení, které řídí sondu připravenosti.

Zobrazí se v:

- "Konfigurace správce front QueueManager" na stránce 41

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch.
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

Specifikace QueueManager

Požadovaný stav správce front.

Zobrazí se v:

- "QueueManager" na stránce 39

Pole	Popis
`license` "Licence" na stránce 40	Nastavení, která řídí převzetí licence a které metriky licencí se mají používat.
`pki` "PKI" na stránce 41	Nastavení Public Key Infrastructure pro definování klíčů a certifikátů pro použití se zabezpečením Transport Layer Security (TLS) nebo MQ Advanced Message Security (AMS).
`queueManager` "Konfigurace správce front QueueManager" na stránce 41	QueueManagerKonfigurace definuje nastavení pro kontejner správce front a základní správce front.
`securityContext` "Security Context" na stránce 47	Nastavení zabezpečení, které má být přidáno do kontextu securityContext podu správce front.
`tracing` "TracingConfig" na stránce 49	Nastavení pro integraci trasování s produktem Cloud Pak for Integration Operations Dashboard.
`version` string	Nastavení, které řídí, jaká verze produktu MQ bude použita (povinné). Například: "9.1.5.0-r2" uvedete MQ verze 9.1.5.0pomocí druhé revize obrazu kontejneru. Opravy specifické pro kontejner jsou často používány v revizích, jako např. opravy v základním obrazu.
`affinity`	Standardní pravidla afinity Kubernetes. Další informace viz https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.17/#affinity-v1-core.
Pole `imagePullSecrets` "Odkaz LocalObject" na stránce 41	Volitelný seznam odkazů na tajné údaje ve stejném oboru názvů, které mají být použity pro stažení libovolného z obrazů používaných tímto správcem front. Je-li tato možnost určena, budou tyto tajné údaje předány jednotlivým stahujícím (puller) implementacím typu, aby je použily. Například v případě dockeru jsou uznány pouze tajné údaje typu DockerConfig. Další informace viz https://kubernetes.io/docs/concepts/containers/images#specifying-imagepullsecrets-on-a-pod.
`template` "Šablona" na stránce 48	Rozšířené vytváření šablon pro prostředky Kubernetes. Šablona umožňuje uživatelům potlačit způsob, jakým produkt IBM MQ generuje základní prostředky typu Kubernetes, jako např. StatefulSet, Pods a Services. Tento postup je určen pouze pro pokročilé uživatele, protože má potenciál narušit normální provoz produktu MQ, pokud je použit nesprávně. Všechny hodnoty zadané kdekoli jinde v prostředku správce front budou přepsány nastaveními v šabloně.
`terminationGracePeriodSeconds` integer	Volitelná doba trvání v sekundách, které Pod potřebuje k řádnému ukončení. Hodnota musí být nezáporné celé číslo. Hodnota nula označuje okamžité odstranění. Cílový čas, v němž se pokouší správce front provést ukončení, eskaluje fáze odpojení aplikace. V případě potřeby jsou nezbytné úkoly údržby správce front přerušeny.
`web` "Konfigurace WebServer" na stránce 50	Nastavení pro webový server MQ.

QueueManagerStatus

Pozorovaný stav správce front.

Zobrazí se v:

- "QueueManager" na stránce 39

Pole	Popis
Pole `endpoints` "QueueManagerStatusEndpoint" na stránce 45	Informace v koncových bodech, které tento správce front vystavuje, jako např. koncové body rozhraní API nebo uživatelské rozhraní.
`name` string	Název správce front.
`versions` "QueueManagerStatusVersion" na stránce 45	Verze používaného produktu MQ a další verze dostupné z produktu IBM Entitled Registry.
`adminUiUrl` string	Adresa URL pro uživatelské rozhraní administrace.
Pole `conditions` "QueueManagerStatusCondition" na stránce 45	Podmínky reprezentují nejnovější dostupná pozorování stavu správce front.

QueueManagerStatusCondition

QueueManagerStatusCondition definuje podmínky správce front.

Zobrazí se v:

- "QueueManagerStatus" na stránce 45

Pole	Popis
`message` string	Zpráva čitelná pro člověka označující podrobnosti o posledním přechodu.
`type` string	Typ podmínky.
`lastTransitionTime` string	Poslední čas, kdy podmínka přešla z jednoho stavu do druhého.

QueueManagerStatusEndpoint

QueueManagerStatusEndpoint definuje koncové body správce front.

Zobrazí se v:

- "QueueManagerStatus" na stránce 45

Pole	Popis
`name` string	Název koncového bodu.
`type` string	Typ koncového bodu, například „UI“ pro koncový bod uživatelského rozhraní, „API“ pro koncový bod rozhraní API, „OpenAPI“ pro dokumentaci rozhraní API.
`uri` string	Identifikátor URI pro koncový bod.

QueueManagerStatusVersion

Verze používaného produktu MQ a další verze dostupné z produktu IBM Entitled Registry.

Zobrazí se v:

- “QueueManagerStatus” na stránce 45

Pole	Popis
`available` “QueueManagerStatusVersionDostupná” na stránce 46	Další verze produktu MQ dostupné z produktu IBM Entitled Registry.
`reconciled` string	Používá se specifická verze produktu IBM MQ. Je-li zadán vlastní obraz, pak se nemusí shodovat s aktuálně používanou verzí produktu MQ.

QueueManagerStatusVersionDostupná

Další verze produktu MQ dostupné z produktu IBM Entitled Registry.

Zobrazí se v:

- “QueueManagerStatusVersion” na stránce 45

Pole	Popis
Pole `channels`	Kanály, které jsou k dispozici pro automatickou aktualizaci verze MQ.
Pole `versions` “Verze” na stránce 50	Specifické verze produktu MQ, které jsou k dispozici.

Úložiště QueueManager

Nastavení úložiště pro řízení použití trvalých svazků a úložných tříd správce front.

Zobrazí se v:

- “Konfigurace správce front QueueManager” na stránce 41

Pole	Popis
`persistedData` “QueueManagerOptionalVolume” na stránce 43	Podrobnosti o PersistentVolume pro trvalá data pro produkt MQ, včetně konfigurace, front a zpráv. Povinné při použití správce front s více instancemi.
`queueManager` “Svazek QueueManager” na stránce 46	Výchozí svazek PersistentVolume pro veškerá data běžně pod `/var/mqm`. Bude obsahovat všechna trvalá data a protokoly zotavení, pokud nejsou určeny žádné jiné svazky.
`recoveryLogs` “QueueManagerOptionalVolume” na stránce 43	Podrobnosti o PersistentVolume pro protokoly zotavení produktu MQ. Povinné při použití správce front s více instancemi.

Svazek QueueManager

Výchozí svazek PersistentVolume pro veškerá data běžně pod `/var/mqm`. Bude obsahovat všechna trvalá data a protokoly zotavení, pokud nejsou určeny žádné jiné svazky.

Zobrazí se v:

- “Úložiště QueueManager” na stránce 46

Pole	Popis
`class` string	Paměťová třída, která se má použít pro tento svazek. Platné pouze, je-li "typ" je "persistent-claim".
`size` string	Velikost objektu PersistentVolume pro předání do Kubernetes. Platné pouze, je-li "typ" je "persistent-claim".

Pole	Popis
`sizeLimit` string	Omezení velikosti při použití svazku "efemérní". Soubory jsou stále zapisovány do dočasného adresáře, takže můžete tuto volbu použít k omezení velikosti. Platí pouze tehdy, je-li `type` "pomíjející".
`type` string	Typ svazku, který se má použít. Vyberte `ephemeral` , chcete-li vytvořit dočasný svazek "emptyDir", nebo `persistent-claim` pro použití trvalého svazku.

Požadavky

QueueManagerResourceList definuje nastavení CPU a paměti.

Zobrazí se v:

- “Prostředky” na stránce 47

Pole	Popis
`memory`	
`cpu`	

Prostředky

Nastavení, která řídí požadavky na prostředky.

Zobrazí se v:

- “Konfigurace správce front QueueManager” na stránce 41

Pole	Popis
`limits` “Limity” na stránce 40	QueueManagerResourceList definuje nastavení CPU a paměti.
`requests` “Požadavky” na stránce 47	QueueManagerResourceList definuje nastavení CPU a paměti.

Tajné údaje

Zadejte klíč pomocí tajného údaje Kybernetes.

Zobrazí se v:

- “PKISsource” na stránce 41

Pole	Popis
Pole `items`	Klíče uvnitř tajného údaje Kubernetes, které mají být přidány do kontejneru správce front.
`secretName` string	Název tajného údaje Kubernetes.

SecurityContext

Nastavení zabezpečení, které má být přidáno do kontextu securityContext podu správce front.

Zobrazí se v:

- “Specifikace QueueManager” na stránce 44

Pole	Popis
Pole `supplementalGroups`	Seznam skupin aplikovaných na první proces spuštěný v každém kontejneru kromě primárního GID kontejneru. Není-li zadán, nebudou žádné skupiny přidány do žádného kontejneru.
`fsGroup` integer	Speciální doplňková skupina, která se vztahuje na všechny kontejnery v podu. Některé typy svazků umožňují Kubelet změnit vlastnictví tohoto svazku, které má být vlastněno tímto podem: 1. Vlastnící GID bude skupina FSGroup 2. Bit setgid je nastaven (nové soubory vytvořené ve svazku budou vlastněny skupinou FSGroup) 3. Bity oprávnění jsou OR d with rw-rw---- Pokud nejsou nastaveny, Kubelet neupraví vlastnictví a oprávnění žádné svazku.
`initVolumeAsRoot` boolean	To ovlivňuje securityContext použitý kontejnerem, který inicializuje PersistentVolume. Nastavte tuto hodnotu na "true", pokud používáte poskytovatele úložiště, který vyžaduje, abyste byli kořenovým uživatelem pro přístup k nově zajišťovaným svazkům. Nastavení této hodnoty na hodnotu "true" ovlivní objekt SCC (Security Context Constraints), který můžete použít, a správce front se nemusí spustit, pokud nemáte oprávnění k použití SCC, který povoluje uživatele root. Další informace viz https://docs.openshift.com/container-platform/latest/authentication/managing-security-context-constraints.html.

Šablona

Rozšířené vytváření šablon pro prostředky Kubernetes. Šablona umožňuje uživatelům potlačit způsob, jakým produkt IBM MQ generuje základní prostředky typu Kubernetes, jako např. StatefulSet, Pods a Services. Tento postup je určen pouze pro pokročilé uživatele, protože má potenciál narušit normální provoz produktu MQ, pokud je použit nesprávně. Všechny hodnoty zadané kdekoli jinde v prostředku správce front budou přepsány nastaveními v šabloně.

Zobrazí se v:

- “Specifikace QueueManager” na stránce 44

Pole	Popis
pod	Potlačení pro šablonu použitou pro Pod. Viz https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.17/#podspec-v1-core.

TracingAgent

Pouze v produktu Cloud Pak for Integration můžete konfigurovat nastavení pro volitelného agenta trasování.

Zobrazí se v:

- “TracingConfig” na stránce 49

Pole	Popis
`image` string	Kontejnerový obraz, který bude použit.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz.
`livenessProbe` “TracingProbe” na stránce 49	Nastavení, která řídí sondu živosti.
`readinessProbe` “TracingProbe” na stránce 49	Nastavení, které řídí sondu připravenosti.

TracingCollector

Pouze v produktu Cloud Pak for Integration můžete konfigurovat nastavení pro volitelný kolektor trasování.

Zobrazí se v:

- "TracingConfig" na stránce 49

Pole	Popis
`image` string	Kontejnerový obraz, který bude použit.
`imagePullPolicy` string	Nastavení, které se řídí, když se kubelet pokusí stáhnout uvedený obraz.
`livenessProbe` "TracingProbe" na stránce 49	Nastavení, která řídí sondu živosti.
`readinessProbe` "TracingProbe" na stránce 49	Nastavení, které řídí sondu připravenosti.

TracingConfig

Nastavení pro integraci trasování s produktem Cloud Pak for Integration Operations Dashboard.

Zobrazí se v:

- "Specifikace QueueManager" na stránce 44

Pole	Popis
`agent` "TracingAgent" na stránce 48	Pouze v produktu Cloud Pak for Integration můžete konfigurovat nastavení pro volitelného agenta trasování.
`collector` "TracingCollector" na stránce 49	Pouze v produktu Cloud Pak for Integration můžete konfigurovat nastavení pro volitelný kolektor trasování.
`enabled` boolean	Zda se má povolit integrace s produktem Cloud Pak for Integration Operations Dashboard přes trasování, či nikoli.
`namespace` string	Obor názvů, kde je nainstalován produkt Cloud Pak for Integration Operations Dashboard.

TracingProbe

Nastavení, které řídí sondu připravenosti.

Zobrazí se v:

- "TracingCollector" na stránce 49

Pole	Popis
`failureThreshold` integer	Minimální počet po sobě jdoucích selhání pro sondu, aby to bylo považováno po úspěšném dokončení za nezdar.
`initialDelaySeconds` integer	Počet sekund po spuštění kontejneru, než budou zahájeny sondy živosti. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.
`periodSeconds` integer	Jak často (v sekundách) provést sondu.
`successThreshold` integer	Minimální počet po sobě jdoucích úspěšných dokončení pro sondu, aby to bylo považováno po nezdaru za úspěch.

Pole	Popis
`timeoutSeconds` integer	Počet sekund, po jejichž uplynutí dojde k překročení časového limitu sondy. Další informace: https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probes.

Verze

QueueManagerStatusVersion definuje verzi produktu MQ.

Zobrazí se v:

- “QueueManagerStatusVersionDostupná” na stránce 46

Pole	Popis
`name` string	Verze "name" pro tuto verzi správce front QueueManager. Toto jsou platné hodnoty pro pole `spec.version`.

Konfigurace WebServer

Nastavení pro webový server MQ.

Zobrazí se v:

- “Specifikace QueueManager” na stránce 44

Pole	Popis
`enabled` boolean	Zda povolit nebo zakázat webový server.

Poznámky

Tyto informace byly vyvinuty pro produkty a služby poskytované v USA.

Společnost IBM nemusí nabízet produkty, služby nebo funkce uvedené v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou ve vaší oblasti aktuálně dostupné, získáte od místního zástupce společnosti IBM. Odkazy na produkty, programy nebo služby společnosti IBM v této publikaci nejsou míněny jako vyjádření nutnosti použití pouze uvedených produktů, programů či služeb společnosti IBM. Místo toho lze použít jakýkoli funkčně ekvivalentní produkt, program nebo službu, které neporušují žádná práva k duševnímu vlastnictví IBM. Ověření funkčnosti produktu, programu nebo služby pocházející od jiného výrobce je však povinností uživatele.

Společnost IBM může vlastnit patenty nebo nevyřízené žádosti o patenty zahrnující předměty popsané v tomto dokumentu. Vlastnictví tohoto dokumentu neposkytuje licenci k těmto patentům. Dotazy týkající se licencí můžete posílat písemně na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Odpovědi na dotazy týkající se licencí pro dvoubajtové znakové sady (DBCS) získáte od oddělení IBM Intellectual Property Department ve vaší zemi, nebo tyto dotazy můžete zasílat písemně na adresu:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE" , BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH VÝSLOVNĚ NEBO VYPLÝVAJÍCÍCH Z OKOLNOSTÍ, VČETNĚ, A TO ZEJMÉNA, ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL VYPLÝVAJÍCÍCH Z OKOLNOSTÍ. Některé právní řády u určitých transakcí nepřipouštějí vyloučení záruk výslovně vyjádřených nebo vyplývajících z okolností, a proto se na vás toto omezení nemusí vztahovat.

Uvedené údaje mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené jsou pravidelně upravovány a tyto změny budou zahrnuty v nových vydáních této publikace. Společnost IBM může kdykoli bez upozornění provádět vylepšení nebo změny v produktech či programech popsaných v této publikaci.

Veškeré uvedené odkazy na webové stránky, které nespravuje společnost IBM, jsou uváděny pouze pro referenci a v žádném případě neslouží jako záruka funkčnosti těchto webů. Materiály uvedené na tomto webu nejsou součástí materiálů pro tento produkt IBM a použití uvedených stránek je pouze na vlastní nebezpečí.

Společnost IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vyžádání vašeho svolení.

Vlastníci licence k tomuto programu, kteří chtějí získat informace o možnostech (i) výměny informací s nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) oboustranného využití vyměňovaných informací, mohou kontaktovat informační středisko na adrese:

IBM Corporation
Koordinátor spolupráce softwaru, oddělení 49XA
148 00 Praha 4-Chodby

148 00 Praha 4-Chodov
U.S.A.

Poskytnutí takových informací může být podmíněno dodržením určitých podmínek a požadavků zahrnujících v některých případech uhrazení stanoveného poplatku.

IBM poskytuje licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály na základě podmínek smlouvy IBM Customer Agreement, IBM International Program License Agreement nebo jiné ekvivalentní smlouvy mezi námi.

Jakékoli údaje o výkonnosti obsažené v této publikaci byly zjištěny v řízeném prostředí. Výsledky získané v jakémkoli jiném operačním prostředí se proto mohou výrazně lišit. Některá měření mohla být prováděna na vývojových verzích systémů a není zaručeno, že tato měření budou stejná i na běžně dostupných systémech. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky mohou být jiné. Čtenáři tohoto dokumentu by měli zjistit použitelné údaje pro své specifické prostředí.

Informace týkající se produktů jiných výrobců pocházejí od dodavatelů těchto produktů, z jejich veřejných oznámení nebo z jiných veřejně dostupných zdrojů. Společnost IBM tyto produkty netestovala a nemůže potvrdit správný výkon, kompatibilitu ani žádné jiné výroky týkající se produktů jiných výrobců než IBM. Otázky týkající se kompatibility produktů jiných výrobců by měly být směrovány dodavatelům těchto produktů.

Veškerá tvrzení týkající se budoucího směru vývoje nebo záměrů společnosti IBM se mohou bez upozornění změnit nebo mohou být zrušena a reprezentují pouze cíle a plány společnosti.

Tyto údaje obsahují příklady dat a sestav používaných v běžných obchodních operacích. Aby byla představa úplná, používají se v příkladech jména osob a názvy společností, značek a produktů. Všechna tato jména a názvy jsou fiktivní a jejich podobnost se jmény, názvy a adresami používanými ve skutečnosti je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Tyto ukázkové programy můžete bez závazků vůči společnosti IBM jakýmkoli způsobem kopírovat, měnit a distribuovat za účelem vývoje, používání, odbytu či distribuce aplikačních programů odpovídajících rozhraní API pro operační platformu, pro kterou byly ukázkové programy napsány. Tyto příklady nebyly plně testovány za všech podmínek. Společnost IBM proto nemůže zaručit spolehlivost, upotřebitelnost nebo funkčnost těchto programů.

Při prohlížení těchto dokumentů v elektronické podobě se nemusí zobrazit všechny fotografie a barevné ilustrace.

Informace o programovacím rozhraní

Informace programátorských rozhraní, je-li poskytnuta, vám pomohou vytvořit aplikační software pro použití s tímto programem.

Tato příručka obsahuje informace o zamýšlených programovacích rozhraních, které umožňují zákazníkům psát programy za účelem získání služeb produktu WebSphere MQ.

Tyto informace však mohou obsahovat i diagnostické údaje a informace o úpravách a ladění. Informace o diagnostice, úpravách a vyladění jsou poskytovány jako podpora ladění softwarových aplikací.

Důležité: Nepoužívejte tyto informace o diagnostice, úpravách a ladění jako programátorské rozhraní, protože se mohou měnit.

Ochranné známky

IBM, logo IBM , ibm.comjsou ochranné známky společnosti IBM Corporation, registrované v mnoha jurisdikcích po celém světě. Aktuální seznam ochranných známek IBM je k dispozici na webu na stránce "Copyright and trademark information"www.ibm.com/legal/copytrade.shtml. Ostatní názvy produktů a služeb mohou být ochrannými známkami společnosti IBM nebo jiných společností.

Microsoft a Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených státech a případně v dalších jiných zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse ve Spojených státech a případně v dalších jiných zemích.

Tento produkt obsahuje software vyvinutý v rámci projektu Eclipse Project (http://www.eclipse.org/).

Java a všechny ochranné známky a loga založené na termínu Java jsou ochranné známky nebo registrované ochranné známky společnosti Oracle anebo příbuzných společností.

Číslo položky:

(1P) P/N: